Received: 25 April 2023 | Revised: 8 September 2023 | Accepted: 9 September 2023

DOI: 10.1111/puar.13743

SCHOLARLY TAKES

PAR Public Administration Review ASPA

Local government cyber insecurity: Causes and recommendations for improvement

Donald F. Norris[1] | Laura Mateczun[1] | William Hatcher[2] | Wesley L. Meares[2] | John Heslen[2]

[1]School of Public Policy, University of Maryland, Baltimore County, Baltimore, Maryland, USA

[2]Department of Social Sciences, Augusta University, Augusta, Georgia, USA

Correspondence
William Hatcher, Department of Social Sciences, Augusta University, 1120 15th Street, Augusta, GA 30912, USA.
Email: wihatcher@augusta.edu

Abstract

In this paper, we address several facets of the problem we call local government cyber insecurity—a problem that plagues such governments across the nation, if not the world. We describe this problem and discuss its manifestations in local governments. This is followed by our analysis of why, on average, local government cybersecurity is managed and practiced so poorly. Next, we discuss several constraints on local governments that may help to explain why so many of these governments are not able to provide highly effective cybersecurity. We then discuss steps that local governments can and should take to improve their cybersecurity, including adopting dedicated cybersecurity budgets, adopting several highly recommended cybersecurity policies, and following best cybersecurity practices.

Evidence for Practice

- Cybersecurity is a significant public problem for local governments.
- Local governments do not manage and practice cybersecurity effectively.
- Local governments need specific line items for cybersecurity in their budgets, effective cybersecurity policies, and practices.

INTRODUCTION: WHAT IS THE PROBLEM?

Local governments, really all organizations, inhabit a location in cyberspace that constitutes a new normal (well, not so new after all!). This "normal" for local governments consists of them being under are under constant or nearly constant cyberattack (Norris et al., 2018, 2019, 2022). Nearly half of local governments in a 2016 survey reported being under attack either hourly or daily. Unfortunately, however, nearly 30 percent did not know how often they were under attack (Norris et al., 2019). Of 14 local governments included in a key informant survey in 2020, eight said they were under attack constantly, four said hourly, and two said daily. Moreover, half said that they had been breached at least once in the previous year (Norris et al., 2021, 2022).

There is a saying in the cybersecurity business that it is not if an organization will be breached, *but when*. These data certainly support that saying. Consequently, local governments must be highly vigilant in protecting all of their information assets, and they must protect those assets with high levels of cybersecurity. We discuss what local governments must do to protect their information assets in the "WHAT TO DO" section.

Local governments not only face relentless cyberattacks, but the types of attacks vary. In recent years, ransomware attacks have become one of the most, if not the most prominent type of attack. Successful ransomware attacks can be very costly (and embarrassing) to local governments. Atlanta spent approximately $17 million recovering from a ransomware attack in 2018. In 2019, Baltimore paid about $19 million to recover from one, after experiencing a much less damaging ransomware attack in 2018. In Baltimore's case, the city evidently did not learn much from the 2018 experience. As often happens when significant breaches occur, city officials look for scapegoats. Baltimore's CIO, who had been warning city officials for some time that greater cybersecurity funding was needed and that employees needed to be properly trained in cyber, became that scapegoat. He was fired (Norris et al., 2022).

Ransomware is not an attack per se but a type of malware that can be delivered to local governments by different methods of cyberattack, such as phishing and spear phishing, brute force, zero-day, denial of service (DDS) and distributed denial of service (DDoS), and others. All of these methods, and more, can be and are used to deliver malware to information systems. Ransomware is just a particularly nasty form of malware in which the attackers attempt to induce a ransom payment in order to remove the malware and decrypt affected data and systems. (See definitions of these common attack vectors in Appendix A.).

Attackers vary as well. Moschovitis (2018) identified seven types of attackers and their motives for conducting cyberattacks, including cybercriminals (whose motive is money), online social hackers (money), cyberspies (espionage), hactivists (activism), cyberfighters (patriotism), cyberterrorists (terror), and script kiddies (curiosity, thrill, fame, money). Norris et al. (2022) found by comparing Moschovitis' list to a report from the President's Commission on Critical Infrastructure (Ellis et al., 1997) "…the cyberthreat landscape has not changed much in the last two decades."

The purpose of this paper is to highlight the pertinent issue of local government cybersecurity and engage scholars and practitioners to consider how to address cyber insecurity. There is little scholarship surrounding cybersecurity in public administration and public policy. While we have published on the topic, this paper is unique in that we emphasize intergovernmental collaboration and call for efforts by the broader field, academics and practitioners, to work together in responding to the cyber insecurity of local governments. Considering the state of developing scholarship surrounding cybersecurity, this paper is intended to ignite conversation on this timely issue.

In the remainder of this paper, we discuss why local government cybersecurity, on average, is so poor and what local governments can and should do to improve their cybersecurity. We do so by reviewing the literature and data developed around the issue of local government cybersecurity. Following this section, we identify major constraints, such as inadequate training, lack of accountability, and lack of support from top officials, limiting local governments from providing higher quality cybersecurity. The next section involves an analysis of key findings from the literature to provide action steps for local governments to address four major issues: cybersecurity budget, cybersecurity policies, best practices, and constraints. We conclude with a brief summary of our findings and recommendations.

WHY IS LOCAL GOVERNMENT CYBERSECURITY SO POOR?

As we noted in the "INTRODUCTION: WHAT IS THE PROBLEM?" section, local governments are under constant or nearly constant cyberattack. With over 90,000 local governments in the USA, cybercriminals have nearly an endless supply of a lot of potential victims with local governments often being ripe targets.

Some, perhaps many local governments understand well the need for cybersecurity. In one survey, seventy-one percent of cities have a formal cybersecurity policy (Hatcher et al., 2020). However, our combined research has shown that local governments, while perhaps having cybersecurity policies in place, are not taking the crucial next steps to ensure cybersecurity by integrating these policies into their daily management practices (Norris et al., 2019; Norris et al., 2022; Hatcher et al., 2020). Many local governments do not implement policies effectively, nor do they have processes in place to hold users accountable for improper use, whether accidental or intentional. Too many are also not fully aware of their current cybersecurity posture and attack environment as nearly one out of three (29%) indicated they did not know how often their local government was under attack (Norris et al., 2019). In addition, as Hatcher et al. (2020) found, only 37 percent of surveyed cities reported keeping a record of cybersecurity attacks, and 41 percent of the surveyed cities were not providing cybersecurity training on an ongoing basis. Not keeping track of incidents and attacks and not knowing what your local government is experiencing in terms of cyberattacks are akin to cybersecurity malpractice.

Local government cybersecurity is also poor because they are under constant attack, they lack adequate budgetary resources to mitigate and prevent such attacks, they lack adequate cybersecurity staffing (which is related to inadequate funding), they provide inadequate (or no) cybersecurity training, their top officials often do not "buy-in" to the need for high levels of cybersecurity and do not act as "champions" for it, and too many local government employees do not practice proper cyberhygiene. Cyber criminals, on the other hand, are incredibly motivated and talented at exploiting vulnerabilities, and with a plethora of available targets and the minimal likelihood of being apprehended, there is little incentive for these actors to alter their behavior. In addition, they are good at what they do!

CONSTRAINTS ON LOCAL GOVERNMENTS

Local governments face several constraints that limit their ability to provide high levels of cybersecurity. We mentioned two of perhaps the most important constraints above: inadequate funding of and staffing for cybersecurity. Inadequate funding is also often responsible, in large part, for weaknesses in local government cybersecurity resulting from those governments failing to upgrade IT hardware and software to at least the state of the practice, consolidate and upgrade IT networks, meet various compliance and privacy standards, and pay competitive salaries to cybersecurity staff.

It is beyond the scope of this paper to address all of the constraints to effective cybersecurity that local governments confront. However, we strongly note that if local elected officials and top management fail to ensure adequate funding and staffing, their governments are almost certain to experience adverse cybersecurity outcomes, which can be quite damaging, expensive, and embarrassing. See Atlanta and Baltimore above.

Here, instead, we discuss constraints that are more easily and less expensively addressed. These constraints are well known both in the literature and among cybersecurity professionals and include lack of mandatory cybersecurity training for employees and officials, lack of enforcement of accountability of employees and officials for their actions impacting information security, lack of support for cybersecurity from top officials, and failure to adopt and implement well-known and highly recommended cybersecurity policies (please see the "WHAT TO DO?" section). These constraints bear repeating here because they are consistently cited as the biggest barriers to improving cybersecurity in government, or any organization, in academic, professional, and private industry studies of cybersecurity. They represent basic fundamentals of cybersecurity management, and until they are addressed, they will likely persist as top barriers to overcome.

Training

One of the easiest and least expensive actions that local governments can take to improve their cybersecurity is to require periodic cybersecurity awareness training for all staff, elected officials, and top appointed officials. The purposes of this training, among other things, are

- to train everyone to understand the need for high levels of cybersecurity in their organizations,
- to teach the dos and don'ts of cybersecurity—that is, what actions that personnel may and probably should take in their daily online activities and actions that they must not take, and
- to begin building or to expand upon a culture of cybersecurity across the organization. At the minimum, this means that every party in the organization, "…regardless of their place on an organization's hierarchy, is thoroughly committed to cybersecurity, understands the importance of cybersecurity in everything they do, and practices proper cyber-hygiene. They know that Cyber is Job One" (Norris et al., 2022, p. 42).

Accountability

Training without accountability is largely a waste of time and effort. All parties, regardless of rank, title, or position, should understand that there are consequences for proper and improper cyber-hygiene. This should, of course, be emphasized in the periodic, mandatory cybersecurity awareness training that they receive. For example, personnel should be rewarded, even if symbolically, for their proper use of the organization's information resources and for identifying problems (e.g., potential attacks) and reporting them to the proper authority. They should also be punished for improper online actions and for not following the organization's cybersecurity regulations and policies. Punishments can include re-training, restricting, or removing IT privileges and even dismissal.

Support from top officials

A common complaint of IT and cybersecurity staff in local governments (indeed, in organizations of nearly all types) is that top officials are not sufficiently supportive of cybersecurity. In a 2016 survey, responding local government IT and cybersecurity officials said that while nearly 62 percent of top appointed managers were moderately or exceptionally aware of the need for cybersecurity, only 42 percent of department managers and 32 percent of elected officials were (Hatcher et al., 2020). A 2020 survey of CISOs, CIOs, and IT directors in mostly large and more well-funded and staffed local governments found that 79 percent of elected executives were exceptionally or mostly supportive of cybersecurity followed by 50 percent of elected councilors, 57 percent of top appointed administrators, and 50 percent of department heads (Norris et al., 2022). This represents a substantial improvement over the 2016 survey but still leaves room for improvement.

For many years, a standard in the information security industry has been that CEOs and Corporate Boards must be ultimately responsible for cybersecurity in their organizations. This is also true of their counterparts in local government, elected executives, and councilors. However, it is too often not the case in practice. In too many local governments, cybersecurity is mostly the domain of the technologists (IT department, CIO, CISO, etc.). In addition, more often than not, these officials do not have seat at the tables where high-level decisions, such as allocating scarce resources, are made and thus have too little influence on how cybersecurity is funded and practiced.

The idea that top officials should be responsible for cybersecurity recently received a strong endorsement from the Director of the Cybersecurity and Infrastructure Agency (CISA), Jen Easterly, and Executive Assistant Director of the same agency, Eric Goldstein, in an article in the journal *Foreign Affairs* (February 1, 2023). They wrote that a new model for cybersecurity in organizations is needed. Under that model, IT and cybersecurity directors would no longer have the primary responsibility for cybersecurity, especially since these officials are often not given the "…resources, influence or accountability to ensure that security is appropriately prioritized" (2). Easterly and Goldstein went on to say "Under this new model, cybersecurity would ultimately be the responsibility of every CEO and board (Easterly & Goldstein, 2023)."

While it is unclear that this model will be readily adopted among American local governments, it certainly deserves serious consideration. Although this model may evolve, it is clear that top local government officials must fully support cybersecurity because they are ultimately in charge of their governments. Moreover, and as we have written elsewhere, if these officials are perceived as not supporting cybersecurity and giving it priority status, others in the local government will say "If they don't care about cyber, why should I?" (Norris et al., 2022). We recently published a primer to help encourage top leadership to become champions of cybersecurity within their local governments by learning more about cybersecurity, fostering it throughout their organization, knowing what to ask their IT and cyber staff, and looking to the future of cybersecurity (Norris & Mateczun, 2023). The primer also has a section dedicated to recommendations for smaller local governments facing greater cost and staffing hurdles than larger governments.

WHAT TO DO?

To help improve their cybersecurity, local governments must effectively address at least the following four issues and do so effectively: cybersecurity budget, cybersecurity policies, best practices, and constraints. This must not be an on–off exercise but a continuing effort.

Dedicated cybersecurity budget

As previously discussed, the first step toward improving local government cybersecurity involves adequately funding and staffing cybersecurity in these organizations. In order to do so, top elected and appointed officials must champion the importance of cybersecurity to build and grow a culture of cybersecurity in their governments. When top officials champion and support cybersecurity, they can advocate for and defend dedicating a portion of their governments' information technology budget to cybersecurity. Challenges can arise with the resource scar. In 2022, 50 percent of states had a dedicated budget line item for cybersecurity (Subramanian & Ward, 2022). Only eight percent of state enterprise security offices dedicated more than 10 percent of their IT budget to cybersecurity in 2022, while private sector companies, on average, allocated about 12.7 percent of their IT budget to IT security (Sava, 2022; Subramanian & Ward, 2022).

According to the Nationwide Cybersecurity Review (NCSR) conducted by the Multi-State Information Sharing & Analysis Center (MS-ISAC), state, local, tribal, and territorial (SLTT) governments that dedicated at least three percent of their IT budget to cybersecurity scored 21 percent higher on the maturity level than those that did not dedicate a portion of their budget and those that dedicated one percent scored 15 percent higher (MS-ISAC 2021). Close to 15 percent of responding SLTT governments indicated they did not have a dedicated cybersecurity budget as a portion of their IT budget. It should be noted that these figures also include state, tribal, and territorial governments, making it difficult to discern the exact numbers for local governments. Funding helps to address the barriers that studies and surveys consistently identify as hampering their organization's cybersecurity. These barriers include (but are not limited to) lack of funding, lack of adequately trained cybersecurity staff, and inability to pay competitive salaries. As to why it is difficult for some local governments to have a dedicated cyber budget, we speculate that the cause is much like a chicken or egg dilemma; there is no dedicated budget because of lack of funding, and there is a lack of funding because there is no dedicated budget.

While it is not precisely known how much local governments should dedicate to cybersecurity, the NCSR results indicate that even a modest budget allocation of three percent is associated with meaningful improvements. Cybersecurity champions also help to build trust with all local government employees and staff so that they understand their role in practicing good organizational cybersecurity.

Adopt cybersecurity policies

Cybersecurity policies set the standards and requirements that control local government cybersecurity practice. Policy adoption and implementation are essential for the ability of these governments to provide high levels of cybersecurity. Yet, research has shown that too few local governments have adopted the menu of highly recommended cybersecurity policies and that many of these same governments question the effectiveness of adopted policies (Hatcher et al., 2020; Norris & Mateczun, 2023; Norris et al., 2022).

The cybersecurity policies that are fairly consistently recommended for organizations, including local governments, include (Norris et al., 2022)

- Acceptable Use Policy (AUP), sometimes known as a Policy for Responsible Computing: broadly, this policy describes activities that are permitted and prohibited on the local government's IT system,
- Information Security Policy: this describes how information is created, exchanged, stored, protected, and handled on the local government's IT system,
- Privacy Policy (which may be a stand-alone policy or part of the Information Security Policy): this describes the types of information collected, used, stored, and shared by the local government and security protocols in place to protect the information,
- Identity and Access Management Policy (IAM): this establishes who has access to what information and other resources on the local government's IT system and how they may access and use that information,
- Incident Handling Policy (IHP): local governments must be prepared for inevitable cyberattacks and breaches,

and this policy describes how the local government will respond when they occur, and
- Disaster Recovery/Business Continuity Policy (DR/BCP): this describes how the local government "…will respond to emergencies that disrupt governmental operations, including cyberattacks as well as natural disasters, terrorist attacks and other [adverse cyber events]…" (Norris et al., 2022, 121).

Local governments of all sizes and budget capacities must seriously consider adopting and carefully implementing these "essential" cybersecurity policies. This is because cybersecurity policies, like many policies in other fields, are equivalent to the owner's manuals or detailed instructions that come with many purchases. These instructions tell buyers what to do and how to do it (and what not to do) to effectively and safely use the product they bought. Without such policies, and their careful implementation, local governments are essentially operating in the equivalent of the cybersecurity "Wild West," where nothing is controlled and everything goes!

Follow best practices

Local governments should implement and follow cybersecurity best practices published by federal organizations such as the Department of Commerce's National Institute of Standards and Technology (NIST) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). NIST's Cybersecurity Framework and related Special Publications, such as the Risk Management Framework (SP 800-37 Rev. 2), provide adaptable and customizable routes through which to understand an organization's current cybersecurity posture and steps to take to improve from the status quo. CISA publishes a catalog of known exploited vulnerabilities describing cybersecurity threats, as well as patches and other fixes as they become available. CISA also shares best practices specifically for SLTT governments and critical infrastructure providers and provides other services, programs, resources, and training opportunities on a voluntary basis. Some of these services include Assist Visits, Automated Indicator Sharing, and Business Impact Analysis. The Federal Bureau of Investigation (FBI) is responsible for investigating cyberattacks, and its contact information should be in the rolodex of every local government (Norris et al., 2021).

Information sharing organizations, such as Information Sharing and Analysis Centers (ISACs), offer sector-specific advice, threat information, cybersecurity tools, and networking opportunities. Local governments should seriously consider joining and following organizations such as MS-ISAC, which aim to help improve cybersecurity among SLTT governments and is the preeminent ISAC for local governments. Other sector-specific ISACs that might be of interest to certain sector-specific local governments include EI-ISAC for election officials, REN-ISAC for research and higher education institutions, EMR-ISAC for emergency management and response, Surface Transportation, Public Transportation and Over-the-Road Bus ISACs, and critical infrastructure ISACs such as WaterISAC and Electricity ISAC.

Local governments are also encouraged to build and maintain relationships with other similarly situated local governments, especially those within their regions and states, state-level organizations, and state National Guard units that may provide cybersecurity assistance, including assistance during successful cyberattacks. Membership organizations such as the International City County Management Association (ICMA), the National League of Cities (NLC), the U. S. Conference of Mayors, and the National Association of Counties (NACo) hold conferences of various sorts, including those that address cybersecurity issues and publish materials that are helpful to their members about cybersecurity. The National Association for State Chief Information Officers (NASCIO) publishes helpful information about cybersecurity, conducts a biennial survey entitled "Deloitte-NASCIO Cybersecurity Study," and conducts studies about cybersecurity that should be of interest to local governments.

Overcome lack of cybersecurity knowledge constraints

Perhaps the most significant constraint that many, but certainly not all, local elected officials and top managers in local governments face is lack of knowledge about and education or training in at least the basics of cybersecurity. As such, these officials are not likely to be effective in overseeing cybersecurity programs in their governments. In order to overcome this deficiency, we recommend that they take advantage of one or more of the following to improve their knowledge of and comfort levels with their governments' cybersecurity:

- attend their governments' cybersecurity training or cybersecurity training programs (if offered),
- attend cybersecurity training offered by membership and professional associations,
- read papers, news articles, reports, and other written materials about cybersecurity from these organizations,
- enroll in online or in person cybersecurity courses at colleges, universities, and community colleges. This may include one of a few courses in the basics of cybersecurity as well as certificate and even degree programs. All of these opportunities will strengthen these officials' knowledge of cybersecurity and their ability to better manage its practice in their governments.

There is a role for Public Administration and Public Policy schools and associations in providing educational resources to both elected officials and managers in the public sector, especially those in local governments.

A survey of IT professionals and Masters of Public Administration (MPA) alumni conducted by Christian and Davis (2016) found a disconnect between what MPA students are learning about technology in their programs and what they need to know to be effective public managers. Given the importance of cybersecurity in public administration, we urge MPA programs to integrate it into their curricula better more effectively. Incorporating cybersecurity into MPA curricula will help address one of the "Grand Challenges" put forth by the National Academy of Public Administration (Gerton & Mitchell, 2019).

Recent research helps guide how to integrate e-government coursework into public administration programs. Overton and Kleinschmit (2022) made a strong case for incorporating data science tools in research methods courses in MPA programs. At a more program-wide level, McQuiston and Manoharan (2017) detailed how to integrate e-government courses into Network of Schools of Public Policy, Affairs, and Administration's (NASPAA) five competencies. The authors reviewed syllabi in NASPAA member programs. They examined the IT offerings of academic programs if they "made mention of topics including GIS, cybersecurity and privacy, social media, big data, data analysis, cloud computing, crowdfunding, e-government/service provision, and e-procurement, data privacy and confidentiality, digital divide and accessibility, and/or IT infrastructure" (McQuiston & Manoharan, 2017, p. 177). The authors found most IT-related course offerings to focus on policy, with management being the second most prevalent concern. Strikingly, McQuiston and Manoharan (2017) found the curricula of MPA programs to be even more lacking in the coverage of cybersecurity.

There are at least two academic associations that seem to us to be naturals to take leadership roles in advocating for stronger and more programs in the academy in cybersecurity. They are the American Society for Public Administration (ASPA) and the Network of Schools of Public Policy, Affairs, and Administration (NASPAA). These and other associations within public administration and public policy can materially assist in this advocacy and, even, curriculum development.

A few academic programs already stand out as exemplars in this area. For instance, the MPA program at the O'Neill School of Public and Environmental Affairs at the University of Indiana Bloomington offers a pathway for students to complete an MPA and an MS in Cybersecurity Risk Management.[1] Another example is the cybersecurity concentration offered as part of the MPA program at California State University, San Bernardino.[2]

The solutions to the four issues (cybersecurity budget, cybersecurity policies, best practices, and constraints) while reasonable may face challenges in implementation. These recommendations vary in terms of costs required to implement them. These costs can create barriers which local governments will need to address. The primary challenges, but not inclusive list, of adopting these recommendations are resource availability, organizational buy-in, and issues related to determining compatibility with other local governments and associations. In order to start addressing these potential challenges, officials should start from a foundation of knowledge. Informing local leaders about the need for cybersecurity and the costs associated with cyber insecurity is imperative to address these, and other, challenges. Furthermore, this knowledge and the understanding of the shared responsibility of cybersecurity should be promoted within the organization. As noted above, new policies and training will be needed to share this knowledge and help to create organizational buy-in. Resource availability will most likely be the most significant hurdle. Even with knowledge and organizational buy-in, cultivating the necessary resources will not necessarily come easily. Despite this, promoting the efficiency, stability, and cost-effectiveness of a more secure cyber environment to those with an understanding of cybersecurity will be more conducive to making cybersecurity a higher funding priority.

SUMMARY AND CONCLUSION

As this paper has shown, based on considerable research into local government cybersecurity, local governments are under constant or nearly constant cyberattack. Yet, on average, they do a poor job of managing and practicing cybersecurity. Among the reasons for this state of cyberaffairs among local governments, lack of funding and staffing stand out. Other prominent reasons include lack of understanding of and support for cybersecurity among elected officials and top managers; lack of adoption and implementation of cybersecurity policies; failure periodically offer and to require cybersecurity training for all officials, managers, and staff; failure to hold all users the government's IT system accountable for their cyberhygiene; and the fact that their cyber opponents are numerous, motivated and effective at exploiting cybersecurity weaknesses in all organizations.

Why might these governments be practicing poor cybersecurity despite the fact that they are under nearly constant attack? Beyond the reasons listed above, a huge factor is likely that many of these local governments have yet to experience the consequences of a large-scale, newsworthy breach impacting public services or citizen or business information. It is when the local government leaders experience the embarrassment factor and citizens demand continuity of operations that champions for cybersecurity can arise and funds begin to flow. Many leaders may not realize that cyber insecurity within their local government exists until it is too late. The function of cybersecurity needs to be viewed as a necessary form of risk management and risk mitigation that would be negligent to ignore.

Hence, we have recommended several actions that local governments should take to improve their cybersecurity. Perhaps, the most important is the adoption of dedicated cybersecurity budgets funded at an appropriate level in all local governments. Adequate budgetary resources can help address other limitations in local government cybersecurity programs, including staffing and hardware and software deficiencies. Local governments must also provide periodic, mandated cybersecurity awareness training for all parties, regardless of their place in the local government hierarchy. In addition, these parties must be held accountable for their cyber-hygiene. Finally, local governments must adopt and effectively implement highly recommended cybersecurity policies to manage and regulate actions taken by all that affect the organization's cybersecurity.

The findings we have reported and the recommendations we have made here are hardly novel. They have been made throughout the cybersecurity professional and academic literature for years. Unfortunately, too many local governments have not heeded them in part or in whole. As a result, too many local governments have experienced and will continue to experience breaches of their IT systems that result in losses of data, system shutdowns, the inability to conduct basic government business and provide basic public services, loss of money directly (e.g., paying ransom) or indirectly (e.g., the cost of recovery from successful attacks), and the embarrassment of having failed to adequately protect their information assets.

By taking the actions we have recommended in this paper, local governments will have a better chance to provide high levels of cybersecurity and protect their information assets more effectively. This result will also be more achievable if Public Administration and Policy organizations and schools both advocate for and design and implement improved training and education programs in cybersecurity for local governments.

ENDNOTES

[1] For more information, see https://oneill.indiana.edu/masters/degrees-certificates/dual-degrees/mpa/mpa-ms-cyber.html.

[2] For more information, see https://www.csusb.edu/mpa/concentrations/cyber-security-concentration.

REFERENCES

Christian, P. C., and T. J. Davis. 2016. "Revisiting the Information Technology Skills Gap in Master of Public Administration Programs." *Journal of Public Affairs Education* 22(2): 161–174.

Easterly, J., and E. Goldstein. 2023, February 1. "Stop Passing the Buck on Cybersecurity." Foreign Affairs. https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity.

Ellis, J., D. Fisher, T. Longstaff, L. Pesante, and R. Pethia. 1997, January. *Report to the President's Commission on Critical Infrastructure Protection* (Special Report CMU/SEI-97-SR-003).

Gerton, T., and J. P. Mitchell. 2019. "Grand Challenges in Public Administration: Implications for Public Service Education, Training, and Research." *Journal of Public Affairs Education* 25(4): 435–440.

Hatcher, W., W. L. Meares, and J. Heslen. 2020. "The Cybersecurity of Municipalities in the United States: An Exploratory Survey of Policies and Practices." *Journal of Cyber Policy* 5(5): 302–325.

McQuiston, J. M., and A. P. Manoharan. 2017. "Developing E-Government Coursework through the NASPAA Competencies Framework." *Teaching Public Administration* 35(2): 173–189.

Moschovitis, C. 2018. *Cybersecurity Program Development for Business: The Essential Planning Guide*. Hoboken, NJ: John Wiley & Sons.

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.

Norris, D. F., L. Mateczun, A. Joshi, and T. Finin. 2018. "Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security." *Journal of Homeland Security and Emergency Management* 15(3): 1–14.

Norris, D. F., L. Mateczun, A. Joshi, and T. Finin. 2019. "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity." *Public Administration Review* 79(6): 895–904.

Norris, D. F., L. Mateczun, A. Joshi, and T. Finin. 2021. "Managing Cybersecurity at the Grassroots: Evidence from the First Nationwide Survey of Local Government Cybersecurity." *Journal of Urban Affairs* 43(8): 1173–95.

Norris, D. F., and L. K. Mateczun. 2023. *Cybersecurity for Local Government: A Primer*. https://publicpolicy.umbc.edu/wp-content/uploads/sites/176/2023/08/Cybersec_Primer_NorrisMateczunAug2023.pdf.

Norris, D. F., L. K. Mateczun, and R. F. Forno. 2022. *Cybersecurity and Local Government*. Hoboken, NJ: John Wiley & Sons.

Overton, M., and S. Kleinschmit. 2022. "Transforming Research Methods Education through Data Science Literacy." *Teaching Public Administration*: 014473942210844.

Sava, J. A. 2022, August 31. Average Share of IT Budget Allocated to IT Security by Companies Worldwide 2018-2022. *Statista*. https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/.

Security Magazine. 2020, March 16. U.S. Health and Human Services Department Suffers Cyberattack. https://www.securitymagazine.com/articles/91909-us-health-and-human-services-department-suffers-cyberattack.

Subramanian, S., and M. Ward. 2022. 2022 Deloitte-NASCIO Cybersecurity Study. https://www2.deloitte.com/us/en/insights/industry/public-sector/2022-deloitte-nascio-study-cybersecurity-post-pandemic.html.

AUTHOR BIOGRAPHIES

Donald F. Norris is a Professor Emeritus in the School of Public Policy, University of Maryland, Baltimore County. His principal field of study is public management, specifically information technology in governmental organizations, including electronic government and cybersecurity. He has published extensively in these areas, including seven articles in Public Administration Review. He received his bachelor's degree in history from the University of Memphis and master's and doctoral degrees in political science from the University of Virginia. He can be reached at norris@umbc.edu

Laura K. Mateczun, JD, is a PhD student in the School of Public Policy at the University of Maryland, Baltimore County, where she is writing her dissertation on local government cybersecurity. She received an MPS in Cybersecurity from UMBC in 2023 and a graduate certificate in cybersecurity strategy and policy in 2021. She co-authored the book Cybersecurity and Local Government, published by Wiley in 2022. She is a 2014

graduate of the University of Maryland, Francis King Carey School of Law, and is a member of the Maryland Bar. Laura received a B.A. in public policy and political science from St. Mary's College of Maryland in 2011. She can be reached at lam6@umbc.edu.

William Hatcher is a Professor of Political Science and Public Administration and Chair of the Department of Social Sciences at Augusta University. His research has appeared in journals such as the *American Journal of Public Health, American Review of Public Administration*, and *Public Administration Quarterly*. He is the author of *The Curious Public Administrator* (Routledge, 2023). He can be reached at wihatcher@augusta.edu

Wesley L. Meares is an Associate Professor of Political Science and Public Administration in the Department of Social Sciences at Augusta University, where he serves as the graduate program director for the Master of Public Administration program. His research has appeared in journals such as *Cities*, *Local Environment*, *Journal of Urban Affairs, Housing Studies*, and *Journal of Urbanism*. He can be reached at wmeares@augusta.edu

John Heslen, PhD, is an Assistant Professor of Political Science at Augusta University. He is a retired Lieutenant Colonel who served as an intelligence officer in the USAF with assignments to Defense Intelligence Agency, US European Command and National Intelligence University. His areas of expertise include the US Intelligence Community, strategic cybersecurity, and the cognitive aspects of information warfare. He can be reached at jheslen@augusta.edu

How to cite this article: Norris, Donald F., Laura Mateczun, William Hatcher, Wesley L. Meares, and John Heslen. 2024. "Local Government Cyber Insecurity: Causes and Recommendations for Improvement." *Public Administration Review* 84(4): 651–59. https://doi.org/10.1111/puar.13743

APPENDIX: TYPES OF ATTACKS A

There are numerous types of cyberattacks. Googling the term "cyberattacks" will produce numerous lists of them.

Malware: Malware is not a type of attack but it is often something that attackers do once they have penetrated a victim's IT system—install malware. Malware is malicious software (hence, malware) that can do one of several things (all bad) such as encrypting data and files, blocking user access to systems or components of systems, exfiltrating data and files, and more. Ransomware is a form of malware that is increasingly used in cyberattacks. Significant local government examples include Atlanta, Georgia, and Baltimore, Maryland.

Ransomware: Ransomware is an especially nefarious form of malware. It is typically delivered via social engineering, most often in phishing or spear phishing emails. The object of a ransomware attack is to gain illicit entry into an organization's IT system, find and encrypt sensitive data and files, and possibly lock down the entire system. The criminal then demands a ransom, usually in the form of bitcoin to release the system and its files and data. The threat is that if the organization does not pay the ransom, the cybercriminal will leave the data and files encrypted or the entire system locked down or expose sensitive data.

Phishing: Phishing is a form of "social engineering" in which cybercriminals "go fishing" for victims by sending emails, seemingly from trusted parties, with promises, opportunities, or threats the attackers hope the victims will fall for. A common phishing attack, which many people have received, for example, is an email from a Nigerian promising a large amount of money. The attacker asks the potential victim for their bank account details so that the attacker can transfer the money. Of course, the transfer never happens and the scammer later steals funds from the victim's account. There are variations of this attack, some including URLs or attachments in the email that, if the victim clicks on or opens, will give the attacker access to the victim's computer.

Spear phishing: Spear phishing is a more sophisticated form of phishing in which the criminal uses just enough information to make the victim believe the email came from someone known to the victim or other reliable source. For example, if a victim receives an email that says something like "Hey (victim's name)! Have you seen the latest about (subject familiar to victim)?" and provides a URL or attachment, the victim may be tricked into clicking or opening, giving the same result as with phishing. In the 2020 survey, responding CISOs said that phishing and spear phishing were the most common attacks that they experienced.

Whaling: Whaling is a phishing or spear phishing attack that specifically targets senior executives and organizational leaders such as mayors/elected officials and department heads.

Brute force: In a brute force attack, the attacker "bangs away" at a victim's computer, network, or IT system using specifically designed software to try to guess a password that will enable it to penetrate the system. Once penetration has been achieved, the attacker can then install malware. It was a brute force attack that resulted in the Atlanta, GA, breach and the installation of ransomware.

Zero-day: A zero-day exploit is the attacker's identification and penetration of a hitherto unknown weakness in a network or IT system (typically a defect in software that had not been found and patched) that allows the attacker to break into the system and install malware.

Denial of Service (DoS): A DoS attack occurs when an attacker sends massive volumes of traffic to a website or an organization's server—so much so that the website or server cannot handle the traffic, essentially shutting it down so no one can use it. This can be done for no malicious reason such as when the University of Maryland Baltimore County's (UMBC) website went down because of a traffic overload that occurred when its president was interviewed in the CBS news magazine 60 min. DoS attacks can also be totally malicious, for example, to demand money to stop the attack.

Distributed Denial of Service (DDoS): A DDoS attack is a DoS attack on steroids—the attack on a server or website by many different computers simultaneously for the purpose of shutting it down to all users. Security Magazine, citing Bloomberg News, reported that the US Department of Health and Human Services was hit by a DDoS attack in March of 2019, and "… the cyberattack was called a campaign of disruption and disinformation that was aimed at undermining the response to the Corona- virus pandemic. The attack may also have been the work of a foreign actor" (Security Magazine, 2020).