Cyberattacks on Local Governments 2020:
Findings from a Key Informant Survey

Authors: Donald F. Norris and Laura K. Mateczun

This article, based on a survey conducted by the authors in 2020, updates and expands upon works previously published by the International City/County Management Association (Donald F. Norris and Laura Mateczun, 2021, A Look at Local Government Cybersecurity in 2020) and John Wiley and Sons (Donald F. Norris, Laura Mateczun and Richard F. Forno, 2022, Cybersecurity and Local Government).

American local governments have increasingly become targets of cyberattacks including, perhaps most destructively, ransomware attacks. According to the cybersecurity firm Emsisoft, in 2019 the U.S. experienced "…an unprecedented and unrelenting barrage of ransomware attacks that impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion" (Emsisoft, 2020). Prominently included among organizations hit by ransomware attacks were 113 local and state governments and agencies. In 2020, another 2,354 federal, state and local governments and agencies were hit by ransomware attacks (Emsisoft, 2021). See Appendix A for a description of ransomware attacks.

These statistics include only ransomware attacks when we know from prior research that local governments are under constant or nearly constant cyberattack of many different types (Norris et al., 2018, 2019 and 2020). Attacks include such vectors as email, phishing, spear phishing, brute force, zero day and denial, distributed denial of service and others. (See Appendix B for brief descriptions of the most common types of attacks.) Cybercriminals can and

do use all of these modes to attack local government IT systems, hold them for ransom, exfiltrate data and/or do other damage.

Here is a small sampling from the thousands of organizations that reported breaches of their IT systems in 2020 and 2021. In 2020: Marriott, International, Instagram, Nintendo, Wawa, YouTube, Albany County, NY, Florence, AL, Knoxville, TN, Lasalle County, IL, Olean, NY, Racine, WI and Torrance, CA, and the Russian "mega-hack" of the software firm SolarWinds affected numerous organizations across the globe. In 2021: Colonial Pipeline; JBS, the world's largest meat packing company); software developer Kaseya affecting about 1,500 businesses; T-Mobile; Microsoft Exchange Server; Oldsmar, FL, water utility; New York City's Metropolitan Transportation Authority; Metropolitan Water District of Southern California; Union Community Schools District, Cedar Rapids, Iowa; the city of Tulsa, Oklahoma; and St. Clair County, Illinois, among many others.

The cost of cyberattacks of is enormous, and it increases every year. A 2016 report estimated that cybercrime would have a worldwide annual cost of $6 trillion by 2021, a significant increase over the $3 trillion in 2015. "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined" (Marks, 2020). Moreover, this prediction "…has been corroborated by hundreds of major media outlets, academia, senior government officials, associations, industry experts, the largest technology and cybersecurity companies, and cybercrime fighters globally" (Cybersecurity Ventures-Herjavec Group, 2019). In the U.S., two well-publicized cases of local government breaches,

Atlanta, GA, in 2018, and Baltimore, MD, in 2019, cost those cities an estimated $17 million and $19 million respectively.

Another source has estimated that by 2025 cybercrime will cost the world economy $10.5 trillion annually and be equivalent to the third largest economy in the world after the U.S. and China. Moreover, cybercrime is "…exponentially larger than the damage inflicted from natural disasters in a year" (Morgan, 2020).

Why are local governments targeted (see also Norris, et al., 2019 and 2020)? The first factor is the sheer number of American local governments -- 90,075 units, of which 38,779 are general purpose governments, including 3,031 county governments, 19,475 municipal governments and 16,253 town or township governments (U.S. Census Bureau, 2018). Second, America's local governments store considerable amounts of sensitive information, especially personally identifiable information (PII) such as names, addresses, drivers' license numbers, credit card numbers, social security numbers and medical information that cybercriminals often target.

Third, cybercriminals are very good at what they do. Moreover, in recent years the availability of low cost but effective hacking tools that require little technical knowledge has made it is relatively easy to get into the business of cybercrime, thus increasing the number of cybercriminals. This means that even unskilled hackers can break into well-defended IT systems (Secureworks, 2017).

Fourth, cyberattacks are deployed by a variety of actors, including: external actors (both individuals and organizations), malicious insiders, nation states, hactivists and terrorists.

Perhaps the clearest contemporary example of this is the well-documented ongoing Russian government directed interference in U.S. elections. Fifth, local governments operate under financial constraints, sometimes severe ones, that limit their ability to acquire and implement state of the practice cybersecurity technology, policies and practices.

Last, the Internet of Things (IoT), a global phenomenon that permits electronic devices of various kinds to connect to the internet for various purposes, has introduced new vulnerabilities and risks for local governments. For local governments, the spread of IoT devices greatly increases the "attack surface" that makes them increasingly vulnerable to cybersecurity threats.

For these and perhaps other reasons, it is critical that cybersecurity scholars and local government officials and practitioners understand the cyberthreats that their governments face, the actions they should take to protect their information assets from attack and to mitigate the damage after successful attacks, the gap between the actual cybersecurity practices of local governments and the need for high levels of cybersecurity and, finally, the barriers that their governments encounter when deploying cybersecurity.

This paper is organized as follows. First, we present our review of relevant literature from both scholarly and professional sources about local government cybersecurity. Next, we discuss our research method and data. Third, using evidence from our survey of key informants, we examine cyberattacks on local governments and their attackers. Fourth, we examine these governments' provision of cybersecurity awareness training. Fifth, we review support for cybersecurity among various officials and staff within them. Last, we draw conclusions and

make recommendations to help improve local government cybersecurity and to advance research on it.

Literature Review

Our review of the literature from 2000 to mid-2021 found that local government cybersecurity remains severely understudied in peer-reviewed journals (Hatcher, et al., 2020; Norris, et al., 2019; and Pries & Susskind, 2020). Only 14 articles from social science and computer science journals examine local government cybersecurity (Appendix C). For the purposes of this paper, only three articles specifically address attacks experienced by local governments (Hatcher, et al., 2020; Norris, et al., 2019; Caruson, et al., 2012). In light of the few empirical articles on local government cybersecurity, the search was specifically limited to research based articles and did not include literature reviews. However, the amount of professional literature published by consulting firms, centers and institutes, professional associations, private IT and cybersecurity firms and others helps to make up for the lack of academic research on this topic (Appendix D). The wide variety of professional works provide the most up-to-date information in the field and they are published with more frequency than is possible in the academic peer-review process. We identified a sample of fourteen professional works reports in our literature review that are part of a much large number of publicly available professional works on cybersecurity. While many of these works discuss cybersecurity in the public sector, few directly address local governments (Sophos, 2021; IBM Security and The Harris Poll, 2020; and MS-ISAC, 2019). Nevertheless, the findings from them

are relevant to local governments. For this paper, we selected and provide a brief summary of the findings of each of the three peer-reviewed articles and three professional reports that pertain directly to local government cybersecurity attacks, attackers, training, awareness and support.

Peer-Reviewed Literature

Hatcher, et al., (2020) conducted a survey of 168 U.S. government officials of municipalities with populations of 10,000 or higher. The survey focused on: 1) whether the city had a formal cybersecurity strategic plan in place; 2) the level support received for cybersecurity planning; 3) the types of cybersecurity policies implemented in cities; and 4) the resources necessary for cybersecurity planning. All of the respondents indicated that their municipality maintained a website, 82 percent of which were maintained in-house. Seventy-one percent of the respondents indicated that their city had a formal cybersecurity policy in place, and 77 percent of those without formal policies reported plans to draft one. The authors identified three areas that effective cybersecurity policies should address according to the open-ended responses in the survey: information security access; information security education; and the use of information technology. Additionally, the presence of a formal cybersecurity policy was found to be significantly related to three results a higher likelihood of: having a termination process during which former employees no longer have access to facilities and information systems (and other processes around access); cataloguing attacks and conducting vulnerability scans and penetration testing on a regular basis (and other processes around prevention and response); and to provide cybersecurity training.

Perhaps the most worrisome finding from that survey is that only 37.0 percent of respondents maintained a formal record of cybersecurity attacks they have experienced, 34.6 percent did not keep such records and 28.4 percent did not know if such records were kept. Additionally, 41.4 percent of respondents did not provide ongoing cybersecurity awareness training. Finally, Hatcher, et al., identified three areas for municipalities to improve their cybersecurity: by "maintaining a log of cybersecurity attacks, working with outside auditors and professionals to review policies and practices on a regular basis, and making cybersecurity more of a management function" (Hatcher, et al., 2020, p. 11). Other findings include the need for additional funding to implement cybersecurity policies.

In 2016, Norris, et al., conducted the first ever nationwide survey of local governments in the U.S. (2019). The article paid particular attention to the attack environment experienced by local governments. We compare many of the findings of that survey throughout this paper with findings from this 2020 survey. Hence, we do not discuss the findings of the 2016 survey here.

In their article, Caruson, et al., (2012) discussed data from a survey that they conducted among 466 local government officials in the state of Florida's 67 counties, which produceda response rate of 24 percent. Among the principal findings of the article, just under a quarter (24 percent) of respondents knew whether their government had experienced a cyberattack in the previous year. Fewer than half of officials (48 percent) reported that their government had adopted cybersecurity policies and standards countywide, had conducted a risk assessment (46 percent), or had a cyberattack response plan in place (22 percent). Respondents also reported a number of pressing cybersecurity needs, including better end user awareness and training (53

percent), better access controls (53 percent), and acceptable use policies for end users (51 percent). More than half (60 percent) said that the main barrier to achieving better cybersecurity was a lack of funding. Insufficient training came in second (43 percent), followed by the need for personnel with more expertise (37 percent).

Professional Literature

Sophos' government ransomware report from 2021 surveyed 5,400 IT decision makers in 30 countries, 131 of which were from local government (Sophos, 2021). The lowest of all the sectors surveyed, 73 percent of local governments have a malware recovery plan. Thirty-four percent of local government respondents experienced a ransomware attack in the previous year 69 percent of which had their data encrypted, as compared to 40 percent of national governments that experienced a ransomware attack and 49 percent whose data was encrypted. Forty-two percent of local government respondents paid the ransom to restore their information systems (compared to 26 percent of national governments), and another 42 percent used backups to restore data (61 percent of national governments) meaning 87 percent of local governments were successful in restoring their data. Only the energy, oil/gas and utilities sector had a higher percentage of paying the ransom (43 percent), the cross-sector average being 32 percent. The average overall remediation costs for local governments were $1.64 million, the cross-sector average being $1.85 million. Seventy-three percent of local governments indicated their cybersecurity workload had increased over 2020. Finally, local governments also rated the lowest in having the tools and knowledge to investigate suspicious activities out of all of the sectors (64 percent).

In 2020 IBM and The Harris Poll conducted a survey of state and local government employees on their perception of cybersecurity threats (IBM Security and The Harris Poll, 2020). Local governments employed 58 percent of respondents. Seventy-three percent of employees were concerned about ransomware attacks to cities in the U.S. and 64 percent were somewhat/very concerned about cyberattacks, more so than natural disasters (61 percent) or terrorist attacks (54 percent). However, the employees also were somewhat optimistic about their government's ability to overcome such an attack (65 percent confident) and 74 percent were confident of their own ability to recognize and prevent a ransomware attack. This is surprising given that only 66 percent of employees were somewhat/very familiar with ransomware, 26 percent of employees had not received any basic cybersecurity training and 54 percent of employees believed they had received adequate training on responding to a cyberattack. Eighty percent of employees did not believe it would be likely that their government would make a ransomware payment, and 56 percent believed impact on public safety should be a very important consideration in making the decision to pay.

The Multi-State Information Sharing & Analysis Center (MS-ISAC), which has many local government organizations as members, conducts the Nationwide Cybersecurity Review (NCSR) annually (MS-ISAC, n.d.). The NCSR is a self-assessment tool for state, local, tribal and territorial (SLTT) governments to assess their cybersecurity programs based on the NIST Cybersecurity Framework. The NCSR measures the maturity of the government's cybersecurity program against the functions and categories in the Framework on a scale of one to seven, one meaning the function or category is "not preformed" and seven being that it is "optimized". The minimum recommended level for local governments is a five ("implementation in process").

Participating governments receive individual reports and metrics to compare anonymously against peer governments. MS-ISAC also provides a biennial report to Congress on the NCSR.

The most recent NCSR report was published in 2019 and involved 3,135 SLTT organizations (MS-ISAC, 2019). Local governments made up 80 percent of SLTT respondents. No SLTT organizations reached a maturity level of five, and local governments had an average score of 3.61 (three is "documented policy") second to state governments who had an average score of 4.78 (four is "partially documented standards and/or procedures"). In terms of local government peer groups, the highest scoring was public utilities (3.75), followed by city (3.69), finance/revenue (3.67), all (3.61) and county/parish (3.60). The lowest scoring local peer groups were: community college (2.68); judicial (2.86); K-12 school district (2.93); elections (3.20); and fire department and services (3.24). The top scoring categories for local governments in the NIST Cybersecurity Framework were in the Protect function: identity management and access control (4.66) and awareness and training (4.06). The lowest scoring categories for local governments were from the Identify function: supply chain risk management (2.78) and risk management (3.02). For the fifth consecutive year the top five security concerns facing SLTT governments remained the same: lack of sufficient funding; increasing sophistication of threats; lack of documented processes; emerging technologies; and inadequate availability of cybersecurity professionals.

Research Method and Data

This is an exploratory study that examines data from a survey of top information technology (IT) and cybersecurity officials in a small sample of U.S. Local governments.

Respondents to this survey included 11 Chief Information Security Officers (CISOs) (78.6 percent of participants), one Chief Information Officer (CIO) (7.1 percent) and two Information Technology Department Directors (ITDs) from 11 cities and three counties in the U.S. (Table 1).

As such, this is both a convenience and an expert sample. A convenience sample is method of nonprobability sampling that includes participants because they were convenient to the researchers (Battaglia, 2008). An expert sample involves the selection of participants who are knowledgeable experts in the field of the survey, in this case local government cybersecurity (Patton, 2018). These cybersecurity and IT officials, or key informants, have considerable expertise, experience in and knowledge of the cybersecurity of their local governments, including their governments' cybersecurity management, practices, risks, strengths, limitations and problems. The use of knowledgeable key informants who are trained, experienced practitioner experts working as the top cybersecurity or IT officials their local governments, should mean that the data from the survey is both valid and reliable.

Insert Table 1 Here

The principal strengths and limitations of this method are that it is simpler, easier and less expensive than probability sampling. It is quite useful for pilot and exploratory studies (of which this survey falls into the latter category). It also produces information from knowledgeable key informants, so the data should be both valid and reliable. The principal limitations of this type of research include that the results are not representative of a broader population and, therefore, cannot be generalized to that population. It is also prone to contain bias and sampling error (e.g., Battacherjee, 2012; Dudovskiy, n.d.; Elfil & Negida, 2017; Etikan,

et al., 2016; Herek, 2012; and Patton, 2018). For exploratory studies, the strengths appear to outweigh the limitations of this research method.

We conducted the survey between mid-April and late August 2020. The initial plan was to conduct a combination of face-to-face and telephone interviews. However, because of the COVID-19 pandemic, conducting face-to-face interviews was unsafe. It was also clear that telephone interviews would not be feasible because of the difficulty finding the telephone numbers of IT and cybersecurity officials on many local government websites, the time pressure under which cybersecurity and IT officials across the nation were working during the pandemic, and a reluctance among such officials to respond to surveys (Norris, et al., 2019). Hence, we used email only.

Initially, we directed the emails only to the then approximately 17 members of the *Coalition of City CISOs* (https://cityciso.org/) that had been formed in the Spring of 2020, and we are especially grateful for the Coalition's support for this survey. Indeed, most of the local governments that participated (at least nine) are members of the Coalition. Additional rounds of emails produced only five additional participants. See Table 2 for participating jurisdictions.

Insert Table 2 Here

Calculating a response rate is difficult because four of the five additional non-Coalition jurisdictions did not reveal their identities and we cannot tell if they were among those we directly solicited or those that had been solicited by colleagues. If the number of jurisdictions contacted is 24, then the response rate is 58.3 percent. If the number is 28 to account for the four additional governments, then the response rate is 50.0 percent. Either one represents a

much better than average response rate for this type of survey (e.g., Norris, et al., 2019 and 2020; and Hatcher, et al., 2020).

The most prominent reason for low response rates in this type of research is that many CISOs and other IT and cybersecurity officials feel that revealing anything about their cybersecurity could put the local government at risk. Revealing too much might also be embarrassing. In this and previous research, more than one official has essentially told us: "Our policy is not to respond to such surveys" (Norris, et al., 2019).

The refusal of local government cybersecurity and IT officials to participate in surveys and other types of research into their cybersecurity is unfortunate for at least three reasons. First, it deprives local governments across the nation of reliable information about the state of cybersecurity management and practice among their peers, which knowledge can benefit all local governments. Second, it deprives these governments of evidence-based recommendations to improve their management and practice of cybersecurity. A third reason involves cybersecurity researchers, whose job it is to gather and make sense of the data that can influence local government cybersecurity management and practice. If researchers cannot gather the data, they cannot analyze it and provide results to local governments and to other scholars in the field.

Beyond gathering and analyzing data and providing results to local governments, these scholars can also begin theorizing about aspects of local government cybersecurity management and practice, such as what are the factors or conditions (independent variables) that produce certain cybersecurity outcomes (dependent variables) among local governments

and why? However, without data from studies of various kinds about local government cybersecurity, theorizing is not likely to occur.

Findings

In this section, we present findings from the 2020 survey and, where, possible compare them with the results of the 2016 survey (Norris, et al., 2019). Please note that throughout this paper when we refer to "the survey" or "this survey" we mean the 2020 survey. When we refer to the 2016 surveys, we name it as such.

The section unfolds as follows. First, we examine attacks on these local governments in the 2020 survey, their attackers and the attackers' motives. We follow this with a discussion of these governments' provision of cybersecurity awareness training, and last, we examine support for cybersecurity among various parties in the government.

Attacks and attackers

Both the 2016 survey and earlier research found that local governments are under constant or nearly constant attack (Norris, et al., 2018 and 2019). Those findings are largely confirmed in this survey. Just over half of respondents (57.1 percent) said constantly, more than a quarter (28.6 percent) said hourly, and two (14.3 percent) said daily (Table 3). Unlike the 2016 survey in which 25.6 percent of governments did not know how frequently they were attacked, none of the governments in the 2020 survey said that they did not know. This finding

(zero do not knows) represents a welcome improvement. If local governments (or any organization for that matter) do not know whether they are under cyberattack, they have given the figurative key to the safe to the burglars. All local governments must implement technologies and policies that allow them to be continually aware of their cyber environment and the risks they face in it.

Insert Table 3 Here

In this survey, we also inquired about "incidents" and "breaches" during the previous year (Table 4). We used Verizon's (2015) definition of those terms: an incident is "an event that compromises the confidentiality, integrity or availability of an information asset;" and a breach is "an incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party." Only one of the governments (7.1 percent) reported no incidents in the past year and one (7.1 percent) did not know (Table 4). Three (21.4 percent) said that they had experienced one incident, two (14.3 percent) said two, four (28.6 percent) said three and three (21.4 percent) said more than five times. These data confirm that the bad guys not only attack often, but that they also get through local governments' defenses as well, and they confirm that local governments need to do a better job protecting their information assets.

Insert Table 4 Here

Half of the local governments in the survey had not experienced breaches in the past year (Table 5). However, the remainder had experienced between one and more than three breaches. Four (28.6 percent) had experienced one breach, one (7.1 percent) had been breached once, one (7.1 percent) twice, one (7.1 percent) three times, and one (7.1 percent)

more than three times. Once again there is confirmation that the bad guys are really good at what they do and that local governments need to improve their ability to protect their information assets. The number of governments (3) that experienced multiple breaches is troubling, especially among a set of governments with mostly large populations and presumably sufficient resources to do a better job.

Insert Table 5 Here

Local governments are not only under constant or nearly constant attack, but the frequency of attacks is increasing (Table 6). The 2016 survey found that about one third of local governments (32.5 percent) experienced the same number of attacks in the past year, about the same fraction (34.4 percent) experienced more attacks and one quarter (25.6 percent) did not know. Nearly all governments responding to this survey (13 or 92.9 percent) said attacks had become more frequent over the past year, and only one (7.1 percent) said that they had remained about the same. This suggests, at least for this subset of local governments, a significant increase in the number of attacks, which is consistent with reporting across all or nearly all sectors of the economy. Cyberattacks are steadily increasing.

Insert Table 6 Here

As in the 2016 survey, in this survey we asked whether local governments could determine the types of attackers they were facing. The 2016 survey found that 41.6 percent of governments could determine their attackers and 58.4 percent could not. Data from this survey show a substantial increase in those that can determine their attackers' identities (Tables 7). Two-thirds (nine or 64.3 percent) could determine their attackers' identities, while

four (28.6 percent) could not and one (7.1 percent) did not know. Separately, one responding CISO said: "Attribution is not a critical factor to us. In most cases, we can take educated guesses, but we do not dedicate cycles to attribution." The increase in the fraction of governments that are able to identify attackers noted in these data could be the result of this particular sample of local governments and, therefore, may not be representative of the broader population of local governments, especially smaller ones.

Insert Table 7 Here

The local governments in this survey said that they were most often attacked by external actors-organizations (five or 35.7 percent reporting), followed by hactivists/spammers (three or 21.4 percent), nation states (two, 14.3 percent), external actors-individuals (one, 7.1 percent), and two (14.3 percent) did not provide answers (Table 8). This is somewhat similar to findings from the 2016 survey in which: 71.0 percent said external actors-organizations; 60.7 percent external actors-individuals; and 29.0 percent nation states. It also tracks well with other sources regarding types of attackers over time.

Insert Table 8 Here

We next asked if the pattern of attacks had changed over the past year (Table 9). Ten respondents (71.4 percent) said it had remained the same, while four (28.6 percent) said it had changed. The changes observed by the latter were increased sophistication of spear and whale phishing, and increased phishing, a focus on ransomware and breach of vendors, and use of commodity malware and attacks tied to the social justice movement (Table 10). That so many local governments in the 2020 survey responded "remained the same" is somewhat surprising

given the dramatic increase in ransomware attacks recently as well as an increasing emphasis that attackers have put on breaching third parties in order to get to their ultimate attack destinations.

Insert Tables 9 and 10 Here

The local governments responding to the survey experienced phishing and spear phishing the most among all attack vectors in the past year (Table 11). This was followed by zero-day brute force and other (five or 35.7 percent each), Distributed Denial of Service or DDoS (three or 21.4 percent), and Denial of Service or DoS (one or 7.1 percent).

Insert Table 11 Here

The most frequent cyberattack purposes that these governments identified were: 1) ransom – eight or 57.1 percent; 2) theft of money – six or 42.9 percent; 3) theft of PII – four or 28.6 percent; and 4) theft of confidential records and 5) hacktivism tied at 3 or 21.4 percent each (Table 12). Three governments (21.4 percent) did not know (which is somewhat surprising and not fully consistent with what one might expect from a sample of mainly large governments). The increase in ransomware attacks is consistent with national data as noted earlier. Four of the top five attack purposes identified by the 2016 survey were somewhat similar to the data from this survey, although not in the same order. They were: ransom – 59.4 percent; mischief – 37.6 percent – (in last place in 2016); PII – 27.7 percent; hacktivism – 27.7 percent; and theft of money – 20.8 percent (Norris, et al., 2019).

Insert Table 12 Here

When asked if the attack purposes had changed during the previous year, 11 respondents said no (78.6 percent), one said yes (7.1 percent) and two (14.3) percent did not know (Table 13). The one respondent who said yes added that the change was a "rise in attacks recently tied to the social justice movement."

Insert Table 13 Here

Cybersecurity Training, Awareness and Support

Training for local government officials and staff at all levels is essential in order to ensure that personnel achieve an understanding of and provide support for cybersecurity in their organizations. Therefore, in this survey we asked if the governments provided mandatory cybersecurity training (and how frequently) to the following parties in their governments: mayor/elected county executive, city/county council members, city/county manager/administrators, department heads, and average end users (Table 14). We focus on mandatory training because if training is optional many people in an organization are likely not to take it and, therefore, will not learn the rules of proper cybersecurity hygiene and, especially, the local government's rules regarding use of its IT assets.

More than three-quarters of respondents (78.6 percent) said that their governments provided mandatory cybersecurity training annually to all parties. Slightly more than seven in ten (71.4 percent) said that they provided annual cybersecurity training to the city/county manager/administrator. One (7.1 percent) said some other time period for all of those parties,

and one (7.1 percent) did not know. Two of these governments did not provide training to any of these parties.

Insert Table 14 Here

These findings represent a substantial improvement over the 2016 survey where between 20 percent and 50 percent of local governments did not provide training at all and another eight to 14 percent did not know. These findings are heartening because yet other research shows that a considerably lower proportion of organizations provide any training at all. For example, PWC found that 48 percent of corporations worldwide provided cybersecurity training to its employees (PWC, 2018). Unfortunately, the PWC data do not report the percentage of such training that was mandatory.

Kudos to the local governments that provided annual mandatory training. They are more likely than those that did not to see improved cyber outcomes. Those that did not provide such training at all or provided it in a time frame greater than at least every three years, are almost guaranteeing that their cyber outcomes will be more difficult and should consider instituting mandatory cybersecurity training or increasing its frequency.

Training is linked, or should be, to outcomes like improved awareness of and support for cybersecurity in organizations. The 2016 survey found 61.7 percent of top managers were moderately/exceptionally aware of the need for cybersecurity 42.3 percent of department managers were moderately/exceptionally aware; and 32.0 percent of elected executives were. This means, however, that nearly one in four top managers were not moderately/extremely

aware of the need for cybersecurity nor were majorities of department heads and elected officials.

In this survey we asked about the awareness of (Table 15) and support for (Table 16) cybersecurity among these local governments': mayor/elected county executive, city/county council members, city/county manager/administrator, department heads, and average end users. The results are not encouraging. Respondents did not believe that the officials and staff in their governments were highly aware of the need for cybersecurity. In only one case (mayor/elected county executive) did a majority of respondents (8 or 57.1 percent) believe that incumbents in this office were highly or mostly aware of the need for cybersecurity. And five respondents (35.7 percent) said these office holders were only somewhat/a little aware, and one (7.1 percent) said not at all aware.

Insert Table 15 Here

Perceptions of the cybersecurity awareness of the remaining officials and staff were bleak. Seven respondents each (50.0 percent) said that city/county manager/administrator was highly/mostly aware. Four (28.6 percent) said somewhat/a little, one (7.1 percent) said not at all, and two (14.3 percent) didn't know. Seven (50.0 percent) responded that department heads were highly/mostly aware, while six (42.9 percent) said somewhat/a little and one (7.1 percent) said not at all. Six (42.9 percent) said that city/county council members were highly/mostly aware; seven (50.0 percent) said somewhat/a little and one (7.1 percent) said not at all. Finally, six (42.9 percent) responded that end users were highly/mostly aware; seven (50.0 percent) said somewhat/a little; and one (7.1 percent) said not at all.

In theory, awareness of the need for cybersecurity among local government officials and staff should lead them to provide support for it. In the 2016 survey, respondents said that 54.0 percent of top managers provided strong/full support for cybersecurity. This was followed by 35.0 percent of elected executives and 33.0 percent of department managers. The results from 2016 suggest otherwise – awareness does not necessarily lead to support because in each case respondents said that amount of support provided by various officials and staff was lower than their degree of awareness.

This survey turns the 2016 findings on their head because its results are more positive, showing that the respondents, on the whole, felt that most of the parties in their governments provided a good deal of support for cybersecurity (Table 16). Eleven respondents said that the mayor/elected county executive was highly/mostly supportive of cybersecurity. Two (14.3 percent) said somewhat/a little, and one (7.1 percent) said not at all. Next, 10 respondents (71.4 percent) said that department heads were highly/mostly supportive, three (21.4 percent) said somewhat/a little, and one (7.1 percent) said not at all. This was followed by city/county manager administrator with eight (57.1 percent) reporting highly/mostly, three (21.4 percent) somewhat/a little and one (7.1 percent) not at all. Two (14.3 percent) didn't know. Average end users came next with eight (57.1 percent) of respondents saying highly/mostly, five (35.7 percent) somewhat/a little and one (7.1 percent) not at all. City/county council members fared the worst when seven respondents (50.0 percent) said highly/mostly, six (42.9 percent said somewhat/a little, and one (7.1 percent) said not at all.

Insert Table 16 Here

Other research confirms, however, that top officials in organizations are often not engaged in cybersecurity at high levels. For example, the PWC survey found that only 44 percent of corporate boards "... actively participate in their company's overall cybersecurity strategy" (PWC, 2018). Likewise, noted cybersecurity expert Charles Cresson Wood has concluded, based on his extensive cybersecurity consulting experience, that regardless of type, size, sector or other characteristics of organizations, top management is not sufficiently well informed about or committed to cybersecurity. This is partly because cybersecurity competes with (and often loses to) other organizational needs. Nevertheless, Wood argued that top executives and managers should understand and fully support cybersecurity and should not allow information security to be the domain of technologists alone (Wood, 2010). Local government officials should take heed of these findings and endeavor to ensure higher levels of awareness of and support for cyber from all parties in their organizations, especially from top elected and appointed officials.

Conclusion and Recommendations

The 2020 survey confirmed the 2016 finding that local governments are under constant or nearly constant cyberattack and both surveys showed that successful cyberattacks occurred frequently. That successful cyberattacks occur is, first, because, as we previously noted, the bad guys are good at what they do, do it more frequently every year and constantly evolve their tactics. Second, even large more wealthy local governments are evidently not doing enough to protect their information assets. One almost certain reason that these governments do not

provide sufficient cybersecurity is lack of cybersecurity awareness training for officials and staff at all levels. Both the 2016 and 2020 surveys found insufficient awareness of the need for cybersecurity and weak or limited support for it (though support was somewhat improved in the 2020 survey). Most of the governments in this survey provided mandatory cybersecurity training to all officials and staff, which is commendable. Governments that do not can expect some, perhaps many officials and staff not to take the training and therefore, be more likely than those that did to practice poor cyber hygiene ("…the practices and steps that users of computers and other devices take to maintain system health and improve online security" [Brook, 2020]). Findings from 2020 represent a substantial improvement over the 2016 survey.

While the findings from this survey regarding cybersecurity awareness are somewhat better than from the 2016 survey, the results remain disappointing. Most respondents felt that there was insufficient cybersecurity awareness among their local officials and staff. On a more positive note, respondents to this survey said that majorities of personnel were highly/mostly supportive of cybersecurity. (This was not the case in the 2016 survey).

Based on the evidence presented in this paper, our first recommendation is that elected officials and top management of local governments must adopt comprehensive strategies to address cyberattacks of all kinds. They should also adopt resiliency plans so that they can continue essential operations during breaches and recover from breaches as expeditiously as possible.

Second, most of the local governments in this survey required top elected officials, council members, top administrators, department heads and end users to take cybersecurity

training. However, respondents generally did not rate the effectiveness of the training highly. Thus, we recommend that local governments review and, as necessary, revise their cybersecurity awareness training in order to ensure that it is effective, especially training regarding cybersecurity awareness and support as well as cyber hygiene. Importantly, this training must be directed to and appropriate for an audience that consists mostly of non-technologists.

Third, local governments must take continual actions to inculcate in all officials and staff the importance of awareness of and support for cybersecurity. Moreover, awareness and support must start at the top of the organization because if top officials fail to act aware supportive of cybersecurity, those under them will almost certainly think: "If they don't care about cyber, why should I?"

Fourth, all parties within local governments, including elected officials, top managers and all employees and contractors, must be held accountable for their cyber hygiene. This means, at a minimum, when someone violates a policy regarding use of the local government's IT system, that individual will be required to take refresher training, receive appropriate "counseling" and potentially lose certain system privileges. In the event of further violations, the individual could lose all privileges and potentially be terminated for cause (of course, termination of employment would not apply to elected officials).

Our fifth recommendation, actually several interrelated recommendations, is directed primarily at small local governments that have either few or no professional IT and cyber staff, although larger governments may benefit from some of what is contained in these paragraphs.

- Because of the importance of cybersecurity and the cost to organizations that do not provide it well or at all, even the smallest of local governments must appropriately staff and fund cybersecurity.
- In the absence of professional staff, consider contracting cybersecurity out.
- Establish partnerships to ease the internal burden of providing cybersecurity. Such partnerships might include local or regional universities, colleges, community colleges and technical schools; other local governments; National Guard units in states that offer cybersecurity assistance; national, state, regional and local organizations that provide cybersecurity assistance and support such as an information sharing and analysis center (ISAC); local and state laws enforcement; national membership organizations like the International City/County Management Association, the National League of Cities, the National Association of Counties and more. Partnerships need to be established preferably before breaches occur. See pp. 194-196, Norris, et al., 2022.
- Consider purchasing cybersecurity insurance.
- Consider adopting multifactor authentication and zero trust throughout the organization. See pp. 108 and 212-213, Norris, et al., 2022.

Our sixth recommendation draws on academic and professional literature and is commonly found within the cybersecurity field itself. All local governments should establish and maintain a culture of cybersecurity within their organizations. A culture of cybersecurity means the following, at the minimum. As we noted above, top leadership, including both elected and appointed officials, must fully understand and support cybersecurity and not just at a rhetorical level. They must: understand that cybersecurity is not solely the responsibility of the technologists, they have an active role to play in it, and they must embrace that role; provide the funding needed for effective cybersecurity; practice proper cyber hygiene themselves; promote cybersecurity throughout the organization as job one for everyone; and insist that all parties are held appropriately accountable for their cyber actions. Top leadership

buy-in will make all parties in an organization understand the importance of cybersecurity and their own cyber responsibilities and will make it more likely that they will practice proper cyber hygiene, thus improving cyber outcomes throughout the organization.

Last is a recommendation directed mainly at scholars interested in conducting research into and increasing our knowledge about local government cybersecurity. As noted earlier, conducting research in this area is exceptionally difficult because of the unwillingness' of IT and cybersecurity officials in local governments to participate in such research. Despite this limitation, we urge at least the following: gather data using a variety of both quantitative and qualitative methods; develop relationships with IT and cyber officials in local governments to make data collection easier; develop relationships with state, regional and national organizations invested in local government cybersecurity for the same reason; examine the various relationships between federal, state, and local governments including cybersecurity grants, workforce development efforts, information sharing and critical infrastructure; track federal and state breach notification requirements and other cybersecurity legislation to study their impact; and more.

We conclude on pessimistic as well optimistic notes. On the pessimistic side, the 2020 survey of local government cybersecurity, and others before it, has shown that, on average, these governments do not provide high levels of cybersecurity. As a result, they place their IT systems, their ability to provide critical public services and the communities that they serve at unnecessary risk. Lack of adequate cybersecurity and/or poor cybersecurity hygiene make it much easier for cybercriminals to breach their IT systems and cause great damage and cost. Therefore, all local governments, regardless of size and budgetary capacity, must take whatever

actions are needed to ensure the highest levels of cybersecurity. This said, even if they do so, the cybercriminals are very good at what they do and are relentless. So, the risk of being compromised is never zero or even close to it, even when practicing the best cybersecurity possible. The common saying in the field is that it isn't whether you will be breached but when.

The optimistic note is that the current state of local government cybersecurity presents great opportunities to improve. To do so, however, will not be easy or inexpensive. But securing local governments' IT assets is critical to their continuing ability to function and serve their communities. Thus, local governments, led by their top officials, must act. Over time (and such efforts will take time) and with proper effort, funding and support, most local governments will be able to achieve something at least akin to the state of the practice of cybersecurity. If local governments can then establish and maintain the state of cybersecurity practice across their entire organizations, it will dramatically improve their cybersecurity management, practice and outcomes. We hope that some of the findings and recommendations that we have made in this paper will help local governments to achieve and maintain that state.

Authors' note: We wish to thank the International City/County Management Association (ICMA) for the ICMA Research Fellowship under which the research for this work was conducted (published by ICMA in 2021 as "A Look at Local government Cybersecurity in 2020"). We also thank ICMA for encouraging us to revise it for publication for academic audiences. The initial work was directed principally at audiences of local government practitioners.

Appendix A: Ransomware Attacks

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 ransomware 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 cybercriminal then demands a ransom (usually in the form of bitcoin to release the system and its files and data. The implicit (often explicit) threat is that if the organization does not pay the ransom, the cybercriminal will leave the data and files encrypted so that the organization cannot use them or potentially expose or share sensitive information.

In the early years of ransomware attacks, many organizations paid the ransom to get their systems back. Today, it is commonly thought that paying ransom is a bad idea because it compensates cybercriminals for their criminality and encourages them and others to continue ransomware attacks. And, increasingly organizations refuse to pay the ransom. Certainly, law enforcement frowns on paying, which may very well be illegal in many situations. Moreover, it is never clear that paying ransom will actually result in the cybercriminal releasing the system. Hence, paying ransom entails some risk.

To prevent ransomware attacks from crippling their IT systems, organizations should continually scan their systems for malware, train their employees to never open suspicious emails and regularly back up their systems, store the backups off site, and maintain several historic versions of the backups. The latter is especially important because the ransomware

may have infected the system weeks to months before it was activated, thus, making recent backups vulnerable to the same ransomware attack.

Appendix B: Types of Attacks

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 cybercriminal 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 cybercriminal 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. 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 Minutes. 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 U.S. 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 Coronavirus pandemic. The attack may also have been the work of a foreign actor" (Security Magazine, 2020).

Appendix C: Peer-Reviewed Journal Articles

Cybersecurity Articles in Social Science and Computer Science Journals 2000-2021

Article	Topic
Surveys and Focus Groups	
Hatcher, et al., 2020	Survey of public officials in U.S. cities of cybersecurity strategic plans, support for those plans, types of cybersecurity policies implemented and resources needed for cybersecurity planning
Norris, et al., 2020	Nationwide survey of U.S. local government cybersecurity management
Norris, et al., 2019	Nationwide survey of cyberattacks against U.S. local governments
Norris, et al., 2018	Focus group of local government IT and cybersecurity leaders in one U.S. state on cyberattacks and cybersecurity management
Caruson, et al., 2012	Survey of local government officials in Florida, examining the relationship between agency size and various cybersecurity issues
MacManus, et al., 2012	Survey of local government officials in Florida, measuring cross-pressure between transparency and privacy
Smart Cities	
Ali, et al., 2020	Exploration of critical factors of information security requirements of cloud services within Australian regional and local government context
Habibzadeh, et al., 2019	A survey of cybersecurity, data privacy and policy issues in cyber-physical system deployments in smart cities
Vitunskaite, et al., 2019*	A comparative case study of Barcelona, Singapore and London smart cities governance models, security measures, technical standards and third party management based on 93 security standards and guidance
Case Studies	
Phin, et al., 2020*	Case study evaluation of a Malaysian local government organization for the physical security components of its IT department
Frameworks	
Falco, et al., 2019	A cyber negotiation framework to help defend urban critical infrastructure against cyber risks and bolster resilience
Ibrahim, et al., 2018*	Case study evaluation of a local government organization in Western Australia using the NIST Cybersecurity Framework
Economic Techniques	

Kesan & Zhang, 2019*	Uses linear models to understand the relationship between local government budgets, IT expenditures and cyber losses
Li & Liao, 2018	Study of alternative economic solutions to the cybersecurity threat of smart cities

* Indicates article was published in a computer science journal

Appendix D: Trade and Professional Publications

Report	Name	Description
Annual / Biennial Surveys		
Multi-State Information Sharing & Analysis Center [MS-ISAC], 2019	Nationwide Security Review (Survey conducted annually since 2013 with results shared to Congress every other year)	Survey of state, local, tribal and territorial governments' cybersecurity programs based on the NIST Cybersecurity Framework
Public Technology Institute and Computing Technology Industry Association [PTI/CompTIA], 2021	State of City and County IT National Survey (published annually)	Survey of local government technology executives on current IT practices, technology priorities, budgets, investments, management and evaluation, cybersecurity, emerging technologies, personnel and more
PTI/CompTIA, 2020	Public Technology Institute and Computing Technology Industry Association – National Survey of Local Government Programs (published annually since 2018)	Survey of local government IT executives on cybersecurity including management, practices, managerial support, budgets, policies, training and more
Deloitte-NASCIO, 2020	Deloitte-NASCIO Cybersecurity Study (Published biennially since 2010)	Survey of 50 states and one territory on the role of the CISO, including budget, governance, reporting, workforce and operations
Heid, 2020	SecurityScorecard – State of the States (published biennially)	Report reviewing and grading the cybersecurity posture of the 56 U.S. states and territories
Verizon, 2021	Verizon Data Breach Investigations Report (Published annually since 2008)	Extensive report analyzing incidents and breaches from around the world for trends and provides break out sections for 11 sectors, including the public sector
Lovejoy, 2021	EY – Global Information Security Survey (Published annually since 1998)	Survey of C-suite and business leaders, including the government and public sector, on the role of the CISO in their organization's cybersecurity
Public Sector		
IBM Security and The Harris Poll, 2020	IBM-Harris Poll Survey 2020 – Public Sector Security Research	Survey of U.S. state and local government employees on

		their government's cybersecurity
Donald F. Norris, 2021	Published by the International City/County Management Association	A survey of local government CISOs conducted in 2020
Goel, et al., 2018	IBM Center for the Business of Government – Managing Cybersecurity Risk in Government: An Implementation Model (2018)	Report covering cybersecurity risk management, federal cybersecurity risk and proposing a model for cybersecurity decision-making (PRISM)
Ransomware		
Sophos, 2021	The State of Ransomware in Government 2021	Examines ransomware in government in 30 countries, including local government organizations
Black Fog, 2021	The State of Ransomware in 2021 (Published annually)	Tracks publicized ransomware attacks by industry, country and month
Emsisoft Malware Lab, 2021	The State of Ransomware in the U.S. (Published annually since 2019)	Tracks ransomware attacks in federal, state and municipal governments; healthcare facilities; and schools, colleges and universities
Costs		
IBM Security, 2021	Cost of a Data Breach Report (Published annually since 2004)	Annual report analyzing the cost of cybersecurity breaches from different countries and industries including the public sector
Smith & Lostri, 2020	McAfee - The Hidden Costs of Cybercrime (2020) (Published biennially since 2014)	Report covering the "hidden" costs of cybercrime (other than cash) in the government sector among others

References

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly* (30): 101419.

Battacherjee, Anol. (2012). *Social science research: Principles, methods and practices*. Textbooks Collection.3. https://scholarcommons.usf.edu/oa_textbooks/3

Battaglia, M. (2008). Convenience Sampling. In Paul J. Lavrakas (ED) *Encyclopedia of Survey Research Methods*. Thousand Oaks, CA: Sage Publications: 149.

Black Fog. (2021, August 02). *The State of Ransomware in 2021*. https://www.blackfog.com/the-state-of-ransomware-in-2021/

Brook, Chris. (2020, October 6). What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more#:~:text=Cyber%20hygiene%20is%20a%20reference,health%20and%20improve%20online%20security.&text=Much%20like%20physical%20hygiene%2C%20cyber,natural%20deterioration%20and%20common%20threats

Caruson, Kiki, Susan A. MacManus, and Brian D. McPhee. (2012). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. *Homeland Security & Emergency Management* 9(2): 1-22.

Cybersecurity Ventures-Herjavec Group. (2019). *2019 Official Annual Cybercrime Report: Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.* https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Deloitte-NASCIO. (2020). *2020 Deloitte-NASCIO Cybersecurity Study.* https://www2.deloitte.com/content/dam/insights/us/articles/6899_nascio/DI_NASCIO_interactive.pdf

Dudovskiy, John. (n.d.). *Convenience sampling*. Business Research Methodology. https://research-methodology.net/sampling-in-primary-data-collection/convenience-sampling/

Elfil, Mohamed, & Negida, Ahmed. (2017). Sampling methods in clinical; research; An educational review. *Emergency – Emerg (Tehran)*, 5(1):e52. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5325924/

Emsisoft Malware Lab. (2021, July 18). *The State of Ransomware in the US: Report and Statistics 2020.* https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/

Emsisoft Malware Lab. (2020, December 12). *The State of Ransomware in the US: Report and Statistics 2019.* https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

Etikan, Ilker, Sulaiman Abubakar Musa and Rukayya Sunusi Alkassim. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of theoretical and Applied Statistics*, 5(1): 104.

Falco, G., Noriega, A., & Susskind, L. (2019). Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyberattacks. *Journal of Cyber Policy.* DOI: 10.1080/23738871.2019.1586969

Goel, R., Haddow, J., & Kumar, A. (2018). Managing Cybersecurity Risk in Government: An Implementation Model. *IBM Center for the Business of Government*. http://www.businessofgovernment.org/sites/default/files/Managing%20Cybersecurity%20Risk%20in%20Government.pdf

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society* (50): 101660.

Hatcher, William, Wesley L. Meares and John Heslen. (2020). The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. *Journal of Cyber Policy.*

Heid, A. (2020, October 15). *State of the States*. SecurityScorecard. https://securityscorecard.pathfactory.com/state-of-the-states/state-to-states-map-

Herek, Gregory M. (2012). *A brief introduction to sampling.* https://psychology.ucdavis.edu/rainbow/html/fact_sample.html

Ibrahim, A., Valli, C., McAteer, I., and J. Chaudhry. (2018). A Security Review of Local Government Using NIST CSF: A Case Study. *The Journal of Supercomputing*, 74: 5171-5186.

IBM Security. (2021). *Cost of a Data Breach Report 2021*. https://www.ibm.com/downloads/cas/OJDVQGRY

IBM Security and The Harris Poll. (2020). *Public Sector Security Research IBM-Harris Poll Survey 2020*. https://www.ibm.com/downloads/cas/74JKYWZQ

Kesan, J. P., and L. Zhang. (2019). An Empirical Investigation of the Relationship Between Local Government Budgets, IT Expenditures, and Cyber Losses. *IEEE Transactions on Emerging Topics in Computing.* Advance online publication. Doi: 10.1109/TETC.2019.2915098.

Li, Z., & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly* (35): 151-160.

Lovejoy, K. (2021). *Global Information Security Survey 2021*. EY. https://www.ey.com/en_us/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

MacManus, Susan A., Caruson, Kiki, and Brian D. McPhee. (2012). Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights. *Journal of Urban Affairs* 35 (4): 451-470.

Marks, Joseph. (2020, December 14). *The CyberSecurity 202: A Russian Mega-Hack is Further Damaging Trump's Cybersecurity Legacy*. Washington, D.C.: Washington Post. https://www.washingtonpost.com/politics/2020/12/14/cybersecurity-202-russian-mega-hack-is-further-damaging-trumps-cybersecurity-legacy/

Morgan, Steve. (2020, November 13). *Cybercrime to cost the World $10.5 Trillion Annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerapocalypse-cybercrime-report-2016/

Multi-State Information Sharing & Analysis Center [MS-ISAC]. (2019). *2019 Nationwide Cybersecurity Review*. https://www.cisecurity.org/wp-content/uploads/2021/06/2019-NCSR-Summary-Report.pdf

_____. (n.d.). *Nationwide Cybersecurity Review (NCSR)*. https://www.cisecurity.org/ms-isac/services/ncsr/

Norris, Donald F. (2021). A Look at Local Government Cybersecurity in 2020. *Public Management.* Washington, D.D.: International City/County Management Association. Laura Mateczun contributed materially to the research undertaken for this paper

Norris, Donald F., Laura Mateczun, Anupam Joshi and Tim Finin. (2020). Managing cybersecurity at the grassroots, Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs.* https://www.tandfonline.com/doi/full/10.1080/07352166.2020.1727295

Norris, Donald F., Laura Mateczun, Anupam Joshi and Tim Finin. (2019). Cyberattacks at the grassroots: American local governments and the need for high levels of cybersecurity. *Public Administration Review.* 76(6): 895-904.

Norris, Donald F., Laura Mateczun, Anupam Joshi and Timothy 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.

Patton, M. Q. (2018). Expert sampling. In Bruce B. Frey (Ed). *The Sager encyclopedia of educational research, measurement, and evaluation*. Thousand Oaks, CA: Sage Publications.

Phin, P. A., Abbas, H., & Kamaruddin, N. (2020). Physical security problems in local governments: A survey. *Journal of Environmental Treatment Techniques* 8(2): 679-686.

Pries, B., & Susskind, L. (2020). Municipal cybersecurity: More work needs to be done. *Urban Affairs Review*. DOI: 10.1177/1078087420973760

Public Technology Institute and the Computing Technology Industry Association [PTI/CompTIA]. (2021). *2021 Public Technology Institute (PTI) State of City and County IT National Survey*. https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/2021-pti-state-of-city-and-county-it-national-survey.pdf?sfvrsn=bf5e8d49_0

Public Technology Institute and the Computing Technology Industry Association [PTI/CompTIA]. (2020). *PTI/CompTIA 2020 National Survey of Local Government Cybersecurity Programs*. https://comptiacdn.azureedge.net/webcontent/docs/default-source/advocacy-documents/2020-pti-cybersecurity-national-survey.pdf?sfvrsn=b0488502_2

PWC. (2018). *Strengthening Digital Society Against Cyber Shocks: Key Findings from the 2018 Global State of Information Security Survey*. https://www.pwc.com.br/pt/global-state-of-information-security-survey-2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf

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

Secureworks. (2017). *2017 State of Cybercrime*. https://www.secureworks.com/resources/rp-2017-state-of-cybercrime

Smith, Z. M., & Lostri, E. (2020, December 7). The Hidden Costs of Cybercrime. *McAfee*. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Sophos. (2021, June). *The State of Ransomware in Government 2021*. https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-state-of-ransomware-in-government-2021-wp.pdf

Verizon. (2021). *Verizon 2021 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Verizon. (2015). *Verizon 2015 Data Breach Investigations Report*. https://www.verizon.com/about/news/2015-data-breach-report-info

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security* (83): 313-331.

Wood, Charles C. (2010). Preface. In Whitman, Michael E. and Herbert J. Mattord. 2010. *Management of Information Security*, 4th ed. Stamford, CT: Cengage Learning.

U.S. Census Bureau. (2018). *2017 Census of Governments*. Table2. Local governments by type and state: 2017 [CG1700ORG02]. https://www2.census.gov/programs-surveys/gus/tables/2017/cog2017_cg1700org02.zip

Tables

Table 1. What is your official title?

	Number	Percent
CISO	11	78.6
CIO	1	7.1
ITD	2	14.3
Other		
Total	14	100.0

Table 2. Participating local government and their population?

Boston, MA 692,600
Chicago, IL 2,693,976
Dallas, TX 1,343,573
Detroit, MI 670,031
Fairfax County, VA 1,457,532
Los Angeles, CA 3,979,576
Memphis, TN 651,073
Nashville, TN 670,820
San Francisco, CA 881,549
Seattle, WA 753,675

2019 Census estimates, 2019 for counties and for cities and towns. Please note that we received explicit permission from the 10 listed local governments to identify them by name.

Table 3. How often is your local government subject to cyberattack?

	Number	Percent
Constantly	8	57.1
Hourly	4	28.6
Daily	2	14.3
Weekly		
Monthly		
Less frequently than monthly		
Don't know		
Total	14	100.0

Table 4. How many times has your information system experienced an "incident" in the past year?

	Number	Percent
None	1	7.1
Once	3	21.4
Twice	2	14.3
Three times	4	28.6
Five times		
More than five times	3	21.4
Don't know	1	7.1
Total	14	100.0

Table 5. How many times has your IT system or any element of it been breached in the past year?

	Number	Percent
None	7	50.0
Once	4	28.6
Twice	1	7.1
Three times	1	7.1
More than three times	1	7.1
Don't know		
Total	14	100.0

Table 6. Have cyberattacks gotten more or less frequent over the past year?

	Number	Percent
More frequent	13	92.9
About the same	1	7.1
Less frequent		
Don't know		
Total	14	100.0

Table 7. Are you able to determine the types of attackers?

	Number	Percent
Yes	8	57.1
No	4	28.6
Don't know	2	14.3
Total	14	100.0

Table 8. If you are able to determine the types of attackers, are they (check all that apply):*

	Number	Percent
External actors -- organizations	5	35.7
External actors -- individuals	1	7.1
Nation states	2	14.3
Hactivists/spammers	3	21.4
No answer	2	14.3

*Total does not equal 100% due to question wording.

Table 9. Has the pattern of attacks changed or remained the same over the past year?

	Number	Percent
Changed	4	28.6
Remained the same	10	71.4
Don't know		
Total	14	100.0

Table 10. If the pattern has changed, please describe the changes.

- Phishing emails are the biggest threat and the biggest change is more targeted and sophisticated spear phishing and whale phishing.
- Focus on ransomware and breach of vendors.
- More sophisticated use of commodity malware. Increase in attacks tied to social justice movement.
- Broader attempt at phishing has occurred.

Table 11. What are the principal attack vectors (check all that apply)?*

	Number	Percent
Phishing or spear phishing	12	85.7
Zero day	5	35.7
Brute force	5	35.7
DDOS	3	21.4
DOS	1	7.1
Man in the middle		
Other	5	35.7

*Total does not equal 100% due to question wording.

Table 12. What are the principal purposes of the attacks you experience in the past year (check all that apply)?*

	Number	Percent
Ransom	8	51.7
Theft of Money	6	42.9
PII	4	28.6
Hactivism	3	21.4
Confidential records	3	21.4
Mischief	1	7.1
Espionage	1	7.1
Don't know	3	21.4

*Total does not equal 100% due to question wording.

Table 13. Have the purposes of the attacks changed in the past year?

	Number	Percent
Yes	1	78.6
No	11	7.1
Don't know	2	14.3
Total	14	100

Table 14. Does your local government require mandatory cybersecurity training for any of the following and. if so, how often?

	No	Annually	Every 2 or 3 years	Other time period	Don't know	Total
Mayor/elected county executive	2 14.3	11 78.6		1 7.1		14 100.0
City/county council members	2 14.3	11 78.6		1 7.1		
City/county manager/administrator	2 14.3	10 71.4		1 7.1	1 7.1	14 100.0
Department heads	2 14.3	11 78.6		1 7.1		14 100.0
Average end user	2 14.3	11 7 8.6		1 7.1		14 100.0

Table 15. In your opinion, how aware are the following of the need for high levels of cybersecurity?

	Highly	Mostly	Somewhat	A little	Not at all	Don't know	Total
Mayor/elected county executive	5 28.6	3 21.4	2 14.3	3 21.4	1 7.1		14 100.0
City/county council members	3 21.4	3 21.4	3 21.4	4 28.6	1 7.1		14 100.0
City/county manager/administrator	5 28.6	2 14.3	4 28.6		1 7.1	2 14.3	14 100.0
Department heads	3 21.4	4 28.6	6 42.9		1 7.1		14 100.0

Table 16. In your opinion, how supportive of the need to maintain high levels of cybersecurity are the following?

	Highly	Mostly	Somewhat	A little	Not at all	Don't know	Total
Mayor/elected county executive	6 42.9	5 35.7	2 14.3		1 7.1		14 100.0
City/county council members	2 14.3	5 35.7	4 28.6	2 14.3	1 7.1		14 100.0
City/county manager/administrator	6 42.8	2 14.3	3 21.4		1 7.1	2 14.3	14 100.0
Department heads	2 14.3	8 57.1	2 14.3	1 7.1	1 7.1		14 100.0
Average end user	1 7.1	7 50.0	3 21.4	2 14.3	1 7.1		14 100.0