Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 2 Article 9

October 2023

Adoption of cybersecurity policies by local governments 2020

Donald F. Norris PhD
University of Maryland, Baltimore County, norris@umbc.edu

Laura K. Mateczun JD
University of Maryland, Baltimore County, lam6@umbc.edu

Adoption of cybersecurity policies by local governments 2020

Abstract

This paper should be of interest to the readers of this journal because it addresses a subject that has received little scholarly attention; namely, local government cybersecurity. The U.S. has over 90,000 units of local government, of which almost 39,000 are “general purpose” units (i.e., municipalities, counties, towns and townships). On average, these governments do not practice cybersecurity effectively (Norris, et al., 2019 and 2020). One possible reason is that they do not adopt and/or implement highly recommended cybersecurity policies. In this paper, we examine local government adoption or lack of adoption of cybersecurity policies using data from three surveys. Norris, et al, 2019 & 2020; Hatcher, et al., 2020; and Norris and Mateczun, 2023. It will probably not be surprising that our first finding is that, by and large, local governments still do a poor good job of adopting and implementing cybersecurity policies. Thus, our first recommendation is that these governments must take whatever actions are needed to ensure high levels of cybersecurity. If they do not, the consequences will be painful and costly, as demonstrated by examples presented in the text. Among these actions, we next recommend that local governments adopt and effectively implement the highly recommended cybersecurity policies discussed in the concluding section. Last, as we have recommended previously, we again call upon local governments to create and maintain within their organizations a culture of cybersecurity – one in which all parties in these governments fully understand and support cybersecurity at the highest levels in their governments.

Keywords

cybersecurity, cybersecurity policies, cyber policies, local government

Cover Page Footnote

Acknowledgement: 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.

Adoption of cybersecurity policies by local governments: 2020

Donald F. Norris
School of Public Policy
University of Maryland, Baltimore County
Baltimore, Maryland, USA
https://orcid.org/0009-0009-7997-5137

Laura K. Mateczun
School of Public Policy
University of Maryland, Baltimore County
Baltimore, Maryland, USA
https://orcid.org/0000-0002-5540-8308

1. INTRODUCTION

Local governments in America are under constant or nearly constant cyberattack [1] and, as *public* entities, they have an important responsibility to protect their information systems and assets with effectively deployed cybersecurity. Research has shown that, on average, local governments practice and manage cybersecurity poorly [1 & 2]. Among the many reasons for this failure (some of which we discuss later in this paper), a particularly important one is that too many local governments have not adopted and fully implemented highly recommended, industry standard cybersecurity policies.

The purpose of this paper is to examine local government adoption or lack of adoption of cybersecurity policies using data from three surveys. The surveys are: first is the nationwide survey of cybersecurity in American local governments conducted by Norris, et al., in 2016 [1 & 2]; second is the nationwide local government cybersecurity survey conducted by Hatcher, et al., in 2018 [3]; and third is a survey conducted by Norris and Mateczun of a subset of high-level cybersecurity officials in mostly large American local governments in 2020 [4]. Throughout this paper we refer to these surveys by the dates they were conducted. In this paper, we also address a range of barriers to local governments being able to provide high levels of cybersecurity, because these barriers often work to reinforce local governments' failure to adopt and implement cybersecurity policies.

This paper's principal contributions are, first, findings regarding local government adoption of or failure to adopt highly recommended cybersecurity policies, and second, recommendations to these governments regarding actions to take to overcome lack of policy adoption and implementation. These recommendations are important, especially given the failure of too many governments to adopt and implement such policies as shown in the surveys reviewed herein.

The paper unfolds as follows. We follow this introduction with a review of the scholarly and professional literatures that directly address local government cybersecurity. Next, we discuss our research method and the data we use for our analysis. This is followed by our findings, particularly findings about adoption of cybersecurity policies, the perceived effectiveness of adopted policies, and barriers to local government achievement of high levels of cybersecurity. Last, we present our conclusions and make recommendations to local governments to assist them in the adoption and implementation of cybersecurity policies.

2. LITERATURE

Prior research on local government cybersecurity has found that there is relatively little peer-reviewed, scholarly literature on this subject. Indeed, much of the recent local government cybersecurity research has been conducted, in part, in attempt to address the gap in this literature [1, 2, 3, 4, & 5]. Our extensive review of the body of literature, both academic and professional, from 2000 to 2021 identified 14 peer-reviewed journal articles in the social and computer sciences (Appendix A) and 15 works from the profession (Appendix B) that directly address cybersecurity at the level of local government or are otherwise highly relevant to this subject. We limited the search to research articles. For the purposes of this paper, we included only three scholarly articles [2, 3,& 7] and four professional reports [4, 8, 9 & 10]. This is because, among all of the works we identified, only these address local government adoption and implementation of cybersecurity policies and best practices. However, we did not include two papers [2 & 4] in this section because we discuss them in depth in the findings section of the paper.

We begin with the scholarly literature. Hatcher, et al., [3] 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. 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 presence of a formal cybersecurity policy was found to be significantly related to a higher likelihood of local governments: 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 providing cybersecurity training.

Perhaps the most worrisome finding from that survey, however, is that only 37.0 percent of respondents maintained a formal record of cybersecurity attacks they had experienced, while 34.6 percent did not keep such records and 28.4 percent did not know if such records were kept. Only half encrypted sensitive data, and 41.4 percent of respondents did not provide ongoing cybersecurity awareness training. Finally, Hatcher, et al., identified three areas for local governments 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" [3, p. 11]. Another important finding includes the need for additional funding to implement cybersecurity policies.

In their article, Caruson, et al., [7] discussed data from a survey that they conducted among 466 local government officials in the state of Florida's 67 counties, which produced a 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). Yet fewer engaged in cooperative groups with local governments (20 percent), had a computer incident response team (18 percent), or cooperated with the private sector (8 percent) or non-profit firms (3 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).

Next, we examine works from the profession. The Public Technology Institute and the Computing Technology Industry Association (PTI/CompTIA) annually publish what are perhaps two of the most targeted surveys of local government IT and cybersecurity. The first examines city and county IT management more generally, rather than having a sole focus on cybersecurity. The second surveys local government cybersecurity.

The first survey, PTI/CompTIA's State of City and County IT National Survey [8], examines local government IT practices, budgeting, management and more. Respondents to this survey indicated that the highest rated cybersecurity priorities were: data backup, integrity and restoration (86 percent rated highest priority); modernizing defenses (67 percent); further establishing a security mindset (64 percent); training for general staff (62 percent); developing or testing cybersecurity incident response plans (59 percent); adopting a cybersecurity framework based on national standards (51 percent); policies to reflect changing threat landscape (49 percent); and training for existing IT staff (49 percent). The CIOs also identified three areas to improve in order to help bridge the IT skills gap: cybersecurity; cloud, i.e., infrastructure migration, application or platform deployment; and infrastructure, i.e. improvements to network/systems reliability, performance. Largely increasing compared to the findings of the 2020 and 2021 surveys, 84 percent of the CIOs expected their IT budgets to increase in the next year (33 percent increasing by five percent or more and 51 percent increasing one to four percent). Ten percent of respondents did not expect any change to their budget, and six percent anticipated a budgetary decrease.

The second of the surveys is PTI/CompTIA's National Survey of Local Government Cybersecurity Programs [9], which more narrowly focused on local government cybersecurity (2021). First and foremost, nearly 58 percent of respondents did not feel that their government's cybersecurity budget was adequate, down from 67 percent in 2020. A little more than nine in ten (92 percent) governments provided employee awareness training, 59 percent of which was ongoing and 34 percent was provided once a year. Twenty four percent of local governments exempted elected officials and their staff from cybersecurity awareness training. In terms of plans and policies, 81 percent stated their local government had a cybersecurity plan or strategy, 73 percent of which were reviewed within the past year. Fifty percent of these plans allowed for exceptions to be made to the policy, which, in 2020,

anecdotally tended to be for elected officials and their staff. Sixty five percent, of governments had a mobile device management policy in place, up ten percent from 2020. Less than half (42 percent) had formal incident response plans and disaster recovery plans that were tested each year, and only one third of local governments had undergone a network or security audit in the past year (33 percent; 54 percent tested some systems and policies; 13 percent conducted no tests or audit).

The Multi-State Information Sharing & Analysis Center (MS-ISAC), which has thousands of local government organizations as members, conducts the Nationwide Cybersecurity Review (NCSR) annually (MS-ISAC, n.d.) [10 & 11]. Participating governments receive individual reports and metrics to compare their governments anonymously against peer state, local, tribal and territorial (SLTT) governments. MS-ISAC also provides a biennial report to Congress on the NCSR. The NCSR is a self-assessment tool for SLTT governments to assess the cybersecurity programs of these organizations based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework [12]. 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 Performed" and seven being that it is "Optimized." The minimum recommended level for local governments is a five ("Implementation in Process").

The most recent NCSR report [11], published in 2021, was based on responses from 3,267 SLTT organizations [10]). Local governments made up 82 percent of SLTT respondents. Yet of that report, only 20 local respondents had reached a maturity level of seven (0.7 percent), nearly one third scored at or above the minimum recommended level of five, or "Implementation in Process" (31 percent), and one third below level three, or "Documented Policy" (33 percent), meaning they are using ad-hoc processes). For the seventh consecutive year the top five security concerns facing SLTT governments remained the same: lack of sufficient funding; increasing sophistication of threats, emerging technologies, lack of documented processes; and an inadequate availability of cybersecurity professionals. Organizations 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.

3. RESEARCH METHOD AND DATA

To gather data for this research, we conducted a survey among Chief Information Security Officers (CISOs) and other highly placed Information Technology (IT) officials in 11 cities and three counties in the U.S. (Table 1). The distribution of respondents in the 2020 survey is very similar to that of the 2016 survey where the great majority, 89.4 percent, were cybersecurity and IT professionals.

TABLE 1. What is your official title?

	Number	Percent
CISO	11	78.6
ITD	2	14.3
CIO	1	7.1
Other	0	0.0
Total	14	100.0

The cybersecurity and IT officials who responded to both surveys have considerable expertise, experience in and personal knowledge of the cybersecurity of their local governments, including their governments' cybersecurity management, practices, risks, strengths, limitations and problems. As such, these respondents constitute both a convenience sample and an expert sample. Such a sample is highly suitable for exploratory research, which is our purpose here [13, 14, 15, 16, 17, 18, 19 & 20].

The principal strengths of this sampling technique are that convenience sampling is simpler, easier and less expensive than probability sampling. It is especially useful for pilot and exploratory studies. And it produces information from knowledgeable key informants. The principal limitations are that it is not representative of a broader population. Results cannot be generalized to a broader population. And it is prone to contain bias and sampling error.

As a result of the use of knowledgeable key informants who are trained, experienced practitioner experts working as the top cybersecurity or IT officials their local governments, the data from the survey should be both valid and reliable. However, due to the size of the survey, we cannot generalize the findings of this survey to other local governments in the U.S.

We conducted this survey between mid-April and late August 2020. The initial plan was to conduct some face-to-face interviews mixed with others by telephone and email. However, because of the COVID-19 pandemic, conducting face-to-face interviews was unsafe. It became clear that telephone interviews would probably 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 general reluctance among such officials to respond to surveys (Norris, et al., 2022). Hence, we chose to use email only.

Initially, we sent emails only to the then approximately 17 members of the *Coalition of City CISOs* (https://cityciso.org/), that was formed in the spring of 2019 and at whose organizational founding both authors were invited to speak. The Coalition includes the CISOs (or comparable officials) of some of the largest cities in the nation, 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. Two anonymous colleagues who were familiar with this research, one in a city government and one in a local government membership organization, volunteered to solicit responses from other local governments, and we thank them for their assistance as well. See Table 2 for participating jurisdictions.

TABLE 2. Participating Jurisdictions*

Boston, MA
Chicago, IL
Dallas, TX
Detroit, MI
Fairfax County, VA
Los Angeles, CA
Memphis, TN
Nashville, TN
San Francisco, CA
Seattle, WA

*The CISOs or ITDs of these 10 local governments gave us explicit permission to use their governments' names.

In the emails soliciting participation in the survey, we provided potential respondents with a brief description of the survey, noted that it was being conducted under the auspices of a Research Fellowship from the International City/County Management Association (ICMA), provided a link to the survey, promised to provide the responding jurisdictions a copy of the analyses of the data and attached a copy of a White Paper on Local Government Cybersecurity that the authors had prepared at the behest of the Coalition [21].

By mid-July 2020, we had received responses from nine Coalition members. Throughout the late spring and summer of 2020, we sent three rounds of emails to the Coalition CISOs who had not responded (eight cities) and at least one round of emails to either the mayor or chief administrative officer of those governments requesting their participation in the survey. (Recipients of these requests did not respond to them, except for one CISO who responded that he would not participate.) We also emailed seven jurisdictions outside of the Coalition that we believed would be likely to participate. These efforts produced five additional responses for a total of 14 responses. Calculating a response rate is a bit tricky because four of the five additional jurisdictions did not reveal their identities, and we cannot tell if they were among those we solicited or had been solicited by our colleagues. If the number of jurisdictions contacted is 24, then the response rate is 58.3 percent. If that number is 28 to account for the four additional governments, then the response rate is 50.0 percent. Either one represents a better than average response rate.

Perhaps the most prominent reason for low response rates in this type of research is the concern among CISOs and other officials that revealing anything about their cybersecurity management, practices, risks and limitations might put their local governments 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."

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 with 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.

In the survey instrument, we promised respondents anonymity and confidentiality. As a result, we will not reveal anything in this paper that might breach that promise nor will we write anything that could link survey responses to any jurisdiction. Anonymity and confidentiality are essential elements for the conduct of research into sensitive topics, although clearly in this and other surveys, it was not sufficient to produce high response rates. For example, the 2016 survey achieved only an 11.9 percent response rate after several mailings and personal contact by telephone. In their 2018 nationwide survey of local government cybersecurity, Hatcher, et al., [3] achieved only a seven percent response rate.

The great majority of respondents (ten or 71.1 percent) were cities (clearly the result of the support of the Coalition of City CISOs for this survey). See Table 3. Next came counties (three or 21.4 percent), and one (7.1 percent) consolidated city/county.

TABLE 3. Is your local government a:

	Number	Percent
City/Municipality	10	71.4
County	3	21.4
Consolidated city/county	1	7.1
Township	0	0.0
Total	14	100.0

As seen in Table 4, these governments ranged in population from a low of 220,000 to a high of 4 million. Within that range, four were over 1 million, three were from 800,000 to 999,999, and six were from 500,000 to 799,999. That they represent mainly large jurisdictions should not be a limitation of this research. This is because, regardless of size (and presumably the greater budgetary capacity of larger governments), all U.S. local governments confront largely the same cybersecurity landscape, are under constant or nearly constant attack and have limited resources with which to defend themselves. Moreover, as the 2016 survey found, size did not matter statistically to cybersecurity problems, practices, management or outcomes.

TABLE 4. 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.

4. FINDINGS

In this section we discuss findings from the 2020 survey that have direct bearing on American local government adoption of highly recommended, industry standard cybersecurity policies, the perceived effectiveness of those policies and barriers to the ability of local governments to provide effective cybersecurity.

A. Adoption

The reason for inquiring about local government adoption of cybersecurity policies is that cybersecurity experts commonly recommend adoption of such policies to improve cybersecurity management and practice in organizations. Moreover, the failure to adopt and effectively implement cybersecurity policies in organizations is often linked to adverse cybersecurity outcomes [22 & 23]. See Table 5 below.

Although this section focuses primarily on cybersecurity policies adopted by local governments in the 2020 survey, similar questions were asked in the 2018 and 2016 surveys. Table 6 displays the similarities among those surveys on questions of policy adoption. In the 2020 survey eleven governments (78.6 percent) had fully adopted formal cybersecurity policies, which is 30 percent above the 2016 survey and three (21.4 percent) had partially adopted. By contrast, in the 2018 survey by Hatcher, et al. [3], 71.4 percent of governments had adopted cybersecurity policies. However, that survey asked only whether governments had adopted, not whether they had adopted fully or partially. Combining the

full and partial adopters in the 2020 survey, shows that all of the responding governments had at least partially adopted cybersecurity policies, a considerable improvement over the 2016 survey. It is possible that the difference in the samples of the 2020 survey (larger local governments with presumably greater fiscal capacity) and the 2016 and 2018 surveys, which include local governments serving smaller populations (and presumably lesser fiscal capacity), would impart an analytic bias on the results. However, resource constraints did not seem to have a significant impact as roughly 70 to 80 percent of governments had adopted cybersecurity policies in both the 2020 and 2018 surveys.

TABLE 5. Has your local government adopted any of the cybersecurity policies listed below?*

	Adopted fully #	%	Adopted partially #	%	Not adopted #	%	Don't know #	%	Total #	%	% adopted in 2016 Survey
Formal cybersecurity policy	11	78.6	3	21.4					14	100	40.1
Password management policy	11	78.6	3	21.4					14	100	70.7
Policy regarding applying software patches	10	71.4	3	21.4	1	7.1			14	100	Not Asked
Cyber risk management plan	8	57.1	3	21.4	3	21.4			14	100	26.7
Incident response/disaster recovery/business continuity plan	8	57.1	5	35.7	1	7.1			14	100	27.6
Policy on use of external devices (e.g., cell phones/flash drives)	6	42.9	4	28.6	4	28.6			14	100	54.2
Policy for vendors, contractors, cloud services	6	42.9	6	42.9	1	7.1	1	7.1	14	100	27.6

*The question in the 2016 survey was binary, yes or no, and did not ask fully or partially, so the percentages reported there may include governments that had only partially adopted policies.

Table 6. Policy Adoption Questions in the 2020, 2018 and 2016 Surveys

2020	2018	2016
Formal cybersecurity policy	Formal cybersecurity policy	Cybersecurity policy, standards, strategy or plan
Password management policy	Are passwords to critical servers regularly changed	Password Creation Rules & Periodic Password Change Requirement (two separate policies)
Policy regarding applying software patches	Is there a system for tracking software patches and updates	
Cyber risk management plan		Cybersecurity risk management plan
Incident response/disaster recovery/business continuity plan		Plan for recovery from breaches
Policy on use of external devices (e.g., cell phones/flash drives)		Personally-Owned Device Use Policy for Officials and Employees
Policy for vendors, contractors, cloud		Cybersecurity Standards for Contracts with Vendors for Cloud-based Services

Next, we turn to password management policies. In the 2020 survey, 11 governments (78.6%) had fully adopted password management policies, and three governments (21.4 percent) had partially adopted, compared to about 70 percent adoption in 2016.[1] In the 2018 survey 74.7 percent of respondents reported that "passwords to critical servers were regularly changed," while 16.7 said they were not and 8.6 percent did not know. If the full and partial adopters in the 2020 survey are combined, it shows that all governments had at least partially adopted password management policies. This is a substantial improvement over both of the previous surveys.

The 2020 survey found that ten governments (71.4 percent) had fully adopted policies regarding software patches, while three (21.4 percent) had partially adopted and one (7.1 percent) had not adopted such a policy. The 2018 survey found that 75.3 percent of governments had in place "a system for tracking software patches and updates," 9.3 percent had not, and 15.4 percent did not know. Once again, combining the full and partial adopters in the 2020 survey shows that all but one had at least partially adopted this policy, another substantial improvement over the 2018 survey. (This question was not asked in the 2016 survey.)

From the 2020 survey, eight governments (57.1 percent) had fully adopted cyber risk management policies, while three (21.4 percent) had partially adopted them and three (21.4 percent) had not adopted them. This compares favorably to the 2016 survey in which only 26.7 percent of governments had adopted cybersecurity risk management "plans" and 73.3 percent had not. (There was no comparable question in the 2018 survey.) Eight governments (57.1 percent) in the 2020 survey fully adopted incident response plans/disaster recovery/business continuity plans, while five (35.7 percent) had partially adopted and one (7.1 percent) had not adopted. Once again, this compares favorably to the 2016 survey where only 27.6 percent had adopted "plans to recover from breaches."

Six governments (42.9 percent) had adopted policies on the use of external devices (compared to 54.2 percent in 2016), while four (28.6 percent) had percent) had partially adopted, one (7.1 percent) had not adopted and one (7.1 percent) did not know.

Overall, these data show that more of the sample governments had adopted more cybersecurity policies than was true in the 2016 survey. This said, it is also clear that too many had adopted too few policies or had adopted them only partially. Aside from the full

[1] The 2016 survey contained two password related questions, and 70.7 percent of respondents said their local governments had password creation rules while 70.0 percent said they had password change requirements. The authors understand that NIST SP 800-63B "Digital Identity Guidelines" no longer recommends password expiration or arbitrary, periodic change requirements.

adoption of two important policies, these data reveal a surprising lack of full policy adoption among the responding governments, especially since these governments are, for the most part, large in size with potentially adequate budgetary resources that follow population size and trained professionals managing their cybersecurity. The lack of full adoption, in turn, likely means that these governments are not able to derive the full benefits of these policies, their implementation and enforcement. These data do not enable us to know how much "partial" adoption meant to the respondents. This could be important in understanding the policies perceived effectiveness. Further research will be needed to complete our understanding here.

B. Effectiveness

It is not enough to know solely about adoption. The best policies may not work well and, if that is the case, then cybersecurity outcomes are likely to be problematic. Hence, we asked about the perceived effectiveness of the policies (Table 7). Six respondents (42.9 percent) said that their password management policies were highly effective (compared to 56.3 percent in 2016), three (21.4 percent) said somewhat, and one (7.1 percent) said not very. Four (28.6 percent) said their formal cybersecurity policies were highly effective (versus 19.2 percent in 2016), nine said somewhat (64.3 percent) and one (7.1) said not very. Another four said that their software patching policies were highly effective (28.6 percent), eight (57.1 percent) said somewhat and one each (7.1 percent) said not very and not at all.

Three respondents (21.4 percent) said that their incident response plans were highly effective (compared to 21.1 percent in 2016), nine (64.3 percent) said somewhat, and one each (7.1 percent) said not very and not at all. Two (14.3 percent) said their cyber risk management plans were highly effective (versus 19.2 percent in 2016), six (42.9 percent) said somewhat, four (28.6 percent) said not very, and two (14.3 percent) said not at all. Two (14.3 percent) said their policies on the use of external devices was highly effective (compared to 42.1 percent in 2016), eight (57.1 percent) said somewhat, one (7.1 percent) said not very, two (14.3 percent) said not at all and one (7.1 percent) did not know. Finally, two (14.3 percent) said their policies for vendors, etc.,

TABLE 7. How effective, if at all, are these policies?

	Highly #	%	Somewhat #	%	Not very #	%	Not at all #	%	Don't Know # %	Total #	%	% High/ Very High 2016
Formal cyber-security policy	4	28.6	9	64.3	1	7.1				14	100	19.6
Password management policy	6	42.9	6	42.9	2	14.3				14	100.1	56.3
Policy regarding applying software patches	4	28.6	8	57.1	1	7.1	1	7.1		14	100	Not Asked
Cyber risk management plan	2	14.3	6	42.9	4	28.6	2	14.3		14	100.1	19.2
Incident response/disaster recovery/business continuity plan	3	21.4	9	64.3	1	7.1	1	7.1		14	100	21.1
Policy on use of external devices (e.g., cell phones/flash drives)	2	14.3	8	57.1	1	7.1	2	14.3	1 7.1	14	100	42.1
Policy for vendors, contractors, cloud services	2 14.3		7	50.0	2	14.3	1	7.1	2 14.3	14	100	36.5

were highly effective (versus 36.5 percent in 2016), seven (50.0 percent) said somewhat, two (14.3 percent) said not very, one (7.1 percent) said not at all and two (14.3 percent) did not know.

For the most part, responses to the questions of policy effectiveness do not inspire confidence that the policies are working as needed to achieve their objectives. Somewhat and not very effective responses suggest that the policies (and/or their enforcement) contain gaps that are likely to allow problems of cybersecurity practice and management to occur, perhaps serious problems. Consider, for example, the policy on applying software patches where only 28 percent of respondents said that this policy was highly effective. That suggests that too often software patches are not applied in a timely manner, if at all. The literature tells us that failure to apply software patches as soon as possible after they are released by vendors is a major reason that cybercriminals are able to breach local government IT systems [24 & 25).

What we do not know from these data, however, is why the respondents rated the effectiveness of these policies so low. Could it be that the policies themselves were not well written, and, as a result, they would be unlikely to be effective? Could it be that the policies have not been properly implemented or were not being enforced? We also do not know what the term "somewhat effective" meant to the respondents. It could have meant good but not perfect, which generally could suggest a positive outcome. Or it could have meant weak but with some positive qualities or anything in between. Further research will be needed to find answers to these questions.

C. Barriers

It is possible, even quite likely that certain well-known barriers to cybersecurity act in ways that make the adoption and implementation and, hence, the effectiveness of cybersecurity policies less than optimal. Previous research has uncovered a number of barriers to local government achievement of high levels of cybersecurity. For example, the 2016 survey found that the top four barriers were: 1) inability to pay competitive salaries (58.6 percent); 2) insufficient number of staff (53.1 percent); 3) lack of funds (52.8 percent); and 4) lack of adequately trained staff (46.0 percent). Notably, all of these barriers are somewhat or totally related to funding.

The results of the 2020 survey (Table 7) are reasonably consistent with those of the 2016 survey in that the two top barriers reported in the 2020 survey were lack of funds (11 or 78.6 percent responses) and lack of adequate/adequately trained staff (ten or 71.4 percent). All other listed barriers received three or fewer responses.

TABLE 8. What are the three top barriers your local government faces in being able to achieve the highest levels of cybersecurity?

	Number/% reporting
Lack of funds	11 78.6
Lack of adequate staff**	10 35.7
Lack of leadership buy-in/support	3 21.4
Lack of collaboration	2 14.3
Procurement process	2 14.3
Governance	2 14.3

*Total exceeds 100% due to question wording;
**Includes "trained staff."

As previous studies have shown, lack of adequate funding is a major barrier to achieving high levels of cybersecurity [1]. Consequently, we wanted to know the level of cybersecurity spending among the surveyed governments. According to the National Association of State Chief Information Officers (NASCIO), in 2018 not quite half the states had dedicated cybersecurity budgets, and states spent an average of zero to three percent of their IT budgets on cybersecurity [26]. By contrast, according to Gartner, average spending by U.S. businesses on cyber is between five and eight percent of companies' IT budgets [27.]

Among the local governments in this study, the average spending was 4.09 percent of the IT budget, and the range was between zero and 10.0 percent (Table 8). One government did not report its budgetary percentage. Eight of these governments spend less on cybersecurity (as a percent of their IT budgets) than Gartner found among U.S. businesses, while five were within or greater than Gartner's estimate. Six spent less than NASCIO found among state governments while eight spent more. These data tend to confirm that funding for cybersecurity for at least some of these local governments is inadequate.

TABLE 9. What percentage of your IT budget is allocated to cybersecurity?

0.0	3.9
< 1.0	6.0
1.0	6.05
1.0	7.0 to 9.0
1.8	9.1
2.0	10.0

This survey also asked what three things local governments needed to do or possess to be able to achieve the highest levels of cybersecurity (Table 9). The top three from the 2016 survey were: 1) greater funding (54.7 percent); 2) better cybersecurity policies (38.3 percent); and 3) greater cybersecurity awareness among local government employees (35.3 percent). Eight respondents to the current survey identified funding (57.1 percent) and seven (50.0 percent) identified staffing as the top two needs, which are consistent with the top two barriers previously identified. The third need was leadership buy-in (four or 28.6 percent), the lack of which is a common complaint among cybersecurity officials. We return to this issue in the final section of this report.

TABLE 10. What are the three things your local government needs to do to possess or be able to achieve the highest levels of cybersecurity?

	#	%
Funding	8	57.1
Staffing	7	50.0
Leadership buy-in/commitment	4	28.6
Awareness/training	2	14.3
Continuity of operations/ disaster recovery/ incident response	4	28.6
MFA (Multifactor authentication)	3	21.4
No answer	3	21.4

*Total exceeds 100% due to question wording

5. CONCLUSIONS AND RECOMMENDATIONS

Overall, the local governments in all three surveys had not done as good a job as they should have in adopting highly recommended cybersecurity policies. In the 2020 survey among mostly larger local governments, only three of the subject policies had been adopted by substantial majorities of these governments, and fewer than half of respondents said that any policy was highly effective.

Local governments that do not provide high levels of cybersecurity place themselves and their businesses and citizens at great and unnecessary cyber risk. As has been shown repeatedly in recent years, successful attacks on local government IT systems, especially the particularly pernicious ransomware attacks, severely limit these governments' ability to provide critical public services. One example of a recent such attack occurred in Oakland, CA, in February of 2023, causing city officials to shutter many departments to the public for weeks and to declare a state of emergency in order to restore non-emergency services such as payment collection and to continue processing reports, permits and licenses [28]. Additionally, the Oakland Police Department's computers were down, limiting available police services, and the planning and building department was completely closed, placing some construction projects on hold.

As this example shows, lack of adequate cybersecurity allows hackers and cybercriminals to breach local governments' IT systems and cause great harm, at great cost. Then there is the embarrassment factor. See also the successful breaches of the IT systems in Atlanta, GA in 2019, which cost the city $19 million, and in Baltimore, MD in 2018 and 2019, the latter of which cost that city $18 million [22].

Therefore, our first recommendation (which will be obvious to most readers) is that all local governments, regardless of size, must take whatever actions are needed to ensure the highest levels of cybersecurity.

Consistent with the literatures on IT and local government, local e-government and local government cybersecurity, respondents to this survey named lack of funding and lack of staff as their top two barriers to effective cybersecurity. Data from the 2020 survey on local government cybersecurity budgets demonstrate that cybersecurity is substantially under-funded in several of them. Thus, our second recommendation is that elected officials and top management of local governments must, within budgetary limitations, provide adequate funding for cybersecurity, including funding for adequate staffing of this important function. Failure to adequately fund and staff cybersecurity will almost certainly lead to adverse cyber outcomes.

Third, in order to improve their cybersecurity practice and management, local governments should consider a range of cybersecurity policies covering a variety of topics. Some are *essential* to the provision of effective cybersecurity and should be adopted by all local governments, while others are *desirable* but not necessarily essential [22].

The essential policies include:

- an Acceptable Use Policy governing how employees and others use the local government IT systems;
- an Information Security Policy describing how information created, exchanged and stored on a local government information system is protected and handled, including the requirement that data at rest be encrypted at all times;

- a Privacy Policy governing how the local government's public facing websites collects, uses, stores and shares different types of information;

- an Identity and Access Management Policy establishing the process for creating and removing user accounts, categories of users, and the various roles and permissions that may be assigned to users based on their function within the organization;

- an Incident Handling Policy describing how the local government will respond in the event of a cyberattack, which is especially important when critical governmental functions and services are disrupted or disabled; and

- a Disaster Recovery or Business Continuity Policy describing how the organization responds to major emergencies such as a cyberattack or natural disaster.

Desirable policies include the following. It is also possible for local governments to include desirable policies within their essential policies. For example, remote access, BYOD and email use policies could be included in the Acceptable Use Policy and so on.

- a Remote Access Policy describing how remote access to a local government's information system is granted and revoked;

- a Bring-Your-Own-Device Policy governing when and how employee-owned devices can be connected to the local government's information systems;

- an Email Use Policy governing the use of official email;

- a Media and Communications Policy describing who is allowed to communicate to the media in the event of a breach;

- a Change (or Configuration) Management Policy establishing how the local government's information system can be changed;

- a Vulnerability and Patch Management Policy to address how and when vulnerabilities to technology products and applications are handled; and

- a Backup Policy governing the frequency and method of backing up the local government's information systems (Norris, et al., 2022).

However, policy adoption alone is not enough. Our fourth recommendation is that local governments must not only fully adopt but also must effectively implement their cybersecurity policies. This is because if policies are not effectively implemented, they will do little or no good, thus placing local governments at unnecessary cyber risk.

Therefore, governments must put into place measures to ensure the effectiveness of the policies. At the minimum, this includes continuously monitoring for policy effectiveness using appropriate methods and metrics. If any policy is not effective in achieving its objectives, it should be revisited, revised, and re-implemented appropriately.

As we have argued elsewhere [1, 2 & 22], our final recommendation is that local governments should establish and maintain a culture of cybersecurity within their organizations. At a minimum, top leadership, including both elected and appointed officials, must fully understand and support cybersecurity and not just at a rhetorical level. These officials must understand that cybersecurity is not solely the responsibility of the technologists, but that they have an active role to play in it as well, and they must embrace that role. Effectively embracing that role means helping to advocate and secure the funding needed for effective levels of cybersecurity, for adequate staffing, technology and policies in place. Local government leaders must practice proper cyber hygiene themselves and promote cybersecurity throughout the organization as a primary aspect of employment. Therefore, all parties are held appropriately accountable for their cyber actions. If top officials fail to insist on such a culture and act appropriately in their own cyber responsibilities, those under them will almost certainly think: "If they don't care about cyber, why should I?" Top leadership buy-in will make all parties in an organization understand the importance of cybersecurity, including their own contributions and cyber responsibilities making it more likely that they will practice proper cyber hygiene, thus improving cyber outcomes throughout the organization.

ACKNOWLEDGEMENT: 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: 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 [3]	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 [2]	Nationwide survey of U.S. local government cybersecurity management
Norris, et al., 2019 [1]	Nationwide survey of cyberattacks against U.S. local governments
Norris, et al., 2018 [5]	Focus group of local government IT and cybersecurity leaders in one U.S. state on cyberattacks and cybersecurity management
Caruson, et al., 2012 [7]	Survey of local government officials in Florida, examining the relationship between agency size and various cybersecurity issues
MacManus, et al., 2012 [29]	Survey of local government officials in Florida, measuring cross-pressure between transparency and privacy
Smart Cities	
Ali, et al., 2020 [30]	Exploration of critical factors of information security requirements of cloud services within Australian regional and local government context
Habibzadeh, et al., 2019 [31]	A survey of cybersecurity, data privacy and policy issues in cyber-physical system deployments in smart cities
Vitunskaite, et al., 2019* [32]	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* [33]	Case study evaluation of a Malaysian local government organization for the physical security components of its IT department
Frameworks	
Falco, et al., 2019 [34]	A cyber negotiation framework to help defend urban critical infrastructure against cyber risks and bolster resilience
Ibrahim, et al., 2018* [35]	Case study evaluation of a local government organization in Western Australia using the NIST Cybersecurity Framework
Economic Techniques	
Kesan & Zhang, 2019* [36]	Uses linear models to understand the relationship between local government budgets, IT expenditures and cyber losses
Li & Liao, 2018 [37]	Study of alternative economic solutions to the cybersecurity threat of smart cities

* Indicates article was published in a computer science journal

Appendix B: Trade and Professional Publications

Report	Name	Description
Annual / Biennial Surveys		
Multi-State Information Sharing & Analysis Center [MS-ISAC], 2021 [10]	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], 2022 [8]	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, 2021 [9]	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 [38]	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 [39]	Security Scorecard – State of the States (published biennially)	Report reviewing and grading the cybersecurity posture of the 56 U.S. states and territories
Verizon, 2021 [40]	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 [41]	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 [42]	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[4]	Published by the International City/County Management Association	A survey of local government CISOs conducted in 2020

Goel, et al., 2018 [43]	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 [44]	The State of Ransomware in Government 2021	Examines ransomware in government in 30 countries, including local government organizations
Black Fog, 2021 [45]	The State of Ransomware in 2021 (Published annually)	Tracks publicized ransomware attacks by industry, country and month
Emsisoft Malware Lab, 2021 [46]	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 [47]	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 [48]	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

[1] D. Norris, L. Mateczun, A. Joshi and T. Finin, Cyberattacks at the grassroots: American local governments and the need for high levels of cybersecurity. Public Administration Review. 76(6): 895-904, 2019

[2] D. Norris, L. Mateczun, A. Joshi and T. Finin, Managing cybersecurity at the grassroots, Evidence from the first nationwide survey of local government cybersecurity. Journal of Urban Affairs, 2020.

[3] W. Hatcher, W. Meares and J. Heslen. The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. Journal of Cyber Policy, https://doi.org/10.1080/23738871.2020.1792956, 2020, 28 July.

[4] D. Norris and L. Mateczun, A look at local government cybersecurity in 2020, Public Management, Washington, D.C.: International City/County Management Association, 2021.

[5] D. Norris, L. Mateczun, A. Joshi and T. Finin, Cybersecurity at the grassroots: American local governments and the challenges of Internet security. Journal of Homeland Security and Emergency Management. 15(3): 1-14. 2018.

[6] B. Pries, and L. Susskind, Municipal cybersecurity: More work needs to be done. Urban Affairs Review. DOI: 10.1177/1078087420973760, 2020.

[7] K. Caruson, S. MacManus, and B. McPhee. Cybersecurity policy-making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success, Homeland Security and Emergency Management 9(2): 1-22, 2012.

[8] Public Technology Institute and the Computing Technology Industry Association [PTI/CompTIA], 2022 Public Technology Institute (PTI) State of City and County IT National Survey. https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/2022-state-of-city-county-it-national-survey.pdf?sfvrsn=9b7f8f7_0, 2022.

[9] Public Technology Institute and the Computing Technology Industry Association [PTI/CompTIA], 2021 National Survey of Local Government Cybersecurity and Cloud Initiatives. https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/pti-2021-cybersecurity-report-final.pdf, 2021.

[10] Multi-State Information Sharing and Analysis Center [MS-ISAC], 2021 Nationwide Cybersecurity Review Summary Report. https://www.cisecurity.org/insights/white-papers/2021-nationwide-cybersecurity-review-summary-report, 2021.

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

[12] National Institute of Standards and Technology [NIST], Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1., https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf,, 2018.

[13] A. Battacherjee, A. "Social science research: Principles, methods and practices. Textbooks Collection." https://scholarcommons.usf.edu/oa_textbooks/3, 2012.

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

[15] M. Elfil, and A. Negida, Sampling methods in clinical; research; An educational review. Emergency – Emerg (Tehran), 5(1):e52. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5325924/, 2017.

[16] I. Etikan, S. Musa, and R. Alkassim, Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1): 104, 2016.

[17] G. Herek, A brief introduction to sampling. https://psychology.ucdavis.edu/rainbow/html/fact_sample.html, 2012.

[18] G. Mayyan, Gilad David, January 13, The IoT rundown for 2020: Stats, risks, and solutions, SecurityToday. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?p=1, 2020.

[19] Secureworks. (2017). 2017 State of Cybercrime. https://www.secureworks.com/resources/rp-2017-state-of-cybercrime, 2017.

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

[21] D. Norris and L. Mateczun, Laura. (2020). White Paper: What local government officials should know and do about cybersecurity. Coalition of City CISOs. https://cityciso.org/research, 2020 and University of Maryland, Baltimore County, https://publicpolicy.umbc.edu/wp-content/uploads/sites/176/2020/06/Cybersecurity-White-Paper.pdf, 2020.

[22] D. Norris, L. Mateczun and R. Forno. Cybersecurity and local government. Hoboken, NJ: John Wiley and Sons, 2022.

[23]A. Subhani. 2021 (October 11) . Nine lessons to create and implement Effective cybersecurity policies. https://www.forbes.com/sites/forbestechcouncil/2021/10/11/nine-lessons-to-create-and-implement-effective-cybersecurity-policies/?sh=6f5123e03eca

[24] Norton. 2021 (January 23). 5 reasons why general software updates and patches are important. https://us.norton.com/blog/how-to/the-importance-of-general-software-updates-and-patches

[25] Raths, D. (2019, October/November). Managing software updates still a government stumbling block. GovTech. https://www.govtech.com/security/managing-software-.

[26] NASCIO. (2020). Ensure dedicated cybersecurity funding for state and local governments with CIOs as key decisionmakers. www.NASCIO.org/wp-content/uploads/2020/01/NASCIO-Dedicated-Cyber-Funding-2020.pdf

[27] K. Nash, Tech chiefs plan to boost cybersecurity spending. The Wall Street Journal. https://www.wsj.com/articles/tech-chiefs-plan-to-boost-cybersecurity-spending-11577701802, 2019, December 30.

[28] D. Lin, (2023, February 17). Weeklong ransomware attack on Oakland government drags on. CBS News Bay Area. https://www.cbsnews.com/sanfrancisco/news/weeklong-ransomware-attack-on-oakland-government-drags-on/

[29] S. MacManus, K. Caruson and B. McPhee, Cybersecurity at the local government level: Balancing demands for transparency and privacy rights, Journal of Urban Affairs, 35 (4): 451-470, 2012.

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

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

[32] M. Vitunskaite, Y. He, T. Brandstetter, and H. Janicke, 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, 2019.

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

[34] G. Falco, A. Noriega, and L. Susskind, Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyberattacks. Journal of

Cyber Policy. DOI: 10.1080/23738871.2019.1586969, 2019.

[35] A. Ibrahim, C. Valli, I. McAteer and J. Chaudhry. A security review of local government using NIST CSF: A case study, The Journal of Supercomputing, 74: 5171-5186, 2018.

[36] J. Kesan and L. Zhang. 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, 2019

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

[38] Deloitte-NASCIO. 2020 Deloitte-NASCIO Cybersecurity Study, https://www2.deloitte.com/content/dam/insights/us/articles/6899_nascio/DI_NASCIO_interactive.pdf, 2020.

[39] A. Heid, State of the states, SecurityScorecard, https://securityscorecard.pathfactory.com/state-of-the-states/state-to-states-map-, 2020, October 15.

[40] Verizon, Verizon 2021 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf, 2021.

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

[42] IBM Security and The Harris Poll. (2020). Public sector security research IBM-Harris poll survey, https://www.ibm.com/downloads/cas/74JKYWZQ, 2020.

[43] R. Goel, J. Haddow, and A. Kumar, 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, 2018.

[44] Sophos, 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, 2021, June.

[45] Black Fog "The state of ransomware in 2021," https://www.blackfog.com/the-state-of-ransomware-in-2021/, 2021, August 02.

[46] Emsisoft Malware Lab, 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/, 2021, July 18.

[47] IBM Security. (2021). Cost of a data breach report https://www.ibm.com/downloads/cas/OJDVQGRY, 2021.

[48] Z. Smith and E. Lostri, E., The hidden costs of cybercrime. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf, 2020, December 7 .