PAR PUBLIC ADMINISTRATION REVIEW

Donald F. Norris
Laura Mateczun
Anupam Joshi
Tim Finin
University of Maryland, Baltimore County

Research Article

Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity

Abstract: *This article examines data from the first-ever nationwide survey of cybersecurity among American local governments. The data show that these governments are under constant or near-constant cyberattack, yet, on average, they practice cybersecurity poorly. While nearly half reported experiencing cyberattacks at least daily, one-third said that they did not know whether they were under attack, and nearly two-thirds said that they did not know whether their information systems had been breached. Serious barriers to their practice of cybersecurity include a lack of cybersecurity preparedness within these governments and a lack of adequate funding for it. The authors make recommendations to local governments to improve their cybersecurity practice and to scholars for additional research into local government cybersecurity, an area that, to date, has largely been neglected by researchers from the social sciences and computer science.*

Evidence for Practice

- Local governments as a whole do a poor job of managing their cybersecurity.
- Local governments should be aware of and follow the security best practices and recommendations published by relevant federal government organizations.
- Local governments should conduct regular cybersecurity audits or reviews that include their major cybersecurity risks as well as their cybersecurity policies and practices.
- Major barriers to improving cybersecurity practices in local governments are low levels of awareness of and support for cybersecurity and a lack of funding for it; local governments should take action to address these barriers.
- Cybersecurity threats are constantly evolving, so local governments must track and adapt to the changes.

In this article, we examine data from the first-ever nationwide survey of cybersecurity among America's grassroots or local governments. Cybersecurity among local governments is increasingly important because, as we show herein, these governments are under constant or near-constant attack (see Norris et al. 2018). Among the local governments that responded to our survey, 28 percent reported being attacked at least hourly or more frequently, and 19 percent said they were attacked at least once a day (for a total of 47 percent of all respondents). What is troubling, however, is that more than a quarter (nearly 28 percent) said that they did not know how frequently they were being attacked. Local governments "not knowing" this and other basic cybersecurity information is an issue to which we will return later in this article.

There are other reasons, as well, to be concerned about cybersecurity at the grass roots. The first is the sheer number of American local governments—90,000 units, of which nearly 39,000 are general purpose governments, including 3,031 county governments, 19,519 municipal governments, and 16,360 town or township governments (U.S. Census Bureau 2012). Except for the smallest of them, these governments have critical information technology (IT) systems and cumulatively spend billions of dollars each year to support those systems. One estimate placed state and local government spending on IT at more than $60 billion per year (Dixon 2014).

Second, America's local governments maintain and store sensitive information, especially personally identifiable information (PII) such as names, addresses, driver's license numbers, credit card numbers, Social Security numbers, and medical information. Such information is valuable, and obtaining it is often the purpose of cyberattacks. In fact, over the past few years, numerous local governments have reported that some of the PII they stored was lost through data breaches or information exfiltration, and, in some cases, they were threatened with the data being released or destroyed unless a ransom was paid.

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

Laura Mateczun is a graduate of the Francis King Carey School of Law, University of Maryland, and a member of the Maryland Bar. She is currently a PhD student in the School of Public Policy, University of Maryland, Baltimore County, studying public management. Her research interests are local government cybersecurity, criminal justice, and the importance of equity in policy analysis. She received her bachelor's degree in public policy and political science from St. Mary's College of Maryland.
E-mail: lam6@umbc.edu

Anupam Joshi is Oros Family Professor and chair of the Computer Science and Electrical Engineering Department at the University of Maryland, Baltimore County (UMBC). He is also director of UMBC's Center for Cybersecurity and a fellow of the Institute of Electrical and Electronics Engineers. He earned his undergraduate degree from IIT Delhi and a PhD from Purdue University. He has published over 225 technical papers with an h-index of 78 and over 22,750 citations, has been granted several patents, and has obtained grants from a variety of federal and industrial sources.
E-mail: joshi@umbc.edu

Public Administration Review, Vol. 00, Iss. 00, pp. 00.
DOI: 10.1111/puar.13028.

Tim Finin is Willard and Lillian Hackerman Chair in Engineering and professor of computer science at the University of Maryland, Baltimore County. He has more than 40 years of experience in applying artificial intelligence to problems in information systems and language understanding. He is a fellow of the Association for Computing Machinery and the Association for the Advancement of Artificial Intelligence, received an Institute of Electrical and Electronics Engineers technical achievement award, and was the University of Maryland, Baltimore County's 2012 Presidential Research Professor. He holds degrees from the Massachusetts Institute of Technology (MIT) and the University of Illinois and has held positions at Unisys, the University of Pennsylvania, Johns Hopkins University, and MIT's AI Laboratory.
E-mail: finin@umbc.edu

Third, individuals and organizations have become increasingly successful at hacking both private sector organizations (such as Home Depot, Target, JPMorgan Chase, AT&T, Yahoo, eBay, Google, Anthem, Equifax, and many others) and those in the public sector (such as the U.S. Central Command, the U.S. Postal Service, the White House, the National Oceanic and Atmospheric Administration, the cities of Atlanta and Baltimore, and the University of Maryland, College Park). Moreover, the number of cyberattacks grows annually.

Fourth, cyberattacks are deployed not only by individuals and organizations but also by nation-states and their surrogates and by transnational nonstate actors such as terrorists. Perhaps the clearest contemporary example of this is the ongoing "meddling" in U.S. elections by the Russian government. Fifth, cyberattacks are very costly to the U.S. and world economies. A 2015 report estimated that by 2019, the annual cost of data breaches will reach $2.1 trillion worldwide, nearly a fourfold increase over 2015 (Juniper Research 2015).

Fifth, the internet of things (IoT) is a rapidly expanding phenomenon that introduces new vulnerabilities and risks for local governments, especially through new programs aimed at creating "smart cities" by deploying internet-connected devices to sense, collect, and share data and, in some cases, to directly control physical systems for improved monitoring and management of assets and resources. A few years ago, a typical U.S. household with broadband internet service had one or two computers connected. Today, such homes have a Wi-Fi router connecting nearly 15 devices, including computers, televisions, thermostats and smoke alarms, security cameras, and smart speakers like the Amazon Echo (NCTA 2018). Local governments are increasingly using IoT devices to better support their services, such as monitoring traffic and parking, detecting rubbish levels in trash receptacles, and installing smart meters and security cameras. Moreover, as they increasingly manage "smart" physical systems, such as wastewater, electricity, and so on, the consequences of poor defense are more than just data breaches—they include physical harm and damage.

For local governments, the spread of IoT devices greatly increases the "attack surface" that makes them vulnerable to cybersecurity threats. Moreover, the set of devices may be large and very heterogeneous, with different manufacturers, capabilities, and interfaces. The result is a system that is inherently difficult to monitor and update as new security vulnerabilities are discovered.

One risk is that some IoT devices can be infected and used to launch distributed denial-of-service (DDoS) attacks on internet services and sites. For example, in 2016, the Mirai botnet compromised as many as 600,000 IoT devices and used these to attack and cripple several popular internet sites (Antonakakis et al. 2017). Other risks are that the devices can be disabled, have their sensor data stolen or modified, or have their activator functions used inappropriately to cause damage. Before incorporating IoT technologies, local governments must understand and plan for the additional security risks they introduce by developing and supporting policies that will protect them from current and future threats.

Finally, as we discuss in the literature review that follows, there is an enormous gap in the scholarly literature on the subject of local government cybersecurity. Indeed, our review identified only four articles about local government cybersecurity in peer-reviewed journals in the social sciences and computer science between 2000 and early 2018—a problem we hope to begin rectifying with this article.

For these and other reasons, it is critical to understand the cyberthreats that local 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 those actions and the need for high levels of cybersecurity, and, finally, the barriers that these governments encounter when deploying cybersecurity. Understanding these issues will enable us not only to begin closing the gap in the literature but also to make recommendations for improving local government cybersecurity.

Literature Review

We conducted an extensive search for works about local government cybersecurity in journals in the social sciences and computer science between 2000 and March 2018. We searched several academic and peer-reviewed journal databases, such as EBSCOhost and ScienceDirect as well as Google, Google Scholar, and library search engines from the University of Maryland System, using an exhaustive list of key search terms, including *attack, breach, hack, cyberattack* and *cyber attack,* and *incident,* and *local, state, city,* and *county government, e-government, agency, cybersecurity, data, database, infrastructure, information technology,* and *PII*. Through this review, we were able to identify only four articles from the social sciences and none from computer science that addressed some aspect of local government cybersecurity (Caruson, MacManus, and McPhee 2012a, 2012b; Fusi and Feeney 2017; Zhao and Zhao 2010). However, only one of them (Caruson, MacManus, and McPhee 2012b) is directly relevant to the research presented in this article.[1]

As we noted earlier, there is a paucity of scholarship about local government cybersecurity in the social

sciences and computer science. However, this deficiency is partially overcome by the numerous publicly available studies and reports from consulting firms, centers and institutes, professional associations, private IT and cybersecurity firms, and professional organizations. Among those that we found particularly relevant and useful to our research were studies by Deloitte and the National Association of State Chief Information Officers (NASCIO) (2010, 2012, 2014, 2016), the Ponemon Institute (2015), the Center for Digital Government (2014), the IBM Center for the Business of Government (Goodyear et al. 2010), Cisco (2018), and Security Scorecard (2018).[2] Each of these, in one way or another, addressed cybersecurity at the state and or local government level in the United States.

We begin this literature review by discussing the sole peer-reviewed article that we identified that is directly relevant to local government cybersecurity and follow with a discussion of publicly available studies and reports.

In their article, Caruson, MacManus, and McPhee (2012b) discussed data from a survey that they conducted among 466 local government officials in the state of Florida's 67 counties. The survey 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).

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). As we will show later, these results are highly consistent with the findings from our research.

The publicly available studies and reports that we identified, which were produced mainly to provide information to state and local cybersecurity practitioners, provide perhaps the most up-to-date information available about local government cybersecurity. For example, in their 2016 survey, Deloitte and NASCIO found that the top four barriers to state government cybersecurity were a lack of sufficient funding (80 percent), a lack of availability of cybersecurity professionals (51 percent), a lack of documented cybersecurity processes or policies (45 percent), and the increasing sophistication of cyberthreats (45 percent). The top security initiatives for chief information security officers (CISOs) in 2016 were training and awareness (39 percent), monitoring/security operation centers (37 percent), strategy (29 percent), governance (29 percent), operationalizing cybersecurity (29 percent), risk assessments (29 percent), metrics to measure and report effectiveness (29 percent), regulatory and legislative compliance (29 percent), and identity and access management (29 percent). Deloitte also found that the presence of a formalized cybersecurity strategy was correlated with budget increases and securing more cybersecurity staff.

The 2018 Security Scorecard Government Cybersecurity Report graded the security posture of 655 federal, state, and local government organizations and highlighted increasing vulnerabilities to critical infrastructure assets at all levels of government and the related impact on citizen confidence. The report found that government, in comparison with other sectors, has increased its cybersecurity performance, grading higher than health care, manufacturing, and entertainment, ranking 11th out of 18. The top three weaknesses that governments experience are endpoint security, network security, and patching cadence. The government sector's greatest strengths include Domain Name System (DNS) health, social engineering, and application security.

Similarly, Cisco's (2018) Annual Cybersecurity Report, discussing impacts on the government/public sector at large, emphasized the growing threat to public services, utilities, and government operations. Cisco identified three trends that affected the government sector over the previous year: unprecedented levels of malware sophistication, increasing evasion through encryption and weaponizing cloud technologies (e.g., Google and Dropbox), and exploitation of unmonitored and unpatched IoT and cloud devices. It has become clear that all utilities, regardless of size, are high-profile targets. Examples of specific instances of disruption to utilities, payment systems, 911, police, and court systems proliferate in these reports.

In 2014, the Center for Digital Government conducted a survey of IT and security management professionals in local and state government about their ability to achieve effective cybersecurity and how their cybersecurity environments had changed over time. About one-quarter (23 percent) reported that their government's ability to detect and block advanced attacks was average, nearly half (45 percent) said good, while only 10 percent said excellent. Roughly the same proportion reported that malware-related cyberincidents had increased over the past year (40 percent) as reported that the number of incidents remained about the same (36 percent). These governments' most serious concerns centered on email and web-based attacks, especially those targeting PII and other confidential data. This survey also examined the technological tools used by cybersecurity professionals to detect attacks, such as antivirus software (92 percent adoption), web and email gateways (84 percent adoption), and intrusion protection and detection systems (63 percent adoption). The survey also detailed the types of attacks that these governments experienced, such as advanced persistent threats (52 percent), zero-day target attacks (48 percent), bots (43 percent), and worms (30 percent).

The Ponemon Institute examined cybersecurity issues among local and state governments and the federal government and, among other things, found that breaches occur in these governments systems "about every two to three months" (2015, 3). This report also found that among state and local governments, the two top challenges to achieving high levels of cybersecurity were a lack of skilled personnel (62 percent) and insufficient budgetary resources (51 percent). The two top security threats that these governments reported were failure to patch known vulnerabilities (43 percent) and negligent insiders (40 percent).

Respondents to all of the Deloitte/NASCIO surveys reported that the lack of adequate funding constituted a significant barrier to

cybersecurity and that the level of cybersecurity funding lagged substantially behind that of the private sector. Since 2010, a lack of funding has remained the number-one barrier to cybersecurity reported in these surveys. A lack of adequately trained staff was consistently among the top three barriers reported in these surveys (59 percent in 2014, 46 percent in 2012). The 2016 report attributed this to the states' salary rates and pay grades (96 percent), a lack of qualified candidates as a result of demand from federal agencies and private sector (59 percent), and cybersecurity staff leaving for the private sector (47 percent).

The importance of creating and maintaining a culture of cybersecurity within organizations, which today is widely accepted in the cybersecurity field, began entering the literature around 2010 (e.g., Deloitte/NASCIO; IBM Center for the Business of Government). The argument is that although support from top executives may be critical to achieving high levels of cybersecurity, that alone is not sufficient. Cybersecurity must be a priority from the top of the organization (e.g., board members and executives in private sector organizations and elected officials and top managers in governmental organizations) to the bottom, including employees at all levels. As one local government cybersecurity practitioner told us in an earlier research project, "Our biggest struggle now is... the human being, our weakest link" (Norris et al. 2018).

Although the literature on local government cybersecurity is quite limited and nearly all of it is descriptive, it is clear from this literature that local governments are experiencing high levels of cyberattack and that attacks are often successful.[3] Moreover, both this study and the Caruson, MacManus, and McPhee (2012b) study found that sizeable fractions of local government officials are unaware of the attacks against and breaches of their systems. Other findings from this literature include the need for greater levels of funding for cybersecurity, for more trained cybersecurity personnel, for more and better cybersecurity policies, for better cybersecurity awareness in local governments, and for a culture of cybersecurity.

Research Method and Data

To produce the data for this study, we partnered with the International City/County Management Association (ICMA) to conduct a nationwide survey of local government cybersecurity. The ICMA is the premier membership organization of local government professionals in the United States, and it is widely recognized for its research on many aspects of local governance, including IT. The ICMA also has a survey capability that is unsurpassed in reaching local governments in America.

In cooperation with ICMA staff, we drafted the survey instrument based on the limited available literature on local government cybersecurity, on previous research on this subject (e.g., Caruson, MacManus, and McPhee 2012b; Norris et al. 2018), and on the professional literature discussed in the literature review. We then submitted the draft instrument for review and comment to a volunteer advisory group that we had created to assist with this project. The group consisted of IT directors, chief technology officers, and CISOs (or equivalent officials) in 10 cities and counties in our home state (Maryland), as well as the chief information officer (CIO) and CISO of our university. After receiving comments and suggestions from these advisers, we revised the instrument. The ICMA then pre-tested the instrument, and we made appropriate adjustments to it. The process that we used to develop the instrument creates face validity for the instrument, and we are confident that, on the whole, the questions in it produce reliable data.

The instrument examined a wide range of local government cybersecurity issues. For the purposes of this article, we focus on issues related to cyberattacks.

In the summer of 2016, the ICMA mailed the survey to all municipal governments with populations of 25,000 and greater and to all county governments of the same size (a total of 3,423 local governments). The ICMA also provided an online option for completing the survey to all local government respondents. Just over one-third (37.2 percent) of respondents returned paper surveys, while nearly two-thirds (62.8 percent) completed the online version. The ICMA sent three mailings of the survey (one initial and two reminders) and two email reminders. Additionally, in the late fall and early winter of 2016, research assistants at our university made personal telephone calls to all of the local governments with populations of 250,000 and greater that had not responded.

This produced a final response rate of 11.9 percent ($n = 406$ local governments). This may seem a rather low response rate compared with previous surveys of IT at the local government level (e.g., Norris and Reddick 2013; Reddick and Norris 2013). We discovered two potential reasons for this response rate. The first is that there has been a substantial decline in response rates to surveys in recent years (e.g., Anseel et al. 2010), a decline that the ICMA has also experienced (Evelina Moulder, personal message from the ICMA survey manager, 2013). A second reason we learned from the phone calls that our research assistants made: a number of IT and cybersecurity officials said that they would not respond because their responses might reveal sensitive information about their government's cybersecurity problems and practices, something that they would not do.[4]

We can have some degree of satisfaction that a response of 406 among a random sample of 3,400 local governments would have produced a margin of error of 5 percent at a confidence level of 95 percent. Clearly, however, ours was not a random sample but rather a population survey. As a result, we must otherwise be able to make the case that our results should be taken seriously. Here, we ask readers to consider two factors. First, as seen in table 1, the survey results are reasonably representative of the overall population of the local governments that we surveyed. While larger local governments are proportionately overrepresented, smaller local governments are numerically overrepresented. This is not surprising, because it reflects the relative distribution of local governments in the United States. There is also some regional variation, with local governments in the Northeast and North-Central regions being underrepresented and those in the South and West being overrepresented. This is also not surprising, and it is probably because the occurrence of the council-manager form of government is greater in the latter two regions and, as the table shows, council-manager governments are overrepresented.

Second, we can be confident of these survey results because the great majority of respondents (83.4 percent) are experienced local government IT and cybersecurity professionals, mostly IT

Table 1 Local Government Demographics

	Number Surveyed	Number Responding	Response Rate (%)
Total	3,423	406	11.9
Population size			
500,000+	140	31	22.1
250,000–499,999	168	26	15.5
100,000–249,999	532	63	11.8
50,000–99,999	939	107	11.4
25,000–49,999	1,644	179	10.9
Geographic division			
Northeast	574	42	7.3
North-Central	1,048	120	11.5
South	1,148	139	12.1
West	653	105	16.1
City/county			
Municipalities	1,893	262	13.8
Counties	1,530	144	9.4
Form of government 1			
Elected (mayor-council, county commission, county council-elected executive)	1,541	117	7.6
Appointed (city council-manager, county administrator/manager)	1,588	276	17.4
Form of government 2			
Mayor-council	570	46	8.1
County commission	685	33	4.8
County council-elected executive	286	38	13.3
City council-manager	1,035	204	19.7
County administrator/manager	553	72	13.0

Table 2 Respondent Profession and Experience

Profession	N	%
IT Professionals	262	89.4
Other Government	28	9.6
Other	3	1.0
Total	293	100.0
IT Experience		
0–5 Years	23	23.2
6–10 Years	30	30.3
11–19 Years	30	30.3
20 + Years	16	16.2
Total	99	100.0

directors, CIOs, and CISOs (table 2). Thus, the men and women who responded to this survey are knowledgeable, expert local government practitioners who "know their stuff."

We have structured the remainder of this article as follows. First, we discuss the descriptive statistics around attacks and attackers against local government information assets, then local government cybersecurity preparedness, and, last, barriers to achieving high levels of cybersecurity in them.

After the descriptive statistics, we examine cross-tabulations and correlation coefficients for local government characteristics and cybersecurity outcomes to learn whether patterns revealed in previous research on IT and government and e-government appear in the data from this survey (e.g., Norris 1984, 2010; Norris and Campillo 2002; Norris and Kraemer 1996; Norris and Moon 2005; Norris and Reddick 2013; Reddick and Norris 2013). Specifically, are such local government characteristics (independent variables) as population (large versus medium and small), type of government (municipal versus county), form of government (professional administrator versus elected executive), geographic region (South and West versus Northeast and Midwest), median household income (high versus modest and low), education (percentage of college graduates), and percentage white population (versus nonwhite) systematically related to cybersecurity outcomes (dependent variables)? To give an example, we hypothesize that local governments with these characteristics are significantly less likely than their counterparts to *not know* whether they have been attacked or breached.

Next, we discuss conclusions from the data and provide recommendations to local governments for improving their levels of cybersecurity. Lastly, we provide suggestions to scholars for future research into local government cybersecurity.

Findings

We began this study by examining the exposure of American local governments to cyberattack. We wanted to ensure that all respondents would have a common understanding of three important terms used in the survey: attack, incident, and breach. Consequently, we provided definitions of those terms in the questionnaire. We defined an *attack* as any attempt by any party to gain unauthorized access to any component of a local government's IT system for the purpose of causing mischief or doing harm. We employed Verizon's (2015) definitions of incident and breach. According to Verizon, an *incident* is "any event that compromises the confidentiality, integrity or availability of an information asset," and a *breach* is "an incident that result[s] in confirmed disclosure (not just exposure) to an unauthorized party."

Attacks, Incidents, and Breaches

With these definitions in mind, we asked whether local governments cataloged or counted attacks, incidents, and breaches. Fewer than half of respondents (46.5 percent) said that they cataloged or counted attacks, 58.3 percent said that they cataloged or counted incidents, and 60.1 percent did so for breaches (table 3). In terms of the method of cataloging or counting, only 33.1 percent of local governments employed a formal system, while 41.3 percent used an informal system, and 38.2 percent used no system at all (table 4).

Next, we asked about the frequency of attacks, incidents, and breaches (table 5). Attacks occurred the most frequently: hourly or more, 27.7 percent; at least daily, 19.4 percent; less than daily, 23.8 percent. However, nearly 3 in 10 respondents (29.1 percent) said that they *did not know* how frequently their system was attacked. In other research, we found that local governments are under constant or near-constant attack (Norris et al. 2018). So, we strongly suspect that the 23.8 percent who responded that attacks occurred less than daily were not well informed of the frequency of attacks against their systems.

Incidents occurred less frequently than attacks: hourly or more, 4.8 percent; at least daily, 7.7 percent, less than daily, 53.1 percent. And breaches occurred less frequently than incidents: hourly or more, 4.3 percent; at least daily, 3.4 percent; less than daily, 29.9 percent. Just over one-third (34.4 percent) *did not know* how frequently incidents occurred, and nearly two-thirds (62.4 percent) *did not know* how often their systems were breached.

These data, especially the "did not know" responses, strongly suggest that local governments are not practicing cybersecurity well.

Table 3 Does Your Local Government Catalog and Count Attacks, Incidents, and Breaches?

	Yes		No		
	N	%	*N*	%	Total
Attacks	173	46.5	199	53.5	372
Incidents	217	58.3	155	41.7	372
Breaches	221	60.1	147	40.0	368

Table 4 Does Your Local Government Employ a Formal or Informal Method of Cybersecurity Management?

	N	%
Formal	80	33.1
Informal	161	66.9
Total	241	100.0

Table 5 How Frequently Is Your Local Government's Information System Subject to Attacks, Incidents, and Breaches? (percent)

	Attacks	Incidents	Breaches
Hourly or more	27.7	4.8	4.3
At least once a day	19.4	7.7	3.4
Less than daily	23.8	53.1	29.9
Do not know	29.1	34.4	62.4
Total	100.0	100.0	100.0

Table 6 In the Past 12 Months, Has Your Local Government's Information System Experienced More, Less, or About the Same Number of Attacks, Incidents, and Breaches?

	Attacks		Incidents		Breaches	
	N	%	*N*	%	*N*	%
Fewer	27	7.4	47	13.1	47	13.1
Same	125	34.4	149	41.4	164	45.8
More	118	32.5	65	18.1	20	5.6
Do not know	93	25.6	99	27.5	127	35.5
Total	363	100.0	360	100.0	358	100.0

Table 7 Is Your Local Government Able to Determine the Types. of Attackers That Attack Your System?

	N	%
Yes, can determine	151	41.6
No, cannot	212	58.4
Total	363	100.0

Table 8 Types of Attackers

	Yes		No		Total	
	N	%	N	%	N	%
External Actors - Organizations	76	71.0	31	29.0	107	100.0
External Actors - Individuals	65	60.7	42	39.3	107	100.0
State Actors	31	29.0	76	71.0	107	100.0
Malicious Insiders	14	13.0	94	87.0	108	100.0

The data also suggest that although we provided a definition of the term *breach,* some respondents apparently did not understand what constituted a breach, because nearly 8 percent said that their government was breached at least daily.

We then asked whether the frequency of attacks, incidents, and breaches had changed over the 12 months prior to the survey (table 6). Pluralities reported that attacks (34.4 percent), incidents (41.4 percent), and breaches (45.8 percent) remained about the same, while much smaller fractions said they had experienced fewer attacks (7.4 percent), incidents (13.1 percent), and breaches (13.1 percent). Almost a third of governments (32.5 percent) said that attacks had increased; fewer than one in five (18.1 percent) said that incidents had increased; and very few (5.6 percent) said that breaches had increased. Again, however, the number of local governments that *did not know* was not trivial: 25.6 percent for attacks, 27.5 percent for incidents, and 35.5 percent for breaches.

Table 9 Purpose of Attacks

	Yes		No		Total	
	N	%	N	%	N	%
Ransom	60	59.4	41	40.6	101	100.0
Mischief	38	37.6	63	62.4	101	100.0
PII	28	27.7	73	72.3	101	100.0
Hacktivism	26	25.7	75	74.3	101	100.0
Theft of Money	21	20.8	80	79.2	101	100.0
Employee Records	15	14.9	86	85.1	101	100.0
Confidential Records	14	13.9	87	86.1	101	100.0
Customer/ Citizen Records	12	11.9	89	88.1	101	100.0
Espionage	5	5.0	96	95.0	101	100.0
Revenge	2	2.0	99	98.0	101	100.0
Terror	2	2.0	99	98.0	101	100.0

Next, we asked respondents if they could determine the types of attackers against their systems over the 12 months prior to the survey and the attackers' motives. A clear majority (58.4 percent) said that they *could not determine* the types of attackers against their systems (Table 7). Of those who were able to determine the types of attackers, 71.0 percent said attackers included external actors-organizations, 60.7 percent said they included external actors-individuals, 29.0 percent said state actors and 13.0 percent said malicious insiders (Table 8). When asked if they knew or could estimate the purposes of the attacks (Table 9), the top responses were: ransom – 59.4 percent; mischief – 37.6 percent; sensitive information – 27.7 percent; hacktivism – 25.7 percent; and theft of money – 20.8 percent. These findings are consistent with a report by PNC released in 2018 (Kozlik 2018). These findings are consistent with a report by PNC released in 2018 (Kozlik 2018).

Preparedness

We also wanted to know how prepared these governments felt they were to detect, prevent, and recover from several potential events that could adversely affect their systems, including the following: detect attacks, detect incidents, prevent breaches, recover from breaches, detect exfiltration, prevent exfiltration, recover from exfiltration, and recover from ransomware (table 10). Only minorities of local governments reported having a very good or excellent ability to do so, ranging from 48.3 percent with a very good or excellent ability to recover from ransomware attacks to 20.5 percent with a similar ability to detect exfiltration. The remainder reported a very good or excellent ability as follows: detect attacks, 41.9 percent; detect incidents, 38.2 percent; prevent breaches, 36.3 percent; recover from breaches, 36.8 percent; prevent exfiltration, 25.0 percent; and recover from exfiltration, 27.8 percent. Consistent with findings thus far in this article, once again we found that local governments were not practicing high levels of cybersecurity.

Next, we inquired about the level of confidence that these governments had in their ability to prevent all breaches (table 11). About one-third of respondents reported being not at all or only slightly confident (30.3 percent), 31.2 percent reported being

Table 10 Preparedness of Local Governments

	Detect Attacks		Detect Incidents		Prevent Breaches		Recover from Breaches	
	N	%	*N*	%	*N*	%	*N*	%
Poor/fair	97	28.0	98	28.3	98	28.5	90	26.5
Good	88	25.4	98	28.3	103	29.9	79	23.2
Very good/ excellent	145	41.9	132	38.2	125	36.3	125	36.8
Do not know	16	4.6	18	5.2	18	5.2	46	13.5
Total	346	100.0	346	100.0	344	100.0	340	100.0
	Detect Exfiltration		Prevent Exfiltration		Recover from Exfiltration		Recover from Ransomware	
	N	%	*N*	%	*N*	%	*N*	%
Poor/fair	168	49.3	146	42.9	107	31.7	64	18.7
Good	54	15.8	64	18.8	68	20.1	77	22.5
Very good/ excellent	70	20.5	85	25.0	94	27.8	165	48.3
Do not know	49	14.4	45	13.2	69	20.4	36	10.5
Total	341	100.0	340	100.0	338	100.0	342	100.0

Table 11 Confidence in Your Local Government's Ability to Prevent All Breaches

	N	%
Not at all/slightly confident	100	30.3
Somewhat confident	103	31.2
Confident/highly confident	115	34.9
Do not know	12	3.6
Total	330	100.0

somewhat confident, and 34.9 percent were confident or highly confident of being able to prevent all breaches. Viewed differently, nearly two-thirds (61.5 percent) of respondents were less than confident in the ability of their local government to prevent all breaches. This finding will doubtless come as no surprise because, as cybersecurity professionals know, it is not a matter of whether but when an organization will be breached (see Ponemon Institute 2015).

Barriers to Cybersecurity

Clearly, a number of factors may contribute to American local governments' failure to practice higher levels of cybersecurity. With this in mind, we developed a number of questions about barriers to the effective practice of cybersecurity and included them in the survey. We based these questions largely on the types of barriers that prior literature on IT and government and e-government has identified. The five most important barriers reported were: (1) the inability to pay competitive salaries to cybersecurity employees (58.6 percent); (2) an insufficient number of cybersecurity staff (53.1 percent); (3) a lack of funds (52.8 percent); (4) a lack of adequately trained personnel (46.9 percent); and (5) a lack of end-user accountability (37.6 percent). All other potential barriers were selected by fewer than one-third of respondents.

In one way or another, four of the top five barriers involved inadequate funding (table 12). If local governments cannot pay competitive salaries, it is because of their financial limitations (i.e., lack of funds). If local governments lack sufficient numbers of cybersecurity staff, this is also due to financial limitations. This said, it is also true that local governments find it difficult to compete for IT and cybersecurity personnel because private sector salaries are typically much higher than the public sector is able to pay. Lastly, a lack of adequately trained personnel is also related to funding because training is not free. Indeed, training is often cut when local governments face budgetary difficulties, such as those experienced during the Great Recession.

These findings are consistent with several years of research on IT and government and e-government (e.g., Holden, Norris, and Fletcher 2002; Norris and Kraemer 1996; Norris and Reddick 2013) as well as with evidence produced by our literature review (Caruson, MacManus, and McPhee 2012b; Deloitte and NASCIO 2010, 2012, 2014, 2016; Ponemon Institute 2015).

Cross-tabulations

Earlier in the article, we hypothesized that data from the survey would show that several local government characteristics are systematically associated with cybersecurity outcomes. We ran the cross-tabulations using those characteristics (independent variables) against 68 cybersecurity outcomes (dependent variables), for a total of 476 individual cross-tabulations. Only 56 of the 476 cross-tabulations (11.8 percent) produced results that were significant at the $p \leq .05$ level. The directions of these few relationships were not fully consistent with the expected pattern, and the strength of the relationships, as measured by the Cramer's V statistic, were generally weak, ranging from 0.10 to 0.40, with all but five falling between 0.11 and 0.21.[5] Clearly, associations observed in prior research on IT in government and e-government were not found here. Nevertheless, future research should continue to test for such associations in order to identify factors that will help us better understand local government cybersecurity practice.

Conclusions and Recommendations

Evidence from the first nationwide survey of local government cybersecurity in the United States shows that these governments are under frequent, if not constant, attack and that, on average, local governments practice cybersecurity poorly. This is almost certainly a function of the several barriers to cybersecurity found in the survey, among which a lack of funding was the most serious.[6] Indeed, when asked about the top three things needed to ensure the highest level of cybersecurity, survey respondents first named greater funding, followed by better cybersecurity policies and greater cybersecurity awareness among local government employees (table 13).

What else might American local governments consider doing to improve their practice of cybersecurity? We offer four broad recommendations: (1) create and maintain a culture of cybersecurity, (2) address barriers to cybersecurity, (3) follow best cybersecurity practices, and (4) eliminate the "do not knows." The concept of a culture of cybersecurity began to gain traction among practitioners only a few years ago (e.g., Deloitte and NASCIO 2010). Among other things, a culture of cybersecurity means that elected officials and top managers fully embrace and support cybersecurity and play important roles in it, including, but not limited to, practicing it appropriately, insisting that others in government do so as well, and holding all accountable when they do not.

Second, within their fiscal and administrative limits, local governments must address known barriers to cybersecurity, such as those identified in in this article. We note that although a lack

Table 12 Barriers to Achieving Highest Possible Level of Cybersecurity

	Not/Small Barrier		Modest Barrier		Somewhat/ Severe Barrier		Don't Know		Total	
	N	%	*N*	%	*N*	%	*N*	%	*N*	%
Inability to pay competitive salaries	67	19.8	42	12.4	198	58.6	31	9.2	338	100.0
Insufficient number of staff	68	20.2	71	21.1	179	53.1	19	5.6	337	100.0
Lack of funds	57	16.6	95	27.7	181	52.8	10	2.9	343	100.0
Lack of adequately trained personnel	86	25.5	76	22.6	158	46.9	17	5.0	337	100.0
Lack of end user accountability	121	35.8	78	23.1	127	37.6	12	3.6	338	100.0
Lack of trained personnel to hire	120	35.3	73	21.5	108	31.8	39	11.5	340	100.0
Lack of adequate cybersecurity awareness	118	35.1	104	31.0	104	31.0	10	3.0	336	100.0
No end user training at all	172	51.3	64	19.1	86	25.7	13	3.9	335	100.0
Some, but insufficient end user training	158	48.2	88	26.8	65	19.8	17	5.0	328	100.0
Federated nature of local government	183	55.8	41	12.5	58	17.7	46	14.0	328	100.0
Too many IT networks/systems	222	66.1	43	12.8	55	16.4	16	4.8	336	100.0
Lack of support from department managers	209	61.5	70	20.6	47	13.8	14	4.1	340	100.0

Table 13 Top Three Things Needed to Ensure Highest Level of Cybersecurity

	1		2		3		Total	
	N	%	*N*	%	*N*	%	*N*	%
Greater funding for cybersecurity	76	54.7	37	26.6	26	18.7	139	100.0
Better cybersecurity policies	46	38.3	36	30.0	38	31.7	120	100.0
Greater cybersecurity awareness among local government employees	42	35.3	29	24.4	48	40.3	119	100.0
More end user training	22	25.3	32	36.8	33	37.9	87	100.0
More cybersecurity personnel	26	30.2	37	43.0	23	26.7	86	100.0
Improved cybersecurity hardware	35	42.2	26	31.3	22	26.5	83	100.0
More training for cybersecurity personnel	21	28.8	24	32.9	28	38.4	73	100.0
The ability to pay competitive salaries for cybersecurity personnel	15	23.1	30	46.2	20	30.8	65	100.0
More end user accountability	13	20.0	18	27.7	34	52.3	65	100.0
Better enforcement of existing cybersecurity policies	11	20.4	26	48.1	17	31.5	54	100.0
Greater support from top elected officials	9	29.0	9	29.0	13	41.9	31	100.0
Greater support from department managers	5	16.7	13	43.3	12	40.0	30	100.0
Greater support from top appointed officials	7	35.0	3	15.0	10	50.0	20	100.0
Consolidation of numerous IT networks/systems	3	23.1	3	23.1	7	53.8	13	100.0

of funding ranked at the top of the barriers reported in this survey, local governments can take action in a number of areas in which cost is not so great a factor, such as adopting and implementing cybersecurity policies and end user training.

Third, local governments should be aware of and follow the latest cybersecurity best practices, such as those published by relevant federal government agencies. These currently include the 2014 and 2018 National Institute of Standards and Technology cybersecurity frameworks (NIST 2014, 2018a, 2018b) and the U.S. Department of Homeland Security Cyber Security Division's cybersecurity strategy documents (DHS 2018a, 2018b).

Fourth, local governments must take action to reduce, if not eliminate, the "do not knows" found in this study. No top local government official, elected or appointed, and certainly no IT or cybersecurity official should ever have to answer "I do not know" to questions about the cybersecurity of their organization. Knowing the security status of their information system is fundamentally important to a local government's ability to address vulnerabilities and improve cybersecurity outcomes.

Lastly, we address the gap in the scholarly literature on local government cybersecurity that our literature review clearly identified. While our article is a step toward reducing this gap, much more needs to be done. As indicated earlier, our survey produced a baseline of data about local government cybersecurity. It should be followed up with additional surveys at, say, five-year intervals.[7] Among other things, these surveys should seek to validate the findings reported herein, extend and expand on them, document changes in local government cybersecurity problems and practices over time, and, importantly, test causal relationships between a variety of independent and dependent variables that can help us better understand cybersecurity practices and outcomes at the grass roots.

Finally, scholars should begin to use or develop a theory or theories that help explain cybersecurity at the grass roots, especially why one set of governments might appear to have better cybersecurity outcomes than another. We would suggest beginning with the theory of incrementalism because it has been applied successfully to understand the adoption, use, and impacts of both IT and e-government among local governments (e.g., Coursey and Norris 2008; Norris 2010; Norris and Kraemer 1996; Norris and Moon 2005; Norris and Reddick 2013). These are only a few of the many opportunities for local government cybersecurity research that can and should be undertaken and that can produce findings of value to both scholars and practitioners.

Acknowledgments

The authors wish to acknowledge funding for our local government cybersecurity survey from the offices of the Dean of the College of Arts, Humanities and Social Sciences and the Vice President for Research at the University of Maryland, Baltimore County (UMBC).

Notes

1. Caruson, MacManus, and McPhee (2012b) report the results of a survey of the technical and managerial cybersecurity environment of a subset of American local governments (Florida counties). The remaining three articles address issues of transparency and privacy (Caruson, MacManus, and McPhee 2012a), specific state government websites (Zhao and Zhao 2010), and electronic monitoring of local government employees (Fusi and Feeney 2017).

2. While we found reports on various other aspects of cybersecurity, none was directly applicable to our research because of differences in scope, such as state and federal website privacy and security policies (West 2008), state e-government strategies (Seifert and McLoughlin 2007), and the roles of multistate and federal organizations in connecting federal and state homeland security operations in the area of cybersecurity (Democratic Staff of the Committee on Homeland Security 2006).
3. We agree with one of the anonymous reviewers who pointed out that although various sources report "high levels of attack," these reports "do not directly show that a majority" of attacks are successful. Thus, the frequency of success of attacks is "indeterminate." Certainly nothing like a majority or even a strong plurality of attacks succeed. Yet attacks continue relentlessly.
4. Here, we are grateful for (and agree with) a comment by one of the anonymous reviewers of this paper who observed that IT and CS practitioners are widely known in the profession for their unwillingness to respond to questions about the state of cybersecurity in their organizations.
5. The Cramer's V statistic ranges from 0.00 to 1.00. The closer to 1.00, the stronger the relationship is: 0.1 to 0.30 describes a weak relationship; 0.30 and 0.50, a moderate one; and above 0.50, a strong one (Chapman 1981; Cohen 1988; Elifson, Punyon, and Haber 1990; Murphy and Myors 1998).
6. This finding should not be surprising, as even the federal government, which is arguably larger and has greater funding and more cybersecurity staff, is not able to provide adequate levels of cybersecurity (Hawkins 2018).
7. It is certainly our intent to do so in 2021.

References

Anseel, Frederik, Filip Lievens, Eveline Schollaert, and Beata Choragwicka. 2010. Response Rates in Organizational Sciences, 1995–2008: A Meta-analytic Review and Guidelines for Survey Researchers. *Journal of Business Psychology* 25(3): 335–49.

Antonakakis, Manos, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, et al. 2017. Understanding the Mirai Botnet. Paper presented at the 26th USENIX Security Symposium, Vancouver, Canada, August 16–18. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf [accessed January 21, 2019].

Caruson, Kiki, Susan A. MacManus, and Brian D. McPhee. 2012a. Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights. *Journal of Urban Affairs* 35(4): 451–70.

———. 2012b. Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. *Journal of Homeland Security and Emergency Management* 9(2). https://doi.org/10.1515/jhsem-2012-0003.

Center for Digital Government. 2014. Advanced Cyber Threats in State and Local Government. https://www.nascio.org/events/sponsors/vrc/Advanced%20Cyber%20Threats%20in%20State%20and%20%20Local%20Government.pdf [accessed January 21, 2019].

Chapman, Dean J. 1981. *Basic Statistics for Social Research*. 2nd ed. New York: Macmillan.

Cisco. 2018. Annual Cybersecurity Report Impacts on Government. https://cisco.com/c/en/us/products/security/security-reports.html?CCID=cc000153 [accessed January 21, 2019].

Cohen, Jacob. 1988. *Statistical Power and Analysis for the Behavioral Sciences*. 2nd ed. Hillsdale, NJ: Lawrence Erlbaum.

Coursey, David, and Donald F. Norris. 2008. Models of E-government: Are They Correct? An Empirical Assessment. *Public Administration Review* 68(3): 523–36.

Deloitte and National Association of State Chief Information Officers (NASCIO). 2010. State Governments at Risk: A Call to Secure Citizen Data and Inspire Public Trust. https://www.nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy2010.PDF [accessed January 21, 2019].

———. 2012. 2012 Deloitte-NASCIO Cybersecurity Study—State Governments at Risk: A Call for Collaboration and Compliance. https://www.nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy2012.pdf [accessed January 21, 2019].

———. 2014. 2014 Deloitte-NASCIO Cybersecurity Study—State Governments at Risk: Time to Move Forward. https://www.nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf [accessed January 21, 2019].

———. 2016. 2016 Deloitte-NASCIO Cybersecurity Study—State Governments at Risk: Turning Strategy and Awareness into Progress. https://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf [accessed January 21, 2019].

Democratic Staff of the Committee on Homeland Security. 2006. The State of Homeland Security: An Annual Report Card on the Department of Homeland Security. https://www.hsdl.org/?view&did=460840 [accessed January 21, 2019].

Dixon, Chris. 2014. Deltek: State, Local Government IT Spending Increase Is an Opportunity for Contractors. *Washington Post,* August 24. https://www.washingtonpost.com/business/capitalbusiness/deltek-state-local-government-it-spending-increase-is-an-opportunity-for-contractors/2014/08/22/4f6f0834–288d-11e4–8593-da634b334390_story.html [accessed January 21, 2019].

Elifson, Kirk W., Richard P. Punyon, and Audrey Haber. 1990. *Fundamentals of Social Statistics*. New York: McGraw-Hill.

Fusi, Frederica, and Mary K. Feeney. 2017. Electronic Monitoring in Public Organizations: Evidence from U.S. Local Governments. *Public Management Review* 20(10): 1465–89.

Goodyear, Marilu, Shannon Portillo, Holly T. Goerdel, and Linda Williams. 2010. *Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers*. Washington, DC: IBM Center for the Business of Government. http://www.businessofgovernment.org/sites/default/files/CybersecurityManagement_0.pdf [accessed January 21, 2019].

Hawkins, Derek. 2018. The Cybersecurity 202: White House Cybersecurity Report Shows Federal Agencies Still Struggling to Get Secure. *Washington Post,* May 30. https://washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/30/the-cybersecurity-202-white-house-cybersecurity-report-shows-federal-agencies-still-struggling-to-get-secure/5b0d79c81b326b492dd07ed3 [accessed January 21, 2019].

Holden, Stephen H., Donald F. Norris, and Patricia D. Fletcher. 2003. Electronic Government at the Local Level: Progress to Date and Future Issues. *Public Productivity & Management Review* 26(3): 1–20.

Juniper Research. 2015. Cybercrime Will Cost Businesses over $2 Trillion by 2019. News release, May 12. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion [accessed January 21, 2019].

Kozlik, Tom. 2018. Cyberattacks: A Real Threat to State and Local Governments, Infrastructure. Municipal Commentary, PNC Financial Services Group, April 23. https://www.pnc.com/content/dam/pnc-com/pdf/corporateandinstitutional/MunicipalBond/Cyberattacks-a-real-threat.pdf [accessed January 21, 2019].

Murphy, Kevin R., and Brett Myors. 1998. *Statistical Power Analysis: A Simple and General Model for Traditional and Modern Hypothesis Tests*. Mahwah, NJ: Lawrence Erlbaum.

National Institute of Standards and Technology (NIST). 2014. NIST Roadmap for Improving Critical Infrastructure Cybersecurity. February 12. https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf [accessed January 21, 2019].

———. 2018a. Cybersecurity Framework State, Local, Tribal and Territorial Perspectives. https://www.nist.gov/cyberframework/perspectives/state-local-tribal-and-territorial-perspectives [accessed January 21, 2019].

———. 2018b. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. April 16. https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final [accessed January 21, 2019].

NCTA—The Internet and Television Association. 2018. Wi-Fi: How Broadband Households Experience the Internet. April 6. https://www.ncta.com/whats-new/wi-fi-how-broadband-households-experience-the-internet [accessed January 21, 2019].

Norris, Donald F. 1984. Small Local Governments and Information Technology: Uses and Users. *Public Administration Review* 44(1): 70–78.

Norris, Donald F. 2010. E-government 2020: Plus ça change, plus c'est la meme chose. Special issue, *Public Administration Review* 70: S180–81.

Norris, Donald F., and Diana Campillo. 2002. Factors Affecting the Adoption of Leading Edge Information Technology by Local Governments. Working paper, Maryland Institute for Policy Analysis and Research, University of Maryland, Baltimore County.

Norris, Donald F., and Kenneth L. Kraemer. 1996. Mainframe and PC Computing in American Cities: Myths and Realities. *Public Administration Review* 56(6): 568–76.

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). https://doi.org/10.1515/jhsem-2017-0048.

Norris, Donald F., and M. Jae Moon. 2005. Advancing E-government at the Grass Roots: Tortoise or Hare? *Public Administration Review* 65(1): 64–75.

Norris, Donald F., and Christopher G. Reddick. 2013. Local E-government in the United States: Transformation or Incremental Change? *Public Administration Review* 73(1): 165–75.

Ponemon Institute. 2015. State of Cybersecurity in Local State & Federal Government. https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6–2563enw.pdf [accessed January 21, 2019].

Reddick, Christopher G., and Donald F. Norris. 2013. E-participation in Local Governments: An Examination of Political-Managerial Support and Impacts. *Transforming Government: People, Process and Policy* 7(4): 453–76.

Security Scorecard. 2018. 2018 Government Cybersecurity Report. https://explore.securityscorecard.com/rs/797-BFK-857/images/2018%20Government%20Cybersecurity%20Report.pdf [accessed January 21, 2019].

Seifert, Jeffery W., and Glenn J. McLoughlin. 2007. *State E-Government Strategies: Identifying Best Practices and Applications*. Washington, DC: Congressional Research Service. https://www.hsdl.org/?abstract&did=479121 [accessed January 21, 2019].

U.S. Census Bureau. 2012. 2012 Census of Governments. https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk [accessed January 21, 2019].

U.S. Department of Homeland Security (DHS). 2018a. Cybersecurity Resources. Accessed July 19, 2018. https://www.dhs.gov/topic/cybersecurity [accessed January 21, 2019]. (This resource is continuously updated by the Department of Homeland Security.)

U.S. Department of Homeland Security (DHS). 2018b. U.S. Department of Homeland Security Cybersecurity Strategy. May 15. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf [accessed January 21, 2019].

Verizon. 2015. 2015 Data Breach Investigations Report. http://www.verizon.com/about/news/2015-data-breach-report-info [accessed January 21, 2019].

West, Darrell M. 2008. State and Federal Electronic Government in the United States, 2008. Brookings Institution, August 26. https://www.brookings.edu/research/state-and-federal-electronic-government-in-the-united-states-2008/ [accessed January 21, 2019].

Zhao, Jenson J., and Sherry Y. Zhao. 2010. Opportunities and Threats: A Security Assessment of State E-government Websites. *Government Information Quarterly* 27(1): 49–56.