Cybersecurity Challenges to American Local Governments

Donald F. Norris, Laura Mateczun, Anupam Joshi and Timothy Finin
University of Maryland, Baltimore County, Baltimore, Maryland, USA
norris@umbc.edu
lam6@umbc.edu
joshi@umbc.edu
finin@umbc.edu

Abstract: In this paper we examine data from the first ever nationwide survey of cybersecurity among American local governments. We are particularly interested in understanding the threats to local government cybersecurity, their level of preparedness to address the threats, the barriers these governments encounter when deploying cybersecurity, the policies, tools and practices that they employ to improve cybersecurity and, finally, the extent of awareness of and support for high levels of cybersecurity within their organizations. We found that local governments are under fairly constant cyberattack and are periodically breached. They are not especially well prepared to prevent cyberattacks or to recover when breached. The principal barriers to local cybersecurity are financial and organizations. Although a number of polices, tools and practices to improve cybersecurity, few local governments are making wide use of them. Last, local governments suffer from too little awareness of and support for cybersecurity within their organizations.

Keywords: Cybersecurity; cybersecurity barrier; cybersecurity policies, practices and tools; local government cybersecurity; local government cyberattack; local government cyber incident; local government data breach

1. Introduction

In this paper we examine the issue cybersecurity among local governments in the United States. Because these are local governments, they are often colloquially referred to as "grassroots" governments, indicating their closeness to local citizens. Local government cybersecurity is an increasingly important issue for at least the following reasons. First, the U. S. has more than 90,000 units of local government in (Census Bureau, 2012), including 3,031 are county governments and 19,519 are municipal governments. Except for the smallest among them, these governments have information technology (IT) systems that are important, if not in some cases critical, to their daily activities. Second, these governments cumulatively spend billions of dollars each year to operate and support those systems. One source estimated that state and local government spending on information technology is growing at a rate of three percent per year, and that by 2019 it will rise to 70 billion per year, up from at over $60.4 billion per year in 2014 (Dixon, 2014).

Third, American local governments maintain and store considerable amounts of sensitive information, especially personally identifiable information, or PII, that is vulnerable to cyberattack, (e.g., individuals' names, addresses, driver license information, health records, social security numbers, credit card numbers, etc.). As we show below, over the past few years, many local governments have experienced data breaches, exfiltration of PII and even ransom demands made on their information systems and data.

Fourth, the websites of many if not most public, non-profit and private organizations in this country and abroad are under nearly constant cyberattack. According to the Ponemon Institute (2015), in the previous two years, governments in the US experienced "data breaches about every two to three months" (p. 3). Federal agencies experienced breaches about every nine (9) weeks, and state and local agencies experienced breaches about every 12 weeks.

Fifth, cybercrime is very costly to the U. S and world economies. In a report for the Center for Strategic and International Studies (2014), McAfee estimated that in 2013 cybercrime cost the world economy more than $400 billion, and the cost of cybercrime continues to increase. The Ponemon Institute (2015) examined the dollar impact of cybercrime on 252 organizations in seven nations in FY 2015 and found that it cost of $45.74 billion dollars. The U.S. reported the highest cost, $15.42 billion, and Russia the lowest at $2.37 billion.

Finally, as we discuss in the literature review that follows this section, there is an enormous gap in the scholarly literature on the subject of local government cybersecurity. Our in-depth literature review on this subject identified a minimal number of works, only three peer-reviewed articles. This finding is consistent with Perez' (2014) study of Orange County's e-government that similarly described a lack of scholarly work in this

area. Indeed, addressing this gap in the literature has been a major reason that we conducted the research that we report here.

For these and perhaps other reasons, it is important to understand the cybersecurity problems that local governments face and the actions they take to mitigate it. Such understanding twill allow scholars and practitioners develop recommendations for improved local government cybersecurity.

2. Literature Review

In preparing for this survey, we conducted an extensive literature review searching for books, peer-reviewed articles, reports and the like that address local government cybersecurity. We were particularly interested in works on this subject from the social science and computer science disciplines. With this focus, the literature review yielded only three peer-reviewed articles from social sciences and none from computer sciences (Caruson, et al., 2012a; Caruson, et al., 2012b; Zhao & Zhao, 2010), one government report (Malashenko, et al., 2012), and six publicly available reports by private information technology and cybersecurity firms, professional organizations and independent institutes (Ponemon Institute, 2015; Deloitte and NASCIO, 2016; Center for Digital Government, 2014; Deloitte and NASCIO, 2014; Deloitte and NASCIO, 2012; IBM Center for The Business of Government, 2010) that are explicitly concerned with cyber threats and cybersecurity at the state and local government level in the United States.

Although we found three scholarly works on cybersecurity and local government in the literature, only one is directly relevant to this paper (Caruson, et al., 2012a) and is based on a survey with a response rate of 24 percent of county government officials in a Florida. Among the principal findings of that survey, less than a quarter (24 percent) of respondents acknowledged that their governments had experienced a cyberattack in the previous year. Fewer than half of officials (48 percent) reported that their governments 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 lack of funding. Insufficient training came in second (43 percent), followed by the need for personnel with more expertise (37 percent). As we show later, with one major exception, these results are mostly consistent with the findings from our research.

The six reports we found provide the most recent, and perhaps most thorough, information regarding what is currently known about local government cybersecurity. Deloitte and NASCIO have been conducting a biennial survey of Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) since 2012 and have tracked the fast growth in importance, responsibility, and now respect of the role of CIOs and CISOs in state and local governments. For example, the 2016 report indicates a rise in executive-branch awareness, as a growing number of CISOs report to their governor monthly (29 percent, from 17 percent in 2014) (Deloitte and NASCIO). This represents a maturation of the role from the need to secure adequate budgets and stakeholder buy-in, reported in 2012, and the increase in authority and reporting relationships in 2014 (Deloitte and NASCIO).

What has persisted over time is the complexity of cyber threats and the need to maintain a sufficient budget to fulfill strategic needs. The report found that the top five functions of the CISO in 2016 were strategy and planning (96 percent), awareness and training (96 percent), audit logs and security event monitoring (90 percent), incident management (90 percent) and vulnerability management (88 percent). The top five barriers in cybersecurity administration were lack of sufficient funding (80 percent), inadequate availability of cybersecurity professionals (51 percent), lack of documented processes (45 percent), increasing sophistication of threats (45 percent) and lack of visibility and influence within the enterprise (33 percent). This survey also found the presence of a formalized cybersecurity strategy to be correlated with budget increases, and obtaining more full time equivalents focused on security.

The 2014 survey of 126 IT and security management professionals in local and state government by the Center for Digital Government found half of respondents reporting their agency's ability to detect and block advanced

attacks as good (45 percent), a quarter or so as average (23 percent), and only 10 percent as excellent. Roughly the same proportion of respondents reported that malware related cyber incidents had increased over the past year (40 percent) as reported that the number of incidents remained about the same (36 percent). The biggest concerns seemed to be email and Web-based attacks, especially those related to gaining access to PII or other confidential data. This survey also examined the technological tools utilized by cybersecurity professionals to detect attacks, such as anti-virus software (92 percent employed), web and e-mail gateways (84 percent), and intrusion protection and detection systems (63 percent), and details the types of attacks experienced, from advanced persistent threats (52 percent) and zero-day target attacks (48 percent) to bots (43 percent) and worms (30 percent).

A report issued by the California Public Utilities Commission represents a sizable segment of cybersecurity literature focusing on smart grids and the utilities industry (Malashenko, et al., 2012). This report examines the role of state regulation to fill gaps remaining from federal compliance-based models. Specifically, the need to determine and implement cybersecurity best practices, policies, and procedures to ensure uniform standards is discussed. Last, the Ponemon Institute (2015) 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 (p. 3)." This report also found that, among state and local governments, the two top challenges to achieving high levels of cybersecurity were 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).

3. Method and Data

To produce the data needed for this study, we contracted with the International City/County Management Association (ICMA) to conduct a survey of local government cybersecurity. ICMA is the premier organization of local government professionals in the U.S. and is widely recognized for its research into many aspects of local governance, including information technology. ICMA also has a survey research capability that is unsurpassed in reaching local governments in America.

In cooperation with staff at the ICMA and also our own advisory group of local government information technology (IT) and cybersecurity professionals, we drafted the survey instrument based on the extant literature and also on our previous research (Norris, et al., 2015). ICMA then pre-tested the instrument and we made adjustments to it accordingly. The instrument examined a wide range of local government cybersecurity e-government issues, many of which we address in this paper.

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 3,423governments). ICMA provided an online option for completing the survey to the 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. ICMA sent three mailings of the survey (one initial and two reminders), and sent two email reminders (one to the chief elected official and one to the chief appointed official of these local governments). In addition, in late fall and early winter 2016, research assistants at our University made personal telephone to all of the local governments that had not responded.

This produced a response rate of 12 percent (411 local governments). This is a much smaller percentage than the ICMA typically receives in other surveys, depending on the subject ranging from 30 percent to over 50 percent. ICMA and the authors (especially based on feedback received from the telephone calls) suspect that the sensitive nature of the subject matter – cybersecurity – kept a sizeable number of local governments from responding. Additionally, ICMA has noticed a decline in responses to its surveys in recent years and attributes this, in part, to the impact of the "Great Recession" on local staff cutbacks. As a result, local governments understandably have fewer resources to devote to completing surveys (Moulder 2011). Last, local governments in the U.S. also suffer from being over-surveyed and are increasingly reluctant to respond to any surveys.

Nevertheless, we can be confident of the reliability and validity of the data for at least two reasons. First, this was a population survey, not a random sample. That is, we sent instruments to all US local governments over

25,000 in size and received responses from 411 of them. If this had been a randomly conducted survey with 411 responses, the results would have a margin of error of +/- 5 percent at a confidence level of 95 percent.

Second, although the responses were not perfectly representative of the overall all local governments of greater than 25,000 in size, they were representative enough for present purposes, and especially because the responding officials were heavily from the information technology and cybersecurity fields. Hence, respondents were mainly practitioner experts in the field of the survey, which lends considerable weight to their responses.

Nevertheless, there were some differences in response rates among groups in the survey. In terms of population size, the largest local governments (those of 500,000 in population and greater) were overrepresented in the sample (22.2 percent responding), while smaller local governments (i.e., with populations from 25,000 to 250,000) were somewhat underrepresented in the sample (between 11 and 12 percent responding). However, because smaller local governments are more numerous than their large counterparts, they represented 86.1 percent of the sample (n = 354) Local governments with populations from 250,000 to 499,999 responded at the rate of 15.5 percent. Comparing form and type of government, municipalities responded at about the average of all respondents while county governments underrepresented. Among municipal governments, mayor-council governments were underrepresented and council manager/ administrator were overrepresented. Among counties, council administrator or manager forms were overrepresented while council-elected executive and county commission governments were underrepresented. Finally, local governments in metropolitan areas were overrepresented while those outside of meter areas were underrepresented.

4. Findings

In the following pages, we provide our analysis of data from the survey. We have organized the results as follows: attacks, incidents and breaches; cyber preparedness; barriers to effective cybersecurity; policies, tools and practices; and awareness of and support for cybersecurity.

Attacks, incidents, and breaches

For the purpose of the survey, we defined attack as*: an attempt by any party to gain unauthorized access to any component of your local government's information technology system for the purpose of causing mischief or doing harm*. We used Verizon's definitions of incident and breach (2015 Data Breach Investigations Report). According to Verizon, an incident is: *"Any event that compromises the confidentiality, integrity or availability of an information asset."* A breach is: *"An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party."*

First, we asked about the frequency of attacks, incidents, and breaches. See Table 1. These local governments reported that attacks occurred the most frequently, one quarter (26 percent) said at least hourly or more; nearly one in five (18 percent) said at least once a day; nearly eight percent said at least once a week (7.7 percent); The remaining responses were: at least once a month – 6.6 percent; at least once a quarter – 4.6 percent); at least once per year – 3.8 percent). More than a quarter (27.6 percent) said that they did not know.

As would be expected, the local governments reported that incidents occur less frequently: hourly or more (4.09 percent), at least once a day (4.9 percent), at least once a week (5.7 percent), at least once a month (10.4 percent), at least once a quarter (13.35 percent), at least once annually (16.35 percent), and nearly three in ten (29.7 percent) did not know. Breaches occurred even less frequently and followed a similar pattern: only 2.8 percent experienced them hourly or more, 2.2 percent at least once a day, 1.1 percent at least once a week, 0.8 percent at least once a month, 3.31 percent at least once a quarter, 14.1 percent at least once annually. Four in ten (41.1 percent) did not know. And 34.7 percent said "Other," and we are in the proves of examine the written responses to determine what other frequency(ies) these local governments reported.

The responses on breaches are of some concern to us because they seem relatively high when compared to national data. We will examine the data on breaches further in additional analyses that we are conducting.

Table 1: How frequently is your local government's information system subject to attacks, incidents, and breaches (in %s)?

	Attacks	Incidents	Breaches
Hourly or more	26.0	4.0	2.8
At least once a day	18.0	4.9	2.2
At least once a week	7.7	5.7	1.1
At least once a month	6.6	10.4	0.8
At least once a quarter	4.6	13.4	3.3
At least once annually	3.8	16.4	14.1
Other	5.7	15.5	34.7
Don't know	27.6	29.7	41.1

We also asked about the number of breaches, attacks, and incidents experienced in the past twelve months. The great majority of respondents (80.8 percent) reported that no breaches occurred over the past twelve months. Just over one in ten local governments (10.9 percent) experienced one breach, two breaches (2.6 percent) in the past 12 months and, as expected, fewer still experienced more than two breaches – three breaches (1.7 percent), four breaches (1.15 percent), six breaches (0.6 percent), seven breaches (0.3 percent), or did not know (0.9 percent). However, these data are rather inconsistent with the data in Table one that showed a higher frequency of breaches. We have not yet delved deeply enough into the data to understand the apparent contradiction here but intend to do so in further analyses that we are conducting.

We next asked whether the frequency of attacks, incidents and breaches had increased or decreased. See Table 2. Pluralities of respondents reported that the frequencies in all three categories remained the same. Only a few local governments reported declines and all reported increases – though mostly in attacks (32.3 percent) versus incidents (18.3 percent) and breaches (5.5 percent). The latter should be heartening news for local governments because it says that although attacks and incidents are on the rise, the increase in breaches is minimal. Unfortunately, sizeable percentages of these governments did not know whether the frequencies of attacks, incidents and breaches had risen or fallen.

Table 2: 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
A lot fewer	3.80%	4.66%	7.99%
Fewer	3.80%	8.49%	5.23%
Same	34.24%	41.10%	45.73%
More	22.01%	14.79%	3.86%
A lot more	10.33%	3.29%	1.65%
Don't know	25.82%	27.67%	35.54%

Cybersecurity preparedness

We next inquired about the level of cyber-preparedness of local governments. See Table 3. The first observation we draw from the data in this table is that, by their own reporting, local governments are not highly confident of their cyber-preparedness. Only four in ten (42.2 percent) said that their preparedness to detect attacks was very good or excellent; 38.5 percent said the same about the ability to detect attacks; 36.7 percent to prevent breaches; 36.7 percent to prevent breaches; 37.7 percent recover from breaches; 20.3 percent detect exfiltration; 25.4 percent prevent exfiltration; 28.3 recover from exfiltration; and 48.4 percent recover from a ransomware attack. Clearly, earlier data show that local governments are at high cyber-risk. They are equally clearly not well enough prepared for such risk. This led us then to inquire, in order, about barriers to cybersecurity that local governments and about their use of various policies, tools and practices to improve cybersecurity.

Table 3: How well prepared is your local government to (in %):

	Detect attacks	Detect incidents	Prevent breaches	Recover from breaches	Detect exfiltration of data / info	Prevent exfiltration of data / info	Recover from exfiltration of data / info	Recover from Ransomware attack
Poor	7.7	7.7	6.6	5.8	22.5	19.7	12.5	6.1
Fair	20.2	20.5	21.5	20.6	26.3	22.9	18.9	12.68%
Good	25.4	28.2	30.1	22.9	15.9	18.5	19.8	22.5
Very Good	27.4	26.5	26.1	28.1	15.3	20.2	21.0	31.1
Excellent	14.8	12.0	10.6	9.0	5.4	5.2	7.3	17.3
Don't Know	4.6	5.1	5.1	13.6	14.5	13.3	20.4	10.4

Previous research has uncovered a number of barriers to the ability of local governments to adopt and implement information technology and electronic government (e.g., Norris and Kraemer, 1996; Coursey and Norris, 2008; and Norris and Reddick, 2013). We adopted a similar list of potential barriers, somewhat expanded, for this survey. As in previous research lack of adequate funding and lack of adequate staff (in this case cybersecurity staff) topped the list of barriers reported by local governments to their ability to achieve the highest possible level of cybersecurity. Here, we report only the top nine barriers (those that achieved a majority or near majority of respondents). More than half of respondents (52.3 percent) said that lack of funds constituted either a somewhat severe or a severe barrier and 27.9 percent said it was a modest barrier. Next, 52.9 percent said that an insufficient number of cybersecurity staff constituted a somewhat severe or a severe barrier, while 21.4 percent said modest barrier. Nearly half (48.3 percent) said that the inability to pay competitive salaries for cybersecurity personnel a somewhat severe or a severe barrier, while 12.2 percent said modest barrier. This was followed by lack of end user accountability (37.3 percent somewhat severe or severe and 23.4 percent modest barrier); lack of cybersecurity awareness in the organization (30.8 percent somewhat severe or severe and 31.4 percent modest barrier); lack of availability of trained cybersecurity personnel to hire (31.3 percent somewhat severe or severe and 21.7 percent modest barrier); lack of adequately trained cybersecurity personnel in the local government (22.3 percent somewhat severe or severe and 23.2 percent modest barrier); no end user training at all (25.6 percent somewhat severe or severe and 20.0 percent modest barrier); and, some but insufficient end-user training (19.5 percent somewhat severe or severe and 27.6 percent modest barrier).

Three of the top five barriers are directly related to funding – lack of funds, lack of cybersecurity staff, and inability to pay competitively; five are related to organizational issues – end user accountability, lack of trained cyber staff in the local government, end user training (twice) and cyber awareness; and one to market conditions. This suggests that local governments, if they so choose, have the ability to address all but one of these barriers to at least some extent.

Policies, tools and practices

One way that local governments can improve cybersecurity is to the best available policies, tools and practices. Our findings indicate that local governments are woefully behind in this area. For example, the majority of them said they had not adopted a formal, written cybersecurity policy, standards, strategy or plan (60 percent), or a cybersecurity risk management plan (73 percent). Those governments that had adopted both cybersecurity policies (46.4 percent) and risk management plans (44.7 percent) were rated as having only an average level of effectiveness. Local governments also overwhelmingly do not maintain formal, written plans for recovery from breaches (72 percent), and those that did only rated them as average in effectiveness (44.3 percent).

A majority of local governments (70 percent), however, had adopted formal written rules regarding the creation or passwords (71 percent) and for end users to change passwords periodically. Additionally, these governments rated the password rules rated as effective (74.7 percent high or very high). Slightly over half (55 percent) of local governments had written policies governing the use of personally-owned devices by government officials or employees, which is also rated as effective (40.6 high or very high).

Finally, we asked about the use of various cybersecurity tools. The tools used by the most local governments include anti-virus software (84 percent), web and e-mail gateways (72 percent), Virtual Private Networks or VPNs (71 percent), intrusion detection and prevention systems (65 percent), and next generation firewalls (63 percent). Less frequently utilized tools include automated malware protection systems (53 percent), network traffic analysis or network visualization (46 percent), and multi-factor/biometric authentication (22 percent). Regarding cybersecurity insurance, which not only can protect from loss but also require organizations to conduct risk analysis as a condition of purchase, only 44 percent of local governments had purchased such insurance. Of the local governments that chose cybersecurity insurance, 21.1 percent purchased very little or limited coverage, 36.2 percent purchased a moderate range of coverage and 27 percent said that they had purchased most or full coverage.

Awareness of and support for cybersecurity

Like other organizations, local governments can benefit from the understanding or awareness of and support for cybersecurity from within, from elected officials, management and end-users. The theory is that the stronger the awareness and support is, the easier it is for the organization to maintain a high level of cybersecurity Therefore, we asked questions precisely about this issue. Among all actors within local governments, respondents said that top managers possessed the most cybersecurity awareness (61.7 percent moderately to exceptionally aware, 19.0 percent somewhat aware and 14.0 percent slightly or not aware). This was followed by department managers (42.5 percent moderately to exceptionally aware, 32.3 percent somewhat aware and 21.5 percent only slightly or not aware). Next came the average end user (34.1 percent moderately to exceptionally aware, 33.2 percent somewhat aware and 28.8 percent only slightly or not aware); the elected executive (42.5 percent moderately to exceptionally aware, 32.3 percent somewhat aware and 27.8 percent only slightly or not aware); and elected councilors/commissioners (25.6 percent moderately to exceptionally aware, 26.5 percent somewhat aware and 40.67 percent only slightly or not aware).

We asked about levels of support received for cybersecurity from various local government actors as well. Again, in the perception of the respondents, the top appointed manager provides the greatest amount of support for cybersecurity (53.8 percent strong to full support, 23.71 percent moderate support and15.8 percent limited or no support). In order, this is followed by: the elected executive (35.6 percent strong to full support, 20.1 percent moderate support and 25.0 percent limited or no support); department managers (33.3 percent strong to full support, 34.8 percent moderate support and 26.8 percent limited or no support elected councilors/commissioners (30.4 percent strong to full support, 28.4 percent moderate support, although 31.8 percent of the said respondents and limited or no support among these officials); and the average end-user (21.9 percent strong to full support, 36.8 percent moderate support, although 31.8 percent of the said respondents and limited or no support among end-users).

It would appear from these data that various actors within local governments are aware of the need for and support cybersecurity to at least some degree. However, it is also clear for both awareness and support that local governments have a task before them to better inform and persuading actors within their organizations of the importance of cybersecurity.

We also asked the respondents whether top elected officials and appointed officials feel that cybersecurity belongs mostly to the technologists or do these officials believe that they have an important role to play in it. Responses were on a one to five scale where one meant responsibility mostly belongs to technologists and five meant officials have an important role to play. For ease of analysis we combined responses one and two to mean mostly to technologists, three meant both and four and five to mean important role for officials. Here respondents indicated that, in their opinions, top elected officials did not feel they had an important responsibility in cybersecurity (9.49 percent said important role, 10.7 percent both, and 66.8 percent said mostly technologists' role). Regarding the top appointed officials, the responses were quite similar, although top appointed officials were seen as slightly more likely to support a role for themselves (17.4 percent said important role, 13.8 percent both, and 56.9 percent said mostly technologists' role). It is commonly understood among cybersecurity specialists that, in order for organizations to achieve high levels of cybersecurity, top policy makers and top managers must play important roles. Therefore, it is clear that local governments have another task of informing and persuading persuasion before them – this with their elected and appointed officials.

5. Conclusion

Data from this first ever nationwide survey of local government cybersecurity in America allow us to draw at least the following conclusions. First, local governments are under fairly constant attack and their IT systems are periodically breached. Moreover, they are not especially well prepared to prevent attacks, incidents or breaches and are nor well prepared to recover from breaches. Local governments face a number of barriers to being able to have the highest possible level of cybersecurity. These barriers are principally financial and organizations. A number of polices, tools and practices are available to local governments to improve cybersecurity. However, few local governments are not making wide use of them.

References

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

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

Center for Digital Government. 2014. *Advanced Cyber Threats in State and Local Government*. Folsom, CA. Accessed September 23, 2016 at: http://www.nascio.org/events/sponsors/vrc/Advanced%20Cyber%20Threats%20in%20State%20and%20%20Local%20Government.pdf.

Coursey, David, and Donald F. Norris. (2008). Models of e-government: Are they correct? An empirical assessment." *Public Administration Review*. 68(3): 523-536

Deloitte and National Association of State Chief Information Officers. 2012. *2012 Deloitte-NASCIO Cybersecurity Study State governments at risk: a call for collaboration and compliance.* Accessed September 23, 2016 at: http://www.nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy2012.pdf.

Deloitte and National Association of State Chief Information Officers. 2014. *2014 Deloitte-NASCIO Cybersecurity Study – State Governments at Risk: Time to Move Forward.* Lexington, KY: Authors. Accessed September 23, 2016 at: http://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-state-nasciocybersecuritysurvey_102714.pdf.

Deloitte and National Association of State Chief Information Officers. 2016. *2016 Deloitte-NASCIO Cybersecurity Study State governments at risk: Turning strategy and awareness into progress.* Accessed September 23, 2016 at: http://dupress.deloitte.com/content/dam/dup-us-en/articles/3470_2016-Deloitte-NASCIO-cybersecuritystudy/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf.

IBM Center for The Business of Government. (2010). *Cybersecurity Management in the States: The Emerging Role of Chief Informtion Security Officers*. Washington, DC: Goodyear, M., Goerdel, H. T., Portillo, S., and L. Williams.Accessed September 23, 2016 at:http://www.businessofgovernment.org/sites/default/files/CybersecurityManagement_0.pdf.

Malashenko, Elizaveta, Chris Villarreal and J. David Erickson. 2012. *Cybersecurity and the Evolving Role of State Regulations: How it Impacts the California Public Utilities Commission Grid Planning and Reliability Policy Paper.* Moulder, Evelina. 2011. Personsl communication with ICMA's survey research director.

Norris, Donald F, Anupam Joshi and Timothy Finin. 2015. *Cybersecurity Challenges to American State and Local Governments.* A paper presented at the 2015 European Conference on E-government, Portsmouth, England, June 18-19, 2015.

Norris, Donald F., and Kenneth L. Kraemer. (1996). Mainframe and PC computing in American cities: Myths and realities. *Public Administration Review*, *56(6),* 568-576.

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

Ponemon Institute. 2015. State of Cybersecurity in Local, State & Federal Government. Accessed August 30, 2016 at: http://www.ponemon.org/library/the-state-of-cybersecurity-in-local-state-and-federal-government

Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly* 27(1), 49-56.