DE GRUYTER Journal of Homeland Security and Emergency Management

Cyber-Security at the Grassroots: American Local Governments and the Challenges of Internet Security

Journal:	*Journal of Homeland Security and Emergency Management*
Manuscript ID	jhsem-2017-0048.R1
Manuscript Type:	Research Article
Classifications:	
Keywords:	Cybersecurity, cyber attack, local government,

Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security

The issue that we examine in this paper is that of cybersecurity at the grassroots in the United States, by which we mean at the local government level. This 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 nearly 39,000 general purpose governments, of which 3,031 are county governments, 19,519 are municipal governments and 16,360 are town or township 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.).[1] These data are kept in local government IT systems as a result of a variety of citizen-local government interactions, such as paying water

[1] Today, cyber criminals seek PII perhaps more than any other single item in order to impersonate individuals whose identities have been stolen and then to use those stolen identities to steal money and goods (e.g., Ablon, et al., 2014; Finklea and Theohary, 2015).

and sewer bills, signing up for recreation activities, paying fines and fees, securing locally required licenses and permits, and much more. 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.

According to the Privacy Rights Clearinghouse, which maintains a list of all publicly reported data breaches, there have been 286 breaches in local, state and federal governments since 2011, of which 195 were at the state and local level (Privacy Rights Clearinghouse, 2016). While a number of these events involved the unintended disclosure of PII (91), there have also been hacking or malware incidents (89) that steal PII or hold sites or databases for ransom and a smaller number of insider breaches (27). Additionally, 257 educational institutions have been breached since 2011, 200 being public institutions.

Here is a short list that is typical of the local governments that have experienced breaches in recent years: Baltimore County, MD (2013) (insider breach with contractor saving PII of 12,000 county employees), the New York City Police Department (2013) (former detective pled guilty to paying hackers to steal passwords for e-mail accounts of other officers), the Oregon Employment Department (2014) (PII of 850,000 people seeking employment hacked and compromised), the City of Akron, OH (2014) (47,452 records posted online after hack by international group), the City of Detroit, MI (2014) (hack and breach of 1,700 city employee files), Jefferson County, TX (2015) (disclosure of thousands of Social Security Numbers of current and former county residents in online records), Dallas County, TX (2015) (data breach of resident information available online for over six months), Illinois Board of Elections and

Arizona State Board of Elections (2016) (alleged international state actor hack compromising 200,000 Illinois personal voter records, and voter information going back a decade in Arizona) (Privacy Rights Clearinghouse, 2016).[2] More recently the cities of Atlanta, GA, and Baltimore MD, experienced serious breaches to their systems (Blinder and Perlroth, 2018; and Rector, 2018).

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 Ponemom 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.

The World Wide Web presents one of the most commonly used vectors for attacks. This attack vector can be divided into two major components. One is the fact that organizations large and small, public and private have developed web sites to provide information and services online. In some cases, especially for governments, this information is legislatively mandated. For governments, also, web presence is tied to e-government -- providing citizens with online access to governmental information and services and interaction with government personnel. Such web sites, which will typically have data driven backends (hard drives, servers, and the like) that contain the organization's data and forms to accept input, can be attacked

[2] While this paper is about local government cybersecurity, we would be remiss not to note prominent federal government agencies and private sector companies that have experienced breaches including: the U. S. Central Command's Twitter account (2015), the U. S. Postal Service (2014), the National Oceanic and Atmospheric Administration (2014), the United States Office of Personnel Management (2015), the White House (2015), Target (2013), Home Depot (2014), JPMorgan Chase (2014), Anthem, Inc. (2015), MedStar Health (2016) and numerous others.

using a variety of "injection" attacks, where cybercriminals attempt to place malware or malformed input into a backend to cause it to run specific code. A good example of this is SQL injection attacks, where the database of the government that contains its information is attacked.[3]

The second major attack vector component is the use of Internet enabled technologies, especially social media, email, and mobile apps. To attack specific targets, "spear phishing" is increasingly used. Cyber criminals gather publicly available information (e.g., from websites, social media sites like Facebook and even public records) to build the profile of a person, and then craft email messages that are very specific (for example, from a person's college friend talking about a proposed reunion and providing an attachment). These emails tempt end-users to open the attachment, which in turn installs malware on their computers.

Fifth, cyberattacks have moved from being a nuisance to something very serious and are deployed not only by state actors (national governments or their surrogates), but also by sophisticated transnational, non-state actors such as terrorists and financial criminals (U.S. Navy, 2012). Sixth, 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

[3] SQL stands for Structured Query Language and is the standard language for managing relational database systems (Groff and Weinberg, 2010).

dollars.[4] 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, while there is an abundance of reports, studies, and other documents in the professional literature about cybersecurity, 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 that are directly on topic. 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 threats to cybersecurity that local governments face, the actions they take to protect their IT systems from attack and to mitigate after a successful attack, the gaps between those actions and requirements for high levels of cybersecurity and, finally, the barriers these governments encounter when deploying cybersecurity. Understanding these issues will also allow scholars and practitioners develop recommendations for improved local government cybersecurity.

The Literature

[4] The seven nations, in order of cost of cybercrime to each, were: US, Germany, Japan, UK, Brazil, Australia and Russia.

In preparing for this article, we conducted an extensive review searching for all existing literature, academic or professional, that directly examine local government cybersecurity. We were particularly interested in works from the social science and computer science disciplines. We conducted the search using an exhaustive list of key search terms including: attack, breach, hack, cyberattack and cyber attack, and incident; and local, state, city, county, and municipal government, e-government, agency, cybersecurity, data, database, infrastructure, information technology and PII.

With this narrowed focus on local government issues, the scholarly literature review yielded only three relevant peer-reviewed articles from social sciences and none from computer science (Caruson, et al., 2012a; Caruson, et al., 2012b; Zhao & Zhao, 2010). However, the lack of academically driven research in this area is ameliorated by the abundance of reports from professional organizations, private information technology and cybersecurity firms, and independent institutes (Pomenon Institute, 2015; Deloitte and NASCIO, 2010, 2012, 2014, and 2016; Center for Digital Government, 2014; and IBM Center for The Business of Government, 2010). Additionally, we found at least one related government report (Malashenko, et al., 2012). We will address each in turn: scholarly and professional local government cybersecurity literature.

E-government performance literature examining issues of technological architecture and maturity exist (Almarabeh & AbuAli, 2010, Lambrinoudakis, et al., 2003). However, the majority focuses on the federal and international levels, and fails to address human error and management concerns. E-government adoption literature covers matters of management and barriers to implementation (Halchin, L. E., 2004), as well as the effectiveness of practical IT

strategy guides developed by governments to assist in implementation (Gil-Garcia & Pardo, 2005), but similarly does not fill the research gap in terms of addressing information security and system protection. However, the overlap between these areas of research, and their major findings, applies to cybersecurity in that both technical expertise, and effective management and implementation of cyber policies, are essential to maintaining high levels of cybersecurity. Academic research specifically on how, and the extent to which, local governments are able to effectively implement and manage cybersecurity standards, is minimal.

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)[5] 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

[5] The remaining two articles address issues of transparency and privacy (Caruson, et al., 2012b), and specific state government websites (Zhao & Zhao, 2010).

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.

We found a number of professional reports that were relevant to state and local government cybersecurity. We discuss seven of them here as they provide the most recent, and perhaps most thorough, information regarding what is currently known about this subject. Deloitte and NASCIO have been conducting a biennial survey of Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) since 2010 and have tracked the fast growth in importance, responsibility, and, now, respect of the role of CIOs and CISOs in state 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. Since 2010, Deloitte and NASCIO have consistently found the number one barrier to cybersecurity to be lack of funding. Similarly, respondents listed lack of adequately trained staff as another consistent top three barrier (59 percent in 2014, 46 percent in 2012). The top five barriers in cybersecurity administration in 2016 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). The top five functions of the CISO 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). 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 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).

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 detailed 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).[6]

Last, 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 examined the role of state regulation to fill gaps remaining from federal compliance-based models. Specifically, the report discussed the need to determine and implement cybersecurity best practices, policies, and procedures to ensure uniform standards.

Issues such as these have led to the development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework standards that provide non-mandatory best practice information to local government practitioners (2018). Organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) similarly provide neutral best practice information to practitioners. While these standards and practices, along with professional reports and the like are undoubtedly useful, they rarely go beyond description and perhaps

[6] Advanced persistent threats (APTs) involve a hack in which the attacker remains within the network and continuously attacks or exfiltrates data over time. A zero-day attack involve vulnerabilities in software that were previously unknown and occur before the software is fixed. Attackers can create “bots,” or malicious software that run automated attacks against a specific target or the internet at large. Worms are stand-alone viruses or malicious code, which can be activated through clicking on a spear phishing e-mail. (Center for Digital Government, 2014).

limited analysis. This is where we believe that our work, and that of other scholars, will be useful in filling the gap in the scholarly literature on state and local cybersecurity.

Method

In order to begin to address the issue of cybersecurity among American local governments, we conducted a focus group in late 2013 that included information technology (IT) and cybersecurity professionals from the state government and several local governments in our home state of [redacted] and lasted approximately two hours. Focus group research has a long history in the social sciences and is well-recognized for the ability to "provide in-depth exploration of a topic about which little is known (Stewart, et al., 2007, p. 109)." Focus groups operate by collecting data via interaction among members of a group selected on a topic also selected by researchers (Morgan, 1996). Hence, we chose this method because of the paucity of information available either in the scholarly or popular literature about local government cybersecurity and because of its utility in exploratory research.

The participants included the Chief Information Officer (CIO), Chief Information Security Officer or Chief Technology Officer [redacted]

[redacted][7] Thus, our participants, or key informants, were top level IT and cybersecurity professionals who literally are on the front line of fighting cybercrime on a daily basis. As we will show throughout this paper, their knowledge, expertise and experience were incredibly valuable to this research.

Four of the local jurisdictions included in the focus group represent the greatest concentration of population in the state, and two of them [redacted][8] are the wealthiest in the state and among the wealthiest in the nation. This is important to note because research over the past decades has revealed that local government adoption of information technology, especially innovative technology, is related to local government size and resources [redacted]. Size is also important because it means that larger local governments have larger and more extensive IT systems and websites, maintain and store larger volumes of sensitive information, and are under greater treat of cyberattack.

In preparing for the focus group the authors developed a protocol that addressed three broad areas: 1) cyberattacks, including the number, frequency, type and severity of cyberattacks; likely origin of attacks; number, frequency, type and severity of breaches; policies, practices and tools employed to prevent breaches and their success; 2) barriers to successful cybersecurity including funding and staffing, governance and policy; and 3)

[7] We have blocked any identifying information because it would almost certainly reveal the location and probably also the identities of the authors. This information will be un-blocked if the paper is approved for publication. All participants were local government high level IT or cybersecurity professionals.

[8] Identifying information blocked.

recommended improvements to local government cybersecurity. We recorded the entire focus group meeting event on a digital recorder and had the recording professionally transcribed. We then reviewed the transcription against the recording for any discrepancies, of which we found none of consequence.

An important purpose of focus group data analysis "is to identify areas of agreement and controversy…" within the group (Kidd and Parshall, 2000). Upon reviewing the transcript, we utilized a rigorous coding process, incorporating both axial and thematic coding, in order to ensure the validity of our findings. Thus, the authors of this paper individually read the transcript and, based on the words of the participants, excerpted the key points that the participants had made in response to questions on the protocol. Here, we were especially interested in finding common themes that emerged as well as for deviations from those themes. These themes were also disaggregated and compared, using axial coding, in order to fully examine the framework of relationships between them, and how they each relate to the protocol we initially developed.

We then met to discuss our respective analyses of the focus group transcript in order to produce the narrative of our findings, which follows. As Stewart, et al., (2007) note, in exploratory research such as ours, "a simple descriptive narrative is quite appropriate and often all that is necessary (109)." And further: "When the results of a focus group are so obvious as to require little supporting documentation, detailed analysis is probably not worthwhile (110)."

What emerged from our review of the transcript were several common themes (which we discuss in the narrative) on which the participants achieved complete or nearly complete

consensus (e.g., Cyr, 2016; and Liamputtong, 2011.) There were no areas of disagreement among the focus group participants. We suspect that this was the case because the participants were practitioner-experts in local government cybersecurity with many years of direct experience in this field.

Of course, this research has limitations. First, this is an explorative study that only begins to identify and examine issues that American local governments face as they address the serious challenges of cybersecurity. It is not an in-depth examination of these issues across a broad array of local governments. As such, one should be cautious extrapolating from our findings. However, as Vicsek (2010) has observed:

> …when one finds that certain perspectives or aspects are common to the research subjects belonging to a particular social category in small sample research, one infers from it, that it is likely that not just the members of the sample, but others belonging to the target population – consisting of people of the same category – might share similar views (125).

Second, although we can infer that the views of the members of this focus group might be true of similarly situated individuals (local government cybersecurity practitioner-experts), these findings should not be generalized because the focus group was small and was not representative of local governments across the nation.

Third, findings from focus group research are limited to the content of the focus group discussion itself. If focus group participants did not raise or discuss certain aspects of the topic under investigation (in this case state and local government cybersecurity), then investigators cannot report on those aspects. Fourth, the limited time available for this focus group meant also that not all aspects of the topic could not be addressed.

Fourth, data from a focus group conducted four and one half years ago may be viewed by with suspicion since much has changed in the world of cybersecurity during that period. However, we completed the first ever nationwide survey of local government cybersecurity in late 2016, and its results closely mirror the findings from the 2013 focus group (Norris, et al., 2017). Thus, while much may have changed, much also remains very similar. Hence, the earlier findings remain relevant today.

Despite these limitations, however, our findings are heuristically valuable. In fact, they have enabled us to develop research questions and hypotheses that have formed the basis for further research into local government cybersecurity that we conducted in 2016 and are currently conducting. In the following pages we discuss the most important findings from this focus group.

Findings

We began the focus group by asking the participants questions about the cyberattacks that their governments experienced. A cyberattack is any attempt by an unauthorized party to gain access to the local government's information system for the purpose of mischief or harm. We followed this with questions about barriers that local governments face in successfully deploying cybersecurity. We then asked about actions that they believe should be taken to improve cybersecurity practice at the local level. [9]

[9] Because some of the information that the participants revealed was highly confidential, we anonymized all participant responses. Thus, we have not identified the names of individual participants or their respective governments nor did we associate names with the responses we reported in this paper. In the final paper we will

Attacks

We first asked how frequently these governments' web sites were attacked. The participants told us that in previous years, local governments worried mainly about direct attacks on firewalls. Today, however, the routine attacks are different in both size, and as one participant explained, "…the nature has changed so [that]… we're more micromanaging these little events versus this… big huge crash of the website." While larger attacks might occur once few months or so, attacks, or intrusion incidents occur in large numbers on a daily basis.

Participants said that most attacks are made against a government's public facing website, or via email, and that most attacks involve social engineering and phishing rather than direct attacks on firewalls. Depending on the size of the government, attacks can number in the tens to hundreds of thousands or more every day. Cyberattack is a 24/7/365 phenomenon. However, as one participant noted, "…but, you know what? We've come to the point where we don't characterize those events as attacks. They're routine."

This finding is quite different from the results of the Caruson survey where only about a quarter of respondents acknowledged that their system had been attacked (2012a). However, the private industry reports have found a higher awareness of the presence attacks and incidents. For example, the Center for Digital Government found both a perceived increase in attacks (40 percent) and perceived stability in the number of attacks (36 percent) amongst the IT and security management professionals, of state and local governments serving

include a list of participants in the Appendix. To provide it here would reveal the state in which this research was conducted and, quite possibly, therefore, the identity of the authors of this work.

constituencies of more than 500,000, who were surveyed (2014). Further research is needed to understand this difference, although we suspect that it may be something as simple as the definition of the term attack and/or the level of knowledge that various elected and appointed county officials in Florida had about the attacks on their local government's IT systems (versus the knowledge of our cybersecurity practitioner-experts).

Of course, as practitioners and scholars alike know, organizations can only know about the attacks and breaches that they are able to identify. Thus, the frequency and types of attacks and the frequency and severity of breaches may be greater than reported in virtually any research. In the 2016 survey we referenced above, significant numbers of responding governments said that they did not know of the frequency of attacks on or breaches of their systems (Norris, et al., 2017).

We next asked the participants if the technical side of cybersecurity was especially problematic for them. They said that, while they were not perfect at it, they felt that for the most part they had the technical side of cybersecurity under control. As one participant said: "We know that we block a huge amount. We know that some of the things we block, our users want to have come through and some of the things that we would like to block come through anyway." Another participant estimated that, in his county, about 40 percent of emails were blocked. And this means that "…you're in the hundreds of thousands if not near a million a month that we're just blocking and [are] not even making it to the end-user." Recent studies (e.g., Gudkova, et al., 2016) estimate than over 55 percent of all email is spam. While much of it is merely unwanted advertising, a non-trivial fraction is sent as an attempt to get the

recipient to open or download a malicious attachment or to be enticed to provide valuable personal information such as account data.

The participants unanimously noted that the end-user is the principal problem they face in being able to maintain high levels of cybersecurity. One participant said: "And our biggest struggle now is…the human being, our weakest link." The crux of the matter is that, inevitably, an end-user will download and open an attachment or click on a link sent in an email phishing attack that allows an attacker into the local government's IT system. This happens mainly as a result of human error – most often an end-user who unknowingly clicks on a malicious link or opens a malicious document.

Focus group members also noted that the phishing attacks are becoming more sophisticated and less easy to readily identify as such. In one case reported by a participant, two governmental employees out of 10,000 inadvertently opened a malicious URL. And, as this participant noted, while two out of 10,000 is statistically impressive, the damage was nonetheless done because the attacker was able to penetrate this government's IT system. Participants also reported that malice by end-users occurs, although it is rare.

According to Verizon's 2013 Data Breach Investigations Report, the likelihood of a phishing attack succeeding is quite high. Among other things, the report inquired about how many email messages would be required to get a single user to click on a malicious attachment.

> It's pretty easy to see why [phishing]…is a favored attack…and the answer to our question is "three." Running a campaign with just three e-mails gives the attacker a better than 50% chance of getting at least one click. Run that campaign twice and that probability goes up to 80%, and sending 10 phishing e-

> mails approaches the point where most attackers would be able to slap a "guaranteed" sticker on getting a click. To add some urgency to this, about half of the clicks occur within 12 hours of the phishing e-mail being sent (p. 38).

We asked where cyberattacks originated, and the participants told us that attacks come from across the globe. As the 2013 Verizon report found, however, most attacks come from within a relatively few nations, with China (30 percent), Romania (28 percent), the U.S. (18 percent), Bulgaria (seven percent), and Russia (five percent) comprising 88 percent of identified attacks.

The participants noted that most attacks are automated. "These people are literally setting up complex systems and letting it just hit global to see what they can get." Additionally, participants said that the attackers mostly were criminals rather than, for example, political activists, young people breaking into systems for sport or terrorists. One participant put it this way: "The perpetrators are looking for opportunity…Primarily its financial opportunity. These people are thieves." The participants said that the attackers want PII in order to impersonate their victims for financial gain. One participant agreed, saying: "So, yeah, there's a lot are other causes for it, or there [are] lots of other motivations. There is espionage, there is notoriety, there is revenge, but money is on the top of the list and it is the lion's share of why this occurs."

Participants noted other risks from cyberattacks, including three of particular concern. First, there is a risk of having an agency's computers compromised and subsequently used as part of a botnet controlled by the attackers, which can then be used to launch attacks on other

computers.[10] A second risk is that a compromised computer or account in one agency can be used to try to gain access to a related agency that may have valuable information or control important assets. For example, a compromised computer in a county parks department might be used to launch an attack on a state database and from there try to gain access to a federal computer system. Third, some local agencies are responsible for maintaining critical cyber-physical infrastructure systems such as traffic and water utilities. Attackers who gain access to these could potentially do great harm.

Barriers

It was, thus, clear from this focus group that cybersecurity poses a serious challenges to local governments. They face constant attacks, and local IT and cybersecurity professionals know that some attacks will eventually succeed. The sources of at least some of these challenges can be found in barriers that local governments face in achieving high levels of cybersecurity. According to the focus group members, the major barriers, which we address the following paragraphs, were:

- insufficient funding and staff
- governance and federation (executive, legislative and judicial branches and divisions within the executive)

[10] A botnet is a collection of computers connected to the Internet that have been infected with malicious software that allows them to be controlled remotely. Botnet can be exploited without the knowledge of their computer's owners for many illegal purposes including sending spam email, engaging in click fraud, launching distributed denial of services attacks, bitcoin mining or stealing private information (Stone-Gross, et al., 2009). The U. S. Federal Bureau of Investigation (FBI) estimated that the GameOver Zeus botnet comprised over one million computers in 2014 (FBI, 2014).

- insufficient or under-enforced cybersecurity policies

Funding and Staffing: The focus group participants were unanimous in saying that insufficient funding and staffing, which are closely related, made it difficult for local governments (or any organization) to hire and retain qualified IT and cybersecurity staff and provide the needed level of cybersecurity protection. Lack of funding and staff are also among the top barriers reported in surveys of IT and e-government among U. S. local governments since at least the 1990s [redacted] Note also that 80 percent of respondents to the 2016 Deloitte and NASCIO survey listed lack of sufficient funding as the number one barrier in cybersecurity administration, as did 60 percent of the respondents in the Caruson, et al., survey (2012a), and 53 percent in the 2015 Ponemon Institute study.

Additionally, funding constraints mean that local governments are not in a strong position (if any position at all) to compete with salaries that private sector organizations can offer to IT and cybersecurity professionals. This competition is particularly acute in our home state of [redacted] because of the extraordinary demand for qualified IT and cybersecurity staff by [redacted][11]

One participant noted that the IT budget in his county was:

> …less than two percent of the overall budget. Less than two percent. Yet 100 percent of the people in [the county] are using IT. So, you know, you're right,

[11] Identifying information blocked.

> you know, we don't have the resources, we don't have the manpower. [We]…try and use our money the best way we can and…you're right, sometimes things can be solved with money.

Insufficient funding has increasingly led local governments to investigate alternative ways of addressing cybersecurity, including outsourcing. One county represented on the focus group reported that 90 percent of its programs and data were running on cloud computing infrastructure.[12] This transfers much of the responsibility of securing the data and services to the cloud service providers for whom cybersecurity is a central part of their business. Other participants noted that they are beginning to view cybersecurity as a commodity or a service that they purchase on the market. One of the advantages of this, in addition to potential cost savings, is improved cybersecurity. As one participant put it, is: "Google has 2,000 security engineers…I've got four."

On a somewhat discouraging note, however, the participants agreed that even with greater funding and more staff, their systems will continue to be attacked and almost certainly some attacks will be successful. Therefore, there is a clear need to continually harden the IT infrastructure, to provide better end-user training and control, and to have recovery plans in place in the event of a successful attack. One participant, however, cautioned about overdoing recovery. He put it this way: "So…what would happen to us if our system went down. I mean the world is not going to end. We are not Amazon. We're not Google…That [the IT system] is not the crux of our business." The core business of local government, to which he was

[12] The "cloud" is a misnomer that, for good or ill, is now part of the lexicon. It really means that companies with large computer systems and excess mass storage (e.g., Amazon, Google, Microsoft, Oracle and other providers) offer their services to both public and private sector organizations for IT outsourcing.

referring, involves service delivery, most of which would continue in spite of a loss of IT services. Moreover, some of the participants said that they were not terribly worried about having their information exfiltrated since most of it is public data. [13]

This said, they nevertheless agreed that cybersecurity should be a high priority for local governments because of the possibility of PII and other sensitive information being exfiltrated and because of the cost of recovering from breaches. Although not explicitly stated, the impression from the participants clearly was that there is a high embarrassment factor associated with being breached. And that this was also reason to maintain the highest levels of cybersecurity possible

Governance: According to our participants, governance poses a major problem for effective local government cybersecurity. They agreed that the first and most important governance problem is the federated nature of local government. The separation of powers among the executive, legislative and judicial branches means that the governmental cybersecurity function is also divided. While this function is most often located in the executive branch, typically in the information technology department (ITD), the executive branch has no authority over the legislative and judicial branches. As one participant put it: "I've got responsibility over all three branches of government. However, I can't legally enforce policy, due to the pesky constitution, over the legislative and judicial branches. But I am responsible for their security." Thus, federation presents an important limitation on or barrier to what can

[13] In cybersecurity contexts, exfiltration is the unauthorized release of data from within a computer system, typically done by malicious software that has been installed on the system.

be done to ensure the highest levels of cybersecurity within local governments. We will address this further in the next section of this paper.

A second important governance issue is that, even within the executive branch, there can be departments or units that may have "special protection" and remain outside of the purview of the ITD. Participants mentioned police departments as entities that were sometimes the "favorites" of elected officials and, therefore, were granted special dispensation from oversight by the ITD and its cybersecurity policies and regulations. Additionally, some units within local governments may have their own IT systems that they operate and manage separately from the ITD and its cybersecurity policies and practices.

A third governance issue is found in differences in risk tolerance among departments within the executive branch. One participant put it this way:

> And well, even within the executive branch we've got 35 different departments, each with varying levels of risk tolerance. So being able to enforce a policy on department X versus department Y is vastly different depending upon what their leadership thinks is important to them and what their mission is. Recreation feels like they have to provide services for ball fields and for swimming pools, etc., etc. That's what their mission is but then…you start thinking about the millions of dollars that they get in credit card transactions every year and that then becomes a big potential security risk.

A fourth governance issue is that, at least in some local governments, there are multiple networks, sometimes involving multiple local government departments and agencies, to manage. One focus group participant said that in his local government "… there are eleven, I stopped counting at eleven, different data networks, eleven different data networks. Over the years, well-meaning people patched weird connections to them that we may or may not understand and we're trying to untangle that..." Among other things, the need to manage

multiple networks produces increased organizational complexity and makes high levels of cybersecurity more difficult to achieve (Deloitte and NACSIO, 2014).

Policy: The participants told us that many cybersecurity vulnerabilities originate in the risky behavior of end-users. Among others, these behaviors include such things as choosing insecure passwords, failing to keep software updated, clicking on URLs or downloading attachments from unknown email correspondents, connecting insecure external devices to their desktops and publishing personal information online. Organizations can combat these problems by developing cybersecurity policies and implementing procedures to enforce them, by training their employees in cybersecurity best practices and by holding end-users accountable for any actions that jeopardize cybersecurity. According to one participant: "There has to be someone in charge [and]…there has to be policy…the rules of the road."

Unfortunately, not all local governments or units within them have appropriate cybersecurity policies and not all implement the policies that they have well. A common example is not enforcing rules that require users to undergo cybersecurity training. In the words of one participant: "Well, as far as security awareness is concerned, our struggle it getting it [training] to be mandatory." However, another participant said that in his county: "The county executive backed it up. People had to come to training centers." The lesson here is that local governments need rigorous cybersecurity policies and those policies need to be stringently implemented and enforced.

An important observation here is that technology is expensive, but adopting and enforcing policy, providing end-user training, and holding end-users accountable, while

certainly not free, is much less expensive. We will return to this point in the next section of this paper.

According to the participants in this focus group, funding (and staffing), governance and policy constitute substantial barriers to achieving high levels of local government cybersecurity. In the following section, we discuss actions that these practitioner-experts recommended be taken to help mitigate these barriers and improve local government cybersecurity.

Improving local governmental cybersecurity

The final set of questions we asked the focus group concerned ways to improve local government cybersecurity. Specifically, we asked what actions they believed could and should be taken to improve local government cybersecurity. As mentioned above, each of these findings can be considered valid, as there was zero disagreement between respondents. Their recommendations fell into three categories: technical, managerial and policy, and governance.

Technical: To repeat an earlier finding – technology is not the biggest problem that confronts local government cybersecurity. Nevertheless, the participants offered two technical recommendations. The first was two factor authentication and authorization, which would require all users to have to enter two separate factors in order to sign on to the IT system, say a password and a PIN. "Two factor auth" (as it is often called) makes it much more difficult for a cybercriminal, for example, to pose as an authorized user, enter an organization's IT system and

take malicious actions. Some participants strongly supported "two factor auth," but others noted that it was expensive and intrusive and users do not like it.

"Two factor auth" is more than a technical issue. It also involves a governance and policy because it would require the creation and implementation of authentication policy. In this instance, local governments would have develop rules that mandate a certain level and type of authentication, would have to develop procedures to implement these rules and would have to create mechanisms for end-user training and to ensure end-user accountability.

The second technical recommendation consisted of continually scanning and testing. (This is the only completely technical recommendation the participants made.) This recommendation calls for local IT and cybersecurity officials to be constantly aware of cyber threats and to scan for them continually. It also stresses the need to regularly access vulnerabilities in local government IT systems and to test these systems' capacity to prevent cyberattacks and to recover from attacks that are successful. These findings mirror those seen in the 2016 Deloitte and NASCIO survey in which 90 percent of respondents indicated audit logs and security event monitoring to be a top function of a CISO, along with incident management (90 percent) and vulnerability management (88 percent).

Managerial and Policy: As we noted earlier, the focus group participants unanimously agreed that the end-user was the major problem for local governments to be able to maintain high levels of cybersecurity. As a result, their first recommendation was that local governments need to do a much better job providing user training in proper cybersecurity techniques and procedures, in establishing and enforcing policies to control end-users and, finally, in holding

end-users them accountable for their actions. Over half (53 percent) of respondents in the Caruson, et al., survey said that better user awareness and training were needed in their governments (2012a), and 96 percent of respondents in the 2016 Deloitte and NASCIO survey indicated awareness and training to be a top function of CISOs.

Related to this, the group strongly suggested that local governments impose tighter control over external devices. Here, participants noted that end-users inadvertently upload dangerous files to the governmental unit's IT system through personal flash drives, tablets, smart phones and the use of Dropbox. Policy and policy enforcement lag behind the use of external devices and need to catch up in order to help prevent breaches resulting from their use.

To repeat the point we made in the previous section, creating policy and enforcing it, providing end-user training and holding end-users accountable is much less expensive than the cost of cybersecurity technology. And, while we would not advise local governments to invest less than is warranted in cybersecurity technologically, addressing management and, especially end-user behavior, is likely to be highly cost-effective in preventing end-user error, the biggest cybersecurity challenge that local governments face.

Second, the participants noted that local governments must improve the assessment of their cybersecurity vulnerabilities. We asked whether their governments formally and continually assessed their cybersecurity vulnerabilities. The response was that most did so, but only an on ad hoc basis. Moreover, when they did assess vulnerabilities, it was more of an audit than a formal assessment. Caruson, et al., found that only 46 percent of counties in

Florida had conducted risk assessments (2012a). Now, it seems as if focus has shifted toward constant monitoring of threats and incidents and the management thereof.

Third, participants recommended that local governments consider cybersecurity insurance, which is intended to provide financial remuneration to mitigate losses from cybersecurity incidents such as data breaches, business interruption and network damage (DHS, 2014). One participant noted that local governments across the nation are beginning to buy cybersecurity insurance and observed that, at least as of the date of the focus group meeting, this insurance was relatively inexpensive. Acquiring such insurance also affords a local government the opportunity to conduct a formal risk assessment, because doing is part of the insurance application process for these programs.

Fourth, participants noted that there is an abundance of information about cybersecurity, especially information about threats and best practices. Indeed, there is so much information, one participant noted, that the sheer amount could be overwhelming. Therefore, he suggested the creation of a clearinghouse that would be able to collect information on cybersecurity, triage it and would know how to and to whom to circulate it.[14]

Fifth, the most overarching recommendation the participants made concerned the need for local governments to create a culture for cybersecurity. This would be a culture in which all parties, especially end-users, but also elected officials and top managers, would understand

[14] This could be prohibitively expensive in an already highly constrained state and local government fiscal environment.

and embrace the need for high levels of cybersecurity, would be well trained in appropriate cybersecurity policies and techniques, would practice cybersecurity, and would be held accountable for their actions regarding cybersecurity. As one participant noted, it is about organizations being aggressive, not passive, toward cybersecurity.

Last, although this was not an explicit recommendation, it followed from earlier discussion by focus group members. Local governments should consider outsourcing cybersecurity. The participants agreed that IT and cybersecurity are increasingly becoming commodities or services that can be procured through various qualified organizations. Large, sophisticated technology companies like Google, Amazon and others, for example, really do have thousands of security engineers, while the average local government (even a large local government with a sizeable budget) may have only a few. As a result, outsourcing local cybersecurity may increasingly make practical as well as budgetary sense.

Governance: The constitutional separation of powers, imbedded in the American governmental system, poses an important challenge to local cybersecurity. And, this challenge is likely going to be difficult to address effectively. This is because IT and cybersecurity officials in the executive branch do not have the legal authority to control the cybersecurity policies and practices in the legislative and executive branches. This, then, constitutes an area in which policy and practice must be modified in order to provide appropriate authority to IT and cybersecurity officials to enable them to exercise control over all IT assets for which they are responsible. Although there has been a decreasing emphasis on executive buy-in, as seen in the 2016 Deloitte and NASCIO biennial surveys, the relationship between the executive and CIO

or CISO is significant as there has been a marked increase in those who report monthly to the executive (29 percent).

At least two possible paths exist to address this governance issue. First, officials from all three branches could work together cooperatively to agree upon common cybersecurity policies and procedures and on methods to implement them. Then, they would also have to agree on which entity or entities in the local government would have the authority to enforce those policies and procedures. A second path would be for the executive branch to establish the cybersecurity "rules of the game" for all IT activity over which it has responsibility, regardless of branch of government, and insist that those rules be followed. If the other branches failed to "follow the rules," then the executive branch would have the right to either a) hold the offending unit accountable through some means (e.g., suspension of computer privileges) and/or b) withdraw its support of the other branches' IT operations altogether. Either path would provide the executive branch with a powerful tool to ensure that the legislative and judicial branches follow policy and procedure. Either path should also produce improved cybersecurity local government-wide, although the latter path is potentially more conflictual.

Conclusions, Implications and Future Research

The results of this focus group with expert state and local government IT and cybersecurity practitioners in one American state found that the computer systems of their

governments are under constant cyberattack and that attacks can range in the tens of thousands or more per day. Indeed, cyberattacks are now so common that they viewed by these practitioners as "routine." We also found that at least some cyberattacks will inevitably be successful, if only because of the sheer number of attacks and the high mathematical probability of their success.

A particularly important finding of this research is that the technological side of the cybersecurity equation is not most problematical for local governments. Instead, it is the human element – people are the weakest link. By this, the participants meant that either because of carelessness, lack of training, lack of attention to training or (rarely) malice, some governmental employees will inevitably take actions that will compromise cybersecurity. The most common actions among these include opening dangerous URLs or file attachments or attaching external devices with malware on them to the local government's IT system. This finding is not new or novel – indeed, it has been common knowledge for some time among IT and cybersecurity professionals.

What is not known from this findings -- and something that should be the subject of further research – is the extent to which top elected and appointed local government officials and end-users themselves understand that end user error (or malice) poses perhaps the most serious threat to the security of local government IT systems. So serious, indeed, is this threat that it is incumbent on top local officials to ensure that proper policies and procedures are adopted and enforced to minimize end-user error (and malice) that can compromise local government cybersecurity.

We also note a possible missing element from these practitioner-experts' recommendations. They did not make suggestions about increasing funding for cybersecurity. The absence of such a recommendation is interesting because the focus group participants cited lack of funding as the top barrier to their ability to achieve high levels of cybersecurity. The data from the focus group do not allow us to know why they did not make a recommendation regarding funding. Based on our knowledge of and experience with US local governments, however, we can speculate that, as local government professionals, our participants constantly operate in a world of budgetary constraints. As such, they have may well have become accustomed to "muddling through" and "satisficing." As professional managers, part of their job if not also part of their ethic is to find the best ways possible to ensure the security of their systems within the limits of the available funding. Our speculation here, of course, should be subject validation through further research.

The principal implications of these findings, thus, involve management and policy, and less so technology. The IT and cybersecurity practitioner-experts in our focus group clearly felt that they had the technical aspects of cybersecurity reasonably well in hand. They also knew that they must be constantly vigilant to ensure that their cybersecurity technology keeps pace with that of the cyber criminals who place them under constant attack.

The main efforts by local governments to improve cybersecurity, our participants argued, therefore, should be in end user training and control, vulnerability assessment, cybersecurity insurance, outsourcing cybersecurity, creating an organization-wide culture of cybersecurity and addressing the problem of federated government as it affects cybersecurity.

As we noted earlier, because this focus group was conducted among a few IT and cybersecurity officials (albeit expert practitioners) in a single American state, our findings cannot be generalized. However, we suspect that these findings will resonate among local IT and cybersecurity officials in local governments around the nation, if not also the world (see also, Vicsek, 2010). These findings also suggest the need for further and more in-depth research into local government cybersecurity, which, based on our in-depth review of the literature, to date has been the subject of few systematic studies.

We believe that such research should be directed to at least the following areas:

- The types of cyberattacks that local governments face and how they change over time;
- The types of policies and practices that local governments adopt to prevent the attacks from being successful;
- Any gaps between those policies and practices and their success in preventing breaches;
- The types of policies and practices that local governments adopt to mitigate the results of successful attacks;
- Gaps between these governments' need to prevent and mitigate cyberattacks and their ability to do so;
- Barriers faced by local governments in their ability to achieve high levels of local cybersecurity;
- Best cybersecurity practices; and
- Recommendations for improving local government cybersecurity technology, policy and practice.

Research into local government cybersecurity can and probably should be undertaken using several a variety of research methods, including but not limited to surveys, case studies, focus groups, and the quantitative analysis of large sets of local cybersecurity data, if and when

such data sets may become available. Such research could also benefit from a multi-disciplinary approach, for example combining information and computer scientists with social scientists and management scientists. In the end, however, we urge researchers not to be overly concerned about methods and teams at this early point in local government cybersecurity research, but, instead, to move forward to conduct local government cybersecurity research that is theoretically sound and that will produce results that are both valuable to scholars and that will also be of practical utility to local governments.

References

Ablon, Lillian, Martin C. Libricki, and Andrea A. Golay. 2014. Markets for cybercrime tools and stolen data: Hackers' Bazaar. Santa Monica, CA: Rand Corporation. Accessed January 11, 2015 at: http://www.rand.org/pubs/research_reports/RR610.html.

Almarabeh, T. & AbuAli, A. 2010. A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success. *European Journal of Scientific Research.* 39(1): 29-42.

Blinder, Alan, and Nicole Perlroth. 2018. March 27. A Cyberattack Hobbles Atlanta, and Security Experts Shudder. New York, NY: *New York Times.*

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.

Center for Strategic and International Studies. 2014 (June). *Net Losses: Estimating the Global Cost of Cybercrime.* A report prepared for the Center by McAfee. Accessed September 21, 2014 at: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

[redacted]

Cyr, Jennifer. 2016. The Pitfalls and Promise of Focus Groups as a Data Collection Method. *Sociological Methods and Research.* 45(2): 231-259.

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-nascio-cybersecuritysurvey_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-cybersecurity-study/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf.

Dixon, Chris. 2014. "Deltek: State. Local government IT spending increase is an opportunity for contractors." Washington Post, August 24, 2014. Accessed May 3, 2016 at: 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.

Ebrahim, Z. & Irani, Z. 2005. E□government adoption: architecture and barriers. *Business Process Management Journal*. 11(5): 589-610.

Finklea, Kristin, and Catherine A. Theohary. 2015 (January). *Cybercrime: Conceptual issues for Congress and U. S. law enforcement.* Washington, D.C.: Congressional Research Service. Accessed Fevruary 11, 2015 at: fas.org/sgp/crs/misc/R42547.pdf.

Gil-Garcia, J. R. & Pardo, T. A. 2005. E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly*. 22(2): 187-216.

Groff, J., and P. Weinberg. 2010. *SQL: The Complete Reference. (3rd Ed.)* New York: McGraw-Hill.

Gudkova, D., Vergelis, M., Demidova, N., and T. Scherbakova. 2016. Spam and phishing in Q1 of 2016. Securelist,Accessed October 18, 2016 at: https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/.

Halchin, L. E. 2004. Electronic government: Government capability and terrorist resource. *Government Information Quarterly*. 21(4): 406-419.

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.

Kidd, P.S., & Parshall, M. B. 2000. Getting the Focus and the Group: Enhancing Analytical Rigor in Focus group Research. *Qualitative Health Research.* 10(3):293-308.

Lambrinoudakis, C., Gritzalis, S., Dridi, F., & Pernul, G. 2003. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications*. 26(16): 1873-1883.

Liamputtong, Pranee. 2011. *Focus Group Methodology.* Los Angeles: Sage Publications.

Malashenko, E., Villarreal, C. and J. D. Erickson. 2012. *Cybersecurity and the Evolving Role of State Regulations: How it Impacts the California Public Utilities Commission Grid Planning and Reliability Policy Paper.* Accessed October 18, 2016 at: http://www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=3314.

Morgan, David L. 1996. Focus Groups. *Annual review of Psychology.* 22(1): 129-152.

[redacted]

Perez, T. J. 2014. (January). *Municipal E-Government Security: Insights from a Study of Orange County, California*. Lecture presented at 47th Hawaii International Conference on System Science, Waikoloa, HI. Accessed September 23, 2016 at: http://ieeexplore.ieee.org/document/7070085/.

Ponemon Institute. 2015. 2015 Cost of Cyber Crime Study: Global. Accessed August 30, 2016 at: http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states

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

Privacy Rights Clearing House. Data Breaches. 2016. Retrieved September 23, 2016, from https://www.privacyrights.org/data-breaches?title=&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=257&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306.

Rector, Kevin. 2018 (March 27). Baltimore 911 dispatch system hacked, investigation underway, officials confirm. Baltimore, MD: *Baltimore Sun.*

Stewart, D. W.. Shamdasani,P. N., & Rook, D. W.. 2007. *Focus Groups: Theory and Practice.* 2d ed. Thousand Oaks, CA, Sage Publications.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., & Vigna, G. 2009. Your botnet is my botnet: analysis of a botnet takeover. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*. November 9-13, 2009. Chicago, IL.

U. S., Census Bureau. 2012. *2012 Census of Governments*. Accessed February 8, 2015 at: http://www.census.gov/govs/cog/

U. S., Department of Homeland Security. National Protection and Programs Directorate. 2012 (November). Cybersecurity *Insurance Workshop Readout Report*. Accessed September 17, 2014 at: http://www.dhs.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf .

U. S., Federal Bureau of Investigation. 2014. *GameOver Zeus Botnet Disrupted.* Accessed February 13, 2015 at: http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted.

U.S., Navy. 2012. (November). *Navy Cyber Power 2020*. Accessed September 23, 2016 at: http://www.public.navy.mil/fccc10f/Strategies/Navy_Cyber_Power_2020.pdf.

Verizon. 2013. 2013 Data Breach Investigations Report. Author. Accessed January 21, 2014 at:

http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Vicsek, Lilla. 2010. Issues in the Anaslysis of Focus Groups: Generalisability, Quantifiability, Treatment of Context and Quotations. *The Qualitative Report.* 15(1): 122-141.

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.

Responses to reviewer's questions:

We want to thank the reviewers for their constructive and helpful comments. Here are our responses to the issues that they raise.

Reviewer #1

1. The reviewer observes that practitioner perspectives may have evolved considerably since the focus group was conducted. While we concur that this is certainly possible, we would note that the findings of a nationwide survey of local government cybersecurity that we completed in late 2016 were highly consistent with the results of this focus group. Moreover, while some specifics around attacks change (5 years ago it was one kind of attack, today it may be a different one), some of the fundamental issues that the focus group raised are unlikely to have changed. For example, today local government policies and budgets are as big or bigger an issue for them than technology, especially dealing with end user education. Better assessment of vulnerabilities remains fundamental. The need for consideration of cybersecurity insurance and for creating a cyber culture both remain important.

   Additionally, we would argue that the results of the focus group on state and local government cybersecurity, even one conducted in 2013, should be valuable to *scholars* because of the dearth of scholarly literature in this field.
2. The reviewer states that the title of the paper implies "…that the challenge of cybersecurity for state and local governments rests solely on website security throughout." We certainly did not mean to imply this and have changed the title to reflect same.
3. The reviewer states that we claim that there is a gap in the professional literature about state and local government cybersecurity. This is not the case. We claim, correctly so based on our extensive literature review, that there is a gap in the *scholarly* literature. We are aware the considerable professional literature that is relevant to state and local government cybersecurity and have endeavored to bring it more up to date by discussing additional relevant works in the revised literature review.
4. The reviewer states that we completely bypassed the literature on cybersecurity risk management in governmental contexts. With respect, we disagree. Our literature review found no *scholarly* literature at all on this subject. And none of the professional reports and the like that we identified focused on local governments. In 2014 the U.S. National Institute of Standards and Technology (NIST) published a voluntary Framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risk. Version 1.1 of the Framework was released in April 2018. These documents cover the broad spectrum of cybersecurity risk management with a focus on assessing cybersecurity risks and the ecosystem of cybersecurity tools and guidance on their use. The framework is intended to apply to a wide variety of organizations of any size and in any sector of the economy or society, including companies, government agencies, and not-for-profit organizations. Consequently, it does not specifically address many of the

special issues that arise in many local governments. See NIST, 2018, 2018 (April 16) and 2014.

5. The reviewer notes that "…significant aspects of cybersecurity for state and local governments…go unaddressed…" We agree, but note that our source data (the words of the focus group participants) did not address the aspects of cybersecurity noted by the reviewer. Therefore, we could not report on them as findings. In the revision, we note that one of the limitations of focus group research is that scholars are unable to go beyond the actual results of the focus group participants and may necessarily, therefore, miss certain aspects of the issue under investigation.

6. Last, we concur with the reviewer's suggestion that the focus group be repeated at perhaps five year intervals and look forward to doing, although probably not this year due to other scholarly commitments including completion of papers from the data from our nationwide survey.

Reviewer #2

1. The reviewer asked us to "update to include the City of Atlanta breach and its implications," which we have done in the introduction, and we also included the Baltimore breach.
2. The reviewer asks for tables from the focus group data "…to identify a typology of types of attacks and then the manor issues, management needs for each." Unfortunately, the focus group, which lasted approximately two hours, did not produce sufficient information to enable us to create such a typology. This must be left to future research.
3. The reviewer notes, correctly, that organizations only know about the cyberattacks that they catch. This is a very good point, and we addressed it in the location the reviewer mentions.

References

National Institute of Standards and Technology. 2018. Cybersecurity Framework State, Local, Tribal and Territorial Perspectives. Accessed June 1, 2018 at: https://www.nist.gov/cyberframework/perspectives/state-local-tribal-and-territorial-perspectives

U.S. NIST, NIST Roadmap for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 12 February 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

U.S. NIST, Framework for Improving Critical InfrastructureCybersecurity, Version 1.1, National Institute of Standards and Technology, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf