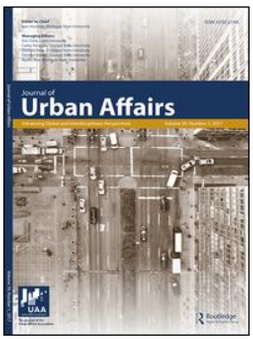

Journal of Urban Affairs

ISSN: 0735-2166 (Print) 1467-9906 (Online) Journal homepage: https://www.tandfonline.com/loi/ujua20

Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity

Donald F. Norris, Laura Mateczun, Anupam Joshi & Tim Finin

To cite this article: Donald F. Norris, Laura Mateczun, Anupam Joshi & Tim Finin (2020): Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity, Journal of Urban Affairs

To link to this article: https://doi.org/10.1080/07352166.2020.1727295

Published online: 17 Apr 2020.

JOURNAL OF URBAN AFFAIRS
https://doi.org/10.1080/07352166.2020.1727295

Routledge
Taylor & Francis Group

Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity

Donald F. Norris, Laura Mateczun, Anupam Joshi, and Tim Finin

University of Maryland, Baltimore County

ABSTRACT

This paper, based on data from the first nationwide survey of cybersecurity among local or grassroots governments in the United States, examines how these governments manage this important function. As we have shown elsewhere, cybersecurity among local governments is increasingly important because these governments are under constant or nearly constant cyberattack. Due to the frequency of cyberattacks, as well as the probability that at least some attacks will succeed and cause damage to local government information systems, these governments have great responsibility to protect their information assets. This, in turn, requires these governments to manage cybersecurity effectively, something our data show is largely absent at the American grassroots. That is, on average, local governments fail to manage cybersecurity well. After discussing our findings, we conclude and make recommendations for ways of improving local government cybersecurity management.

Over the past few years, cybersecurity has become an essential function within organizations because organizations of nearly all types and sizes are under constant cyberattack and routinely experience breaches (e.g., Verizon, 2019 Data Breach Investigations Report, DBIR).[1] In this paper, we use data from the first ever nationwide survey of cybersecurity among local governments in the United States (which are sometimes referred to as grassroots governments) to conduct an exploratory analysis of these governments' management of cybersecurity. We chose local governments for this study because they are under constant or nearly constant cyberattack, are often breached (Norris, Mateczun, Joshi, & Finin, 2018, 2018), and because cybersecurity among these governments has not been the subject of much scholarly study to date. As we note in the methods section below, most of the local governments in our sample were "urban" governments. As a result, this paper should be of interest to readers of the *Journal of Urban Affairs*.

Among the local governments responding to our survey, 28% reported being attacked at least hourly and 19% said at least once a day, for a total of 47% (Norris et al., 2018).[2] In related study, all of the local government participants in a focus group that we conducted said that their organizations were under constant cyberattack (Norris et al., 2018). Due to the frequency of cyberattacks, as well as the probability that at least some attacks will succeed and cause damage, local governments have great responsibility to protect their information assets. This, in turn, requires these governments to manage cybersecurity effectively, something that we show in this paper is largely absent at the American grassroots.

To assist with this study, we conducted an extensive literature review to identify and examine relevant works on this subject from scholarly, professional and popular media sources. As we show in that review, there are very few publications of any kind, especially scholarly works, on local government cybersecurity. This said, since at least the 1980s, if not earlier, scholars from various academic disciplines, have shown that "management matters" in the world of information technology (IT) in local government.

CONTACT Donald F. Norris norris@umbc.edu School of Public Policy, University of Maryland, Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250.

(See, for example Kraemer & Dedrick, 1997; Kraemer, King, Dunkle, & Lane, 1989; King & Kraemer, 1985).

More recently, scholars and professionals in the fields of computer science, information technology, and cybersecurity have concluded that management matters for cybersecurity as well. Indeed, it is now common for cybersecurity experts and practitioners, for example, to strongly recommend that the CEOs, corporate board members, and top managers of private sector organizations understand the need for and fully support cybersecurity in their organizations (e.g., Buszta, 2003; Gibson, 2015; Merko & Breithaupt, 2014; Whitman & Mattord, 2010; Wood, 2010). These experts also argue that top officials must play key roles in creating and maintaining what is also commonly known as a "culture of cybersecurity" throughout their organizations (e.g., Norris et al., 2018, 2018).

While such recommendations have been directed mainly at top officials in private sector organizations, we believe that they apply equally to the chief elected officials, elected legislators and top appointed managers of America's local governments. This is because without these officials' full support, the management of cybersecurity and, therefore, cybersecurity outcomes, will likely be less than optimal.

The successful ransomware attacks in March 2018 on the city of Atlanta, Georgia, and in May 2019 on the city of Baltimore, Maryland, are but two of many examples that could be cited to show an alarming lack of awareness of and support for cybersecurity among American local governments. After her city's IT systems were held hostage for several days by a ransomware attack, Atlanta Mayor Keisha Bottoms said that while cybersecurity "had not been a top priority before, 'it certainly has gone to the front of the line'" (Blinder & Perlroth, 2018, p. 3).[3] In the Baltimore case, only a few months prior to the attack, the city's chief information officer (CIO) had told the city planning commission of a number of serious weaknesses in the city's cyber management and noted that Baltimore was "woefully behind in cybersecurity capabilities, staff needs and infrastructure" (Duncan & Zhang, 2019).

As we demonstrated in an earlier paper, additional reasons exist to be concerned about cybersecurity at the grassroots (Norris et al., 2018). These include at least the following: (1) America has many local governments—90,000 in total including nearly 39,000 that are general purpose governments (Census Bureau, 2018) that annually spend billions of dollars each year to support their IT functions (Dixon, 2014). (2) America's local governments store considerable amounts of sensitive and potentially valuable information, especially personally identifiable information (PII), that is vulnerable to exfiltration. (3) Entities that engage in cyberattacks have become increasingly successful in hacking both private and public sector organizations, and the number of cyberattacks grows annually (Accenture, 2019). (4) Cybercrime is very costly to the United States and world economies and is estimated to exceed $6 trillion annually by 2021 (Morgan, 2019). (5) The Internet of Things (IoT) is a rapidly expanding phenomenon that introduces new vulnerabilities and risks for local governments in the movement toward smart cities, especially because of the increasing number of devices (including personal devices) connected, often not securely, to local networks as well as increasing local government use of social media (e.g., Li & Liao, 2018). And, (6) as we discuss in the literature review that follows, there is an enormous gap in the scholarly literature on the subject of local government cybersecurity that, as scholars in this field, we believe needs to be addressed.

It is, therefore, important to understand how local governments manage cybersecurity and how effective (or not) they are at it. Understanding cybersecurity management at the grassroots will enable us to make recommendations that local governments can act upon to achieve high levels of cybersecurity.

Literature review

We conducted an extensive search for works about local government cybersecurity in journals in the social sciences and computer science between 2000 and July 2019. Through this review, we were able to identify only five articles from the social sciences and two from computer science that addressed local government cybersecurity (Caruson, MacManus, & McPhee, 2012a, 2012b; Fusi & Feeney, 2018;

Ibrahim, Valli, McAteer, & Chaudhry, 2018; Kesan & Zhang, 2019; Wolff & Lehr, 2018; Zhao & Zhao, 2010). However, only one of them is directly relevant to the research into local government cybersecurity management (Caruson et al., 2012a).[4]

Caruson et al. (2012a) examined results from a survey conducted among 466 local government officials in the state of Florida's 67 counties. The survey produced a response rate of 24%. Of particular interest was the impact of agency size on various cybersecurity issues. The median number of employees of agencies surveyed was 750. This number determined the dividing line between a larger or smaller institution, with more than half of respondents residing in a small agency (54%), which in turn reflects the overall population of the county. Administrators from larger agencies, and therefore more populous counties, were more likely to perceive malicious insider attacks, system penetration, DNS attacks, and phishing as more significant of a threat than administrators from smaller agencies. However, sources of attack and perception of increased threat of terrorism over natural disaster (69%) did not vary by agency size. Fewer than half of officials (48%) reported that their governments had adopted cybersecurity policies and standards countywide, had conducted a risk assessment (46%), or had a cyberattack response plan in place (22%). Respondents also reported a number of pressing cybersecurity needs, including better end-user awareness and training (53%), better access controls (53%), and acceptable use policies for end-users (51%). More than half (60%) said that the main barrier to achieving better cybersecurity was lack of funding. Insufficient training came in second (43%), followed by the need for personnel with more expertise (37%). Responses to these activities and priorities did not vary due to agency size, and, as we show later, are highly consistent with the findings from our research.

Since we were unable to find much scholarly literature on local government cybersecurity management, we examined scholarly research from related areas that bear directly on this subject. Here we found research that began in the 1980s and that since has focused on computing and IT, e-government and most recently cybersecurity among local governments. In a ground-breaking study of management of computing in organizations, King and Kraemer (1985) tested the then widely accepted belief that "computing is manageable in a rational manner" (p. 12). They examined "a much larger set of variables … in keeping with the view of computing as a 'package' consisting of many interrelated parts, rather than simply a tool consisting of hardware and software techniques" (p. 14). In particular, they "investigated the relationships between the characteristics of organizations, the policies used to manage computing, and the benefits and problems of computing in those organizations" (p. 14). They found that the management of computing itself was one of, if not the most important, variables affecting computing in local governments.

In a later study, Kraemer et al. (1989) noted that prior literature had held that technological advancement was the prime driver of computing in organizations and that literature gave little consideration to the role of managers and management. What their research discovered, however, was that external forces played little role in computing outcomes. Instead, management played an overarching role. They went on to conclude that management action was the single most important factor for computing in organizations.

Additional works by Kraemer and his associates between the early 1980s and the 2000s routinely found evidence of the importance of management in computing. For example, in a 1997 review of the public administration literature between 1981 and 1995, Kraemer and Dedrick again observed the importance of management to computing in local governments. To give but one example, the application of IT in local and state governments can be significantly affected by actions of management. This was true even though many of their works also showed how complex and difficult managing computing in organizations could be (e.g., King & Kraemer, 1985).

Thus, by the late 1980s, the message, at least among social science scholars, was that management is critical to computing development and success. Indeed, today, King and Kraemer advocate for a greater role for the information systems community in the creation of policy to help ensure desired management outcomes (2019). This message also resonated with scholars who followed in the footsteps of Kraemer and associates to examine the adoption of PCs by local governments and

their adoption of e-government (e.g., Holden, Norris, & Fletcher, 2003; Moon & Norris, 2005; Norris, 2010, 1984; Norris & Campillo, 2002; Norris & Kraemer, 1996; Norris & Moon, 2005; Norris & Reddick, 2013; Reddick & Norris, 2013). One of the principal findings of the latter studies is that professionally managed local governments (versus those with elected chief executives) generally are more advanced in their adoption and use of PCs and e-government and have arguably better PC and e-government use outcomes.

It is also common among scholars and practitioners in the information systems field to argue that management matters. For example, managers need to understand and participate in IT decisions because those systems affect the entire enterprise and also to ensure that these decisions have the necessary support, funding and other resources necessary to succeed (e.g., Laudon & Laudon, 2014; Pearlson & Saunders, 2006). Likewise, the importance of management to the achievement of high levels of cybersecurity in organizations is widely accepted and highly recommended by authors in this field (e.g., Whitman & Mattord, 2010).

In the foreword to Whitman and Mattord's text, long-time information security consultant Charles Cresson Wood wrote that his experience conducting risk assessments of more than 125 different organizations around the world led him to conclude that, regardless of type, size, sector, or other characteristics of organizations, management is not sufficiently well informed about or committed to cybersecurity. This is partly because cybersecurity is a new field that competes with (and often loses to) other organizational needs. Nevertheless, Wood argued that top executives and managers should understand and fully support cybersecurity and should not allow information security to be the domain of technologists alone (See also Wood, 2005, 2016).

Here are but a few of many examples of writers in the field of cybersecurity who echo Wood's observations. Buszta (2003) argued that the chief executive and the company board of directors (analogous to the chief elected officials, elected legislators and top appointed manager of local governments) must be committed to information security. If they are not, then this can result in the likely failure of information security. According to Merko and Breithaupt (2014), effective cybersecurity requires sponsorship from the top of the organization in order to be successful. Last, Gibson (2015) has argued that top managers must be committed to cybersecurity because in the absence of their commitment others in the organization will realize that it is not valued and may act accordingly.

It seems clear from prior research on IT and e-government among local governments that management is highly important to positive IT, e-government outcomes. More recent works by scholars and practitioners in the fields of IT and cybersecurity make the same argument for management of cybersecurity in organizations. By extension, we expect that the same will be true of local government cybersecurity. That is, management matters to cybersecurity among those organizations as well.

Research methods and data

This paper is an exploratory study. Exploratory research allows scholars to investigate little known and/or understood phenomena. In our case, little is known about the management of cybersecurity in American local governments because it is an understudied area. One strength of exploratory research is that it can provide a foundation for better understanding of such phenomena. In this paper, for example, we have found several factors that may help to explain why cybersecurity is not well managed in local governments. Scholars who engage in studies of local government cybersecurity in the future will be able to compare and contrast their findings with the benchmarks from this study. Researchers can build from this groundwork and utilize our results to create robust research designs and methods. Exploratory research also allows scholars to raise new research questions and hypotheses. Last, exploratory studies can use various research methods including case studies, interviews, surveys and quantitative data.

Of course, this method also has limitations. Researchers cannot, for example, test hypotheses nor establish causality. Bias in the interpretation of results is also possible. Therefore, it should be emphasized that results are preliminary in nature. (See, for example, Stebbins, 2001; Swedberg, in press).

To produce the data for this study, we partnered with the International City/County Management Association (ICMA) for a nationwide survey of local government cybersecurity. ICMA is the premier membership organization of local government professionals in the United States and is widely recognized for its research into many aspects of local governance, including IT. ICMA also has a survey capability that is unsurpassed in reaching local governments in America (ICMA, 2019).

In cooperation with staff at the ICMA and an advisory group of local government IT and cybersecurity professionals within our home state of Maryland, we drafted the survey instrument based on the limited available scholarly literature on local government cybersecurity as well as the more numerous works from the professional practice that were particularly relevant to this paper.

We then submitted the draft instrument for review and comment to a volunteer advisory group that we had created to assist in this project. The group consisted of the IT directors, CIOs, Chief Technology Officers (CTOs), and Chief Information Security Officers (CISOs) or equivalent officials in 10 cities and counties in Maryland, as well as the CIO and CISO of our university. After receiving comments and suggestions from these advisors, we revised the instrument. ICMA then pre-tested the instrument, and we made appropriate adjustments to it. The process we used to develop the instrument creates face validity for the instrument, and we are confident that, on the whole, questions in it produce reliable data.

The instrument examined a wide range of local government cybersecurity issues. For the purposes of this paper, we focused on issues related to management.

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

This produced a final response rate of 11.9% (n = 406 local governments). While this may seem a rather low response rate compared with previous surveys of IT at the local government level (e.g., Norris & Reddick, 2013; Reddick & Norris, 2013), we identified two potential reasons for this rate. The first is that there has been a substantial decline in response rates to surveys in recent years (e.g., Anseel, Lievens, Schollaert, & Choragwicka, 2010), one that ICMA has also experienced (Evelina Moulder, 2013, personal message from the survey manager of ICMA). A second reason we learned from phone calls made by our research assistants. Here, a number of IT and cybersecurity officials said that they would not respond because their responses might reveal sensitive information about their governments' cybersecurity problems and practices, something that they would not do.[5]

We can have some degree of satisfaction that a response of 406 to a random sample of 3,400 local governments would have produced a margin of error of 5% at a confidence level of 95%. Clearly, however, ours was not a random sample, but rather a population survey. As a result, we must be able otherwise to make the case that our results should be taken seriously. Here, we ask readers to consider two factors. First, as seen in Table 1, the survey results are reasonably representative of the overall population of the local governments that we surveyed. While larger local governments are proportionately overrepresented, smaller local governments are numerically overrepresented. This is not surprising because it reflects the relative distribution of local governments in the United States. There is also some regional variation, with local governments in the Northeast and North Central regions being underrepresented and those in the South and West being overrepresented. This is probably because the occurrence of the council manager form of government is greater in the latter two regions and, as the table shows, council-manager governments were overrepresented. This is also not surprising because council-manager governments, which constituted 55% of all municipal governments in 2006, are most numerous in the southeastern and Pacific Coast states (National League of Cities, 2018).

Second, we can be confident of these survey results because the great majority of respondents (89.4%) were experienced, local government IT and cybersecurity professionals (Table 2). Thus, the men and

Table 1. Local government demographics.

	Number Surveyed	Number Responding	Response Rate (%)
	3423	406	11.9
Population Size			
500,000+	140	31	22.1
250,000– 499,999	168	26	15.5
100,000– 249,999	532	63	11.8
50,000– 99,999	939	107	11.4
25,000– 49,999	1644	179	10.9
Geographic Division			
Northeast	574	42	7.3
North Central	1048	120	11.5
South	1148	139	12.1
West	653	105	16.1
City/County			
Municipalities	1893	262	13.8
Counties	1530	144	9.4
Form of Government 1			
Elected (Mayor-Council, County Council-Elected Executive, County Commission)	1541	117	7.6
Appointed (City Council-Manager, County Administrator/Manager)	1588	276	17.4
Form of Government 2			
Mayor-Council	570	46	8.1
County Commission	685	33	4.8
County Council-Elected Executive	286	38	13.3
City Council-Manager	1035	204	19.7
County CA/CM	553	72	13.0

women who responded to this survey were knowledgeable, expert local government practitioners who "knew their stuff."

Last, we assessed the "urban-ness" of our sample to show its relevance to the readers of the *Journal of Urban Affairs*. First, nearly two thirds of the 406 local governments in the sample (260 or 64.5%) were municipalities with populations of 25,000 or greater (most of which were greater than 50,000); clearly urban areas. Second, of the 144 responding counties, 67 (or 46.5%) had populations of 100,000 or more, a threshold that suggests that at least parts of these counties are urban. Third, all but one of these counties were included in metro areas (either an MSA or a CMSA). Finally, 52 had cities with 50,000 or more residents (of which 33 had greater than 100,000) and 10 with populations of between 25,000 and 49,999. So, we can be confident that a substantial majority of the jurisdictions represented in the sample are urban.[6]

Findings

The rest of this paper is organized as follows. First, we discuss descriptive statistics around issues of cybersecurity management addressed in the paper, including the location of responsibility for cybersecurity within local governments, whether these governments outsource cybersecurity and

Table 2. Respondent profession and experience.

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

purchase cybersecurity insurance, whether their investment in cybersecurity had changed over the previous 5 years, the range of cybersecurity tools utilized by local governments, actions taken and policies adopted by them to better manage cybersecurity and, last, local officials' awareness of and support for cybersecurity.

After the descriptive statistics, we examine cross-tabulations and correlation coefficients for local government characteristics and cybersecurity outcomes to learn whether such characteristics are associated with cybersecurity management outcomes (e.g., outsourcing of cybersecurity, purchasing cybersecurity insurance, changes in cybersecurity investment, etc.). We do so because studies of local government IT and e-government over the past 30 years have consistently found associations between certain local government characteristics and IT and e-government outcomes (e.g., Norris, 1984, 2010; Norris & Campillo, 2002; Norris & Kraemer, 1996; Norris & Moon, 2005; Norris & Reddick, 2013; Reddick & Norris, 2013).

As a result, we wanted to learn if this pattern is repeated in research into local government cybersecurity. Specifically, are such local government characteristics (independent variables) as population (large v. medium and small), type of government (municipal v. county), form of government (professional administrator v. elected executive), geographic region (South and West v. Northeast and Midwest), median household income (high v. modest and low), education (percent college graduates) and percent White population (versus nonwhite) systematically related to cybersecurity management outcomes (dependent variables)? To give an example, we hypothesize that local governments with these characteristics will be significantly more likely than their counterparts to have increased their investment in cybersecurity over the 5 years prior to the survey.

Last, we provide a brief summary of our findings and conclude with recommendations to improve local government cybersecurity management.

The structure of cybersecurity management

In this section, we discuss some important structural characteristics of cybersecurity management. The first of which is the location of responsibility for cybersecurity management in these governments; that is, which local government office was in charge of cybersecurity (Table 3). Not surprisingly, cybersecurity was the responsibility of information technology departments (ITDs) for nine in 10 local governments (89.4%). In 2.8% of governments responsibility for cybersecurity resided in the top appointed manager's office; in 2.0%, in the chief elected official's office; in 0.8%, in a stand-alone cybersecurity office; and, last, in 5.1%, in some "other" office.

That cybersecurity management is housed mostly in local government ITDs is not surprising because in most local governments the ITD has responsibility for the government's IT system. Logically, therefore, the ITD should also have responsibility for protecting that system and all associated assets from cyberthreats.

Next, we asked about whether the local governments outsourced any of their cybersecurity functions. The main reasons that local governments may decide to outsource cybersecurity include: (1) their inability to hire and retain qualified cybersecurity staff due to insufficient budgetary resources, (2) to benefit from the cybersecurity expertise of organizations that specialize in this area, (3) to reduce both cost and risk, and (4) to increase the organization's focus on its core functions, and perhaps others (CivicPlus, 2018).

Although there is little data about cybersecurity outsourcing by local governments, it is increasingly common for organizations in general to outsource at least some responsibility for cybersecurity (e.g., EY.com, 2017; Landi, 2017). Nearly four in 10 respondents (39.5%) to our survey reported that their local governments either fully (8.2%) or partially (31.3%) outsourced this function (Table 4). This rate of outsourcing is consistent with that found by Deloitte and NASCIO (2018) in their surveys of state government cybersecurity and among other types of organizations (e.g., Earnst and Young, 2016; EY.com, 2017; Medical Group Management Association, 2017). It is also a much higher outsourcing rate than that reported in the Multi-State Information Sharing and Analysis

Table 3. Location of responsibility for cybersecurity management within local government.

	n	%
IT Department	353	89.4
Appointed Manager	11	2.8
Chief Executive's Office	8	2.0
Stand-Alone Department	3	0.8
Other	20	5.1
Total	395	100.0

Table 4. Does your local government outsource its cybersecurity responsibility?

	n	%
Fully Outsource	31	8.2
Partially Outsource	119	31.3
Do Not Outsource	230	60.5
Total	380	100.0

Center (MS-ISAC) 2016 Nationwide Cyber Security Review, which found that only 7% of local governments outsourced at least some cybersecurity functions (Center for Internet Security, 2017).

We also wanted to learn the office to which local governments required their cybersecurity contractor to report (Table 5). It should not be surprising that most local governments (79.1%) required their outsourcing contractor to report to one of their top technology offices almost certainly because those offices, among all offices in local governments, are likely to be the most well prepared to manage this function (ITD—33.1%; CIO or IT Director—26.4%; CISO—8.8%; and CTO—2.7%). Next came top appointed manager's office (11.5%), followed by chief elected official's office (4.7%).

In addition to outsourcing cybersecurity, local governments appear to be increasingly purchasing cybersecurity insurance to help manage this function. According to the U.S. Department of Homeland Security (DHS, 2019), cybersecurity insurance "is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage." Local governments may also consider cybersecurity insurance because doing so can result in these governments adopting technologies, policies, procedures and practices that can improve their levels of cybersecurity and also enable them to purchase better insurance coverage at lower cost (DHS, 2019). As part of the application process for cybersecurity insurance, local governments may be required to engage in cybersecurity risk management exercises. These exercises can help local governments identify cybersecurity weaknesses that they then can address, even if they do not ultimately purchase the insurance (e.g., Norris et al., 2018).

With this in mind, we asked whether the local governments had purchased cybersecurity insurance (Table 6). Slightly under half of the responding governments (44.6%) had purchased cybersecurity insurance, while just over half (55.4%) had not. Although we know of no data concerning previous rates of local government adoption of cybersecurity insurance, adoption by

Table 5. Local government office to whom outsourced contractor reports.

	n	%
IT Department	49	33.1
CIO or IT Director	39	26.4
Top Appointed Manager's Office	17	11.5
CISO	13	8.8
Elected Chief Executive's Office	7	4.7
CTO	4	2.7
Other	19	12.8
Total	148	100.0

nearly half of local governments appears impressive and likely represents a substantial increase over the past few years (Public Technology Institute, 2018). This is also at least partly so because cybersecurity insurance is a relatively new insurance product (Marvin, 2018).

We next asked those local governments that had purchased cybersecurity insurance about the extent of their coverage (Table 7). One in five (21.1%) said very little or limited coverage, one in three (36.1%) said moderate coverage, and one in four (27.0%) said most or full coverage. Just under one in six respondents (15.0%) said that they did not know the extent of their cybersecurity insurance coverage. Due to the limited space available in the survey, we were unable to probe further to learn about the coverages that these governments had secured, the elements of cybersecurity insurance they had forgone, and the cost of their policies. These should be areas for further research.

We also examined whether local governments' annual cybersecurity investment had changed over the past 5 years in each of the following areas: (1) technology (hardware and software), (2) additional staffing, (3) higher staff compensation, (4) training for staff, and (5) policies and procedures (Table 8).

In only one category, technology, did a majority of local governments (58.8%) report that their spending over the previous 5 years had increased slightly or greatly. For all others, majorities or near majorities said that spending had remained about the same: higher staff compensation—62.8%; additional staff—55.0%; training for staff—49.0%; and policies and procedures—47.9%. Few governments reported that spending in these areas actually decreased.

These findings should be understood in the context of local government budgeting and finance. First, there is rarely if ever enough money in a local government's budget to meet all needs, real and perceived. Second, local government budgets are especially sensitive to economic downturns, such as the Great Recession, when many are obliged to reduce funding to some functions and/or initiate service cutbacks. Third, arguably important things like higher salary and additional hiring, and "frills," such as travel and staff training, are often cut to preserve core functions. Last, even in good times, funding of such things as travel, training, policies, and procedures has historically been low across many if not most local governments. So, these data, especially when combined with the knowledge that local governments consider lack of adequate funding to be among the top barriers to cybersecurity, suggest anything but a robust pattern of recent investment for cybersecurity at the grassroots (Norris et al., 2018).

Table 6. Cybersecurity insurance purchase rates.

	n	%
Yes	150	44.6
No	186	55.4
Total	336	100.0

Table 7. Extent of cybersecurity insurance coverage.

Extent of Coverage	n	%
Very limited Coverage	32	21.1
Moderate Coverage	53	36.1
Most/Full Coverage	41	27.0
Don't Know	22	15.0
Total	147	100.0

Table 8. Cybersecurity investment changes over the last five years.

	Decreased Greatly/Slightly		About the Same		Increased Slightly/Greatly		Don't Know		Total	
	n	%	n	%	n	%	n	%	n	%
Technology	22	6.4	107	31.3	201	58.8	12	3.5	342	100.0
Additional Staff	39	11.5	187	55.0	100	29.4	14	4.0	340	100.0
Higher Staff Compensation	38	11.2	213	62.8	100	29.4	14	4.0	339	100.0
Training for Staff	43	12.7	167	49.0	113	33.2	17	5.0	340	100.0
Policies and Procedures	25	7.4	163	47.9	132	38.8	20	5.9	340	100.0

Cybersecurity tools, actions, and training

We next asked which of eight tools (see Appendix B for descriptions of these tools) local governments employed in their cybersecurity efforts (Table 9). In order of frequency of adoption these included: anti-virus software (83.5% had adopted); web and e-mail gateways (71.9%); virtual private networks (VPNs) (71.2%); intrusion detection and prevention systems (65.3%); next-generation firewalls (62.8%); automated malware protection systems (52.7%); network traffic analysis or network virtualization (46.6%); and multi-factor or biometric authentication (22.7%). We should take some degree of confidence in these governments' adoption of cybersecurity tools. Four tools had been adopted by about two thirds or more of governments. Half or nearly so had adopted two other tools. Yet, it might also be argued that anything short of nearly total adoption of highly recommended cybersecurity tools by local governments places the laggard governments at unnecessary risk.

In addition to tools, we wanted to learn which of a set of commonly recommended actions local governments had taken to improve their cybersecurity practice. We divide these actions into two groups: (1) actions involving testing of some sort (Table 10); and (2) actions involving training (Table 11). We initially asked if the governments had taken any of these actions at least monthly, at least quarterly, at least annually, at least every 2 years, never or if they did not know. For ease of analysis, we combined the results into four response categories: monthly/quarterly, every 1 to 2 years, never and don't know.

We report these findings in order of frequency or responding. Readers should note that not all actions should be taken at the same frequency. For example, organizations should conduct scanning and testing regularly to learn, at the minimum, their systems' vulnerabilities and whether they are under cyberattack. Indeed, some sources recommend that organizations scan at least monthly while others suggest continually (Browning, 2017; SecureWorks, 2019). Organizations should undertake other actions more or less frequently depending on such things as the risks that they face, legal requirements, contractual obligations, and whether they choose to adopt the "best practices" of cybersecurity within their organizational domain (e.g., financial institutions vs. retailers, etc.). Last, forensic services should be employed not on any schedule but, rather, after any known incident that compromises the integrity of an information system. We begin with scanning and testing.

Table 9. Cybersecurity tools utilized.

	n	%
Antivirus Software	339	83.5
Web and E-mail Gateways	292	71.9
Virtual Private Networks (VPNs)	289	71.2
Intrusion Detection and Prevention Systems	265	65.3
Next Generation Firewalls	255	62.8
Automated Malware Protection Systems	214	52.7
Network Traffic Analysis or Network Visualization	189	46.6
Multi-factor/Biometric Authentication	92	22.7
Other	18	4.4
Total	406	100.0

Table 10. Actions to improve cybersecurity (testing).

	Monthly/Quarterly		1–2 Years		Never		Don't Know		Total	
	n	%	n	%	n	%	n	%	n	%
Scanning and Testing	199	57.5	103	29.8	26	7.5	18	5.2	346	100.0
Risk Assessment	78	22.5	198	57.1	47	13.5	24	6.9	347	100.0
Technical Security Review	88	25.4	190	54.9	41	11.9	27	7.8	346	100.0
Audit of our Cybersecurity Practices	28	8.2	191	56.0	92	27.0	30	8.8	341	100.0
Cybersecurity Exercises	35	10.2	127	37.0	141	41.1	40	11.7	343	100.0
Forensic Services After Incidents or Breaches	34	16.0	44	20.7	92	43.2	43	20.2	213	100.0

Table 11. Actions to improve cybersecurity (training).

	Monthly/ Quarterly		1–2 Years		Never		Don't Know		Total	
	n	%	n	%	n	%	n	%	n	%
Cybersecurity Staff Training	66	19.2	178	51.7	72	20.9	28	8.1	344	100.0
End User Training	51	15.0	156	45.8	101	29.6	33	9.7	341	100.0
Cybersecurity Awareness Training for Local Government IT Personnel	71	20.8	164	48.0	81	23.7	26	7.6	342	100.0
Cybersecurity Awareness Training for Local Government Cybersecurity Personnel	82	24.6	137	41.0	84	25.2	31	9.3	334	100.0
Cybersecurity Awareness Training for Local Government Employees	45	13.2	159	46.8	109	32.1	27	8.0	340	100.0
Cybersecurity Awareness Training for Local Government Elected Officials	19	5.6	104	30.4	171	50.0	48	14.0	342	100.0
Cybersecurity Awareness Training for Contractors	15	4.5	45	13.4	208	61.9	68	20.2	336	100.0
Cybersecurity Awareness Training for Citizens	5	1.5	20	6.0	239	71.6	70	21.0	334	100.0
Other	1	2.3	4	9.1	12	27.3	27	61.4	44	100.0

Over half of the respondents (57.5%) reported having conducted scanning and testing on a monthly or quarterly basis. However, 29.8% said 1 to 2 years, 7.5% said never, and 5.2% did not know (totaling 42.5%).

Next, we examine the frequency with which local governments undertake risk assessments. Here, nearly eight in 10 (79.6%) reported conducting risk assessments at least every one to two years, which is probably a reasonable frequency. However, 13.5% said never and 6.9% did not know (for a total of 20.4%). Next came technical security review where slightly more than half (54.9%) said at least every 1 to 2 years. Nearly one quarter (25.4%) said monthly/quarterly, which seems to us to be rather unusual because of the nature of such reviews. Almost one in eight (11.9%) said never and 7.8% did not know (totaling 19.7%).

This was followed by the frequency of audits of cybersecurity practices, where 8.2% said monthly/quarterly and just under two thirds (64.6%) said at least 1 to 2 years. However, more than one in four (27.0%) said never and 8.8% did not know (for a total of 35.8%). Cybersecurity exercises came next, where 47.2% reported that they conducted these exercises at least every 1 to 2 years. However, 41.1% said never and 11.7% did not know (for a total of 58.8%).

We next inquired about local government use of forensic services after incidents or breaches. This question was worded poorly and, instead of time periods of use, the instrument should have asked if the local governments used forensic services after every incident or breach, after most, after a few, after none, or if such services were inapplicable. So, the best we can do here is to report these data as given and then endeavor to interpret them. About one in six governments (16.0%) said monthly/quarterly and just over one in five (20.7%) said 1 to 2 years (for a total of 36.7%). A strong plurality of governments (43.2%), however, said they never used forensic services, and 20.2% did not know (totaling nearly two thirds of governments, 63.4%).

We now address the extent to which local governments provided training for several groups in or associated with local governments. Here again frequencies will vary, although this time by audience, where those more closely associated with cybersecurity practice should receive training more frequently, but all should receive at least some training (PCI Security Standards Council, 2014). We believe, for example, that it is essential that local governments provide continuous training for cybersecurity staff so that they can stay abreast of developments in the rapidly changing field. However, it is probably reasonable to provide training less frequently to others, e.g., annual training to end-users and contractors and cybersecurity awareness training every 1 to 2 years for all categories of personnel (e.g., CivicPlus, 2018; ICMA, 2018).

We begin with cybersecurity staff training where slightly over half (51.7%) provided training to cybersecurity staff every 1 to 2 years, while 19.2% said monthly/quarterly (totaling 70.9%). However, one in five (20.9%) said never and 8.1% did not know (totaling 29.0%).

Next, we address end-user training, which we suggested above should occur at least annually. Here, 15.0% of local governments reported providing end-user training saying monthly/quarterly and close to half (45.8%) said every 1 to 2 years (totaling 60.8%). Nearly one in three (29.6%), however, said never and 9.7% did not know (totaling 39.3% or almost four in 10 of these governments).

Now we examine the frequencies by which local governments provide cybersecurity *awareness* training to various constituencies. First came cybersecurity awareness training for IT personnel (not cybersecurity staff), where 20.8% said monthly/quarterly and 48.0% said 1 to 2 years (totaling 68.8%). This frequency of awareness training seems quite reasonable. However, it is troubling that so many governments either did not offer such training or did not know (23.7% said never and 7.6% did not know—totaling 31.3%).

This was followed by cybersecurity awareness training for cybersecurity personnel where 24.6% of local governments said monthly/quarterly and 41.0% said 1 or 2 years (totaling 65.6%). This frequency of awareness training also seems quite reasonable. However, it remains troubling that so many governments either did not offer such training or did not know (25.2% said never and 9.3% did not know—totaling 34.5%). Cybersecurity awareness training for local government employees came next, with 13.2% responding monthly/quarterly and 46.8% responding 1 or 2 years (totaling 60.0%). Still, nearly one third (32.1%) said never and 8.0% did not know (totaling 40.1%, another troubling figure).

The data thus far suggest that local governments appear to be doing a decent job of providing cybersecurity training for certain categories of employees, at least as measured by the frequency of training offered. As can be seen in the remainder of Table 11, however, this is not the case for cybersecurity awareness training in other categories: (1) local elected officials (50.0% of local governments said never and 14.0% did not know, totaling 64.0%), (2) contractors of the local governments (61.9% never and 20.1% did not know, totaling 82.0%), and (3) local residents (71.6% never and 21.0% did not know, totaling 92.6%).

Cybersecurity policies

Next, we address the extent to which local governments had adopted policies that are important to effective cybersecurity management (Table 12). We also asked the governments that had adopted them to rate the effectiveness of these policies (Table 13). We discuss the policies in the order of most to least frequently adopted. Only three policies had been adopted by majorities of local governments: password creation rules (70.7%); periodic password change requirements (70.0%); and policies regarding the use of personally owned devices (54.2%). All remaining policies had been adopted by less than half of respondents: cybersecurity policy, standards, strategy or plan (40.1%); plan for recovery from breaches (27.6%); cybersecurity standards for contracts with vendors for cloud-based services (27.6%); and cybersecurity risk management plan (26.7%). These data tell us that far too many local governments have not adopted policies that are essential to managing cybersecurity.

The two policies rated highly/very highly effective by a majority of respondents, periodic password creation requirement (58.3%) and password creation rules (56.3%), were also the two most frequently adopted. However, the National Institute of Standards and Technology (NIST) has

Table 12. Cybersecurity policies adopted.

	Yes		No		Total	
	n	%	n	%	n	%
Password Creation Rules	188	70.7	78	29.3	266	100.0
Periodic Password Change Requirement	187	70.0	80	30.0	267	100.0
Personally-Owned Device Use Policy for Officials and Employees	155	54.2	131	45.8	286	100.0
Cybersecurity Policy, Standards, Strategy, or Plan	120	40.1	179	59.9	299	100.0
Cybersecurity Risk Management Plan	83	26.7	228	73.3	311	100.0
Cybersecurity Standards for Contracts with Vendors for Cloud-based Services	82	27.6	215	72.4	297	100.0
Plan for Recovery from Breaches	85	27.6	223	72.4	308	100.0

Table 13. Effectiveness of cybersecurity policies.

	Very Low/ Low		Average		High/Very High		Total	
	n	%	n	%	n	%	n	%
Periodic Password Change Requirement	19	11.3	51	30.4	98	58.3	168	100.0
Password Creation Rules	20	12.0	53	31.7	94	56.3	167	100.0
Personally-Owned Device Use Policy for Officials and Employees	25	18.8	52	39.1	56	42.1	133	100.0
Cybersecurity Standards for Contracts with Vendors for Cloud-based Services	20	27.0	27	36.5	27	36.5	74	100.0
Plan for Recovery from Breaches	24	31.6	36	47.4	16	21.1	76	100.0
Cybersecurity Policy, Standards, Strategy, or Plan	32	29.9	54	50.5	21	19.6	107	100.0
Cybersecurity Risk Management Plan	23	31.5	36	49.3	14	19.2	73	100.0

recently recommended removing periodic password change requirements because some studies have indicated they may be counterproductive to ensuring security (NIST Special Publication 800-63B Section 5.1.1.2, June 2017). The remaining policies were rated highly effective by fewer (some by far fewer) governments: policies governing personally owned devices—42.1%; policies governing vendors—36.5%; and the rest by one fifth or fewer governments.

Cybersecurity technology, practices, policies, and ability

In this section, we address whether respondents believed that their local governments had kept their cybersecurity technologies (hardware and software), practices (methods used, etc.) and policies (written or unwritten "rules" or procedures) up to date and whether they had the ability to address various cybersecurity events. These are important to know because local governments that lag behind the current state of the practice likely place themselves at greater cybersecurity risk than those at the state of the practice. Likewise, those that are not able to respond to adverse events are more likely to experience breaches, data exfiltration, ransomware attacks, etc.

Therefore, we asked whether these governments considered their cybersecurity technology, practices and policies to be state of the art, current best practice, one generation behind current best practice, more than one generation behind, or do not know (Table 14). Because only 5% of governments rated their technology as state of the art and less than 2% did so for practices and policies (1.2% and 0.9%, respectively), we collapsed the ratings of state of the art and current best practice to simply "best practice." Just over half (55.8%) rated their cybersecurity technologies as best practice, nearly three in 10 (29.2%) said one generation behind, almost one in 10 (8.9%) said more than one generation behind and only a small fraction (6.2%) did not know. This reinforces what local government cybersecurity practitioners have told us previously—that they have the technology part of the cybersecurity equation reasonably well in hand (Norris et al., 2018).

The same cannot be said of local government cybersecurity practices and policies. A plurality slightly greater than four in 10 (43.1%) said that their cybersecurity practices were best practice. Half (50.5%) said either one generation (32.2%) or more (18.3%) behind, and 6.5% did not know. Less than one third (31.1%) said that their policies were best practice, while almost six in 10 (58.5%) said either one generation (32.2%) or more (26.3%) behind, and one in 10 (10.3%) did not know. The previously noted lack of effectiveness of cybersecurity policies might be due to the fact they do not reflect today's best practices.

We next asked respondents to rate their local governments' ability to address eight potential cybersecurity events (Table 15). In our opinion, a rating of anything other than very good/excellent suggests that a policy is not sufficiently effective, leaving these governments unnecessarily vulnerable to adverse cybersecurity events. The results are decidedly poor. Only minorities of local governments rated their ability to respond to the listed events as very good/excellent: Recover from ransomware attack—just under half (48.3%); detect attacks—41.9%; detect incidents—38.2%; and the rest about one third or fewer. These data suggest that local governments' ability to respond to adverse cybersecurity events is severely lacking.

Table 14. Rate technologies, practices, and policies.

	Best Practice		One Generation Behind		More than One Generation Behind		Don't Know		Total	
	n	%	n	%	n	%	n	%	n	%
Technology	189	55.8	99	29.2	30	8.9	21	6.2	339	100.0
Practices	146	43.1	109	32.2	62	18.3	22	6.5	339	100.0
Policies	106	31.3	109	32.2	89	26.3	35	10.3	339	100.0

Table 15. Local government ability.

Ability of your local government to:	Poor/Fair		Good		Very Good/Excellent		Don't Know		Total	
	n	%	n	%	n	%	n	%	n	%
Recover from Ransomware Attack	64	18.7	77	22.5	165	48.3	36	10.5	342	100
Detect Attacks	97	28	88	25.4	145	41.9	16	4.6	346	100
Detect Incidents	98	28.3	98	28.3	132	38.2	18	5.2	346	100
Detect Breaches	98	28.5	103	29.9	125	36.3	18	5.2	344	100
Recover from Breaches	90	26.5	79	23.2	125	36.8	46	13.5	340	100
Recover from Exfiltration of Data/Info	107	31.7	68	20.1	94	27.8	69	20.4	338	100
Prevent Exfiltration of Data/Info	146	42.9	64	18.8	85	25.0	45	13.2	340	100
Detect Exfiltration of Data/Info	168	49.3	54	15.8	70	20.5	49	14.4	341	100

Cybersecurity awareness, support, and responsibility

Three additional factors may help to explain the weaknesses in cybersecurity management among U.S. local governments. The first two are awareness of and support for cybersecurity among elected officials and top management. The third factor is the extent to which those officials embrace an important role in responsibility for cybersecurity.

Awareness of and support for cybersecurity within an organization can operate as facilitators of, or barriers to, how it practices cybersecurity. For example, if top local government officials (for present purposes this means top elected officials and top appointed managers) are aware of the need for cybersecurity and provide high levels of support for it, then their governments will be more likely to be able to establish and maintain high levels of cybersecurity.[7] Here, we focus only on whether officials provided high levels of awareness and support (moderately/exceptionally aware in the table) because anything else, we argue, suggests the opposite (i.e., inadequate levels of support).

Respondents reported that top appointed managers possessed the greatest cybersecurity awareness in their organizations—61.7% moderately/exceptionally aware (Table 16). However, respondents also reported that one third (33.0%) were not aware, slightly aware or only somewhat aware of cybersecurity. Next in order were department managers at 42.3% moderately/exceptionally aware. This was followed by the average end user (33.4%) and all others falling below one third.

We found a similar pattern regarding support for cybersecurity from each group (Table 17). Here, a bare majority of respondents (54.0%) felt that only one official, the top appointed manager, provided either strong or full support for cybersecurity, and about one third reported so for the elected executive (35.4%) and department managers (33.0%).

A common proposition in the cybersecurity field, especially in private sector organizations, is that top executives and board members must be fully engaged in and supportive of cybersecurity. They should not leave cybersecurity solely or even predominately to technologists. Thus, we asked whether top elected and appointed officials in American local governments believed that responsibility for cybersecurity lies mainly with technologists or if these officials felt that there was an important role for them to play in cybersecurity (Table 18). Not surprisingly, respondents said that, for the most part, top elected and appointed officials believed that cybersecurity belonged mainly with technologists: top elected officials (67.3%) and top appointed officials (57.3%). Respondents also reported that only 9.3% of top elected officials and 17.0% of top appointed officials felt that there was an important role in cybersecurity for them.

Table 16. How would you rate the cybersecurity awareness of each of the following in your local government?

	Not/Slightly Aware		Somewhat Aware		Moderately/Exceptionally Aware		Don't Know		Total	
	n	%	n	%	n	%	n	%	n	%
Top Appointed Managers	47	14.0	64	19.0	208	61.7	18	5.3	337	100.0
Department Managers	76	21.3	117	32.8	151	42.3	13	3.6	357	100.0
Elected Executives	85	27.5	82	26.5	99	32.0	43	13.9	309	100.0

Table 17. How would you rate the amount of support cybersecurity receives in your local government from each of the following?

	No/Limited Support		Moderate Support		Strong/Full Support		Don't Know		Total	
	n	%	n	%	n	%	n	%	n	%
Top Appointed Manager	51	15.7	76	23.5	175	54.0	22	6.8	324	100.0
Elected Executive	71	25.4	72	25.7	99	35.4	38	13.6	280	100.0
Department Managers	94	26.9	122	35.0	115	33.0	18	5.0	349	100.0

Table 18. Responsibility of top elected and appointed officials versus technologists for cybersecurity.

	Mainly with Technologists		Both		Important Role for Officials		Don't Know		Total	
	n	%	n	%	n	%	n	%	n	%
Top Elected Officials	224	67.3	34	10.2	31	9.3	44	13.2	333	100.0
Top Appointed Officials	189	57.3	45	13.6	56	17.0	40	12.1	330	100.0

Taken together, the data in these three tables (reporting limited awareness of and support for cybersecurity, and the lack of acceptance of cyber roles and responsibility by top elected and appointed officials) may help to explain why local governments, on average, practice cybersecurity so poorly. We return to this issue in the conclusion.

Cross-tabulations

Earlier in the paper, we hypothesized that data from the survey would show that several local government characteristics are systematically associated with cybersecurity outcomes. We ran the cross-tabulations using those characteristics (seven independent variables) against 57 cybersecurity outcomes (dependent variables) for a total of 399 individual cross-tabulations. Only 65 of the 399 cross-tabulations (16.2%) produced results that were significant at the p = <0.05% level. Moreover, the directions of these few relationships were not fully consistent with the expected pattern (only 43.1% were in the predicted direction (n = 28) while 56.9% were not (n = 37)). Additionally, the strength of the relationships, as measured by the Cramer's V statistic, was generally weak, ranging from 0.14 to 0.30., with the great majority (61 of 86) falling between 0.20 and 0.29. Only one reached 0.30.[8] Similar to Caruson et al. (2012a), associations observed in prior research on IT in government and e-government were not found here. Nevertheless, future research should continue to test for such associations in order to identify factors that will help to better understand local government cybersecurity practice.[9]

Conclusion and recommendations

The findings from a previous paper using data from our survey of local government cybersecurity showed that large fractions of these governments did not practice cybersecurity well (Norris et al., 2018). For example, many local governments did not know if they were under cyberattack or if they had been breached; did not count or catalog attacks, incidents, or breaches; and could not determine the types of attackers against their systems. They also were not well prepared in several important cybersecurity arenas such as detecting and recovering from breaches and data exfiltrations.

The data in this paper enable us to hypothesize that one almost certain reason for such poor cybersecurity practice is that, on average, local governments do not manage cybersecurity well.[10]

Perhaps three key (and related) reasons for this are that respondents to the survey said the top elected and appointed officials in their governments were insufficiently aware of the need for cybersecurity, did not support cybersecurity strongly enough and believed that cybersecurity was a role mainly for technologists and not for themselves (See Tables 15, 17 and 18). If this is true, and there is ample evidence that it is, then unless this situation changes and top elected appointed and officials become more knowledgeable about, and supportive of, cybersecurity and accept responsibility to play active roles it, the problems of cybersecurity management identified herein are not likely to diminish greatly over time.

Here is a brief reprise of other important findings. Local governments:

- Had not invested sufficiently in cybersecurity over the 5 years prior to the survey;
- Had not adequately applied highly recommended tools and actions to their management of cybersecurity;
- Did not provide sufficient cybersecurity training to a variety of constituents within their organizations;
- Had not adopted appropriate cybersecurity policies;
- Were unaware of and/or had not implemented applicable and highly recommended cybersecurity standards;
- Reported that their cybersecurity technologies, practices, and policies, for the most part, were one generation or more behind the current best practice;
- Demonstrated limited ability to address a number of adverse cyber events; and
- Reported that their top officials were insufficiently aware of the need for cybersecurity, provided insufficient levels of support for it, and did not embrace a role in or responsibility for it.

These findings, which are borne out repeatedly by the data from our survey, offer what can only be considered an indictment of the current state of local government cybersecurity management. This said, local governments certainly are not alone in this regard. Few organizations of any kind manage cybersecurity well.[11] On a more positive note, despite these findings (indeed, perhaps because of them), substantial opportunities exist for local governments to improve their cybersecurity management.

If most organizations encounter difficulties with cybersecurity, this might suggest that something other than poor management may be involved.[12] As we reported in a prior paper from this survey (Norris et al., 2018), several barriers exist to achieving high levels of cybersecurity, including: (1) the inability to pay competitive salaries to cybersecurity employees (58.6% responding), (2) insufficient number of cybersecurity staff (53.1%), (3) lack of funds (52.8%), and (4) lack of adequately trained personnel (46.9%). Each of these barriers involve funding, something over which local government elected officials and managers have only limited control and must balance among competing demands within their organizations.

To these barriers, we would add that it is now well recognized in the field that cybercriminals are highly motivated (usually for financial, but also political and ideological reasons), are numerous, are as skilled as (or more than) those they are attacking, and are constantly innovating and deploying newer and more effective cyberattacks. Against this array of attackers, many, if not most organizations, local governments included, are not well positioned to provide continuous, successful cybersecurity.

Nevertheless, and even recognizing the existence of limiting external factors, we remain confident that management is important to effective cybersecurity. As we demonstrated in our literature review, for decades research has shown that management matters to IT outcomes in local governments, and more recent research shows that it matters with respect to cybersecurity. Certainly, improved understanding of and support for cybersecurity among top elected and appointed officials in local governments may not be the sole or even the most important factor to achieving high levels

of cybersecurity. It would be foolish to think so. But, without these officials' understanding and support, it is also hard to imagine that local governments will be able to do a better job of achieving high levels of cybersecurity.

Beyond improving local officials' awareness of and support for cybersecurity, what should local governments do to improve cybersecurity management? In a previous paper based on our survey, we recommended, among other things that to improve cybersecurity *practice*, local governments should create and maintain a culture of cybersecurity; address barriers to cybersecurity; and follow best cybersecurity practices (Norris et al., 2018). While these recommendations certainly apply to cybersecurity management, there is no need to repeat them in detail here. Instead, we recommend actions in areas that directly relate to local government cybersecurity *management*.[13]

At the least, local governments should take appropriate actions to address each of our major findings. For example, local governments must increase their investments in cybersecurity. Local governments should adopt and implement appropriate cybersecurity policies; learn about and implement appropriate tools and actions to better manage cybersecurity; identify appropriate areas for cybersecurity training and offer such training on an ongoing basis. Local governments should hold accountable officials and employees who, despite proper training or for other reasons, violate basic cybersecurity rules and requirements.

Last, local governments should take full advantage of the array of recommendations, guidance, tools, workshops, etc., available from organizations such as NIST, DHS, the Public Technology Institute and their own membership organizations (e.g., ICMA, National League of Cities, National Association of Counties, and others).

We conclude by addressing the gap in the scholarly literature on local government cybersecurity. This paper constitutes a small step toward reducing this gap and much more needs to be done. Our survey has produced a baseline of data about local government cybersecurity. It should be followed up with additional surveys at, say, 5-year intervals.[14] Among other things, these surveys should seek to validate the findings reported herein, extend and expand upon them, document changes in local government cybersecurity problems and practices over time, and, importantly, test causal relationships between a variety of independent and dependent variables that can help us to better understand cybersecurity practices and outcomes at the grassroots.

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

Notes

1. Actually, all of these reports, dating to 2008, are considered "required reading" in the cybersecurity field (p. 4, 2019 DBIR).
2. To promote as much consistency in responses as possible, we defined the terms attack, incident, and breach in the survey instrument immediately preceding the questions about these events. We defined *attack* as "any 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 (2015) definitions of *incident* and *breach*, in which an incident is "Any event that compromises the confidentiality, integrity or availability of an information asset" and a breach is "An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party."
3. We do not intend to suggest that Atlanta and Baltimore are outliers. They are but two of many, quite probably a majority, of local governments that do not take cybersecurity seriously enough.
4. Please see Appendix A for explanation of why articles are not directly relevant to research into local government cybersecurity management.

5. Here, we are grateful for (and agree with) a comment by one of the anonymous reviewers of an earlier paper who observed that IT and CS practitioners are widely known in the profession for their unwillingness to respond to questions about the state of cybersecurity in their organizations (Norris et al., 2018).
6. It is certainly also possible, if not likely, that among at least some of the less populated counties there are "urban" population centers.
7. In the survey, we also asked about the levels of awareness and support among other constituencies in local governments (i.e., end-users, elected councillors and their staff and the average citizen). Here we report only those that can be said to play a management role.
8. The Cramer's V statistic ranges from 0.00 to 1.00. The closer to 1.00 the stronger is the relationship—0.1 to 0.30 describes a weak relationship, between 0.30 and 0.50 a moderate one and above 0.50 a strong one (Chapman, 1981; Cohen, 1988; Elifson, Punyon, & Haber, 1990; Murphy & Myors, 1998).
9. While we have no data from the survey to establish this, we suspect that because nearly all organizations, governmental and non-governmental, are under constant or nearly constant attack, there is little or no systematic variation in attack patterns to be found. This could also play out in organizations' management responses. Further research should be undertaken to determine if our suspicion here is correct.
10. We say "on average" because there certainly are local governments, especially larger, better financed and more well-staffed local governments, that are doing exceptional jobs managing and practicing cybersecurity. Indeed, one area of future research might be to identify a number of these governments and conduct in-depth case studies of them to learn how they are able to achieve such results.
11. We thank one of the external reviewers of our paper for this observation, with which we fully agree.
12. Again, our thanks to the external reviewer for this comment, with which we also agree.
13. Some readers may feel that these recommendations are fairly basic and are commonly found in the cybersecurity literature, and we would agree. However, because the data from our survey clearly show that local governments are not managing cybersecurity well, evidently even these basic recommendations bear repeating.
14. Something that we fully intend to do.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

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

Data availability statement

Data from this survey are available from the International City/County Management Association.

About the authors

Donald F. Norris is Professor Emeritus, School of Public Policy, University of Maryland, Baltimore County. His principal field of study is public management, specifically information technology in governmental organizations, including electronic government and cybersecurity. He has published extensively in these areas. He received a BS in history from the University of Memphis and an MA and a PhD in political science from University of Virginia.

Laura Mateczun is a graduate of University of Maryland Francis King Carey School of Law and is a member of the Maryland Bar. She is currently a PhD student at the University of Maryland, Baltimore County School of Public Policy studying public management. Her research interests involve local government cybersecurity, criminal justice, and the importance of equity in policy analysis. She received her BA in Public Policy and Political Science from St. Mary's College of Maryland.

Anupam Joshi is the Oros Family Professor and Chair of CSEE Department at the UMBC, Director of UMBC's Center for Cybersecurity and a Fellow of IEEE. Joshi obtained a B. Tech degree from IIT Delhi, and a PhD from Purdue. He has published over 225 technical papers with an h-index of 78 and over 22,750 citations, has been granted several patents, and has obtained grants from a variety of federal and industrial sources.

Tim Finin is the Willard and Lillian Hackerman Chair in Engineering and Professor of Computer Science at UMBC. He has over 40 years of experience in applying AI to problems in information systems and language understanding. He is an ACM and AAAI fellow, received an IEEE technical achievement award and was UMBC's 2012 Presidential Research Professor. Finin has degrees from MIT and the University of Illinois, Urbana-Champaign and has held positions at Unisys, the University of Pennsylvania, Johns Hopkins University and the MIT AI Laboratory.

References

Accenture. (2019, July 18). *The cost of cybercrime: Ninth Annual Cost of Cybercrime Study unlocking the value of improved cybersecurity protection*. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Anseel, F., Lievens, F., Schollaert, E., & Choragwicka, B. (2010). Response rates in organizational sciences, 1995-2008: A meta-analytic review and guidelines for survey researchers. *Journal of Business Psychology*, *25*, 335–349. doi:10.1007/s10869-010-9157-6

Blinder, A., & Perlroth, N. (2018, March 27). A cyberattack hobbles Atlanta, and experts shudder. *New York Times*. Retrieved from https//www.newyorktimes.com/2018/03/27/cyberattacl-atlanta-ransomware.html

Browning, E. (2017). *Scanning for vulnerabilities: When, why and how often—Prevent threat actors from exploiting vulnerabilities in your network by eliminating the risks*. Retrieved from https://www.secureworks.com/blog/scanning-for-vulnerabilities-when-why-and-how-often

Buszta, K. (2003). Security management. In H. F. Tipton & M. Krause (Eds.), *Information security management handbook* (4th ed., pp. 263–274). New York, NY: Auerbach Publications.

Caruson, K., MacManus, S. A., & 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. doi:10.1515/jhsem-2012-0003

Caruson, K., MacManus, S. A., & 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 Internet Security. (2017). *National cyber security review: Summary report*. Retrieved from https://www.cisecurity.org/wp-content/uploads/2017/07/2016_NCSR_Report_85x11_SinglePP_v4.pdf

Chapman, D. J. (1981). *Basic statistics for social research* (2nd ed.). New York, NY: MacMillan.

CivicPlus. (2018, December 19). The reality of the local government cybersecurity skill gap. *Governing*. Retrieved from http://www.governing.com/topics/mgmt/Cybersecurity-Month-Addressing-the-Biggest-Cybersecurity-Challenges-Facing-Local-Governments.html

Cohen, J. (1988). *Statistical power and analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Coursey, D., & Norris, D. F. (2008). Models of e-government: Are they correct? An empirical assessment. *Public Administration Review*, *68*(3), 523–536. doi:10.1111/j.1540-6210.2008.00888.x

Dell Technologies SecureWorks, Inc. (2019). Retrieved from https://www.secureworks.com/blog/scanning-for-vulnerabilities-when-why-and-how-often

Deloitte and National Association of State Chief Information Officers. (2018). *2018 Deloitte-NASCIO cybersecurity study—States at risk: Bold plays for change*. Lexington, KY: Authors. Retrieved from https://www2.deloitte.com/insights/us/en/industry/public-sector/nascio-survey-government-cybersecurity-strategies.html

Dixon, C. (2014, August 24). Deltek: State. Local government IT spending increase is an opportunity for contractors. *Washington Post*. Retrieved from 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

Duncan, I., & Zhang, C. (2019, May 17). Analysis of ransomware used in Baltimore attack indicates hackers needed 'unfettered access' to city computers. *Baltimore Sun*.

Earnst and Young. (2016). *Path to cyber resilience: Sense, resist, react*. EY 19th Global Information Security Survey 2016–17. Retrieved from https://www.ey.com/Publication/vwLUAssets/Global_Information_Security_Survey_2016/$FILE/REPORT%20-%20EY's%2019th%20Global%20Information%20Security%20Survey.pdf

Elifson, K. W., Punyon, R. P., & Haber, A. (1990). *Fundamentals of social statistics*. New York, NY: McGraw-Hill.

EY.com. (2017). *Cybersecurity regained: Preparing to face cyber attacks. 20th Global Information Security Survey 2017-2018*. Retrieved from https://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18

Fusi, F., & Feeney, M. K. (2018). Electronic monitoring in public organizations: Evidence from USIbr local governments. *Public Management Review*, *20*(10), 1465–1489. doi:10.1080/14719037.2017.1400584

Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones and Bartlett Learning.

Holden, S. H., Norris, D. F., & Fletcher, P. D. (2003). Electronic government at the local level: Progress to date and future issues. *Public Productivity and Management Review*, *26*(3), 1–20.

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. *The Journal of Supercomputing*, *74*, 5171–5186. doi:10.1007/s11227-018-2479-2

ICMA. (2018, February 2). *Expert interview: Cybersecurity awareness training for local government employees*. Retrieved from https://icma.org/blog-posts/expert-interview-cybersecurity-awareness-training-local-government-employees

ICMA. (2019, July 19). *Survey research overview*. Retrieved from https://icma.org/survey-research-overview

Kesan, J. P., & Zhang, L. (2019). An empirical investigation of the relationship between local government budgets, IT expenditures, and cyber losses. *IEEE Transactions on Emerging Topics in Computing*. doi:10.1109/TETC.2019.2915098

King, J. L., & Kraemer, K. L. (1985). *The dynamics of computing*. New York, NY: Columbia University Press.

King, J. L., & Kraemer, K. L. (2019). Policy: An information systems frontier. *Journal of the Association for Information Systems*, *20*(6), 842–847. doi:10.17705/1jais.00553

Kraemer, K. L., & Dedrick, J. (1997). Computing and public organizations. *Journal of Public Administration Research and Theory*, *7*(1), 89–112. doi:10.1093/oxfordjournals.jpart.a024344

Kraemer, K. L., King, J. L., Dunkle, D. E., & Lane, J. P. (1989). *Managing information systems: Change and control in organizational computing*. San Francisco, CA: Jossey-Bass.

Landi, H. (2017, July 24). Survey: 47 percent of healthcare orgs outsourcing some of their cybersecurity needs. *Healthcare Informatics*. Retrieved from https://www.healthcare-informatics.com/news-item/cybersecurity/survey-47-percent-healthcare-orgs-outsourcing-some-their-cybersecurity-needs

Laudon, K. C., & Laudon, J. P. (2014). *Management information systems: Managing the digital firm* (13th ed.). Indianapolis, IN: Pearson.

Li, Z., & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly*, *35*(1), 151–160. doi:10.1016/j.giq.2017.10.006

Marvin, R. (2018, January 24). What is cyber insurance and should you get it? *PC Magazine*. Retrieved from https://www.pcmag.com/feature/358453/what-is-cyber-insurance-and-should-you-get-it

Medical Group Management Association. (2017). *Practice leaders manage cybersecurity with in-house and outsourced resources*. Retrieved from https://www.mgma.com/data/data-stories/practice-leaders-manage-cybersecurity-with-in-hous

Merko, M. S., & Breithaupt, J. (2014). *Information security: Principles and practices* (2nd ed.). Indianapolis, IN: Pearson.

Moon, M. J., & Norris, D. F. (2005). Does managerial orientation matter? The adoption of reinventing government and e-government at the municipal level. *Info Systems Journal*, *15*(1), 43–60. doi:10.1111/j.1365-2575.2005.00185.x

Morgan, S. (2019, July 19). *2019 official annual cybercrime report: Cybercriminal activity is one of the biggest challenges humanity will face in the next two decades*. Cybersecurity Ventures and Herjavec Group. Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Murphy, K. R., & Myors, B. (1998). *Statistical power analysis: A simple and general model for traditional and modern hypothesis tests*. Abingdon, UK: Routledge.

National Institute of Standards and Technology [NIST] Special Publication 800-63B Section 5.1.1.2. (2017, June). *Digital identity guidelines—Authentication and lifecycle management*. Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html

National League of Cities. (2018, May). *State of the cities 2018*. Retrieved from https://www.nlc.org/sites/default/files/2018-05/NLC%20State%20of%20the%20Cities%202018%20FINAL%20WEB.pdf

Norris, D. F. (1984). Small local governments and information technology: Uses and users. *Public Administration Review*, *44*(1), 70–78. doi:10.2307/975666

Norris, D. F. (2010). E-government 2020: Plus ca change, plus c'est la meme chose. *Public Administration Review*, *70* (Special Issue), S180. doi:10.1111/j.1540-6210.2010.02269.x

Norris, D. F., & Campillo, D. (2002). Factors affecting the adoption of leading-edge information technology by local governments. *Working paper*. Baltimore County: Maryland Institute for Policy Analysis and Research, University of Maryland.

Norris, D. F., & Kraemer, K. L. (1996). Mainframe and PC computing in American cities: Myths and realities. *Public Administration Review*, *56*(6), 568–576. doi:10.2307/977255

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cyberattacks at the grassroots: American local governments and the need for high levels of cybersecurity. *Public Administration Review*. doi:10.1111/puar.13028

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cyber-security at the grassroots: American local governments and the challenges of Internet security. *Journal of Homeland Security and Emergency Management*, *15*. doi:10.1515/jhsem-2017-0048

Norris, D. F., & Moon, M. J. (2005). Advancing e-government at the grass roots: Tortoise or hare? *Public Administration Review*, *65*(1), 64–75. doi:10.1111/j.1540-6210.2005.00431.x

Norris, D. F., & Reddick, C. G. (2013). Local e-government in the United States: Transformation or incremental change? *Public Administration Review*, *73*(1). doi:10.1111/j.1540-6210.2012.02647.x

PCI Security Standards Council. (2014). *Information supplement: Best practices for implementing a security awareness program*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Pearlson, K. E., & Saunders, C. S. (2006). *Managing and using information systems: A strategic approach*. Hoboken, NJ: John Wiley and Sons.
Public Technology Institute. (2018). *Local government survey research*. Retrieved from http://www.pti.org/civicax/inc/blobfetch.aspx?BlobID=23038
Reddick, C. G., & Norris, D. F. (2013). E-participation in local governments: An examination of political-managerial support and impacts. *Transforming Government: People, Process and Policy*, *7*(4), 453–476. doi:10.1108/TG-02-2013-0008
Stebbins, R. A. (2001). *Exploratory research in the social sciences*. Thousand Oaks, CA: Sage Publications.
Swedberg, R. (in press). On the uses of exploratory research and exploratory studies in social science. In J. Gerring, C. Elman, & J. Mahoney (Eds.), *Producing knowledge*. Cambridge, UK: Cambridge University Press.
U. S., Census Bureau. (2018). *2012 Census of governments – Organization – Table 2 local governments by type and state: 2012*. Retrieved from https://www.census.gov/data/tables/2012/econ/gus/2012-governments.html
U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. (2019, July 26). *Cybersecurity insurance*. Retrieved from https://www.dhs.gov/cybersecurity-insurance/
Verizon. (2015). *2015 data breach investigations report*. Author. Retrieved from http://www.verizon.com/about/news/2015-data-breach-report-info
Verizon. (2019 June 14). *2019 data breach investigations report*. Author. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/
Whitman, M. E., & Mattord, H. J. (2010). *Management of information security* (4th ed.). Stamford, CT: Cengage Learning.
Wolff, J., & Lehr, W. (2018). When cyber threats loom, what can state and local governments do? *Georgetown Journal of International Affairs*, *19*, 67–75. doi:10.1353/gia.2018.0008
Wood, C. C. (2005). All aboard! *Information Security*, *8*(7), 52–55.
Wood, C. C. (2010). Preface. In M. E. Whitman & H. J. Mattord (Eds.), *Management of information security* (4th ed., pp. XV–XXV). Stamford, CT: Cengage Learning.
Wood, C. C. (2016). Solving the information security & privacy crisis by expanding the scope of top management personal liability. *Journal of Legislation*, *43*(1), 65–121.
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. doi:10.1016/j.giq.2009.07.004

Appendices

Appendix A. Other Local Government Cybersecurity Articles

Article	Topic
(Caruson et al., 2012b)	Survey of local government officials in Florida, measuring cross-pressure between transparency and privacy
(Zhao & Zhao, 2010)	Security assessment of specific state e-government websites
(Fusi & Feeney, 2018)	Examination of electronic monitoring of local government employees
(Wolff & Lehr, 2018)	Review of research on status quo of state and local cybersecurity and partnerships with the federal government
(Ibrahim et al., 2018)	Case study evaluation of a local government organization in Western Australia using NIST CSF
(Kesan & Zhang, 2019)	Uses linear models to understand relationship between local government budgets, IT expenditures and cyber losses

Appendix B. Cybersecurity Tools

Tool	Description
Anti-virus software	Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems.
Web and e-mail gateways	An e-mail security gateway is a product or service that is designed to prevent the transmission of e-mails that break company policy, send malware or transfer information with malicious intent.
Virtual private networks of VPNs	A virtual private network (VPN) is programming that creates a safe and encrypted connection over a less secure network, such as the public internet. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.
Intrusion detection and prevention systems	An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.
Next generation firewalls	A next-generation firewall (NGFW) is a part of the third generation of firewall technology that is implemented in either hardware or software and is capable of detecting and blocking sophisticated attacks by enforcing security policies at the application, port and protocol levels.
Automated malware protection systems	Antimalware (anti-malware) is a type of software program designed to prevent, detect and remove malicious software (malware) on IT systems, as well as individual computing devices. Antimalware software protects against infections caused by many types of malware, including all types of viruses, as well as rootkits, ransomware and spyware. Antimalware software can be installed on an individual computing device, gateway server or dedicated network appliance. It can also be purchased as a cloud service – such as McAfee's CloudAV product – or be embedded in a computing device's firmware.
Network traffic analysis or network virtualization	Network virtualization is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time. Each channel is independently secured. Every subscriber has shared access to all the resources on the network from a single computer.
Multi-factor or biometric authentication	Two-factor authentication (2FA), sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access. Two-factor authentication provides a higher level of assurance than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor – typically a password or passcode. Two-factor authentication methods rely on users providing a password as well as a second factor, usually either a security token or a biometric factor like a fingerprint or facial scan. Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Typically, biometric authentication is used to manage access to physical and digital resources such as buildings, rooms and computing devices.

Note: These definitions were taken verbatim from https://searchsecurity.techtarget.com/.