CYBERSECURITY

ARE FLORIDA'S LOCAL GOVERNMENTS PREPARED?

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

Local Government Cybersecurity Survey, 2019

FINAL REPORT, SEPTEMBER 2019

A Report and Recommendations by Cyber Florida and the University of South Florida School of Public Affairs

Prepared by:

Stephen Neely, PhD

Ron Sanders, DPA

University of South Florida School of Public Affairs
4202 E. Fowler Ave, SOC 107
Tampa, FL 33620

Prepared for:

Florida Center for Cybersecurity
Cyber Florida at the University of South Florida
4202 E. Fowler Ave., ISA 7020
Tampa FL, 33620

Partnering Organizations

Florida City and County Management Association (FCCMA)

Florida League of Cities (FLC)

Florida Association of Counties (FAC)

Florida Local Government Information Systems Association (FLGISA)

Disclaimer: This study was conducted on behalf of the Florida Center for Cybersecurity (Cyber Florida) as part of the organization's ongoing training development and quality improvement efforts. The findings of this study should not be construed as generalizable research.

1: Introduction & Overview

Governments are reliant on technology to provide even the most basic services to their constituents, making them vulnerable to the risks of cybercrime, everything from data theft and spillage to ransomware and sophisticated information operations (what the Russians call "active measures"). This is a fact, as true for smaller government agencies and jurisdictions as it is for large ones, perhaps even more so. But are local jurisdictions ready? Are they as prepared–especially given the constraints in forced transparency, competing public priorities, resource trade-offs, and limited talent–as they need to be?

With that question in mind, the Florida Center for Cybersecurity (aka Cyber Florida) at the University of South Florida (USF) commissioned the university's School of Public Affairs to conduct a survey of local government 'chief executives'–i.e., city managers, county administrators, and their equivalents–about the priority they place on cybersecurity, and more importantly, the steps they have taken to ensure that the governments they lead have done everything possible to mitigate the risk of cybercrimes committed against their citizens.[1]

> ...although many local government chief executives believe their jurisdictions are prepared for a cyberattack, there is substantial room for improvement when it comes to actually following basic cybersecurity best practices.

This project was not intended to be a survey of local government chief information officers (CIOs) nor was it of chief information security officers (CISOs), for those larger jurisdictions that could afford them. We know that they know about the cybersecurity threat, but we also know that no matter how effectively they may communicate that threat within their jurisdictions, they are not in charge. They don't make budget and resource allocation decisions or set policy and program priorities–their bosses do, and those are the people we wanted to hear from. What follows is a detailed discussion of the survey instrument as well as the findings and results. But first, note that in the aggregate, we found that although many local government chief executives believe their jurisdictions are prepared for a cyberattack, there is substantial room for improvement when it comes to actually following basic cybersecurity best practices.

[1] *The study was conducted in partnership with the Florida League of Cities, the Florida City and County Management Association, and the Florida Local Government Information Systems Association, and we are grateful for their assistance.*

For example, we found that

- Approximately **35%** of all reporting jurisdictions **do not require new employees to receive basic cybersecurity training,** while another 45% do not require regular (e.g., annual) cybersecurity refresher training for existing employees.

- **One-fifth** of all respondents reported that their jurisdiction **does not have an official cybersecurity strategy,** while a similar number do not have a cyber incident response plan in place. In each case, less than half of the responding chief executives had reviewed and approved either the jurisdiction's official cybersecurity strategy or its cyber incident response plan.

- **Less than 30% of the responding jurisdictions provide their external vendors and contractors with cybersecurity standards or guidelines for doing business with the organization.**

- Jurisdictions that have previously been victimized by a cyberattack are more likely to have adopted many key cybersecurity best practices.

- The vast majority of local government chief executives cited **resources constraints as the single biggest barrier** to their jurisdiction's cybersecurity preparedness. Other commonly cited constraints include insufficient staff training in cybersecurity and outdated IT hardware and software.

Those findings are not particularly surprising. As a general matter, local government chief executives understand the cybersecurity threats that face their jurisdictions, at least conceptually. However, the survey suggests that not nearly as many of those chief executives have been willing, or more likely able, to translate that conceptual understanding into concrete actions (i.e., the best practices that experience tells us can significantly mitigate the risks of cybercrime). The reasons for that disconnection are many, and the survey reveals some of them, but the report closes with a number of recommendations that can help bridge the troubling gap between intellectual understanding and real-world action.

2: The Challenge: Ensuring Government Cybersecurity

The threats posed by lax cybersecurity are not new. These days, we live most of our lives on the internet, whether it's to do our jobs, get the latest news, shop, or keep in touch with friends and family, almost everything we do today involves some form of information and communications technology (ICT). It's become second nature to us, and while most of us may have no clue as to what's 'behind the screen' on our laptop or smartphone, we still demand the very latest tech-enabled convenience, even though we implicitly know that it comes with some risk.

In that regard, we are constantly bombarded with news of the latest cybercrime, and many of us have probably had something personal of ours–a credit card account, a social security number, our medical prescriptions, perhaps even real money–hacked or stolen online, in part because of a lapse in cybersecurity somewhere along the invisible line between us and a provider of goods or services. The fact that the vast majority of those lapses are preventable is of little solace when we have to go through the suspense (and hassle) of recovering whatever was stolen or hacked. Government is no different.

2.1: Local Government's Cyber 'Crown Jewels'

Citizens demand the same ease of access and interaction from their governments–elected officials, public administrators, agency services, etc.–as they get from retailers and service providers. Indeed, some would argue that government has had little choice but to meet this demand, regardless of the inherent risks or resources involved. In any case, that means that governments at every level are rich in terms of high-value cyber 'crown jewels' that are worth stealing, disrupting, or holding hostage.

Governments are a veritable treasure trove of personally identifiable information (PII) as well as its commercial counterpart (CII). This includes things like social security numbers, bank account information, and credit card numbers as well as proprietary business records and intellectual property. Every city and county has gigabytes of information about its local citizens and businesses, as do the many state and federal agencies that collect information on individuals and businesses within their programmatic purview. So, to say that government is a tempting target for cybercriminals is an understatement.

However, it's more than just the protection of PII and CII. Governments these days are increasingly reliant on technology to provide even the most basic of services. Indeed, some would argue that they have become over-reliant. This is certainly true of large government entities, in part because

they can afford to buy state-of-the-art tech, but it is no less true at the local level, where even the smallest (and least wealthy) jurisdictions have had to embrace technology, if for no other reason than it promises to be less expensive over time than humans to do many of government's essential tasks.

The availability of relatively inexpensive commercial-off-the-shelf (COTS) administrative applications–for internal communications (email and instant messaging), record-keeping, personnel and payroll management, procurement, finance and accounting, etc.–means that even the smallest jurisdiction can buy, install, and use these applications. Whether one calls it 'smart cities' or e-government or something else, the same is true for citizen/customer-facing technologies. Simply put, almost any interaction or transaction with government, from paying bills and applying for permits to tracking how your government is performing–is being done online.

2.2: A Tempting Target for Cybercriminals

Given the ubiquity and convenience of technology today, many citizens take these tools for granted in their daily lives, and they demand the same level of convenience from their governments. However, with these demands come risks and vulnerabilities that are also taken for granted. This is especially true for smaller, local government jurisdictions. As noted, every city and county holds gigabytes of PII and CII about their citizens and businesses, and those gigabytes are all too often defended by small, overworked IT staffs that have to worry more about keeping the mayor's PC working than the longer term, far more protracted protection of their jurisdiction's data, systems, and networks.

Bottom line: it no longer takes a computer genius to conduct a cyberattack and local governments are among the most vulnerable entities.

In the harsh calculus of cybercrime, that means vulnerabilities just begging to be exploited. It seems like every time we check the news, there's a report of a local government getting hacked, from Atlanta and Baltimore to Greenville and Lake City here in Florida.[1] Whether it's the theft or spillage of citizen PII, a malicious Distributed-Denial-of-Service (DDoS) attack on an e-government website, or increasingly, ransomware that holds some or all critical systems hostage for a price, local government has become a preferred target of cybercriminals.

While it used to be that such cybercrime required a degree of technical sophistication, that too is no longer the case. All kinds of illegal tools and techniques are for sale on the Dark Web, from zero-day exploits to ransomware kits that can be socially engineered to penetrate even the best-defended jurisdictions. Bottom line: it no longer takes a computer genius to conduct a cyberattack and local governments are among the most vulnerable entities.[2]

[1] *For examples, see https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html; https://wcti12.com/news/local/city-of-greenville-still-working-to-resolve-ransomware-attack; https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline; https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html*

[2] *https://fcw.com/pages/hpsp/hpsp-10.aspx*

2.3: The Question: Are Local Governments Ready?

Why is this happening? Why are local governments coming under cyberattack with alarming frequency? The answer is simple. Local governments depend on their systems, networks, and databases to get their work done, and by necessity, lots of people have access to those systems and networks. So, whether they know it or not, this means that cities and counties have a large attack surface, which makes them a tempting target for anything from a disaffected hacktivist group conducting a DDoS campaign to make a political point to a more mercenary and malicious ransomware attack for financial gain. Local governments also have an abundance of PII and CII to steal.[1]

At the same time, deficits–in fiscal resources, technology, staff talent, and even in the fleeting attention span of citizens (not to mention some elected officials and bodies)–force cities and counties to make tough choices. City managers and county administrators are often faced with untenable, either/or alternatives, and proactive investments in cybersecurity sometimes come in second–to infrastructure repairs, unfunded pension liabilities, and the like–in the competition for budget dollars. The fact that these choices are typically made 'in the sunshine' of public scrutiny, in full view of everybody, just increases the risk. All of that compounds to make local governments even more vulnerable and even more tempting than some alternative targets.

At least that is our premise, and this study was designed to provide a measure of empirical evidence in that regard. It was commissioned by Cyber Florida: The Florida Center for Cybersecurity at the University of South Florida. Cyber Florida was established by the Florida Legislature in 2014 with a charge to, among other things, bring the private, public, and non-profit sectors together with the state's academic institutions to sponsor research and studies relevant to the state's cybersecurity challenges.[2]

Given recent cyberattacks suffered by localities throughout the state of Florida, Cyber Florida has begun to focus on those unique cybersecurity challenges faced by local governments and has undertaken a broad set of initiatives in partnership with USF's School of Public Affairs and other interested organizations. These initiatives include developing this survey and report, a guide to some local government cybersecurity best practices, a series of cybersecurity workshops for senior public officials across the state, and even a tabletop war game exercise designed for those same officials.

[1] Note that this report does not address election security or the vulnerability of local school systems; for the most part, these are beyond the control of most city and county governments.

[2] https://cyberflorida.org

3: Survey & Sampling Methodology

The research objectives were fairly simple and straightforward for this survey and report: given the nature of the cybersecurity threat to local governments, have their 'chief executives' taken sufficient action to mitigate those threats in their jurisdictions? Based on discussions with Cyber Florida, the School of Public Affairs developed a survey instrument specifically designed to ask those questions of the chief executives who actually run Florida's local governments on a day-to-day basis–and who are ultimately held accountable for making the difficult fiscal and programmatic trade-offs alluded to earlier.

The survey's technical content, primarily focused on accepted cybersecurity best practices, was culled from the literature and staff experience provided by Cyber Florida and the School of Public Affairs. In that regard, the survey's design was loosely guided by Mintzberg's classic model of executive/managerial roles–interpersonal, informational, and decision-making–which are further divided into ten distinct executive/managerial functions (Figure 1). The survey instrument included questions related to each of those roles and functions, albeit with a cybersecurity focus. Once designed, the survey instrument was significantly shortened and reorganized for ease of response.

Figure 1: Mintzberg's Managerial Roles

Category	Roles
Interpersonal	Figurehead Liaison Leader
Informational	Monitor Disseminator Spokesperson
Decision-Making	Entrepreneur Disturbance Handler Resource Allocator Negotiator

According to Mintzberg's model, executives perform an interpersonal role (as figurehead, liaison, and leader), an informational role (as monitor, disseminator, and spokesperson) and a decision-making role (as entrepreneur, disturbance handler, resource allocator, and negotiator). From The Nature of Managerial Work *(Mintzberg 1973).*

However, in order to sample that particular population, the School of Public Affairs reached out to and established partnerships with the Florida League of Cities, the association of the state's more than 400 municipalities; the Florida Association of Counties (FAC); the Florida City and County Management Association, which represents professional public administrators in both city and county government; and the Florida Local Government Information Systems Association, which, as its name implies, serves as the professional organization for local government IT officials and practitioners. All three of these organizations agreed to be named as co-sponsors of the study, along with Cyber Florida and the USF School of Public Affairs, and the first two–FCCMA and FLC–actually emailed copies of the survey and instructions to their substantial membership email lists.

As noted, the survey focused specifically on measuring the behavior of chief executives in local jurisdictions. To that end, all communications to potential respondents emphasized this point. For example, the initial cover letter to the sample read as follows:

> *The survey is designed specifically to help us better understand how* ***those who are in charge of Florida's city and county governments****–mayors, council chairs, city managers, county administrators, and the like–are preparing for and managing their jurisdiction's cybersecurity. Since the survey is intended to gather the specific views of government 'chief executives' like yourself,* ***we'd ask that you make every effort to personally respond to its questions*** *(emphasis added).*[2]

The data collected by this survey and its subsequent analysis are intended to help Cyber Florida, the School of Public Affairs, and the co-sponsoring professional organizations and their constituents (1) determine whether local government leaders are taking appropriate steps to mitigate the cybersecurity threats to their jurisdictions; (2) identify strengths, weaknesses, opportunities, and threats in this area; and (3) guide the development of various mitigation strategies, including more relevant and effective training, resource allocation decisions, preventive and protective countermeasures, cybersecurity policies and procedures, legislation, and even 'reverse' social engineering aimed at fostering cyber secure organizational cultures. These are detailed in the report's final section.

3.2 Data-Gathering: Administering the Cyber Readiness Survey

The Local Government Cybersecurity Survey was administered to the chief executive officers of local government jurisdictions throughout the state of Florida in spring 2019. The questionnaire was specifically designed to collect a broad range of data about how chief executives in Florida's local governments prioritized the cybersecurity of their jurisdictions and how they communicated that priority–by their words and actions–to various stakeholders, as well as how they learned about and

[1] *https://www.flcities.com/, https://fccma.org/, https://www.flgisa.org/; in addition, these organizations also reviewed and provided substantial (and appreciated) input on the survey instrument, as well as this report.*

[2] *Survey cover letter dated April 24, 2019*

addressed threats to cybersecurity (for example, through staff training, cybersecurity policies and procedures, and the allocation of resources).

The survey was administered via email between May 24, 2019, and June 21, 2019. It was distributed by FCCMA to its members—the chief executive officers of cities and counties—via a cover email prepared by the survey's designers. That email described the research effort, provided instructions on its completion, and promised confidentiality in reporting results in the aggregate. While this approach limited the sampling frame to FCCMA members, this trade-off was accepted in order to secure a better response rate through partnership with a well-known and respected professional association.

The survey was administered using a "tailored design" survey method,[1] which uses multiple contacts (i.e. pre-notice, follow-ups, etc.) to increase response rates. FCCMA's mailing list included 213 chief executives from local governments in the state of Florida. After four contacts (pre-notice, survey, and two follow-ups), a total of 101 usable responses were received, resulting in a response rate of 47%.

The section below provides a summary of the respondent characteristics (both individual and organizational). These are followed by a summary and analysis of the survey results. Recommendations and conclusions are presented at the end of this report.

3.3: Respondent Characteristics

Table 1 provides a summary of the respondent characteristics, as collected by the survey instrument. Notably, the responses suggest a sample that is more heavily representative of small and mid-sized localities. This is consistent with the use of FCCMA membership as a sampling frame, which tends to be concentrated among jurisdictions of that size. In this case, only one respondent represents a jurisdiction serving a population larger than 500,000, while more than 78% represent communities of 50,000 or less. As such, the results should be seen as representative of the state's small and mid-sized localities. This is consistent with Cyber Florida's initial goals in conducting this study, particularly as these jurisdictions, through a combination of resource and staffing limitations, are often the most vulnerable to emerging cyber threats.

Variation in the type of responding governments was also limited; 92% of the respondents are in municipal governments, with county governments accounting for only 8% of the sample. In addition, 85% describe themselves as a city or town manager, with only 9% responding as county administrators (the remainder describe themselves as 'other'). This is consistent with previous surveys that used FCCMA's mailing list as a sampling frame.[2] As a result, statistical associations between municipal and county responses cannot be meaningfully analyzed in this report.

[1] *Dillman, Don. (2007).* Mail and Internet Surveys: The Tailored Design Method *(2nd Ed.). New York: John Wiley and Sons.*

[2] *For example http://fccma.org/wp-content/uploads/2015/11/Managing-Public-Records-Compliance.pdf*

Table 1: Respondent Characteristics

What is the size of the population served by your jurisdiction?	Frequency	Percent of Total Sample
Less than 10,000	42	41.58%
10,000–24,999	25	24.75%
25,000–49,999	12	11.88%
50,000–99,999	10	9.9%
100,000–249,999	5	4.95%
250,000–499,999	6	5.94%
500,000–999,999	1	0.99%
1,000,000–1,999,999	0	0%

What type of government jurisdiction do you work for?	Frequency	Percent of Total Sample
Municipality	93	92.08%
County	8	7.92%

What is your current position?	Frequency	Percent of Total Sample
City or Town Manager	85	85%
County Administrator	9	9%
Other	6	6%

How long have you held your current position?	Frequency	Percent of Total Sample
Less than 1 year	20	19.8%
1–2 years	18	17.82%
3–5 years	28	27.72%
6–10 years	15	14.85%
11 or more years	20	19.8%

Source: 2019 Local Government Cybersecurity Survey

Interestingly, sample respondents were quite diverse in terms of tenure on the job, with nearly 20% reporting that they have been in their current position for less than one year, while another 20% said they've held their current position for 11 or more years. Overall, the responses suggest a relatively normal distribution when it comes to tenure, with the modal (most common) response being 3–5 years in the current position (27%). This distribution of responses enabled us to examine whether cybersecurity 'readiness' differs significantly based on years of experience in the chief executive position.

In summary, the sample is comprised primarily of city and town managers from Florida's smaller municipal governments, with an average of 3–5 years of experience in their current positions. As noted earlier, this sample is representative of those organizations that are often most vulnerable to cyber threats, as evidenced in several recent high-profile incidents in small-to-medium-sized jurisdictions like Riviera Beach, Lake City, and Naples.[1]

Along with these basic demographic features, we also asked respondents whether their jurisdictions have suffered a cyberattack/incident in the past three years. The responses show that nearly half (47.5%) of all responding jurisdictions have suffered malware attacks in the past three years, while smaller percentages experienced other types of cyber incidents. Approximately one in six respondents (16.8%) reported that their jurisdiction had suffered a ransomware attack, making it the second most common form of victimization among members of the sample. In total, 59 responding jurisdictions suffered at least one cyber incident, while 42 reported not suffering any. As with CEO tenure, we analyze the relationship between this 'prior victimization' and various cybersecurity leadership actions in Section 4.[2]

Table 2: Previous Cyberattack

Source: 2019 Local Government Cybersecurity Survey

Please indicate whether your jurisdiction has suffered any of the following types of cyberattacks in the past three years.	Yes	No	Unsure
Ransomware	16.83%	77.23%	5.94%
Interruption or shutdown of e-government website	8.91%	87.13%	3.96%
Attack on official social media account	3.96%	88.12%	7.92%
Accidental data loss	13%	81%	6%
Deliberate data theft	1.98%	96.04%	1.98%
Monetary theft	6.93%	89.11%	3.96%
Malicious software attack (malware)	47.52%	46.53%	5.94%

[1] *For examples, see https://www.naplesnews.com/story/news/local/2019/08/02/scammers-trick-naples-out-700-000-spear-phishing-cyber-attack/1902321001/; https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html; https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html*

[2] *All "Unsure" responses were coded as "No" for the purpose of this analysis.*

4: Cybersecurity Starts at the Top

As noted, the principal focus of this study was the 'readiness' of local government jurisdictions to deal with the many cybersecurity challenges that they may face, particularly from a non-technical, senior leadership standpoint. While there are clearly difficult technical challenges to ensuring the security of a jurisdiction's systems and networks, our premise was that a local government's cybersecurity 'starts at the top,' with the chief executive.

With that goal in mind, the survey instrument was guided by Mintzberg's[1] classic framework of executive roles as they might be applied to a local government chief executive, as that official dealt with his or her jurisdiction's overall cybersecurity readiness. This was done in part to gauge the degree of cybersecurity engagement on the part of those chief executives–that is, as indicators of executive emphasis and priority–but also in part to determine whether Florida's local government jurisdictions were really 'ready' when it comes to the security of their information, networks, and systems.

For example, we asked local government chief executives how prepared they felt their jurisdictions were when it comes to cybersecurity. With that self-reported assessment in hand, we then looked at how those chief executives organized, resourced, and staffed their jurisdiction's cybersecurity responsibilities, as those decisions may offer some insight into the priority they place on those responsibilities.

In addition, we looked at whether respondents and their jurisdictions had (1) followed established best practices pertaining to cybersecurity; (2) communicated the importance of cybersecurity to employees and other stakeholders; (3) took advantage of cybersecurity information resources and/or professional development; and (4) personally undertook or oversaw a number of other leadership activities identified in the cybersecurity literature as organizational best practices. (5) Finally, we also asked chief executives to identify some of the barriers that they believed were impeding their preparedness. These results are reported in Table 3.

4.1: Are Florida's Local Governments Ready?

As noted, the survey asked local government chief executives whether they thought that their jurisdictions were prepared for a cyber incident, and the majority of respondents indicated that they are relatively confident in that regard. In total, 60.4% of respondents self-reported that their

[1] *Mintzberg, Henry. (1973)* The Nature of Managerial Work. *Harper Collins, College Division. New York: NY.*

jurisdiction is either "prepared" or "very prepared" to respond to a significant cyber incident (Table 3). In contrast, only 16.83% indicated that their jurisdictions may be unprepared.

Table 3: Self-Reported Cyber Preparedness

In your opinion, how prepared is your jurisdiction to respond to a significant cyber incident?	Frequency	Percentage
Very prepared	13	12.87%
Prepared	48	47.52%
Neither prepared nor unprepared	23	22.77%
Unprepared	12	11.88%
Very unprepared	5	4.95%

Source: 2019 Local Government Cybersecurity Survey

This relative confidence notwithstanding, we wanted to look behind those responses to examine the relationship between perceived cyber readiness and a number of key managerial and organizational attributes that are indicative of that readiness. For example, we asked respondents how they went about organizing, resourcing, and staffing their jurisdiction's cybersecurity responsibilities, including the assignment of cyber responsibility in the organization, as well as the level and types of resources devoted to cybersecurity.

In terms of reporting relationships, the survey results were fairly straightforward. A majority of respondents (68.3%) place their cybersecurity responsibilities under the purview of an information technology professional, such as a CIO, Chief Information Security Officer (CISO), or IT director. Interestingly, in 14.7% of the responding jurisdictions, cybersecurity responsibility rests directly with the chief executive, their principal deputy, or the jurisdiction's chief of staff. (See Table A1 in Appendix A).

However, when it came to cybersecurity expertise, responding jurisdictions were relatively split with regard to staffing their own cybersecurity operations as opposed to outsourcing some or all of them to an external vendor (Table 4). Thus, while only about 23% indicated that they outsource all of their cybersecurity operations, another 28.7% partially outsource them. Conversely, almost half (48.5%) of all responding chief executives indicated that all of their jurisdiction's cybersecurity operations are internally staffed[1]

[1] *In the subsequent analysis that follows, we examine whether outsourcing cybersecurity operations has a significant impact on behavioral and/or attitudinal responses. In order to do so, we created a binary variable that distinguishes between those jurisdictions that outsource "All" of their cybersecurity operations versus those that outsource either "Some" or "None."*

Table 4: Contracting Out Cybersecurity (n=101)

Does your jurisdiction currently contract out any portion of its cybersecurity operations?	Frequency	Percentage
Yes (Some)	29	28.71%
Yes (All)	23	22.77%
No	49	48.51%

Source: 2019 Local Government Cybersecurity Survey

Moreover, with respect to actual human and financial resource allocations for cybersecurity, the data was even more revealing. Table 5 summarizes the number of employees that each jurisdiction reported as being dedicated specifically to cybersecurity. The most common response, accounting for nearly half of the sample, was zero (46%). At first glance, this may seem alarming, but further examination indicated that 30 (or 65%) of the 46 jurisdictions that responded this way also reported outsourcing some or all of their cybersecurity operations, and 18 of those 30 contract out all of their cyber operations. Outsourcing is not cheap, so one could surmise that those jurisdictions that did so were actually making significant cybersecurity investments. Nonetheless, we also found that around 16% of all reporting jurisdictions have no staff, internal or contract, dedicated specifically to cybersecurity.

Table 5: Employees Dedicated to Cybersecurity (n=100)

In total, how many employees do you have dedicated specifically to cybersecurity?	Frequency	Percentage
0	46	46%
1	21	21%
2	10	10%
3–5	18	18%
6–10	1	1%
11–15	1	1%
16+	3	3%

Source: 2019 Local Government Cybersecurity Survey

Additionally, more than two-thirds of all responding jurisdictions (67%) reported having only one or no internal employees dedicated specifically to cybersecurity. Only five—presumably the larger government jurisdictions—reported having six or more employees specifically tasked with cybersecurity operations, while 28% have between two and five employees so tasked. While the data suggest a relatively low internal staff investment in cybersecurity operations for many jurisdictions, this is not entirely unexpected in the smaller, resource-strapped local governments that predominated this sample.

The allocation of fiscal resources also seems to be an area of potential weakness. For example, the results show that for the large majority of jurisdictions in this sample (89.1%), cybersecurity is not treated as a specific line item in the annual budget (see Appendix Table A2). Less than 8% of respondents indicated that it is a specific line item. And while line-item status is not necessarily indicative of priority, the majority of our respondents reported only a small portion of their current technology budget is dedicated to cybersecurity, with 44.4% noting that less than 5% of the annual technology budget goes to cybersecurity, while 60.6% reported a budget allocation of less than 10% (Table 6). Notably, almost one-fifth of our responding chief executives (18.2%) reported being unsure about the amount their organization spends on cybersecurity, perhaps indicating the relatively low priority that cybersecurity receives in the budgeting process.

Table 6: Budgeting for Cybersecurity

Roughly what percentage of your organization's annual technology budget is dedicated specifically to cybersecurity?	Frequency	Percentage
Less than 5%	44	44.44%
6–10%	16	16.16%
11–15%	8	8.08%
16–20%	7	7.07%
21–25%	4	4.04%
26–30%	0	0%
31–40%	1	1.01%
41–50%	1	1.01%
51–75%	0	0%
76–100%	0	0%
Unsure	18	18.18%

Source: 2019 Local Government Cybersecurity Survey

When it comes to leadership engagement, structure, and staff and fiscal resources, the responses suggest that while many jurisdictions are making serious efforts to combat cyber threats, cybersecurity has not yet received the priority status that it warrants among local governments in Florida. That is not an indictment of those local governments, especially the smaller ones that predominate this sample, as many of them simply can't afford to make the necessary investments to protect their information assets. However, the results do suggest that they may need help in that regard.

4.2: Cybersecurity Leadership Best Practices

Next, the survey examined several best practices, both at the chief-executive and jurisdictional levels. For instance, we looked at the direct involvement of chief executives in their jurisdictions' cybersecurity activities (Table 7). Note that we examined these activities as indicators of a chief executive's engagement in cybersecurity, as these practices are emblematic of the importance they may (or may not) place in this area. Thus, we consider activities such as these integral to chief executive's overall leadership responsibilities, just as he or she would review the status of major public works projects or the performance of a jurisdiction's social programs.

While the responses show a high level of involvement in some key areas, they also highlight opportunities for greater leadership engagement in others. For example, two-thirds of respondents indicated that they have personally reviewed and approved their jurisdiction's password policies, while three-quarters have done the same with organizational policies related to the use of personal electronic devices. A slightly smaller majority (60.4%) have also been directly involved in reviewing employee training on cybersecurity.

Table 7: Cybersecurity Leadership

Have you personally reviewed and approved the following for your jurisdiction?	Yes	No	Our Jurisdiction Doesn't Have One
Password policies	64.36%	24.75%	10.89%
Cybersecurity training for employees	60.4%	24.75%	14.85%
Official policy regarding the use of personal devices by employees	75.25%	14.85%	9.9%
Official cybersecurity strategy	48%	32%	20%
Official cybersecurity standards for contractors and vendors	26.73%	54.46%	18.81%
Cyber incident response plan	38.61%	39.6%	21.78%

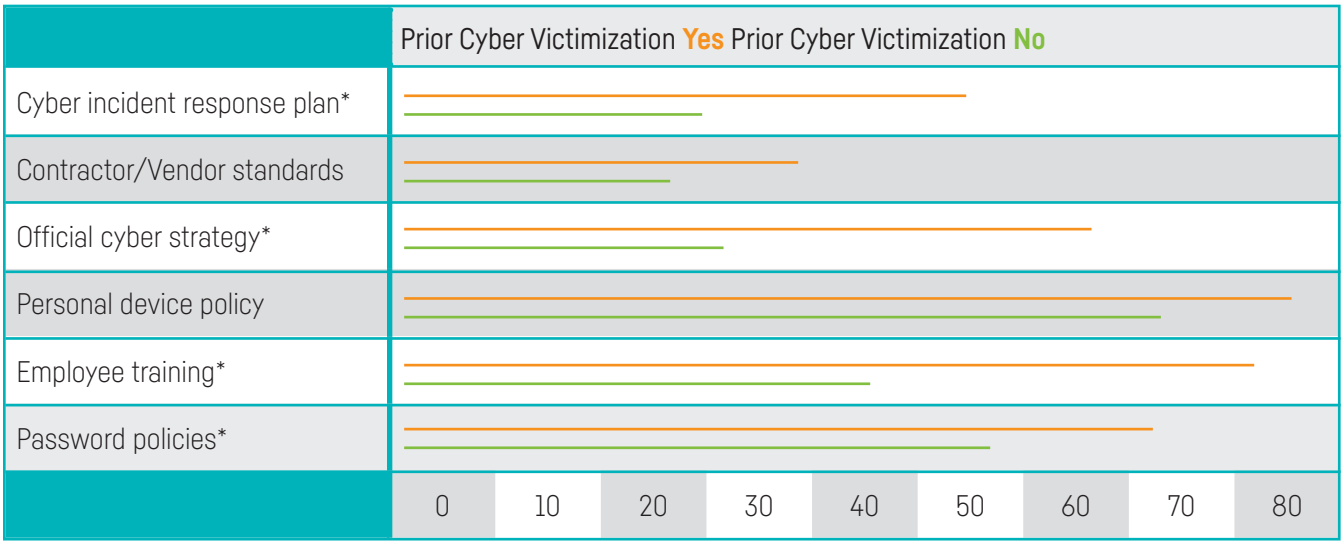
Source: 2019 Local Government Cybersecurity Survey

In contrast, less than half of all respondents indicated personal involvement in reviewing and/or approving their jurisdiction's official cybersecurity strategy (48%), official cybersecurity standards for contractors and vendors (26.7%), and cyber incident response plans (38.6%). These activities represent areas of leadership opportunity when it comes to a jurisdiction's cybersecurity.

Of particular note are the responses found in the far right column of Table 7. As those responses indicate, one-fifth of all respondents reported that their jurisdiction does not have an official cybersecurity strategy (20%). Notably, just under half of those (8 out of 20) were jurisdictions that outsourced all of their cybersecurity operations. Similarly, of the 21.78% that indicated that they have no cyber incident response plan, just under half of them (10 of 22) were also jurisdictions that outsourced cybersecurity (see Appendix Table A3). Things like a cybersecurity strategy and incident response plans are basic to an effective cyber defense, and their absence in many jurisdictions–both those who manage cybersecurity in-house and those that contract out some or all these 'inherently governmental' activities–may be problematic.

Notably, in each case, we found that in jurisdictions that had suffered prior cyber incidents, the chief executives were more likely to have reviewed and approved each of the policies and procedures. This suggests a degree of organizational learning on the part of local jurisdictions. Figure 2 below compares the percentage of chief executives who indicated having personally reviewed and approved each policy and procedure in jurisdictions that have suffered previous cyber victimization with those that have not.

Figure 2: Review and Approval of Policies and Procedures (Percentage)



*Note: * = Statistically Significant at the p ≤ 0.05 level*

Table 8 summarizes responses on the use of several commonly accepted best practices pertaining to organizational cybersecurity within each jurisdiction.[1] Taken together, they constitute a barometer of the 'cyber hygiene' of the state's local governments. On the positive side, the responses suggest a relatively strong level of interaction and information-sharing with regard to cybersecurity among chief executives in local jurisdictions, with a majority (55.4%) indicating that they share cyber incident information with other local jurisdictions. This is consistent with the finding (discussed later) that many local jurisdictions seem to do well communicating about cybersecurity with external partners.

However, in the area of employee training, less than half of all respondents indicated that all new employees receive cybersecurity awareness training as part of their onboarding (45.5%) or that all employees receive annual cybersecurity awareness training (44.5%). A crosstab analysis of these two responses (Appendix Table A4) show that over one-third (33.6%) of all respondents answered in the negative to both of these questions. In other words, it appears that many government

Table 8: Cybersecurity Best Practices – Reported as Percentages

Please indicate whether the following are true in your jurisdiction...	Yes	No	Unsure
All new employees receive cybersecurity training as part of their "on-boarding" process	45.54%	48.51%	5.94%
All employees receive annual cybersecurity awareness training	44.55%	48.51%	6.93%
The jurisdiction currently has cyber insurance	35.64%	46.53%	17.82%
The jurisdiction providers cybersecurity standards to its contractors and vendors	28.71%	53.47%	17.82%
The jurisdiction provides cybersecurity guidance to citizens and local businesses	6.93%	83.17%	9.90%
The jurisdiction shares cyber incident information with other jurisdictions	55.45%	36.63%	7.92%

Source: 2019 Local Government Cybersecurity Survey

[1] These and other cybersecurity best practices are derived from various sources. For example, the US Department of Homeland Security publishes guidelines for small businesses comparable in size to many of the jurisdictions in our survey (https://www.dhs.gov/sites/default/files/publications/Small-Business-Tip-Card_04.07.pdf); as does the US Small Business Administration (https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips) and the Federal Communications Commission (http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db1018/DOC-306595A1.pdf). The Norton Security Co.'s guide to internet security (https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html) also includes many of the best practices identified here.

employees in these jurisdictions receive no cybersecurity training whatsoever. Given that most successful cyber breaches stem from the actions of an unwitting insider–i.e. an employee that inadvertently clicks on a spear-phishing email or reveals his or her password to a cybercriminal–that result is an area of potential weakness.

Additionally, the responses indicate that less than one-third of surveyed jurisdictions (28.7%) provide cybersecurity standards for contractors and vendors. This is another prevalent attack vector for cybercriminals, especially given the extent of local government outsourcing for all kinds of goods and services. This latter finding suggests a significant vulnerability for those jurisdictions. In addition, only one-third of the sampled jurisdictions (35.64%) have purchased insurance against cybercrime; this too is potentially problematic given the recent outbreak of ransomware attacks throughout the state. For Cyber Florida and its partnering agencies, these responses suggest a number of key opportunities to assist the state's local jurisdictions through the promotion of awareness and best practices, particularly in the areas of employee training, cyber insurance, and managing vendor/contractor relations.

When considering factors that might be associated with the presence (or absence) of these policies and procedures, we examined potential relationships between each of the six items in Table 7 and (1) CEO tenure, (2) outsourcing of cyber operations, and (3) prior victimization. CEO tenure was not significantly related to any of the survey items. However, we found that jurisdictions that had suffered prior cyberattacks/incidents were more likely to provide cybersecurity standards to their external contractors and vendors, as well as more likely to share cyber incident information with other jurisdictions. Additionally, jurisdictions that outsourced their cyber operations were less likely to share cyber incident information with other jurisdictions. However, in each case, the statistical strength of these associations was relatively weak. (Results shown in Appendix Tables A5–A6).

Lastly among cyber best practices, we examined participation in two critical cyber learning opportunities over the past year. Given the rapidity with which cyber threats evolve, the time frame for these questions was limited to twelve months, on the assumption that anything later than that was likely to be largely obsolete. These items included participation in a mock spear-phishing exercise within the jurisdiction and participation in a practice drill of the jurisdiction's cyber incident response plan (Table 9).

While nearly one-third reported participating in a mock spear-phishing exercise, approximately 70% have not done so in the past year. Even less reported participating in a cyber incident response drill/exercise, with only 16% indicating that they had done so in the past year. Alarmingly, approximately a quarter of all respondents (24%) indicated that their jurisdiction does not have a cyber incident response plan in place. These data suggest that there is considerable room to increase cyber learning and preparedness at the local government level.

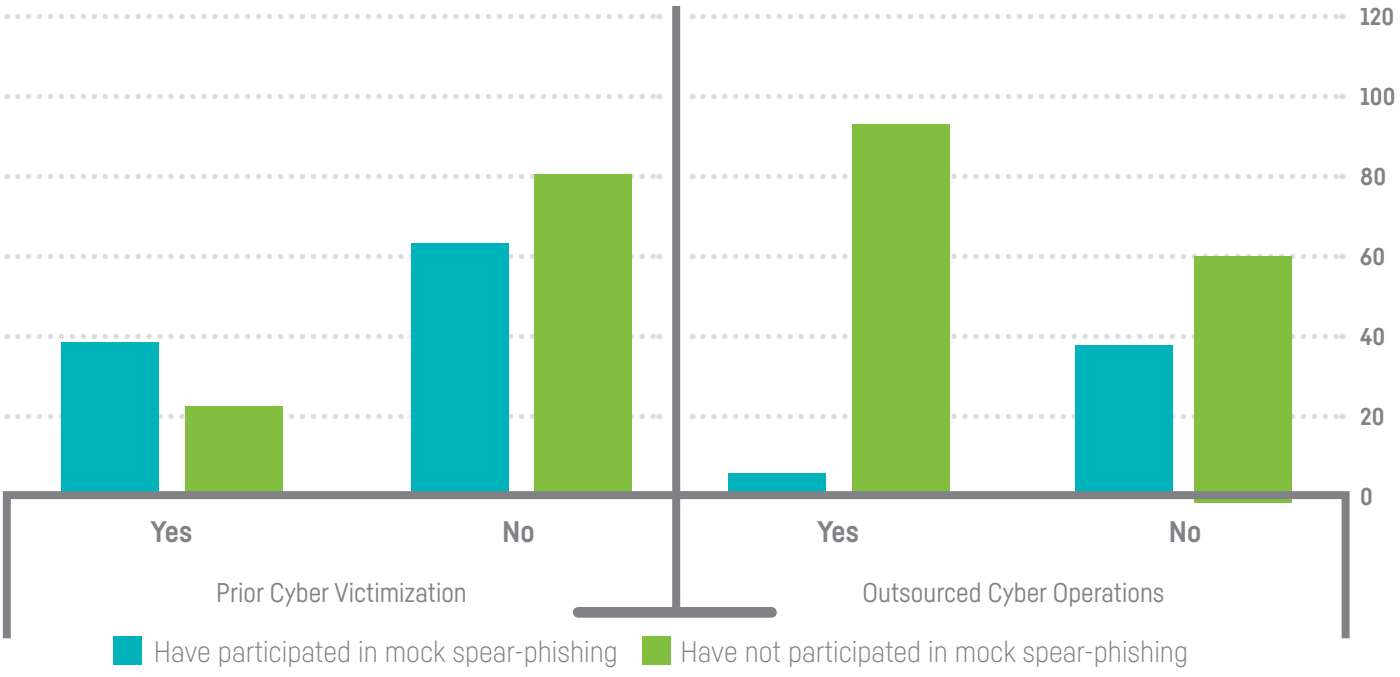
Table 9: Cyber Exercises

In the past 12 months have you attended/participated in...	Yes	No	Jurisdiction Doesn't Have One
Drill/Exercise practicing your jurisdiction's cyber incident response plan	16%	60%	24%
Mock spear-phishing exercise within your jurisdiction	30.69%	69.31%	–

Source: 2019 Local Government Cybersecurity Survey

While both cyber incident response drills and mock spear-phishing exercises were practiced by a stark minority of jurisdictions, we did note that some jurisdictions were more or less likely to utilize these techniques. For example, Figure 3 shows that jurisdictions that have suffered prior cyber incidents were notably more likely to practice a mock spear-phishing exercise in the past year than their counterparts. Conversely, jurisdictions that outsource their cyber operations were highly unlikely to have done so, perhaps assuming that their contractors were now responsible for these things. This is consistent with the hypothesis that jurisdictions become more vigilant in the wake of victimization.

Figure 3: Percentage of Jurisdictions that Participated in Mock Spear-Phishing Exercise



4.3: Communication and Information-Sharing

Mintzberg's model suggests that one of the primary roles of a chief executive is to 'set the agenda' for the organization through regular, recurring formal and informal communications, thereby conveying (and continuously reinforcing) organizational priorities to recipients.[1] With that in mind, we examined cybersecurity communications between local government chief executives and a number of key internal and external stakeholders, including the jurisdiction's senior staff and employees, various elected officials, law enforcement organizations, and the community at large.

We first examined the primary sources of information used by chief executives to keep abreast of cybersecurity related developments. The responses, presented in Table 10, show that communications from professional organizations (such as FCCMA, FLC, and FLGISA) and internal briefings from the jurisdiction's cybersecurity team were the most common means reported by chief executives for keeping abreast of cybersecurity developments. Each was identified as such by approximately 70% of respondents. Professional conferences (52.5%) and publications (65.3%) were also noted by a majority of respondents, while informal peer networks (48.5%) and law enforcement agencies (47.5%) were each noted by just shy of a majority.

Table 10: Sources of Cybersecurity Information

Which sources of information do you use to keep abreast of cybersecurity developments in your field?	Frequency	Percentage of Total Sample
Briefings with cybersecurity team	70	69.3%
Presentations/Meetings with cybersecurity contractors	20	19.8%
ISAC (Information Sharing and Analysis Center)	15	14.8%
Formal organizations (i.e. FCCMA, FLC, FLGISA, etc.)	73	72.3%
Informal peer networks (i.e. trusted counterparts in other jurisdictions)	49	48.5%
Law enforcement (i.e. FBI, DHS, FDLE, etc.)	48	47.5%
Professional conferences that include cybersecurity	53	52.5%
Professional publications	66	65.3%

Source: 2019 Local Government Cybersecurity Survey

[1] The Nature of Managerial Work *(Mintzberg 1990)*

Interestingly, the least utilized method of information gathering was the federally-sponsored Multi-State Information Sharing and Analysis Center (MS-ISAC), which was specifically established to support state and local governments' cybersecurity efforts.[1] Despite this intent, use of this tool was reported by only 14.8% of respondents. Collectively, the responses indicate that professional organizations are doing a very good job of communicating with local jurisdictions on cybersecurity threats and strategies, perhaps suggesting an ideal medium through which critical materials may be circulated and training opportunities promoted. However, the MS-ISAC is underutilized (as are other relevant ISACs), and awareness of these resources could be improved substantially.

We also examined the extent to which the sampled chief executives engaged in learning and information gathering by availing themselves of professional development opportunities, such as attending executive-level cybersecurity training or other relevant professional conferences. The results, presented in Table 11, show that the most common form of professional development among local government chief executives was attendance at a professional conference that included the topic of cybersecurity. However, less than half of all respondents (42.5%) indicated doing so in the past year, while less than a quarter (21.8%) attended an executive-level cybersecurity training.

Given those sources of cybersecurity information, we then looked at the ways and extent to which such information is shared with internal and external stakeholders. This included the frequency with which cybersecurity is treated as unique agenda item in regularly schedule staff meetings. The results, presented in Table 12, show that less than 5% of respondents "always" include cybersecurity as a unique agenda item in their regularly scheduled senior staff meetings. In contrast, more than 77% indicated that it is "rarely" or "never" included as a specific agenda item, suggesting that the vast majority of chief government executives in the sample do not formally discuss cybersecurity with their senior staff on a regular basis.

Table 11: Cyber Training and Development – Reported as Percentages

In the past 12 months have you attended/participated in...	Yes	No
Professional conference with a cybersecurity section	42.57%	57.43%
Executive-Level cybersecurity training	21.78%	78.22%

Source: 2019 Local Government Cybersecurity Survey

[1] *The Center for Internet Security operates the MS-ISAC; see https://www.cisecurity.org/ms-isac/*

Table 12: Cybersecurity as an Agenda Item (n=101)

How often do you include cyber security as a specific agenda item in your regularly scheduled senior staff meetings?	Frequency	Percentage
Always	5	4.95%
Sometimes	47	17.82%
Rarely	31	30.69%
Never	18	46.53%

Source: 2019 Local Government Cybersecurity Survey

While this suggests that there may be a dearth of strategizing between chief executives and their senior staff leaders when it comes to managing cybersecurity concerns, the flow of information from chief executives to the general staff appears to be slightly more robust. A majority of respondents (71.3%) indicated that they at least "Sometimes" share cybersecurity updates (such as best-practices and threat awareness information) with their staff (Table 13). Less than 7% indicated that they "never" do so. While these communications are not the only determinant of priority, the overall responses nonetheless suggest that cybersecurity has not yet reached the 'frequently discussed' status commonly afforded other critical management areas, such as budgets or public safety.

Table 13: Sharing Cybersecurity Updates (n=101)

How often do you share cybersecurity updates with your staff (i.e. best practices, threat intelligence, etc.)	Frequency	Percentage
Often	30	29.7%
Sometimes	42	41.58%
Rarely	22	21.78%
Never	7	6.93%

Source: 2019 Local Government Cybersecurity Survey

We also asked how often local government chief executives communicate with those responsible for their jurisdiction's cybersecurity, and the results were similar (Table 14). Only a quarter of all respondents (26.7%) indicated that they discuss cybersecurity issues with those individuals—whether they were internal staff and/or contractor personnel—on a weekly basis. In contrast, more than half of all respondents (56.4%) indicated that they do so only on a 'monthly' or 'as needed' basis. These results suggest that internal agenda-setting communications from a jurisdiction's chief executive to his or her staff are limited in many cases.

Table 14: Discussing Cybersecurity Issues (n=101)

How frequently do you discuss cybersecurity related issues with the individual responsible for managing it in your jurisdiction?	Frequency	Percentage
Daily	2	1.98%
Weekly	25	24.75%
Bi-weekly	17	16.83%
Monthly	17	16.83%
As needed	40	39.60%

Source: 2019 Local Government Cybersecurity Survey

The same seems to be true for bottom-up communications from a jurisdiction's cybersecurity staff to its chief executive. Less than a quarter of all respondents (24.7%) regularly receive real-time cybersecurity metrics—such as system outages, attempted breaches, data spillage or theft, etc.—as events occur (Table 15). Nearly half (45.6%) indicated that they only receive such updates if they ask for them (21.8%) or not at all (23.8%).

Lastly, we examined the extent to which these chief executives engaged in cybersecurity communications with key external stakeholders, such as elected officials, law enforcement organizations, and members of the public. The results, reported in Table 16, show that within the preceding 12 months, a majority of respondents discussed cybersecurity related issues with local elected officials in their jurisdictions (61%) but rarely with the state legislators or members of Congress who represent their districts (6% and 5% respectively). Over two-thirds also communicated with law enforcement organizations (67%) over the past year, and slightly less than half (45.5%) communicated with the public on these issues over the same time frame.

Table 15: Cybersecurity Metrics (n =101)

Does your IT/cybersecurity staff provide you with specific metrics related to cybersecurity?	Frequency	Percentage
Yes (As they occur)	25	24.75%
Yes (Periodically)	30	29.7%
Yes (But only when I ask)	22	21.78%
No	24	23.76%

Source: 2019 Local Government Cybersecurity Survey

Table 16: Cybersecurity Discussions with Community Stakeholders

How often do you share cybersecurity updates with stakeholders and staff (i.e. best practices, threat intelligence, etc.)?	Frequency	Percentage of Total Sample
Elected officials in your jurisdiction (n=100)	61	61%
Members of your state legislative delegation (n=100)	6	6%
Members of your U.S. Congressional Delegation (n=99)	5	5.05%
Law enforcement (n=100)	67	67%
Citizens/Constituents (n=101)	46	45.54%

Source: 2019 Local Government Cybersecurity Survey

In considering factors that might be associated with organizational communications around cybersecurity, we found that responses to the questions above did not vary significantly based on CEO job tenure or the outsourcing of cyber operations. However, we found strong evidence of a "learning effect" among chief executives in jurisdictions that had previously suffered cyberattacks/incidents. The results (found in Appendix Tables A7–A9) show that CEO's in jurisdictions that have previously been victimized by a cyber attack or incident are more likely to (1) include cybersecurity as a regularly scheduled agenda item, (2) share cyber updates with their staff at more frequent intervals, and (3) receive/monitor cybersecurity metrics in real time (i.e. "As they occur"). These findings

suggest that jurisdictions that have suffered cyber incidents in the past may be more cognizant of and vigilant about emerging cyber threats.

Collectively, the responses discussed above suggest some room for improvement in cybersecurity communications both from and to local government chief executives. In particular, the data indicate an opportunity for more direct, frequent, and strategic communications of cyber-related issues with internal and external stakeholders. In addition to conveying information, more frequent cybersecurity communications can signal to both employees and stakeholders that cybersecurity is an organizational priority, thereby promoting greater vigilance and awareness throughout the organization.

4.4: Potential Predictors of Preparedness

At a glance, several of the responses presented above suggest a potential disconnect between many jurisdictions' level of cyber preparedness as *perceived* by their chief executives and the *actual* level of preparedness, as evidenced by the adoption of various cybersecurity best practices. To put these responses in context, we examined the associations/relationship between perceived cyber readiness and a number of key managerial and organizational attributes, including:

1. Employee cybersecurity training
    a. Whether all employees receive cybersecurity 'onboarding' training;
    b. Whether all employees receive annual cybersecurity training.
2. Prior cyber victimization
3. Outsourcing of cybersecurity operations
4. Employment tenure of chief executive
5. Chief executive engagement with cyber policies/activities (Engagement)
6. Organizational communication around cybersecurity (Organizational Communication)

For the purposes of this analysis: both forms of employee cybersecurity training were measured as categorical variables (Yes, No, Unsure); prior victimization and outsourcing of cybersecurity operations were measured as a binary variable (Yes/No); employment tenure of chief executives was measured as an ordinal variable (less than 1 year, 1–2 years, 3–5 years, 6–10 years, and 11 or more years). Lastly, chief executive engagement and organizational communications were measured as continuous scales, which were calculated through the creation of index variables using the original survey questions.

Chief executive responses regarding preparedness for a cyber incident were recoded into a binary (Yes/No) variable, with "Prepared" and "Very prepared" recoded as "Yes," and all other responses recoded as "No." In order to determine which factors were associated with perceptions of preparedness, we employed chi-square tests to for the categorical variables and independent sample t-tests for the index/scale variables. The results of this analysis are discussed on Table 17.

Neither the chief executive's tenure of employment, nor the outsourcing of cybersecurity operations, were related to differences in perceived cyber readiness. However, we did find several small but meaningful associations between training/learning and perceived preparedness. Table 17 shows the result of three separate chi-square analyses.[1] In this case, we see that chief executives from those jurisdictions that provide cyber training to all new employees, as well as those that require all employees to undergo annual cybersecurity awareness training, were more likely to indicate that their organizations are prepared for a serious cyber incident. Additionally, those jurisdictions that have previously experienced at least one incidence of cyber victimization were also more likely to indicate being "Prepared" for such an occurrence. This latter finding in particular is consistent with the hypothesis that jurisdictions will undergo organizational learning following cyber victimization.

Table 17: Cross-Tabulation of Cyber Preparedness with Training and Policy Learning

In your opinion, how prepared is your jurisdiction to respond to a significant cyber incident?	Yes	No	Unsure
CEO believes that jurisdiction is prepared for a cyber incident			
All new employees receive cybersecurity training as part of their onboarding	22	37	2
All employees receive annual cybersecurity awareness training	35	22	4
Jurisdiction suffered a previous cyberattack	39	22	-
CEO does not believe that jurisdiction is prepared for a cyber incident			
All new employees receive cybersecurity training as part of their onboarding	9	27	4
All employees receive annual cybersecurity awareness training	10	27	3
Jurisdiction suffered a previous cyberattack	20	20	-

** $\chi 2 = 14.480$ ($p = .001$); $\varphi c = .379$ ($p = .001$); ** $\chi 2 = 10.635$ ($p = .005$); $\varphi c = .325$ ($p = .005$); *** $\chi 2 = 1.931$ ($p = .165$); $\varphi c = .138$ ($p = .165$)*

[19] *See Note 12*

[20] *The chi-square test examines differences in* observed *patterns versus those we would* expect *to see if no relationship existed between the variables.*

Along with these associations, we found that both of the index scales were positively associated with perceived cyber readiness on the part of the responding chief executives (as shown in Table 18). This means that chief executives were *more likely* to feel that their jurisdiction is ready to effectively respond to a significant cyber incident if:

- The organization has a higher level of active communication and prioritization around cybersecurity;
- The CEO has *personally* been involved in the development and approval of key cybersecurity policies and procedures;

Collectively, these findings suggest that chief executives among Florida's local government jurisdictions have more confidence in the cyber readiness of their organizations when they and their employees undergo more training and professional development in cyber awareness as well as when there are more open channels of communication throughout the organization (vis-à-vis cybersecurity issues and concerns). While these findings are largely intuitive, they underscore the critical role that organizations like Cyber Florida can play in assisting local governments by creating effective training materials and teaching public managers to effectively facilitate discussions about cybersecurity within their organizations.

Table 18: Managerial Behaviors and Perceived Preparedness

	Scale average	t-stat	sig.
Organizational Communications Scale			
Prepared	8.69	-6.068	0.000
Unprepared	6.08		
Oversight Scale			
Prepared	3.75	-4.808	0.000
Unprepared	2.17		

Note: All depicted relationships are statistically significant at the $p \leq 0.01$ level

4.5: Barriers to Enhancing Cybersecurity

While these results suggest potentially significant vulnerabilities and opportunities to improve on the part of some local government jurisdictions, we understand the many, often conflicting, challenges that these jurisdictions may face. Given that local government budgets are 'zero-sum' in nature, more investments in cybersecurity may mean less resources for something else, and when everything else is just as important, that forces tough, often untenable choices.

However, while fiscal constraints–especially for smaller jurisdictions–are a significant issue, it isn't just about resources. In that regard, we asked respondents to indicate which factors they believed were the most significant barriers for their organization "… when it comes to assuring a reasonable level of cybersecurity." The results are presented in Table 19. As one would expect, by far, the most commonly indicated barrier was fiscal constraints, which more than 6 in 10 respondents (61.4%) indicated is a significant impediment when it comes to ensuring an adequate and effective level of cybersecurity for their jurisdictions.

Table 19: Barriers to Cyber-Security

Which of the following do you consider significant barriers for your organization when it comes to assuring a reasonable level of cybersecurity?	Frequency	Percentage of Total Sample
Fiscal Constraints	62	61.4%
Insufficient Support from Elected Officials	2	1.9%
Insufficient Support from Senior Staff/Management	7	6.9%
Insufficient Cybersecurity Training	39	38.6%
Insufficient Information-Sharing from Peer Jurisdictions	12	11.9%
Insufficient Information Sharing from Law Enforcement	10	9.9%
Insufficient/Outdated Information Technology	27	26.7%

Source: 2019 Local Government Cybersecurity Survey

Interestingly, the second most commonly reported factor was "insufficient cybersecurity training," which 38.6% of all respondents indicated is a significant barrier for their jurisdictions. In light of the importance that training and development might potentially play in promoting cyber readiness (discussed earlier), this finding further underscores the importance of developing informed and effective cybersecurity training for local government institutions. The other barrier that was commonly referenced (26.7% of respondents) is insufficient and/or outdated information technology, but this may be another way of identifying budget limitations as an impediment.

5: Recommendations: What Local Governments Can Do

These survey results offer only a small snapshot of the 'cybersecurity readiness' of Florida's local governments, and we have noted its limitations in that regard (to include the sampling strategy itself). However, those limitations notwithstanding, we believe that the results offer good news and bad. The good news is that many local government chief executives understand the cybersecurity threats to their jurisdictions and are responding to the extent that they are able.

The bad news is that they are finding it difficult to address those threats. Their reasons are varied–conflicting local priorities, severe fiscal constraints, talent shortages, apathetic electorates and stakeholders, to name just a few–but the net effect is to leave our cities and counties (and our citizens) potentially vulnerable to cybercrime.

Faced with all of those barriers, is there anything that local government chief executives can do to improve the cybersecurity of their jurisdictions, despite the many barriers they cite? We believe that the answer is a resounding 'yes' and have set forth a number of recommendations below. In so doing, we do not intend to repeat all of the cybersecurity best practices that others have compiled (although they are certainly consistent with them); rather, these recommendations are based on the survey results discussed above, and given the fiscal constraints facing Florida's local governments, they are listed from the least to most expensive.[1]

That does not mean that they are any less effective. In fact, studies have shown that their 'return on investment' is many-fold. Indeed, given the fact that most successful cybercrimes are not perpetrated by some evil technical genius, but rather stem from some unwitting 'insider' mistake (like clicking on a suspicious email), there is even some cause for optimism here. Thus, while additional resources and expertise would undoubtedly help, Florida's local governments can still significantly improve their cybersecurity at little or no cost by taking some of these steps.

[1] As noted, there is also a whole host of low/no-cost technical fixes that can also significantly bolster a jurisdiction's cybersecurity–simple things like ensuring that the jurisdiction is using the very latest version of a software application, or that security patches and updates are immediately installed. These are not the focus of this paper, but they are things that a chief executive needs to be aware of, so that he or she can say 'yes' when their IT staffs ask for the funding to acquire them, or to hold them accountable when they don't.

5.1: Culture, Culture, Culture

As noted, the vast majority of successful cybercrimes–some estimates are as high as 80 percent–start with an insider's poor cyber hygiene.[1] Someone with access to an organization's data or systems or networks opens the wrong email, plugs in the wrong flash drive, or reveals his or her passcode to the wrong people, and suddenly the cyber gates are open.

That's problematic, but it is also relatively easy to correct. Leaders, both public and private, know how to shape an organization's culture to reward certain behaviors (and punish others), and cybersecurity is no different. A 'cyber-secure' culture–one that values and rewards vigilance when it comes to protecting an organization's systems and networks–is simply the best defense against cybercrime, and it is also the most cost-effective. If employees see a potential cyber vulnerability, will they say something? Can employees self-report their own inadvertent violation of an organization's cybersecurity policy without fear of punishment or will they try to hide it?

These are all manifestations of an organization's culture, and the values and behaviors that underlie them can make it very easy or very hard to breach, and they are just as applicable to local government jurisdictions. Call it 'reverse' social engineering. The techniques associated with shaping an organization's culture are numerous and well-documented, and while they are well beyond the scope of this paper, they can and do work. Local government's chief executives should take notice.[2]

5.2: Training, Training, and More Training

Training is another cost-effective way to bolster a jurisdiction's cybersecurity, and it goes hand-in-hand with a cyber-secure culture. Numerous 'off the shelf' products exist that can help employees realize that each of them–indeed, anyone with access to an organization's systems and networks–has some responsibility for an organization's cybersecurity, from the newest employee to the most senior.

Experience has shown that it's not enough to cover an organization's cybersecurity policies and practices during the orientation of new employees (although, alarmingly, many of our local government survey respondents don't even do that). Instead, they must be continually reinforced through annual refresher training and other techniques. It costs a few hours a year, and while that can add up in a good-sized workforce, the cost of a single ransomware breach typically far exceeds that cost.

That training should not be limited to formal classroom and/or online training, and many organizations are resorting to more subtle means of ensuring that their employees know what it means to be cyber secure. For example, some have taken to testing their employees by periodically sending them fake spear-phishing emails specifically designed to teach them what to look for (or to trick them into opening a potentially malicious attachment). If they fall victim, they are locked out of the organization's

[1] *Ibid*

[2] *See the section on 'creating a cyber-secure culture' in Cyber Florida's recent publication* Cybersecurity for Local Government

systems until they successfully complete additional training, and in some cases, pass a practice or knowledge test. And conversely, if they correctly identify and report the spear-phishing attempt per organizational procedures, they're rewarded.

Two groups bear additional attention when it comes to training. First, while managers typically receive the same training as their staffs, their accountabilities go beyond the individual. They are responsible for continuously communicating and reinforcing an organization's cybersecurity policies to all of their employees, and their words and actions can make or break an organization's efforts to shape a cyber-secure culture. If they practice sloppy cyber hygiene—for example, by pasting a yellow sticky with their password onto their terminal—their employees will likely follow suit.

Similarly, contractors (especially small, ill-equipped ones) can also provide an easy attack vector. Indeed, some of the most notorious cyber breaches have occurred because a contractor or vendor had access to an organization's systems or networks,[1] and given the extent of local government outsourcing today, this should worry city and county officials. Here again, much of this risk can be mitigated by just making sure that contractors are as aware of their cybersecurity responsibilities as their public employee counterparts, and training (perhaps as part of the acquisition process) is the first step. Local governments should also consider establishing cybersecurity standards and oversight mechanisms for their contractors and vendors, but these require additional resources and expertise, whereas training is relatively inexpensive.

[1] Perhaps the most notorious was the 2013 holiday data breach of Target, where cybercriminals gained access through the company's HVAC vendor

5.3: Planning and Practice Make Perfect

While training and culture are critical, a jurisdiction needs some substance behind them. According to the survey results, far too many of Florida's local governments do not have a cybersecurity incident response plan in place, and it is problematic to try to develop one 'on the fly'–that is, in the midst of a cyber incident. These plans are not expensive to develop, and while they require some technical expertise to put together, there are plenty of examples around, not to mention peer jurisdictions that are willing to share them.

Whether they know it or not, almost every jurisdiction probably has the basis for a cyber response plan already on their books. After all, virtually every local government probably has a hurricane response plan that can provide a pretty good start. To be sure, the nature of the crisis may be different, as may some of the key players and contingencies, but many of the responses–in such areas as communications with citizens–may vary only in content. So, cost should not be a barrier here.

Nor should practice. As every emergency planner knows, no disaster response plan survives 'first contact' with the crisis. Every crisis is different, and no plan can anticipate them all. However, all emergency planners also know that it is practice that makes the difference. In this case, city and county leaders should ensure that their jurisdictions not only develop a cyber response plan, but that they practice it as well–not just once, and not just on paper–but several times (until the jurisdiction gets it right), and under the most realistic conditions possible.

And those same leaders–not just a local government's IT staff or its public affairs professionals, but its leaders–should participate in those exercises, so that when (not if) the cyber incident occurs, it won't be unfamiliar to them. Bottom line: Florida's cities and counties are used to planning for and dealing with emergencies. That means they have much of the emergency response infrastructure and protocols in place and need only adapt them to a cyberattack. It also means that they know they need to be resilient, and that resiliency mindset is an asset when it comes to their cybersecurity.

6: What Cyber Florida and its Partners Are Doing to Help

As noted at the outset, we recognize and acknowledge the challenges that Florida's local governments face, not just with their cybersecurity but also in so many other areas. We also recognize and acknowledge that those local governments simply don't have the resources (financial or human) to deal with them all. They need help–from their peers, from the federal government, the state, and from Cyber Florida. So, we close with some of the initiatives that Cyber Florida at USF can (and has) undertaken to support the cybersecurity efforts of the state's local governments.

For example, this survey was funded by Cyber Florida, and while it has a number of limitations, it does represent a start at assessing the cybersecurity 'readiness' of the state's local governments from the vantage of those who actually lead them. Those leaders–the city managers and county administrators

we surveyed—have to make the tough calls when it comes to their jurisdiction's cybersecurity, both 'in the moment' and (perhaps more importantly) well in advance of an incident, when budgets are built and resources allocated, and we hope that this survey has increased their awareness in that regard.

To that end, Cyber Florida has also published a guide to some cybersecurity best practices for the state's local governments. Patterned after a similar effort for Florida's small and medium-sized businesses (https://cyberflorida.org/smb/), the local government version offers tips on how to improve a jurisdiction's cyber defenses, from both a technical standpoint as well as a leadership one, and goes into to step-by-step detail for creating a cyber incident response plan and other helpful preparation strategies.

In addition, Cyber Florida and USF's School of Public Affairs, in partnership with the various organizations that represent the interests of the state's local governments—the Florida League of Cities, the Florida City and County Management Association, and the Florida Local Government Information Systems Association—is sponsoring a series of cybersecurity workshops for local government leaders across the state. These workshops will address many of the issues identified in the survey results, but perhaps more importantly, facilitate even more collaboration amongst the attendees.

Appendix: Supplemental Tables

Table A1: Managing Cybersecurity Operations (n=101)

Who has the primary responsibility for managing cybersecurity in your organization?	Frequency	Percentage of Total Sample
CISO (Chief Information Security Officer)	3	2.97%
CIO (Chief Information Officer)	15	14.85%
Director of Information Technology	51	50.5%
Director of Emergency Management	1	0.99%
Chief Executive (Mayor, City Manager, County Administrator, etc.)	12	11.88%
Chief Deputy (Deputy Mayor, Assistant City Manager, Assistant County Administrator, etc.)	2	1.98%
Chief of Staff	1	0.99%
Other	16	15.84%

Source: 2019 Local Government Cybersecurity Survey

Table A2: Line-Item Budgeting for Cybersecurity

Is cybersecurity a specific line-item in your jurisdiction's annual budget?	Frequency	Percentage of Total Sample
Yes	8	7.92%
No	90	89.11%
Unsure	3	2.97%

Source: 2019 Local Government Cybersecurity Survey

Table A3: Crosstab for Cybersecurity Policies and Procedures and Prior Victimization (% of column totals)

	Outsourced Cybersecurity		
Who has the primary responsibility for managing cybersecurity in your organization?	None	All	Some
Have your personally reviewed and approved your jurisdiction's official cybersecurity strategy?			
Yes	21	8	19
No	20	6	6
Our jurisdiction doesn't have one	8	8	4
Have your personally reviewed and approved your jurisdiction's cyber-incident response plan?			
Yes	15	7	17
No	26	6	8
Our jurisdiction doesn't have one	8	10	4

Source: 2019 Local Government Cybersecurity Survey

Table A4: Crosstab for Employee Training Policies

	Annual Training		
Onboarding	Yes	No	Unsure
Yes	28	14	4
No	14	34	1
Unsure	3	1	2

Source: 2019 Local Government Cybersecurity Survey

Table A5: Crosstab for Cybersecurity Policies and Procedures and Prior Victimization (% of column totals)

	Prior Victimization	
	Yes	No
The jurisdiction provides cybersecurity standards to its contractors and vendors.*		
Yes	37.3%	16.7%
No	47.5%	61.9%
Unsure	15.3%	21.4%
The jurisdiction shares cyber incident information with other jurisdictions **		
Yes	64.4%	42.9%
No	28.8%	47.6%
Unsure	6.8%	9.5%

*$\chi 2 = 5.116$ ($p = .077$); $\varphi c = .225$ ($p = .077$); **$\chi 2 = 4.657$ ($p = .097$); $\varphi c = .215$ ($p = .097$)

Table A6: Crosstab for Cybersecurity Policies and Procedures and Outsourcing (% of column totals)

	Prior Victimization	
	Yes	No
The jurisdiction shares cyber incident information with other jurisdictions		
Yes	34.8%	61.5%
No	56.5%	30.8%
Unsure	8.7%	7.7%

$\chi 2 = 5.532$ ($p = .063$); $\varphi c = .234$ ($p = .063$)

Table A7: Crosstab for Agenda Status of Cybersecurity and Prior Victimization (as a % of Column Total)

	Prior Victimization	
	Yes	No
How often do you include cybersecurity as a specific agenda item in your regularly scheduled senior staff meetings?		
Always	5.1%	4.8%
Sometimes	55.9%	33.3%
Rarely	33.9%	26.2%
Never	5.1%	35.7%

$\chi 2 = 16.088$ ($p = .001$); $\varphi c = .399$ ($p = .001$)

Table A8: Crosstab for Cybersecurity Metrics and Prior Victimization (as a % of Column Total)

	Prior Victimization	
	Yes	No
Does your IT/Cybersecurity staff provide you with specific metrics related to cybersecurity?		
Yes (As they occur)	28.8%	19%
Yes (Periodically)	37.3%	19%
Yes (But only if I ask)	20.3%	23.8%
No	13.6%	38.1%

$\chi 2 = 10.045$ ($p = .018$); $\varphi c = .315$ ($p = .018$)

Table A9: Crosstab for Sharing Cybersecurity Updates and Prior Victimization (as a % of Column Total)

	Prior Victimization	
	Yes	No
How often do you share cybersecurity updates with your staff?		
Often	33.9	23.8
Sometimes	47.5	33.3
Rarely	16.9	28.6
Never	1.7	14.3

$\chi 2 = 9.151$ ($p = .027$); $\varphi c = .301$ ($p = .027$)

Prepared by
Stephen Neely, PhD

Ron Sanders, DPA
University of South Florida
School of Public Affairs

For
Cyber Florida:
The Florida Center for Cybersecurity
at the University of South Florida

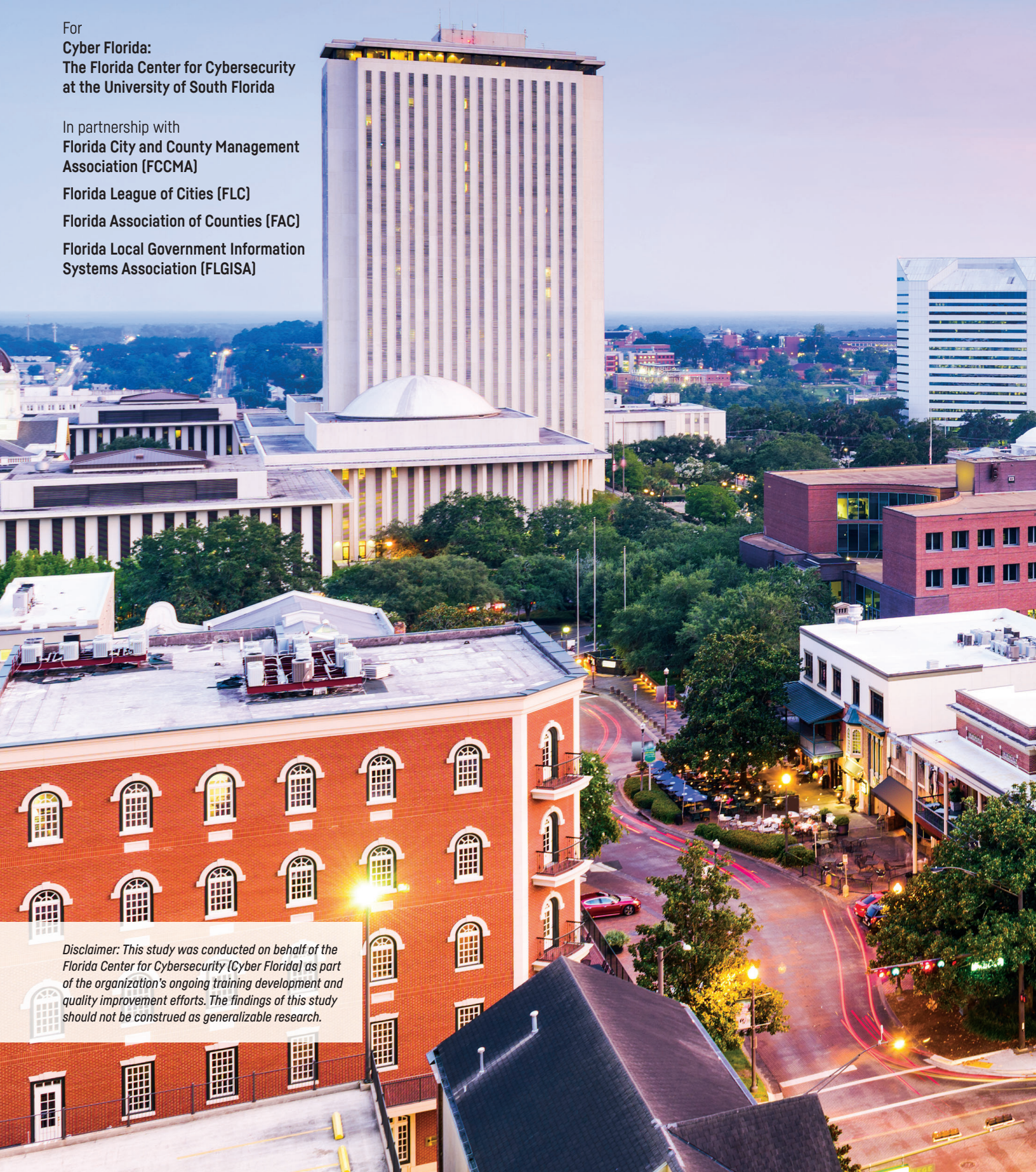
In partnership with
Florida City and County Management Association (FCCMA)

Florida League of Cities (FLC)

Florida Association of Counties (FAC)

Florida Local Government Information Systems Association (FLGISA)

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA



Disclaimer: This study was conducted on behalf of the Florida Center for Cybersecurity (Cyber Florida) as part of the organization's ongoing training development and quality improvement efforts. The findings of this study should not be construed as generalizable research.