



GRAPHIC © GETTY IMAGES

CYBERSECURITY

Readiness Is Key

In light of recent survey results, consider steps to improve your city's status

by **Ron Sanders**
and
Stephen Neely
University of Florida

Governments of all sizes increasingly rely on internet-based technologies to deliver a wide range of public services, as well as to manage and maintain basic administrative functions. Moreover, these same agencies and jurisdictions are often responsible for safeguarding gigabytes of sensitive information about the constituents they serve, including social security numbers, health records and other personally identifiable information. While efficient and convenient, these technological advances bring new cybersecurity-related threats.

From accidental data spillage to malicious ransomware attacks, several local governments have already learned hard lessons about the criticality of cybersecurity and the need for effective planning and leadership in an increasingly connected society. Given the fiscal and staffing constraints often faced by local agencies, adapting to these emerging threats is a particularly acute challenge for municipal governments. Local government leaders are increasingly being asked to do more with less.

To identify opportunities where it can better partner with local governments to meet these challenges, **Cyber Florida** recently sponsored a survey of the state's local government leaders to learn how they are responding to the growing number of cyberthreats. The study was carried out by faculty at the **University of South Florida's School of Public Affairs** with the **Florida League**

of Cities, the Florida City and County Management Association, the Florida Association of Counties and the **Florida Local Government Information Systems Association**. The survey responses highlight effective and relatively inexpensive opportunities to strengthen and improve the cybersecurity-readiness of Florida's local jurisdictions.

The Local Government Cybersecurity Survey was administered in spring/summer 2019 to city managers and county administrators in Florida. The questionnaire specifically examined how those "chief executives" prioritize cybersecurity as well as how they operationalize and communicate those priorities to internal and external stakeholders. The FCCMA distributed the questionnaire electronically to active chief executives among its members. In total, 101 usable responses were received (47% response rate). A complete summary of the survey results is available at cyberflorida.org/gov-survey.

KEY FINDINGS


While Florida's local government leaders demonstrate a keen awareness of the cyberthreats facing their jurisdictions, the responses suggest that cybersecurity has not yet received the same level of prioritization as other areas, such as budgets and public safety.

For example, 77% of survey participants reported that they either “rarely” (30.7%) or “never” (46.5%) list cybersecurity as a regularly scheduled agenda item at senior staff meetings. Less than 5% indicated that they “always” do so.

OTHER KEY FINDINGS:

- ▶ The responses highlight opportunities to increase cybersecurity preparedness through greater employee awareness, especially given that the vast majority of successful cyberattacks are a result of poor cybersecurity practices by unwitting employees. Less than half of respondents (45.5%) reported that “all new employees receive cybersecurity training as part of their on-boarding process.” Similarly, less than half of the respondents (44.5%) indicated that all employees receive annual cybersecurity training updates. In many instances, respondents answered “no” to both questions, which suggests that some employees in these jurisdictions receive no cybersecurity training at all.
- ▶ When it comes to “practicing” cybersecurity in their jurisdictions, nearly 70% of respondents reported that they had not directed or participated in a mock spear-phishing exercise in the past 12 months, while 84% had not practiced their jurisdiction’s cyber incident response plan during the same timeframe. This also represents an opportunity for local jurisdictions to enhance their cybersecurity-readiness.
- ▶ Lastly, the responses highlight opportunities to improve the management of third-party contracts, a prevalent attack vector for cybercriminals, particularly given the extent to which local jurisdictions outsource the provision of public goods and services. Based on the survey results, less than one-third (28.7%) of local jurisdictions provide cybersecurity standards to their external vendors and contractors.

These findings are unsurprising, as Florida’s local governments face significant fiscal constraints. Their leaders must often make hard budgetary choices and trade-offs, including those that involve cybersecurity. However, the good news is that there are simple, low-cost ways to improve the cybersecurity preparedness of any local government or agency. (For recommendations, see sidebar.) For more information on the report and the resources available to help your jurisdiction implement these recommendations, visit Cyber Florida at cyberflorida.org.

Ron Sanders, D.P.A., is director and clinical professor for the School of Public Affairs at the University of South Florida. Stephen Neely, Ph.D., is associate professor for the School of Public Affairs. 

Recommendations

Cyber Florida and its partners offer four simple, strategic recommendations to help local jurisdictions become more “cyber-ready”:

- ▶ **Encourage a “cyber-secure culture.”** Staff and employees identify an organization’s values based on the priorities emphasized and reinforced by senior leaders. Local government leaders are encouraged to make cybersecurity a regularly scheduled agenda item in staff meetings and to routinely communicate cyber-related updates to staff at all levels of the organization.
- ▶ **Provide cybersecurity training for all employees.** Training goes hand-in-hand with a cybersecure culture, and web-based training is a cost-effective way to ensure that all employees understand the risks and responsibilities associated with their use of technology.
- ▶ **Keep in mind that practice makes perfect.** Local government leaders are encouraged not just to proactively develop cyber-incident response plans (based on industry knowledge and best practices) but also to practice these responses regularly to ensure that staff and employees know what to expect if a real cybersecurity crisis occurs.
- ▶ **Engage in active information sharing.** There are a variety of avenues through which local government leaders can share critical information, including threat intelligence, attack forensics, technical expertise and even cyber preparedness and response plans. One such venue, which was found to be underused in the survey results, is the Multi-State Information Sharing and Analysis Center (MS-ISAC), which was developed specifically to connect and support state and local governments in the area of cybersecurity. For more information, go to cisecurity.org/ms-isac.

Cyber Florida at the University of South Florida

The Florida Center for Cybersecurity (Cyber Florida) is a state-funded organization dedicated to positioning Florida as a national leader in cybersecurity through education and workforce development; innovative, interdisciplinary research; and community outreach. Hosted at the University of South Florida, Cyber Florida works with all 12 State University System of Florida institutions as well as industry, government and defense to build partnerships and develop programs that grow and strengthen Florida’s cybersecurity industry. Visit cyberflorida.org for more information.