Public Technology Institute

CompTIA

PTI/CompTIA 2020 National Survey of Local Government Cybersecurity Programs

Cybersecurity has been ranked the No. 1 technology priority for local government IT executives for the past several years, based on research and interviews conducted by the Public Technology Institute (PTI). In 2016 PTI began polling IT executives on an annual basis specifically on cybersecurity-related issues and priorities. The intent: to develop a more comprehensive view of the cyber priorities for local government IT executives and to create educational resources and identify leading practices to help meet those priorities.

For the 2020 survey, because of the COVID-19 pandemic and the rapid move to remote work for government staff, PTI included a couple of questions relating to supporting a remote workforce. Other questions explore employee awareness, policy issues, access management, cyber insurance, and leadership support.

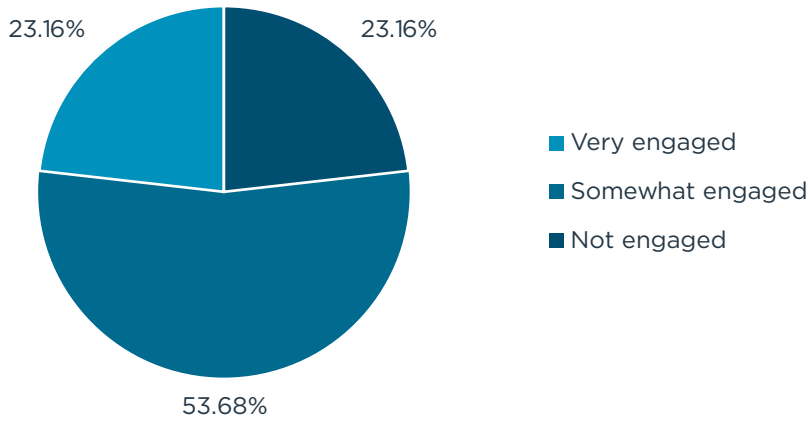
Our hope is that the analysis that follows provides some insight into the major pain points—and successes—for local government IT executives and practitioners as they continue the daunting task of securing their IT infrastructure.

Survey Analysis

The survey began with the question **"How engaged are your elected officials with regards to your cybersecurity efforts?"** PTI felt it important to ask this question as PTI promotes the need for elected officials to be engaged in their government's cybersecurity strategy.

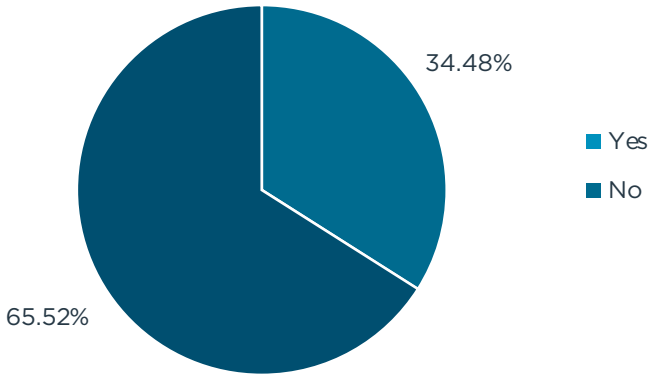
Twenty-three percent of IT executives state that their elected officials are *actively engaged* in their government's cyber efforts. Fifty-four percent state that their elected officials are *somewhat engaged*. Twenty-three percent of IT executives report that their elected officials are *not engaged* at all.

How engaged are your elected officials with regards to your cybersecurity efforts?



With regards to **cybersecurity funding**, 66% of IT executives feel that their cybersecurity budget is not adequate. While many local government budgets (not just IT) will be impacted negatively by the COVID-19 pandemic and resulting loss of revenues, PTI is actively encouraging the strategy that this is not the time to cut cyber or tech budgets, that investments should be made that will provide expanded virtual services and a secure infrastructure as governments face uncertainty in terms of continuing to support a remote workforce.

Do you feel that your cybersecurity budget is adequate?



Eighty-two percent of IT executives state that their local government does have a **cybersecurity plan or strategy**. Of the local governments with a plan, 71% state that their plan has been reviewed within the past year, while 23% state that their plan has been reviewed within the last two years.

Of those respondents who confirm a cybersecurity plan or strategy, 56% share that their plan does allow for exceptions to the policy allowed and that those exceptions are documented. Anecdotally, in conversations with Chief Information Security Officers (CISO), the issue of exceptions is of major concern. The exceptions often tend to be for elected officials, their staffs, and public safety employees, with little oversight or ability to provide corrective action by the IT department. In fact, 15% of IT executives state that their elected officials and their staffs and senior leadership are exempt from their organization's awareness training programs.

Of the 62% of IT executives who state that their organizations have conducted a **network or security audit** of their IT systems and policies within the last twelve months, 79% share that the audit was conducted by an outside vendor or contractor.

Fifty-three percent of IT executives report that they have an individual whose job responsibilities are **specific to managing their cybersecurity efforts** (for example, a Chief Information Security Officer, or equivalent). Eighty-two percent note that these CISO-type positions report directly to the organization's CIO or IT department director, while 13% say the position reports to the city or county manager.

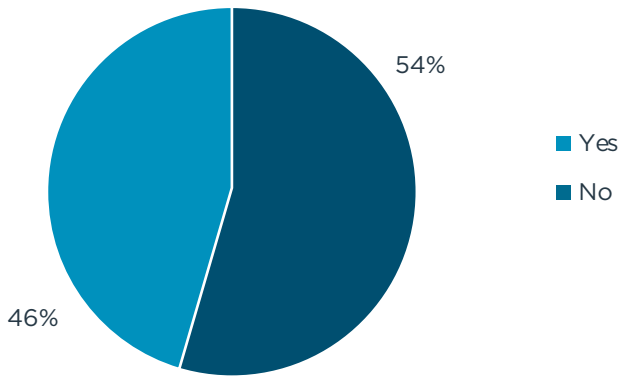
Fifty-five percent of IT executives report that they do have a **Mobile Device Management Policy** for employee or contractor access to government information systems. Thirty-three percent report that their policy addresses *only* government-issued devices for access, while 67% report that their policy addresses *both* government-issued and personal devices.

When asked if their organization either modified their Mobile Device Management policy or implemented a BYOD policy in response to COVID, 76% of respondents state that their policies are adequate and no policy modifications were made.

Eighty-seven percent of local governments do provide **employee awareness training.** Of these local governments, 56% provide ongoing training throughout the year, while 33% provide training once a year. As a leading practice, PTI promotes that training should be held throughout the year and use a variety of formats.

When it comes to addressing cyber **incident response and disaster recovery** planning, 46% of IT executives share that their organizations do maintain a formal incident response plan *and* disaster recovery plan that is tested annually. In conversations with a number of officials, we often hear that a response plan and a recovery plan are one in the same (they are not) or, that plans are developed, often with great effort and cost, but not tested on a routine basis.

Does your organization maintain a formal incident response plan and disaster recovery plan that is tested annually?



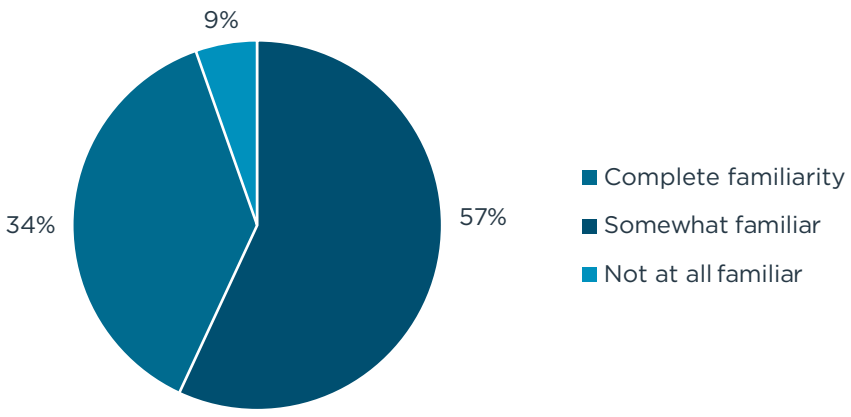
Tying in response and recovery to the COVID-19 pandemic, 29% of organizations have found it necessary to modify either their incident response plan or disaster recovery plan as a result of COVID-19.

Seventy-eight percent of IT executives state that their government does have **cyber insurance**; 13% state they did not have insurance and 8% of respondents are not sure about their government's insurance status.

As for completing the government's cyber insurance application, 32% report that a combination of officials is responsible for completing the application, 28% say that the risk manager is responsible for completing the application, and 20% say it is the responsibility of the IT executive.

Regarding familiarity with their cyber insurance policy, requirements and coverage, 34% of executives state they have complete familiarity with their policy; 57% state that they are somewhat familiar and 9% state they are not familiar at all with their cyber insurance policy.

How familiar are you with your cyber insurance policy, requirements and coverage?



PTI concluded the survey with the open-ended question: **"Is there an issue, topic or concern that was left out of this survey that should be considered by other local governments?"** The intent here is to identify topics to include in future surveys, webinars and interviews.

With regards to the question on having a position or staff person who is responsible for security, a couple of executives reminded us that in many smaller and medium-size jurisdictions, the IT director often wears many hats to include serving as CISO.

Other topics or issues that executives suggested for future consideration: Cloud security, IT staff-to-user ratios, vendor management and resource sharing during times of crisis.

Conclusion

It is our hope that this survey analysis provides a helpful view of the local government cybersecurity landscape and the strategies and tools that IT executives are deploying to secure their technology infrastructure. In the coming months, many IT agencies will be competing with other agencies for resources in an environment of reduced budgets while cyber threats and risks continue to increase. And, unfortunately, some in local government will continue to take security for granted—until a breach occurs or data is held for ransom.

If there is any advice that we can share, it is to be *constantly vigilant*—to be aware, to have strategies and the proper security tools in place and to *communicate* with your elected leaders and your employees about the threats your organization is facing and what they can do to help protect your cyber infrastructure.

Survey Demographics

This survey was conducted in August and September 2020. PTI emailed the survey to a list of local government IT executives that it has developed over the past year. Ninety-five executives participated in the survey.

Breakdown of Respondents

- Under 50,000 population - 46%
- 50,000 to 150,000 population – 22%
- Population of 150,000 and above – 32%

Additional Resources

IT Operations and Support: COVID-19 and the Local Government IT Response
https://comptia.informz.net/COMPTIA/pages/PTI_2020_COVID_CIO_Survey

2020 PTI State of City and County IT National Survey
https://comptia.informz.net/COMPTIA/pages/PTI-2020-State-of-City-County-IT-Survey

Protecting Our Data: What Cities Should Know About Cybersecurity
(produced with the National League of Cities)
https://www.pti.org/civicax/inc/blobfetch.aspx?BlobID=23080

About PTI

Established in 1971 by several major national associations representing state and local governments and now powered by CompTIA, the Public Technology Institute (PTI) has been viewed as the focal point for thought leaders who have a passion for the furtherance and wise deployment of technology. PTI actively supports local government officials through research, education, the development of leading practices, and providing a network to share and to learn from each other. Visit ***pti.org*** to learn more.

About CompTIA

The Computing Technology Industry Association (CompTIA) is a leading voice and advocate for the $5.2 trillion global information technology ecosystem; and the estimated 75 million industry and tech professionals who design, implement, manage, and safeguard the technology that powers the world's economy. Through education, training, certifications, advocacy, philanthropy, and market research, CompTIA is the hub for advancing the tech industry and its workforce. Visit ***CompTIA.org*** to learn more.