PUBLIC TECHNOLOGY INSTITUTE

A DIVISION OF FUSION LEARNING PARTNERS

2023 LOCAL GOVERNMENT CYBERSECURITY NATIONAL SURVEY

FOREWORD

Local officials have spent the past year digesting the details of the federal government's State and Local Cybersecurity Grant Program (SLCGP). In fiscal year 2023, the U.S. Department of Homeland Security (DHS) is providing $374.9 million to address cybersecurity risks and threats to information systems owned, operated by, or on behalf of state, local, tribal and territorial governments.

Since the program's inception, there has been much debate in the local government community about the effect federal funding will have on local cyber initiatives. While the funding impact is limited (because of the number of organizations eligible for grants), it is helping to forge a stronger bond, in terms of communications, and information and resource sharing, between all levels of government while helping to build up our cyber defenses.

The federal SLCGP program is just one of the tools available to local officials in the cybersecurity toolbox. Consider how StateRamp, a national non-profit organization that adopt policies and procedures that standardize security requirements for providers to the public sector, and MS-ISAC, designed to serve as the central cybersecurity resource for the nation's state and local and tribal governments can be utilized by your organization.

Today, no technology article, report, or discussion would be complete without a mention of Generative AI. Local governments are utilizing AI to deliver services to the public, as a tool to make their enterprises more secure, and exploring a variety of potential uses that would improve government operations. As we utilize and explore AI, what are the risks we need to be aware of? What are the possible rewards? And how do we ensure that local government employees understand the impact of how they use AI?

Perhaps most important, as we consider AI and cybersecurity, is the question, "How can AI be applied to bolster our cyber defenses?"

Local government IT executives are not only dealing with threats by outside actors, they are dealing with internal threats: The continuing need to educate employees on their role in securing the organization, coping with often limited budgets and lack of resources, and competition in terms of finding and keeping qualified cyber staff.

The good news is that there is hope! Numerous examples exist of successful vendor and partner engagement; there is increasing recognition by elected officials that cybersecurity is a priority, there is increased resource sharing between state and local government, and many organizations are implementing programs that promote cross-training, internships, and other opportunities to improve the skills of our cyber workforce.

Thank you to the local government IT executives who participated in this survey, and more importantly, the thousands of local government IT and cyber professionals who are on the front lines of protecting our cities and counties in an increasingly aggressive cyber threat environment.

I would also like to thank Dale Bowen, Deputy Executive Director of PTI for his role in managing PTI research activities, and our colleagues with Fusion Learning Partners – PTI's new home – for their enthusiastic support of PTI's local government programs.

Sincerely,

Alan Shark | Executive Director

BACKGROUND

The 2023 Local Government Cybersecurity National Survey was conducted by Public Technology Institute – a division of Fusion Learning Partners. The intent of this analysis is to provide a snapshot of cybersecurity programs, issues and priorities in cities and counties.

Sprinkled throughout the survey are comparisons with the results of our 2022 survey. The survey was conducted in September and October 2023. PTI surveyed PTI member IT executives, and local government IT executives who participate in the PTI / Rutgers University Certified Government CIO (CGCIO) program. Thirty local government IT executives participated in the survey.

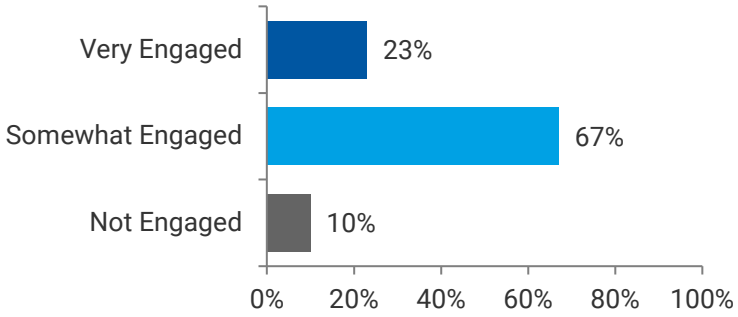
DID YOU KNOW?

- 23% of local elected officials are very engaged when it comes to organization-wide cyber security efforts
- 36% of local IT executives feel that their budget is adequate to support cybersecurity initiatives
- Developing and maintaining a cybersecurity strategy is the number one priority initiative for the coming year
- Increasing sophistication of attacks is the number one barrier that local IT executives believe their organization faces to address cybersecurity challenges
- 40% of local IT executives are turning more to vendors that utilize AI solutions for cybersecurity support

SURVEY RESULTS

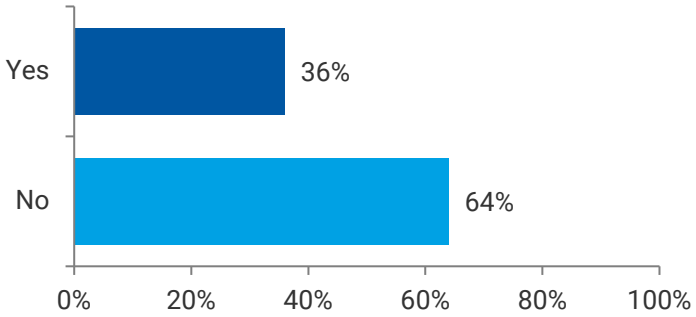
How engaged and familiar are your elected officials with regards to your organization-wide cyber security efforts?

When asked how engaged and familiar are elected officials with regard to organization-wide cyber security efforts, 23% of IT executives responded that their elected officials are very engaged, 67% responded that their elected officials are somewhat engaged, and 10% or elected officials are not engaged.



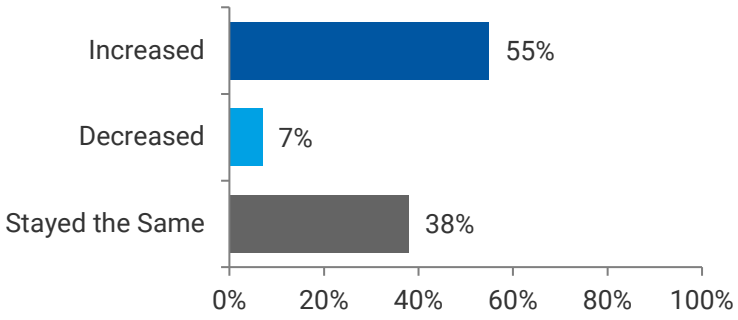
Is your cyber security budget adequate to support cybersecurity initiatives?

Thirty-six percent of IT executives stated that their organization's cyber security budget is adequate to support cybersecurity initiatives, while 64% stated their cyber budget is not adequate. These percentages are almost the same as how IT executives responded to the 2022 survey.



Regarding your current cyber security budget: How has your budget changed in comparison to last year's or your previous cyber budget?

Fifty-five percent of IT executives shared that their current cyber budget is an increase compared to the previous budget. Seven percent shared their budget decreased while 38% of budgets stayed the same.

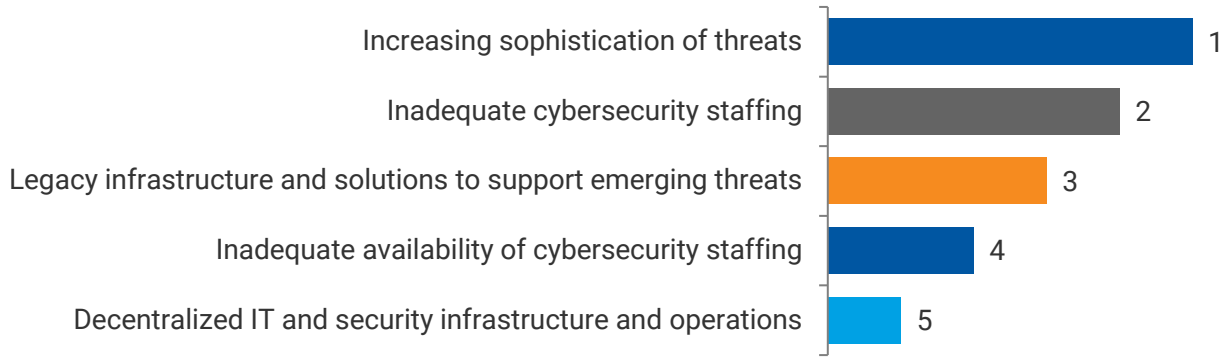


Of the following activities, please rank the priority initiatives for the next twelve months, with 1 being highest priority and 6 the lowest priority.

We provided survey participants with a list of activities and asked that they rank their priority initiatives for the next twelve months. Cybersecurity strategy was ranked number one, followed by conducting risk assessment at number two and malware detection and mitigation following at number three.

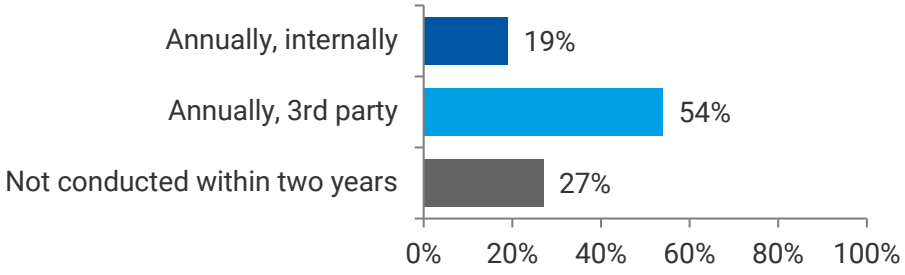
Of the following, please rank the barriers that you believe your organization faces to address cybersecurity challenges, with 1 being the most significant barrier and 5 the least significant barrier.

We asked survey participants to rank the barriers that they believe their organization faces to address cybersecurity challenges. Increasing sophistication of attacks was ranked number one, inadequate availability of cybersecurity professionals at number two, closely followed by legacy infrastructure and solutions to support emerging threats at number three.



When was the last time you conducted a formal cybersecurity risk assessment that looked at how different scenarios would impact the confidentiality, integrity, and availability of your information assets and data?

Conducting a formal cybersecurity risk assessment that looks at how different scenarios would impact the confidentiality, integrity, and availability of organization information assets and data is a vital component of any cybersecurity strategy. When asked the last time that an assessment was conducted, 54% of IT executives responded that they are conducted annually by an independent third-party. Nineteen percent responded that assessments are conducted annually by internal staff. Twenty-seven percent of IT executives responded that they have not conducted an assessment within the last two years.

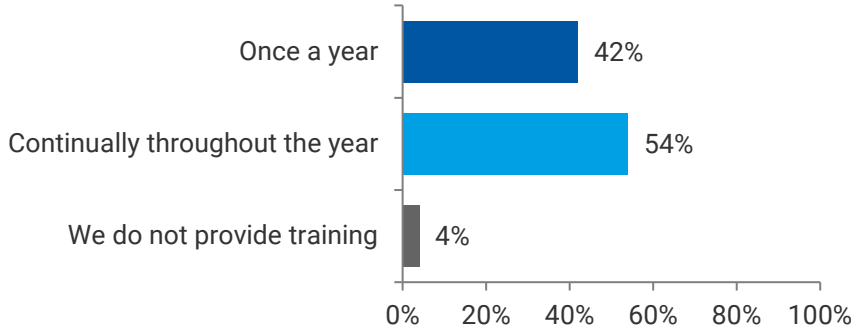


How often do your employees participate in cybersecurity awareness training?

Employees are the front line of cyber defense. When asked how often employees participate in cybersecurity awareness training, 54% of respondents stated that awareness training is provided throughout the year.

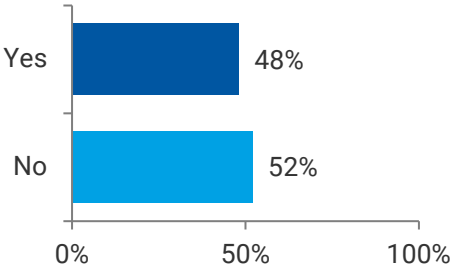
Survey respondents were invited to share the tools and resources that they use as part of their awareness training. Examples include phishing exercises, gaming scenarios, and video training that includes testing.

A comment from one IT executive best summarizes the appropriate approach to awareness training: "Get out from behind the screens, represent the power of collaboration and articulate the risks associated with our daily operations."



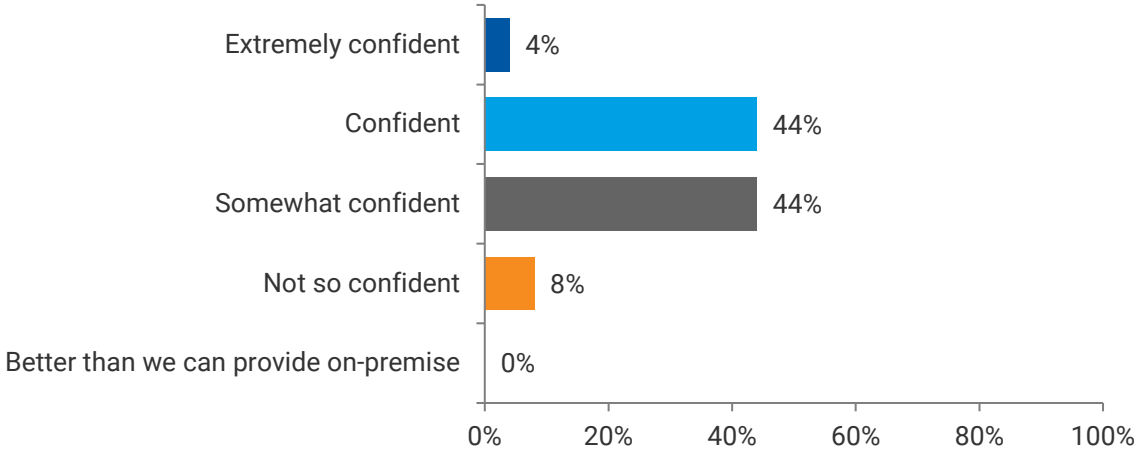
Does your organization have an individual whose sole job responsibilities are managing your organization's cyber security efforts? For example, do you have a CISO or equivalent?

The position of the CISO is growing in importance and it allows for better organization-wide risk management. When asked whether their organization has an individual (CISO or equivalent) whose sole job responsibilities are managing the organization's cyber security efforts, 48% of responding organizations do have a CISO while 52% of organizations do not. (It is important to keep in mind that in many smaller organizations, the IT executive wears many hats, including responsibility for cyber programs.)



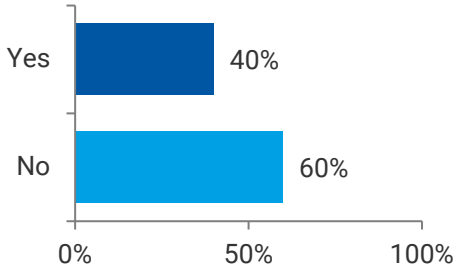
For the cloud services you utilize, how confident are you regarding the security measures of those services or providers?

When it comes to how confident local government IT executives are regarding the security measures of their cloud services providers, 44% of respondents shared that they are confident with the security measures, while 44% shared they are somewhat confident.



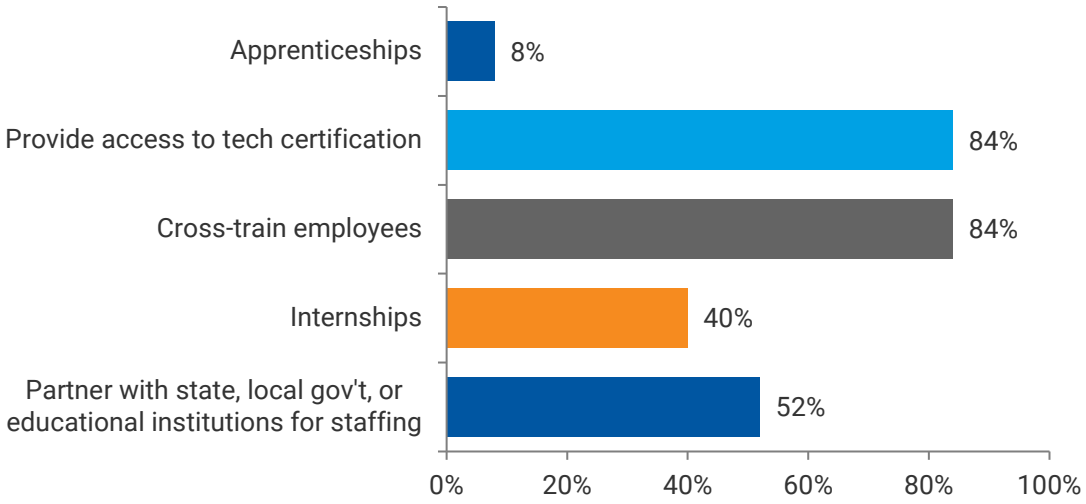
Are you turning more to vendors that utilize AI solutions for cybersecurity support?

As stated at the beginning of this analysis, AI is definitely entering the cybersecurity conversation. Forty percent of IT executives responded that they are turning more to vendors that utilize AI solutions for cybersecurity support.



Of the following activities, please select all that you utilize to strengthen your cyber workforce

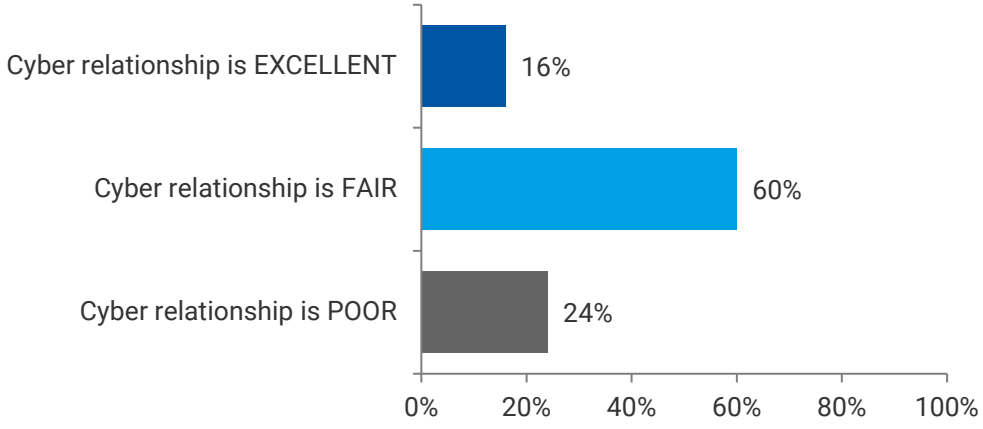
Activities to strengthen the organization's cyber workforce was the focus of our next question. Provided with a list of options, we asked respondents to select all the activities that they utilize. Providing access to tech certification and cross-training of employees tied for number 1, with 84% of responding using implementing these strategies.



Specific to cyber security: How would you rate the relationship between your IT organization and your state's IT organization in terms of information-sharing, resource-sharing, education and training provided by the state to local governments?

When asked to rate the relationship between the local government IT organization and the state IT organization (in terms of information sharing, resource sharing, education and training provided by the state to local governments), 60% rated the relationship as fair, 24% as poor and 16% rated the relationship as excellent.

For comparison to the 2022 survey: Forty-nine percent of IT executives rated the relationship as fair, 39% as poor and 11% rated the relationship as excellent.



CISO ROLES AND RESPONSIBILITIES

Today's local government CISO plays a pivotal role in protecting the digital assets and services of a local government, ensuring that its operations are secure, compliant, and resilient against cyber threats. For those who remain uncertain here are but a few key roles that a CISO plays. For those without a CISO, it should be understood that each of the following responsibilities is already performed by someone (possibly an overburdened CIO) in some form or fashion.

1. Strategic planning: Develop and maintain the information security strategy, ensuring that it aligns with local government objectives and addresses the evolving threat landscape.
2. Policy development: Draft, update and enforce information security policies, procedures and standards to ensure compliance with regulations and best practices.
3. Risk management: Conduct regular risk assessments, identify vulnerabilities and prioritize security initiatives based on potential impact and threat probability. Risk management includes cyber insurance applications, requirements and appropriate policies.
4. Incident response: Develop and maintain an incident response plan to address potential security breaches. Lead the response team during and after security incidents.
5. Security awareness training: Create and deliver training programs to educate employees about security best practices and the importance of protecting government data.
6. Vendor management: Evaluate and ensure the security of third-party vendors that the local government does business with, ensuring that they meet necessary security standards.
7. Technology oversight: Evaluate, recommend and oversee the deployment of security technologies, including firewalls, intrusion detection systems, encryption solutions and endpoint security tools.
8. Regulatory compliance: Ensure that the local government's IT systems and processes comply with applicable laws, regulations and standards.
9. Budget management: Prepare and manage the information security budget, ensuring that adequate funds are allocated for necessary security measures and technologies.
10. Collaboration: Work closely with other departments, such as IT, legal, human resources and emergency management, to coordinate security initiatives and ensure that security considerations are integrated throughout the organization.
11. Reporting and communication: Regularly communicate the security posture of the organization to executive leadership and elected officials, providing them with updates on threats, vulnerabilities, and mitigation efforts.
12. Continual learning: Stay updated with the latest security trends, threats and technologies to ensure that the local government's security posture remains robust and ahead of potential adversaries.

Reprinted from the PTI Commentary Cyber Insecurity, AI and the Rise of the CISO, American City and County: https://www.americancityandcounty.com/2023/10/11/cyber-insecurity-ai-and-the-rise-of-the-ciso/

ABOUT PTI

Public Technology Institute - a division of on-profit Fusion Learning Partners - supports local government officials through research, education, professional development, executive-level consulting services, and national recognition programs.

Since our inception, PTI has focused on raising the profile of today's IT professional, ensuring that IT has a seat at the table when it comes to decisions, and helping to build/strengthen the professional/leadership/management skills of IT professionals. With a focus on navigating the emerging trends that will impact government IT and service delivery, PTI has created a collaborative leadership development environment that rewards sharing solutions and identifying leading practices together. In IT roles that often leave leaders feeling like they're on an island, PTI also provides opportunities to make valuable professional connections.

Cyber Tabletop Assessment

How would your organization react to a cyber attack? Knowing the answer to that question, and addressing challenges before an attack occurs, is essential. PTI's tabletop cyber attack simulation provides a customized, real-world intrusion and allows users to test their response, resilience, and level of readiness. Working closely with leadership teams and organizational staff, PTI shines a light on blind spots and addresses threat areas proactively, helping eliminate the need to react at the moment if an attack occurs.

To find out more about PTI, visit: **PTI.ORG**