CompTIA | pti Public Technology Institute

# 2021 National Survey of Local Government Cybersecurity and Cloud Initiatives

**Dear Local Official:**

I am pleased to present this analysis of the **2021 National Survey of Local Government Cybersecurity Programs and Cloud Initiatives.** For close to a decade now, CompTIA-PTI has conducted this survey of city and county IT executives to identify the pressing cyber issues that you and your colleagues are experiencing. The survey looks at budgeting, policies and procedures, access management, cyber insurance, and leadership support. For 2021 we expanded the survey to include questions relating to cloud services.

The findings we cite in the following pages confirm that there are a wide variety of management and policy issues that are impacting the Cybersecurity posture for many local governments:

- Engaging leadership on Cybersecurity remains a vexing issue for many IT organizations
- While we are seeing an uptick in budgeting for Cybersecurity programming, for some thanks to federal stimulus support, a majority of IT executives feel their funding for cyber is still inadequate
- Cyber insurance rates are rising (and coverage limits are declining)
- The number of organizations that have implemented policies to better manage mobile devices have increased from last year
- IT executives feel a high level of satisfaction when it comes to the security protocols implemented by the service providers of their networks

The past twenty months have been a particularly trying time for the local government community: Add to the health and societal impact of the pandemic on our communities and organizations, city and county IT had to quickly ramp up and provide government services via a vastly expanded remote work environment – for the most part, implemented effectively and securely.

Many of the band-aid approaches local governments had undertaken are now more formal and strategic – and working! Continuing this positive note, local governments are implementing new tech-related programs and initiatives as a result of the federal American Rescue Plan Act and many are using this funding to enhance their Cybersecurity programs.

At the same time, many IT organizations are struggling with staffing and resource issues – some are calling it the "Great Resignation" - similar to how we referred to the "Great Recession" of a decade ago - as staff leave local government IT. While some are retiring, many are moving to the private sector where qualified professionals can easily demand upwards of 40% more in salary and benefits. As unfortunate as it is, this does provide an opportunity to explore apprenticeship programs, resource sharing and public-private initiatives which CompTIA-PTI strongly encourages.

Add to this an increasingly hostile cyber environment, meaning that local governments are more susceptible than ever to cyber threats. We, as public officials, must continue our vigilance protecting our technology infrastructure and the information of the public we serve.

**Dr. Alan Shark**
**Executive Director**
**CompTIA-PTI**

# Background

The **2021 National Survey of Local Government Cybersecurity Programs and Cloud Initiatives** is an annual survey conducted by CompTIA-Public Technology Institute. The intent of the survey – and this analysis - is to provide a snapshot of Cybersecurity programs, issues and priorities in cities and counties.

This survey of local government IT executives was conducted as part of PTI's continued efforts to highlight Cybersecurity as a priority concern for local governments. The following analysis will help to enlighten local elected leaders and management as to the importance they need to place on their cyber programs.

Throughout the survey we compare the 2021 findings with the results of the 2020 survey.

The survey was conducted in August and September 2021. Over seventy-five local government IT executives participated in the survey.

To ensure that the questions we asked were on target and of value, the **2021 National Survey of Local Government Cybersecurity Programs and Cloud Initiatives** was developed with input from members of the CompTIA-PTI CISO/Cyber Leader Forum, the network of officials responsible for cyber programs in local government. Information on this forum can be found later in this report.

Well-deserved recognition must goe to Dale Bowen, Senior Manager, CompTIA-PTI who led this research initiative as well as all other PTI research surveys and reports over the years.

**About CompTIA-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 and the sharing of leading practices. For more information see www.pti.org.

.

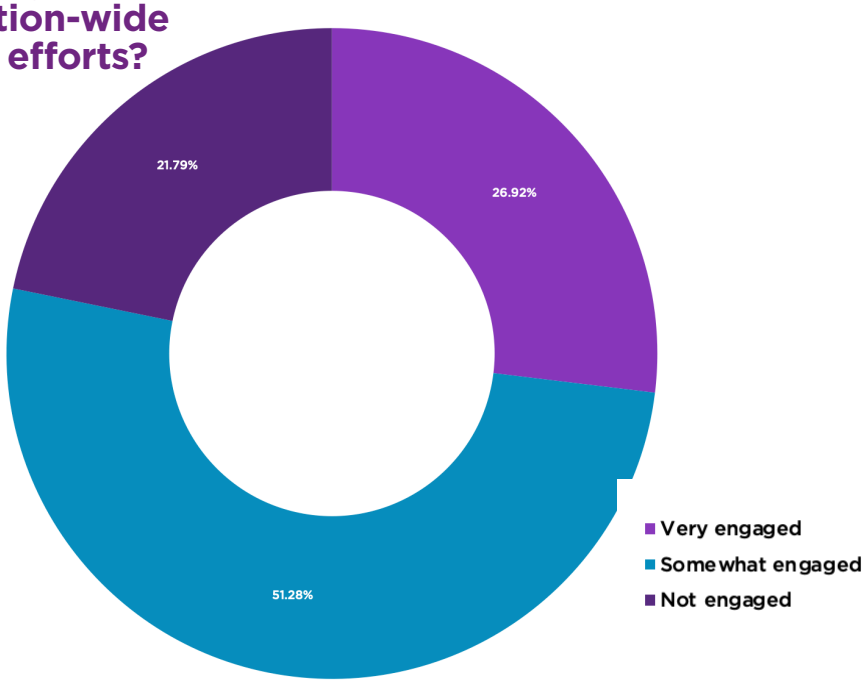
2021 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS AND CLOUD INITIATIVES

# ENGAGING LEADERSHIP

Engagement of elected leaders regarding Cybersecurity continues to be somewhat of a struggle for local government IT executives, with 73% of respondents stating that their leaders are just somewhat engaged (51%) or not engaged (22%) with their organizations' Cybersecurity efforts.

Effective engagement is important: The more familiar that elected leaders and senior managers are with cyber operations, governance, priorities, threats, and their organization's cyber strategy is essential towards the support in making important budgetary as well as broader policy decisions.

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



> “True leaders strive to be engaged in the betterment of their organization; engaging in cybersecurity shows the support and importance to protect the data of our citizens and businesses we support directly and indirectly”

*Adam Frumkin*
*Chief Information Officer, Franklin County, Ohio Data Center; Chair, CompTIA-PTI City/ County Technology Leadership Forum*

2021 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS AND CLOUD INITIATIVES

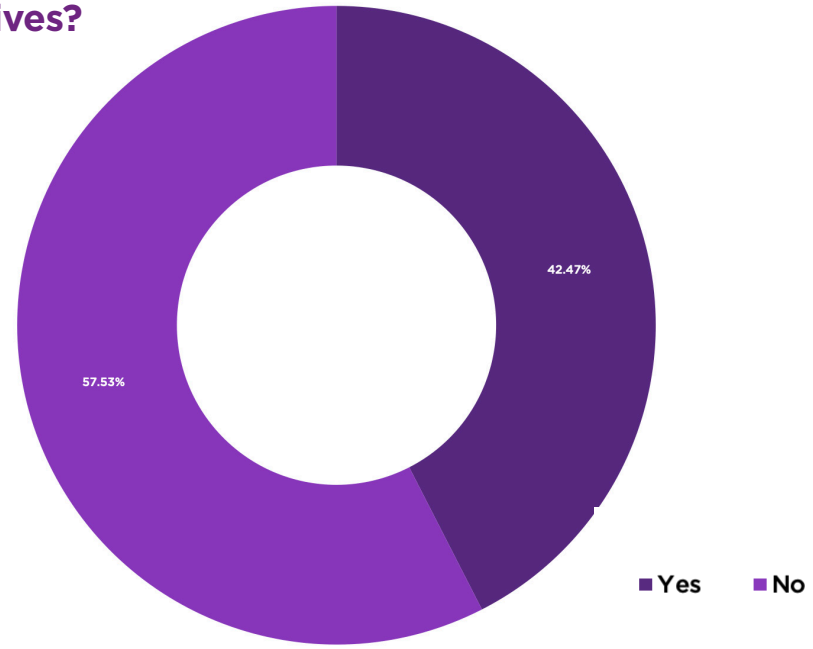
# BUDGETING

Fifty-eight percent of IT executives stated they felt that their organization's Cybersecurity budget is not adequate to support security and cloud initiatives. While still a worrisome concern, this is an improvement from the 2020 survey, where 64% or executives felt that their cyber budget was inadequate.

Fifty-nine percent of IT executives share that their Cybersecurity budget has increased from last year. Thirty-seven percent state that their cyber budget remained the same.

Beyond the survey, PTI members inform us that some federal funding is being specifically directed towards network monitoring and in some cases replacement of aging and hard to secure digital infrastructure.

## Is your Cybersecurity budget adequate to support security and cloud initiatives?



“Budgeting for your Cybersecurity needs should never be a “add on” or an afterthought. Make sure your plans will be funded properly and remember, this is a new concept for your city/county executives. Successful cyber budgeting has to come with an education on both needs and risk both to get buy-in.”

*Bill Hunter,*
*Bill Hunter, Director of Communications and Information Technology, Roanoke County, Virginia; Vice Chair, CompTIA-PTI City/ County Technology Leadership Forum*

2021 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS AND CLOUD INITIATIVES

# POLICIES AND PROCEDURES

Eighty-one percent of IT executives state their local government has a government-wide Cybersecurity policy that sets rules for employee behavior and organization operational safeguards and procedures.

Seventy-three percent of respondents state that their policy has been reviewed over the past twelve months. PTI reminds leaders that policies and procedures are only as effective as their review and, where appropriate, testing.

Of those governments with a policy, 50% share that there are exceptions to the organization-wide Cybersecurity policy that are allowed and those exceptions are documented.

Ninety-two percent of respondents state their jurisdiction provides employees with cyber awareness training – what to do and what not to do when it comes to Cybersecurity. Fifty-nine percent state that training is provided on an on-going basis throughout the year; 34% state that training is provided once a year.

When asked if elected officials, their staff and senior leadership are exempted from awareness training, 24% responded yes. It is important to remember that email addresses and contact information for elected leaders and management are easily available, meaning these officials are prime targets for phishing attempts and probing of government IT systems. Allowing for exemptions may also set a bad and demoralizing example to others in the organization who are required to follow strict protocols.

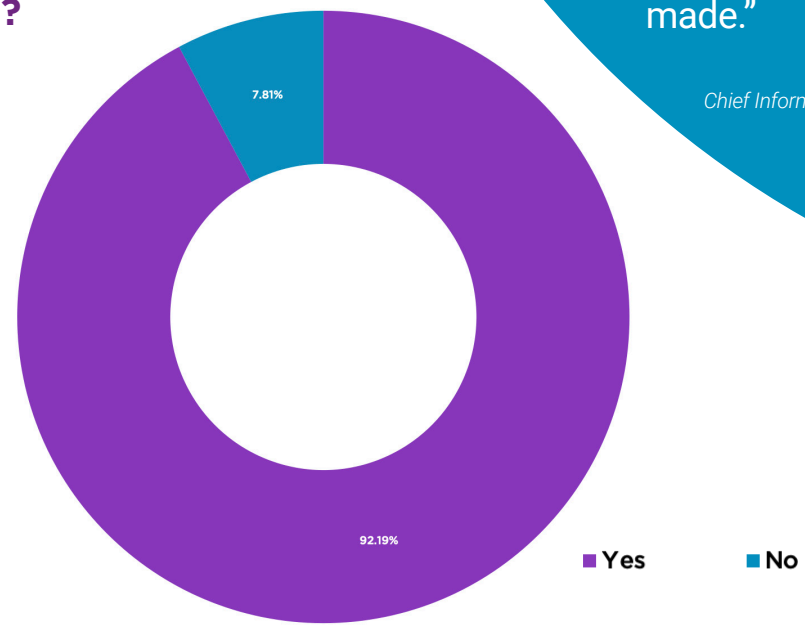
Maintaining a formal incident response plan and disaster recovery plan that is tested annually is a practice that PTI actively promotes. Forty-two percent of respondents do follow this recommended practice – a similar percent of responses from the 2020 survey.

> “Security awareness training comes in multiple forms. Regardless of the form you have, it is critical to do awareness training continuously so users remain vigilant in your organization’s efforts to prevent and defend against attacks. In addition to traditional awareness efforts, CISOs need to ensure they educate the leadership in their respective organizations on the risks they are facing in terms they can understand so the proper decisions on investments for prevention and risk mitigation can be made.”
>
> *Michael T. Dent,*
> *Chief Information Cybersecurity and Privacy Officer, Fairfax County, Virginia*

Regarding network security and auditing: 33% share that their jurisdiction has conducted a network or security audit of all IT systems and policies within the last twelve months, 54% have tested or audited some systems and polices, and an alarming 13% have not conducted any system test or audit in the past year.

When it comes to Mobile Device Management, 65% of IT executives state that their organization has a policy in place for employee or contractor access to government information systems. This is a 10% increase from the 2020 survey.

## Does your jurisdiction provide for employee awareness training (what to do and what not to do when it comes to Cybersecurity)?



2021 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS AND CLOUD INITIATIVES

# THE CHIEF INFORMATION SECURITY OFFICER

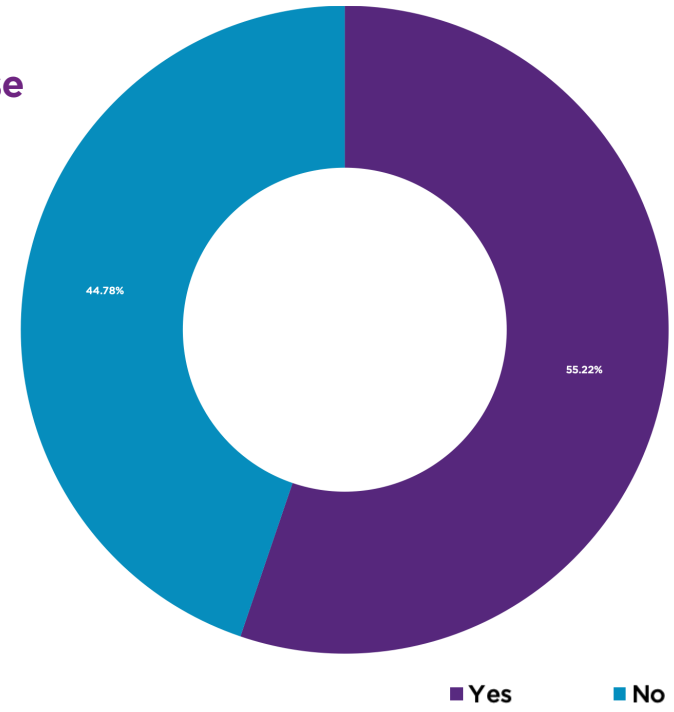
Fifty-five percent of respondents state that their organization has a CISO-type individual whose job responsibilities are both strategic and operational (managing the day-to-day operations) for their organization's Cybersecurity efforts. This is a slight increase from the 2020 survey – up from 53%.

The majority of these officials report to the CIO or IT executive – 59% - while 16% state that this position reports to the city/county manager.

Nineteen percent of IT executives who responded to this question stated that they serve dual roles: CIO and CISO. This is particularly true in many smaller local governments with limited staffing and resources.

Over the past several years the demands for greater high-level cyber planning and coordination has become a fulltime responsibility unto itself.

**Does your organization have an individual whose job responsibilities are both strategic and operational (managing the day to day) for your organization's Cybersecurity efforts?**



> “Having a CISO is growing in importance to better balance and manage cyber risk factors that affect every organization. This role places an importance on innovation and protection of critical data and systems.”
>
> *Adam Frumkin,*
> *Chief Information Officer, Franklin County, Ohio Data Center; Chair, CompTIA-PTI City/County Technology Leadership Forumnia*

2021 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS AND CLOUD INITIATIVES

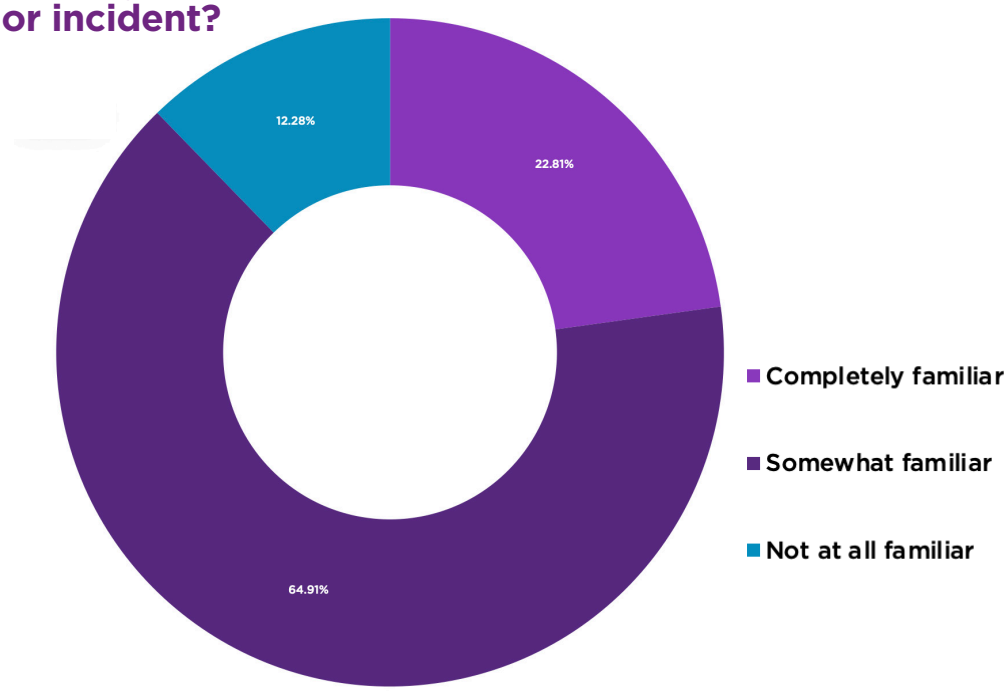
# CYBER INSURANCE

Ninety percent of respondents state that their organization has cyber insurance. This is an increase from the 2020 survey where 78% of respondents stated that they had cyber insurance.

Cyber insurance policies are increasing in complexity with more stringent procedures to adhere to. This could be why only 23% of IT executives share that they are completely familiar with their insurance policy requirements and procedures to immediately follow in the event of a breach or incident; 65% share that they are somewhat familiar with their policy requirements and 12% share that they are not at all familiar with their policy requirements.

Sixty-nine percent share that their cyber insurance premiums have increased since the last renewal date.

## How familiar are you with the insurance policy requirements and procedures to immediately follow in the event of a breach or incident?



> “Cyber insurance has become a critical layer of our Cybersecurity strategy, but like any tool it’s important we know how to use it. It’s important that IT and City Leadership understands exactly what the mechanics of their policies are before an incident if they want to get the full value out of it.”

*Darryl Polk*
*Director of Innovation and Technology*
*City of Rancho Cucamonga, California*

2021 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS AND CLOUD INITIATIVES

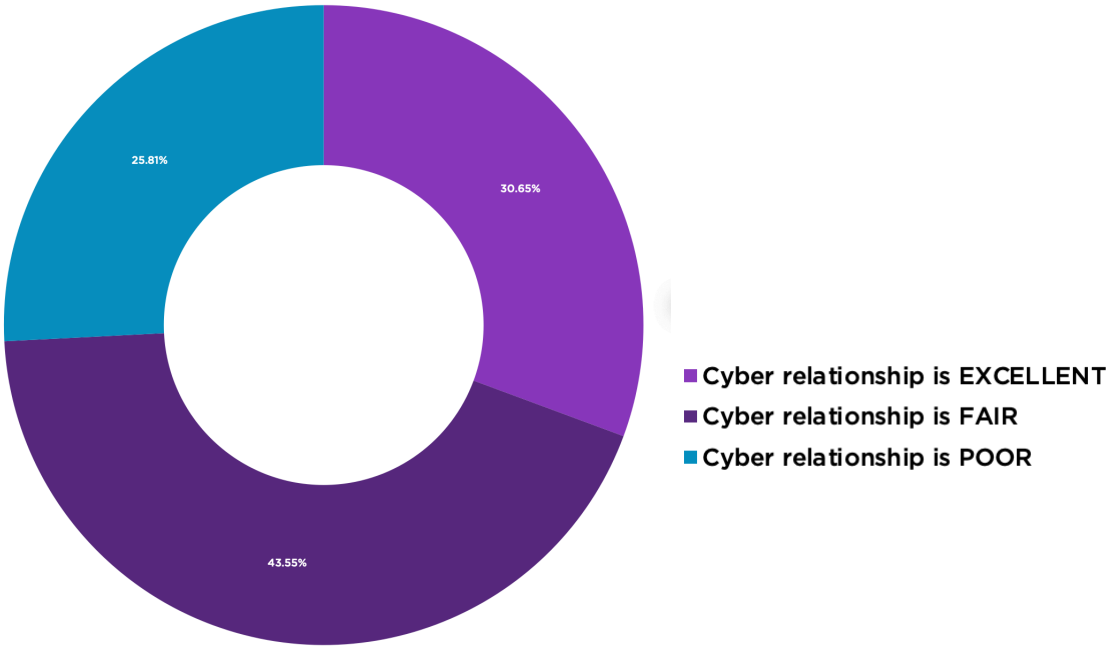
# STATE AND LOCAL COLLABORATION

When asked to rate the relationship between the local government IT organization and their state's IT organization in terms of information-sharing, resource-sharing, education and training provided by the state to local governments – specific to Cybersecurity – 31% rated the relationship as excellent. Forty-four percent of IT executives rate the state-local cyber relationship as just fair, and 25% rate the relationship as poor. Clearly, more work needs to be done to foster collaboration.

Organizations like CompTIA-PTI and the National Association of State Chief Information Officers (NASCIO) continue the push to educate state and local officials as to the need to build effective and trusted partnerships. Despite these worthwhile goals and initiatives, many tech leaders have often lamented that they have almost zero relationship with state IT agencies – let alone the state CIO.

> “Collaboration is a two-way street: Don’t wait for your state colleagues to approach you. Reach out to your state CIO and begin the dialogue around resources, key contacts, and information-sharing that will strengthen your cyber efforts.”
>
> *Dr. Alan Shark,*
> *Executive Director*
> *CompTIA-PTI*

**Specific to Cybersecurity: 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?**



2021 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS AND CLOUD INITIATIVES

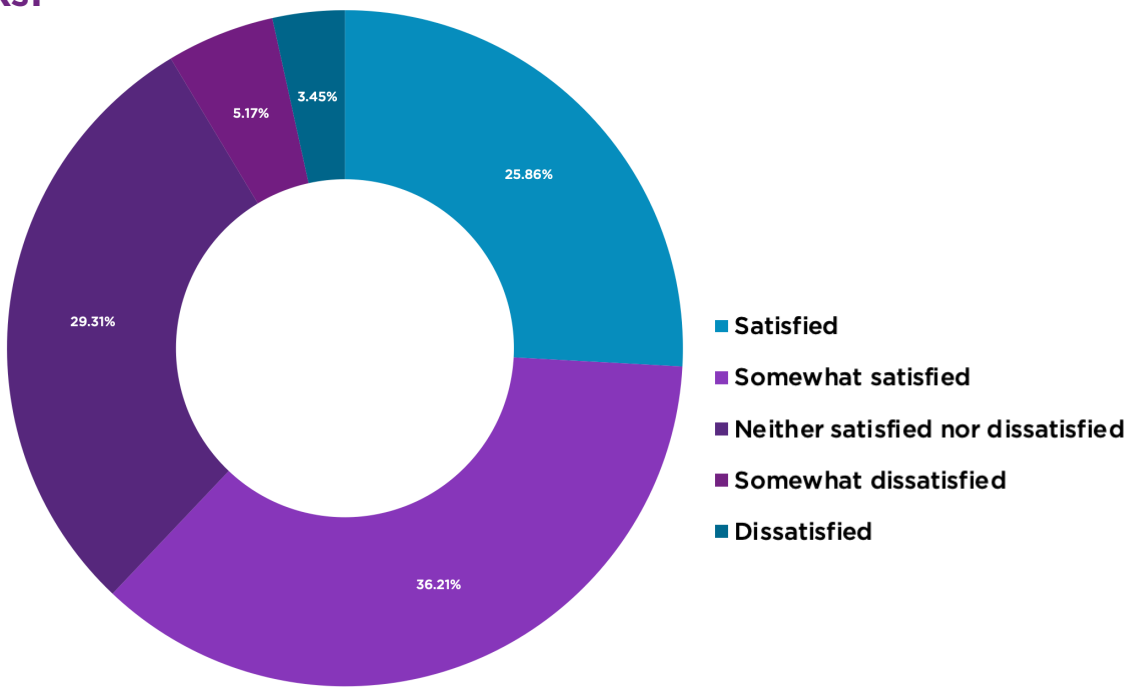
# MANAGED SERVICES

For those IT organizations that rely on a managed service provider, in any form, for IT services, 26% of executives state that they are satisfied with the security protocols for the service providers of their networks. Thirty-six percent share that they are somewhat satisfied, 30% are neutral – neither satisfied nor dissatisfied, and 3% state they are dissatisfied.

Based on dozens of in-depth discussions with tech leaders PTI believes more city and county governments will ultimately turn to managed serve providers given the challenges in attracting and maintaining competed IT staff – let alone supporting legacy systems.

> “In today’s age of ever-growing cyber threats and attacks it is even more important that we in IT dot all our “I’s” and cross all our “T’s” to ensure that both our data and our users are protected. It is so easy to focus on the big picture of attacks that we often forget the little things as we allow vendors the keys to our kingdom; remember the adage ‘Buyer beware!!’”
>
> *James E. Pacanowski II,*
> *Network Administrator, Ventnor City, New Jersey*
> *Leader Forum*

**Recent ransomware attacks on managed services providers and their customers have made headlines. If you rely on a managed service provider in any form, how satisfied are you with the security protocols for the service providers of your networks?**



2021 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS AND CLOUD INITIATIVES

# CLOUD INITIATIVES

Thirty-one percent of IT executives are planning for a substantial cloud computing implementation in the next 12 months, while 27% of respondents say they are already using cloud computing services.

For those planning or already using the cloud, the top five cloud solutions they will invest in are, in order: website hosting, internal operations (email, calendars, communication, etc.), data backup and recovery, data storage, and device management.*

For those planning or already using the cloud, the top five subject matter areas that will utilize cloud computing are information technology, human resources, finance, code enforcement, and community engagement.*

When it comes to the primary benefits that IT executives have either experienced, or expect to experience with cloud computing, the top benefits are: Enables employees to work remotely, enables citizens to interact with government better, and connects departments to each other.*

Local government IT executives feel quite confident regarding the security measures of the cloud services or providers they utilize, with 83% of respondents stating that they are very confident (34%) or confident (49%) with their security posture.

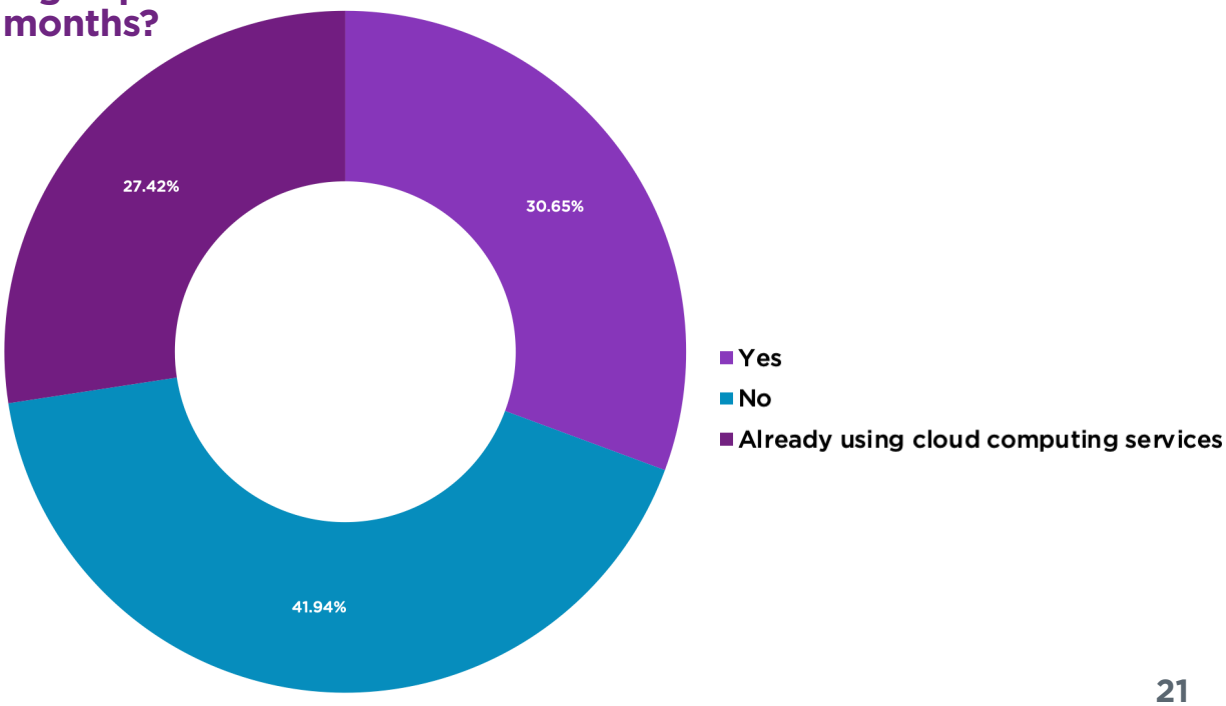
For those organizations not currently using, or considering, cloud computing, the top three reasons given are, in order: cost of services, cost of implementation, and current systems are working well enough now.*

*For each of these questions, survey participants were provided a list of answers to select from. Participants could select as many of the choices that applied to them.

> There are many positive aspects of Cloud Computing. For CIOs, key factors to consider are data security and 'Who's Cloud" am I in?' While the question sounds humorous, many vendors can change Clouds at their discretion and without notifying you. Remember, move at your pace, not that of the vendor."

*Bill Hunter,*
*Director of Communications and Information Technology, Roanoke County, Virginia*
*Vice-Chair, CompTIA-PTI City/County Tech Leader Forum*

## Are you planning for a substantial cloud computing implementation in the next 12 months?



# Conclusion

With a thank you to the local government IT executives who participated in this survey, we have, I believe, a valid picture of the local government Cybersecurity landscape. Threats will never go away – they will only increase. The job of protecting our technology and telecommunications infrastructure will become more complex and difficult – at a time when many local governments are struggling to keep and attract cyber professionals. The frontline of our cyber defense are these professionals – and we must look to invest in new strategies to retain and grow our cyber talent.

CompTIA-PTI has created an important new network for CISOs and officials responsible for IT Security in local government; the CISO/Cyber Leader Forum.

In conversations with many local officials, PTI identified a desire on behalf of officials to form a network of cyber leaders that would foster communications and information sharing with each other, and to further develop CompTIA-PTI's local government Cybersecurity research agenda.

This network is designed to serve as a valued and trusted resource for local government leaders and technology practitioners when it comes to the Cybersecurity issues impacting local government. We also hope to take some of the issues that participants in the forum identify and develop educational programming - webinars, metrics and tools to measure cyber practices, this annual survey - to help all local governments in their cyber programming

For more information on the CISO/Cyber Leader Forum, please contact Dale Bowen, Senior Manager, CompTIA-PTI, dbowen@comptia.org