IT Operations and Support: COVID-19 and the Local Government IT Response

Introduction

Local governments are on the front lines of the nation's ongoing response to the COVID-19 pandemic, providing health and human services and other essential assistance to their constituents on a daily basis.

Information technology professionals within cities and counties of all sizes have been called upon to help other departments and colleagues maintain the delivery of essential programs by enabling remote working (sometimes for staff who had never worked from home) and managing all the logistical and security issues that come with a remote workforce. They are doing this all while dealing with a stressful and constantly changing environment.

Over the course of 45 days, the Public Technology Institute (PTI) interviewed 172 CIOs and other IT leaders to better understand how local government IT professionals are responding to the COVID-19 crisis.

Realizing that a more formal/research-oriented view of local government IT operations was needed – to gauge what local government IT is dealing with now, and how it is bracing for the future – PTI created a survey asking local government CIOs to share their experiences and insight in dealing with the pandemic.

While this research focuses on IT operations and management during the COVID-19 crisis, we felt it important to explore local government technology response and issues related to the pandemic.

The number of responses surprised us. It was comforting, and optimistic, to see how local governments are willing to share their lessons learned with each other, with the hope that we,

as a community of local government officials, can be better prepared for future crises that will undoubtedly impact our communities.

A heartfelt “thank you!” to our local government IT leaders and IT professionals for their work and commitment to help our communities function and deliver services during a difficult and uncertain time.

The following report highlights the results of PTI’s research. In reading through the responses, PTI emphasizes some of the comments and themes that came across during our analysis:

- Execute your Disaster Recovery/Business Resumption plan early
- Watch the trends and prepare early. It is better to be prepared and not implement than to scramble to put a program together
- Security comes first. Stop rushing to cover the bases before running a new system into production
- The "stress testing" that IT has conducted in the past has shown the strengths and weaknesses of remote systems and placed renewed emphasis on security
- Have department directors be more proactive in pursuing and promoting telecommuting capabilities. There is a general feeling that work can't be performed remotely – it can!
- Create a telework policy and ensure that all essential staff are outfitted with mobile devices (laptops) with VPN
- Be informative and direct; communicate often. Think outside the box
- Be prepared to shift to supporting users by phone and email

We also appreciate the comment of one CIO who said: “Trust in your tools and your knowledge, but never underestimate the power of kindness in those that need your help.” Indeed, wise words to keep in mind.

With all the fear and uncertainty that we are experiencing and feeling, consider this: In every crisis there is the opportunity to innovate. Whether it be to identify new work processes or practices, to take advantage of emerging technologies and tools, or to reinforce what we already know and the procedures we have in place: we are now dealing with a new dynamic.

How are you, a technology leader, helping your organization to use innovation to engage the public during this crisis? What innovative tools and techniques are you utilizing to maintain IT operations or assist other departments and agencies in delivering much-needed services? What are you doing to motivate and to recognize your team?

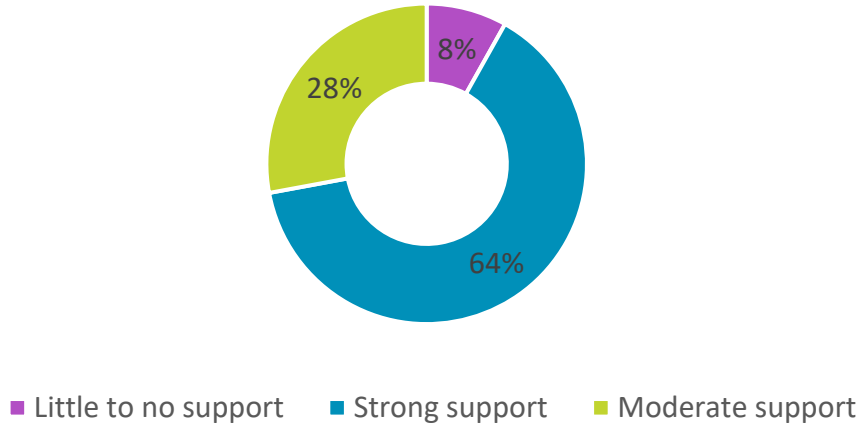
Perhaps, most important, how are you driving innovation with your government’s leadership during this uncertain time?

Finally, before you examine the results of this PTI research report, PTI would like to echo the sentiment of one CIO who responded to our survey: *Stay calm and carry on!*

IT Operations and Support: COVID-19 and the Local Government IT Response

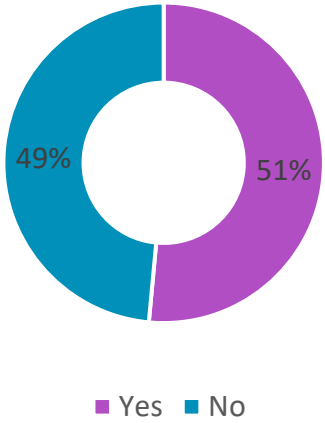
The management support and recognition that the IT department has received as staff has responded to the tech challenges resulting from delivering services during the pandemic has been positive, with 64% of CIOs responding that that have received strong support. 28% stated that they have received moderate support while 8% feel that they have gotten little to no support.

Question: *What type of support and recognition has the IT department received as you and your staff respond to the tech challenges resulting from delivering services during the pandemic?*



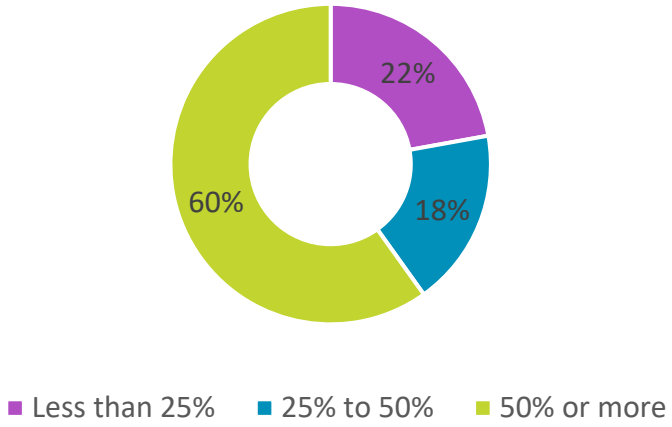
When it comes to the potential economic impact of the pandemic on local revenues and budgets, just over half – 51% - feel that their IT department budget will be reduced by the end of 2020. 49% stated that they do not expect their budgets to be reduced.

Question: *Do you anticipate that your IT department budget will be reduced by the end of 2020 due to the economic impact of COVID-19 on your community?*



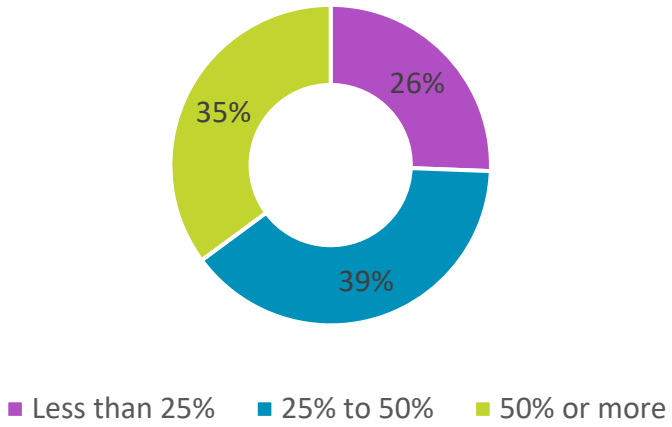
Local governments have had to move quickly to implement work-from-home policies and procedures, with many government facilities closed to both the public and to staff. With regard to *IT staff working from home*, 60% of CIOs state that half or more of their IT staff is working teleworking. 18% of CIOs state that between 25% and 50% of their staff is teleworking while 22% say that less than 25% of IT staff is teleworking.

Question: *What percent of IT employees are now teleworking?*



Local government IT departments have been called on to provide equipment and assistance to other government departments as they ramped up work-from-home for their staff. Government-wide, 35% of CIOs state that more than 50% of *all jurisdiction employees* are teleworking. 40% of CIOs state that 25% to 50% of government employees are teleworking. 26% state that less than 25% of all employees in their respective government are working from home.

Question: *What percent of government-wide employees are now teleworking?*



Several CIOs commented that supervisors and managers need to be more proactive in pursuing and promoting telecommuting capabilities, though in a number of organizations there is a general feeling that work can't be performed remotely. When making the case for telecommuting, supervisors need to define clear work goals for their remote employees so IT can provide the correct solution to the employee.

Just over one-third of CIOs (34%) stated that government employees have complained about or expressed frustration with connectivity issues.

An astounding 98% of IT agencies have been called on to provide access or support for virtual meetings and video conferencing for other departments. The top three platforms being used are Microsoft Teams, Cisco WebEx, and Zoom.

17% of CIOs stated that they have had to install new broadband capacity in order to increase overall broadband/internet connectivity to address teleworking demands and capacity, 14% stated that they have increased server virtualization.

CIOs also shared other insight:

- We have built up our broadband capacity over the last 3 years and are in a good place currently with throughput and redundancy
- We added VPN licenses and added VDI capability in Azure to alleviate bottlenecks on our bandwidth

When provided with a list of choices regarding the priority or training needs that they have identified as lacking or could use improvement with IT staff, 48% cited *network security* as a priority. This was followed by infrastructure management, cloud security, broadband management, and network operations, in order.

CIOs also shared other areas where training and staff development is needed, for IT staff and non-IT staff in government operations:

- End user training as we deployed remote technology and security features like two-factor authentication. Typically, we do a lot of hand holding but with a dispersed staff, it has been even more difficult with more one on one phone support
- Security training and tools for remote workers
- Contingency planning. As a large number of the workforce migrates to a work from home scenario additional machines are needed to send home with them. Ideally, I would have saved more "retired" laptops to be repurposed as home machines for VPN access to City systems and desktops
- End user training, how to VPN, how to access remote devices/services through VPN
- Rolling out and supporting cloud initiatives
- COOP plan testing for departments and end users
- Use of VPN, Microsoft Teams and video conferencing software
- End user training for the use of the technology we already owned (O365). User adoption has dramatically increased out of necessity

- Computer Training. Most of the people working in our government do not know much about computers beyond their specific department programs
- Use of Office365 tools (Teams, Yammer), how to Zoom Conference Call, and the use of our new electronic timesheet (Executime) which we just decided to roll out ahead of schedule
- We need to have increased cloud usage and less centralized file storage
- Basic computer skills for our staff. They have been forced to do more on their own at home. i.e. setting up computers, monitors, printers, etc.
- Cross training

34% of CIOs shared that relaxed or modified BYOD policies for those employees who use their own equipment under telework. For those IT agencies that have modified their policies, several shared:

- If the employee has their own device, they have been permitted to use it; we are small and did not have a surplus of laptops for use offsite. No file transfer is allowed and the connection is secure
- We have allowed more users the authority to use existing VPN capabilities under the same guidelines as before
- The Information Technology Department has to examine the remote device
- We don't even have time to address through policy. We have implemented more security checking through our VPN appliance
- We have allowed employees to use their own equipment to access systems. We have given them guidelines of what they can use
- We revised the remote work policy to tier application use - VPN only used on City owned/managed devices, VDI allowed on BYOD with Department Head approval, encouraged use of Office 365 web portal for all others
- Validating home computer is patched and anti-virus protected
- We typically don't allow home computers to use a VPN to access our network. We've been forced to allow it so they have access to our network

Regarding the steps that CIOs have taken to better secure the enterprise as a result of employees teleworking, 77% stated that they require VPN connectivity. 54% stated that remote employees are permitted to use only approved software, and 53% require employees to have a certain level of malware or virus protection on their devices.

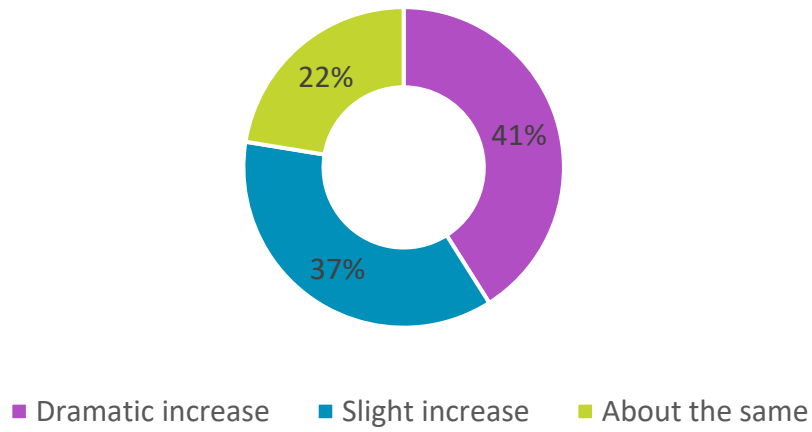
When asked to provide examples of their security efforts, CIOs shared:

- Two-factor authentication (2FA). We already had secured remote access in place but quickly completed 2FA that was in progress to the remaining 70%
- We do allow users to use their own machine, but they must go through a secure web portal to remote into their work machine. Otherwise, they are using their government-supported device with VPN connectivity
- Can only use government-supplied devices. Employees must be enrolled in multi factor authenticity

- Since we have been using VDI technology for over a decade we have always had users use 2FA when attaching to our network externally. We had to provision 2FA for those users who normally never telecommuted and they could then access our resources from outside the government network
- Block Windows 7 and earlier window systems
- Limit the number of employees who can remote in. Non-essential employees do not have VPN access
- Increased phish testing
- Training, warning messages, raising awareness overall
- Employees who work-from-home must fill out an approval form signed by the department head. The approval form includes inventory of equipment taken from the government building (whether on loan, or normally in the office.) IT maintains the inventory
- We already required VPN, only allow approved software, and require agency provided virus protection. None of this needed to change. We had also setup over 95% of our employees with laptops and docs prior to this just in case something came up, so we were prepared in advance

As more government employees work from home and use video or teleconferencing platforms that they may not be used to, 41% of CIOs shared that they have experienced a dramatic spike in IT help-desk requests. 37% say there has been a slight increase while 22% stated that the amount of help requests has remained about the same or even decreased a bit.

Question: *Have you seen a spike in IT help-desk requests?*



As for the types of partnerships, if any, that local government IT departments have entered into with other jurisdictions or the private sector to secure equipment, to share resources, or to share staff expertise, we asked CIOs to cite examples. There are a variety of themes that CIOs identified, including:

- Participating in collaborative networks that provide for information-sharing and city/county officials who volunteer their time to go to a jurisdiction that is experiencing service delivery or security difficulties as a result of a crisis and provide expertise
- Utilizing a consortia of government agencies to share and utilize common IT resources for applications and infrastructure, security initiatives, software procurement and staffing resources

Several CIOs disclosed that as a common practice, they have contracts in place with third-party vendors and other business partners that they are able to utilize during emergency situations.

CIOs also stated that their agencies have agreements or partnerships to work closely with and share resources with other local government IT agencies, school districts, or regional agencies. Some CIOs have reached out, either individually or more formally through their agency, to neighboring communities to provide guidance and insight.

The common theme that arose is the need for CIOs to communicate with each other, not just in terms of a crisis, but to develop and maintain relationships with other technology leaders in their area and in their state.

Working with the Vendor Community

During our analysis of the survey results, we decided to reach out to respondents to ask "As you implement new work processes and business continuity, how has your vendor community - those companies that you have been doing business with for some time – responded?" 46% of CIOs responding to this follow-up question stated that the majority of vendors have been *very fast and responsive to our requests and needs*. 38% responded that the vendor response has been about the same in terms of response time and fulfilling our needs/requests as prior to the start of the crisis. 15% stated that the response has been mixed or poor.

Conclusion

Local government – Leadership, IT professionals, medical practitioners and public safety professionals – continue to provide a most important – if, unfortunately an under-appreciated role – in the response to the COVID-19 pandemic.

Of the IT leadership lessons to be learned, and shared:

- Practice your resiliency and continuity of operations planning
- Position IT as a partner! Communications with staff, elected leaders and management, other departments is imperative
- Always assume government employees may need to work remotely for one reason or another
- Utilize electronic means of conducting business, for example, accepting payments online vs. printing and mailing paper bills and invoices
- Cybersecurity is paramount
- Network and share with other local governments, state agencies and federal partners

About PTI

Established in 1971 by several major national associations representing state and local governments, PTI has been viewed as the focal point for thought leaders who have a passion for the furtherance and wise deployment of technology. PTI's initial funding was through a grant from the National Science Foundation. Today, PTI actively supports local government officials through research, education, professional development, executive-level consulting services, and national recognition programs.

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.