NETWORK NEEDS IN STATE & LOCAL GOVERNMENT

Every few years, a new technology emerges that forces IT organizations to rethink network infrastructure —

the foundation for their applications and activities. In the 1990s, the web emerged as one of those transformative technologies. More recently, cloud services have prompted similar re-evaluations, and the Internet of Things (IoT) will likely do the same.

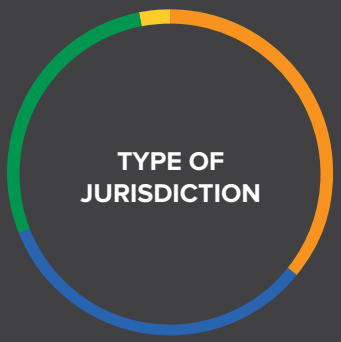
Given that ongoing evolution, it's helpful for state and local governments to examine how they plan for and implement their enterprise networks, and to compare their strategies with the approaches in other jurisdictions.

In October 2017, the Center for Digital Government (CDG) surveyed 318 state and local government IT employees and conducted 12 additional telephone interviews. This research provides interesting insights into their network-related priorities and challenges now and in the future, and highlights what is driving agencies to re-evaluate their networks.

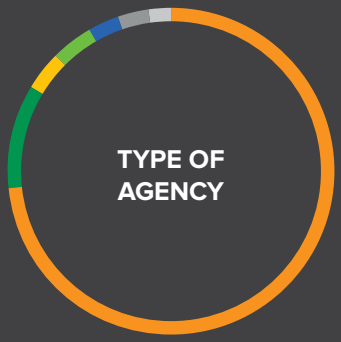
Not surprisingly, increased cloud adoption is putting additional demands on agency networks. Agencies are also concerned about the security of their networks — with good reason. Nearly a third of survey respondents say their networks are very or somewhat vulnerable to a breach. In terms of priorities, agencies are interested in a solution's ability to integrate with existing infrastructure when procuring network services. Nearly 60 percent of respondents listed this as a top factor for their agency as they invest in new technologies. Finally, and perhaps somewhat surprisingly, only one-third of agencies say that IoT has prompted them to re-evaluate their network. However, CDG expects this number to increase as IoT technology adoption increases, and agencies see this adoption strain their networks, similar to cloud.

Respondent Demographics

This report is based on a survey of 318 state and local government officials and 12 additional telephone interviews for more in-depth information.



- State: **36**%
- County: **33**%
- Municipality: **28**%
- Special District: **3**%



- Information Technology: **72**%
- Justice and Public Safety: **10**%
- Public Works and Transportation: **4**%
- Health and Human Services: **4**%
- Administration: **3**%
- Finance: **4**%
- Other: **3**%

IT officials with most state and local governments consistently evaluate their networks.

About two-thirds of survey respondents said they review their networks on a regular basis. However, "regular" does not always mean "frequent." Twelve percent of respondents conduct these reviews only every three to five years, and two percent do so every six to 10 years. Still, more than half of these government officials evaluate their networks every two years or less.

- Annually: **45**%
- Every 2 years: **8**%
- Every 3 to 5 years: **12**%
- Every 6 to 10 years: **2**%
- As-needed: **10**%
- We do not regularly evaluate: **7**%
- Other: **3**%
- Do not know: **14**%

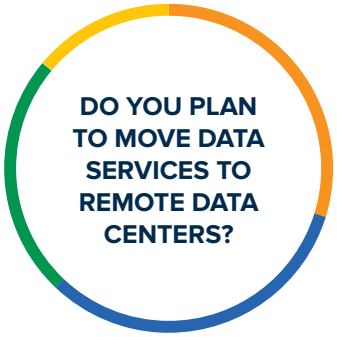
Cloud services are becoming increasingly important — but also strain agency networks.

Two-thirds of respondents currently use cloud services, and another 20 percent plan to procure cloud services. More than half of the responding jurisdictions plan to expand their cloud footprints. About a quarter of respondents said they have already moved data services from on-premises data centers to remote facilities, including public cloud services. Another 30 percent say they plan to make this change.

While cloud often allows state and local government to reduce costs and increase efficiencies, when interviewed, leaders specifically noted that cloud adoption — and shared services in particular — puts additional strain on their networks.

- In-use: **67**%
- Planning to procure: **20**%
- Not in use and not procuring: **9**%
- Do not know: **6**%

- Yes: **56**%
- No: **21**%
- Don't know: **23**%



- Yes: **30**%
- No: **32**%
- Already have: **24**%
- Do not know: **14**%

Network security is a critical concern.

Only a small minority of respondents feel their networks and systems are extremely safe from a potential security breach. Thirty-three percent of them say their networks are somewhat or very vulnerable.

- Very invulnerable: **13**%
- Somewhat invulnerable: **23**%
- Neither: **20**%
- Somewhat vulnerable: **28**%
- Very vulnerable: **5**%
- Do not know: **11**%

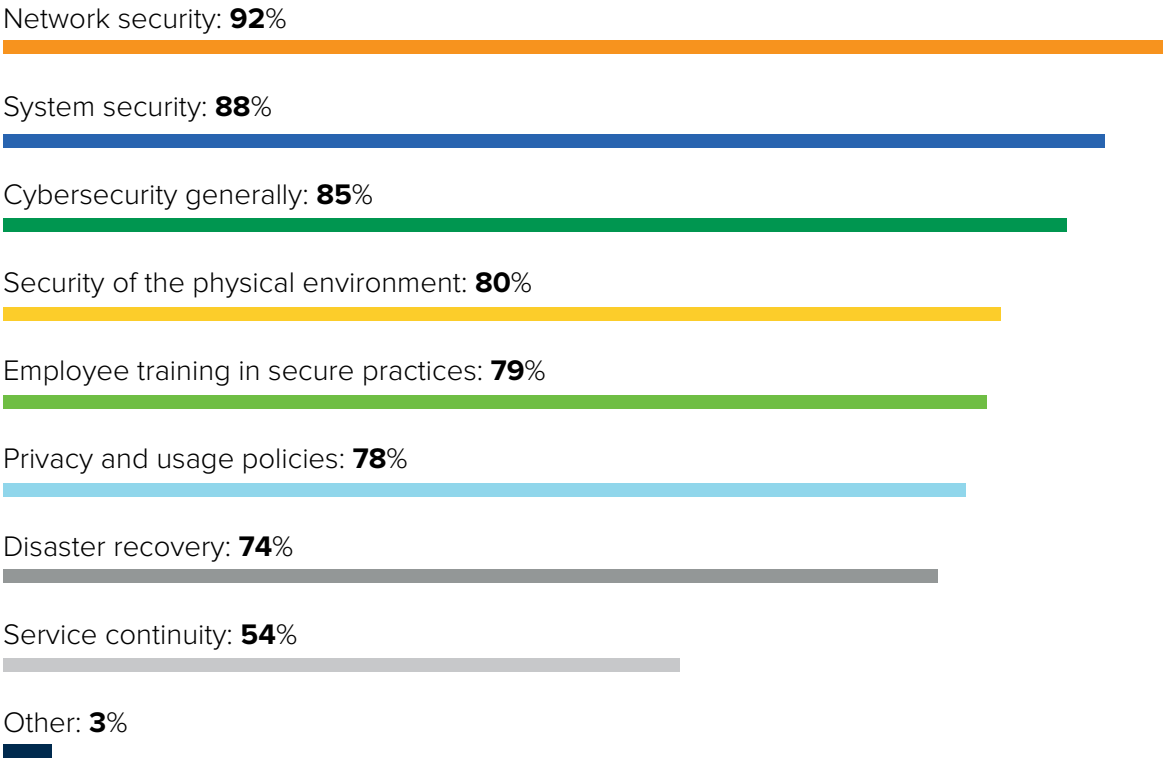
Respondents make these estimates with a fair level of confidence: 69 percent of them consider themselves knowledgeable about network security in their own jurisdictions.

- Very knowledgeable: **22**%
- Somewhat knowledgeable: **47**%
- Neither: **18**%
- Somewhat unknowledgeable: **9**%
- Very unknowledgeable: **3**%

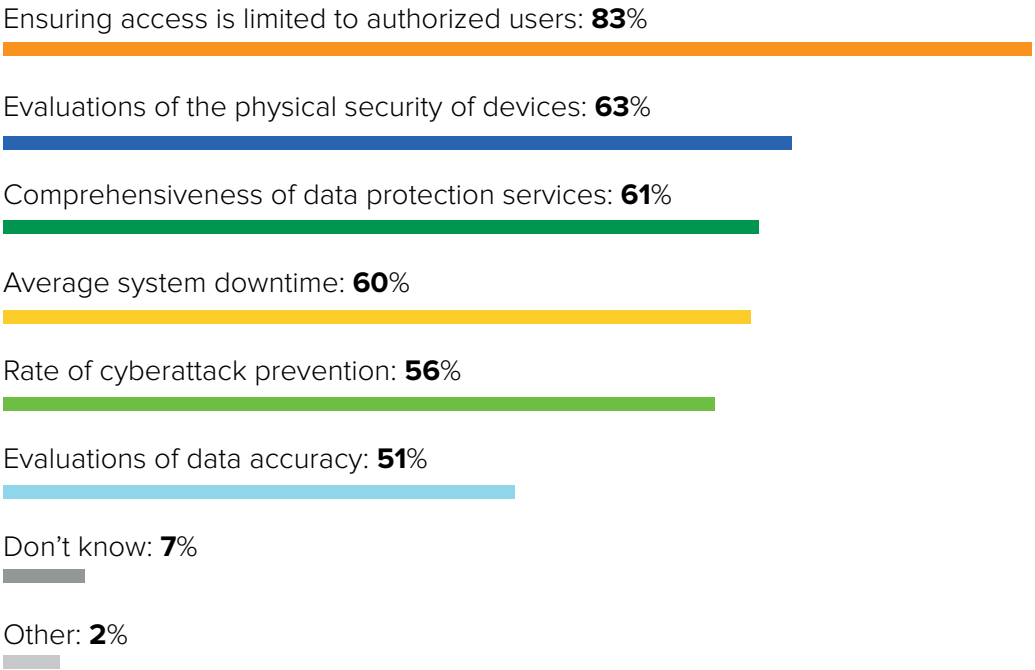
And when respondents talk about "security," they are referring to a broad range of issues. When asked to define security, respondents mentioned: service continuity, disaster recovery, privacy and usage policies, employee training in secure and safe practices, security of the physical environment, cybersecurity in general, system security and network security. Except for service continuity, each of those issues was identified as a component of security by at least 75 percent of respondents.

This broad view of security extends to network evaluations. When asked to name the security issues they focus on when re-evaluating their networks, users chose, on average, three different elements.

WHICH OF THE FOLLOWING ARE PART OF YOUR AGENCY OR DEPARTMENT'S DEFINITION OF "SECURITY"? SELECT ALL THAT APPLY.



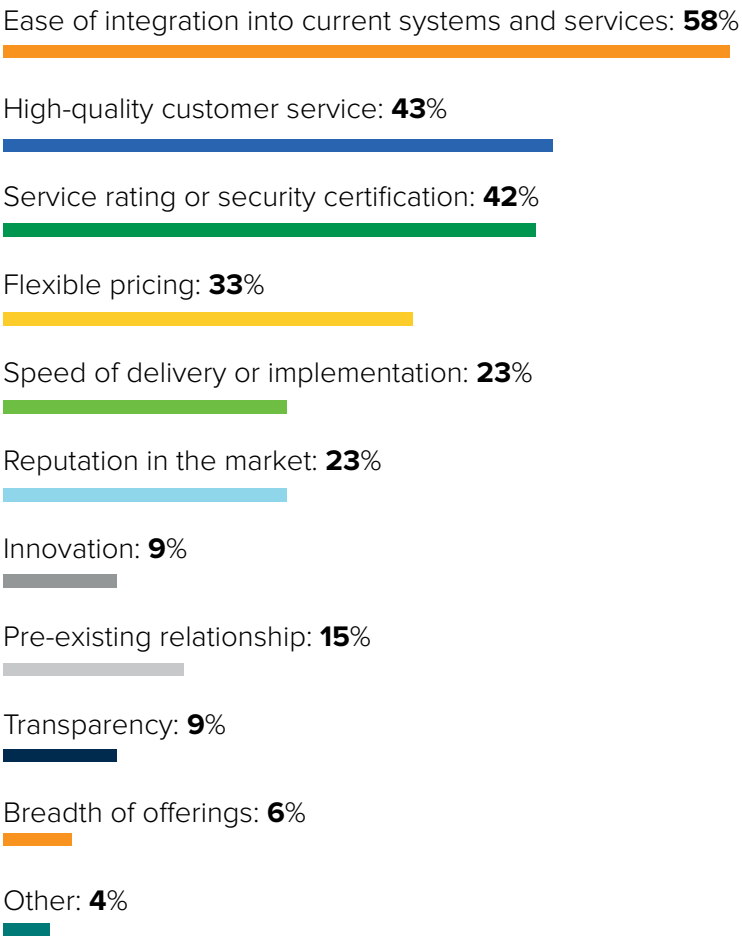
WHICH OF THE FOLLOWING ARE INCLUDED IN AN EVALUATION OF YOUR NETWORK SECURITY? SELECT ALL THAT APPLY.



Integration is highly valued.

Although they express concern about protecting their networks from attack and intrusion, government officials don't necessarily keep that imperative in mind when they procure products and services. When researchers asked respondents to name the most important factors at play when they procure network products and services, the top concern was how easily they will integrate with existing infrastructure.

WHICH OF THE FOLLOWING IS MOST IMPORTANT WHEN PROCURING NEW TECHNOLOGIES? SELECT UP TO THREE.



IoT is not a high priority — yet.

Although IoT has made a big impact in the technology world, this technology has not yet taken center stage in the network plans at many government organizations. A little more than a third of respondents said that the rise of IoT has not prompted them to re-evaluate their networks; another 28 percent didn't know whether it has.

When asked if their networks had enough capacity to handle the demand that IoT will impose on their organizations over the next 12-18 months, the number of respondents who didn't know the answer was roughly equivalent to the number who answered "yes."

- Yes: **34**%
- No: **38**%
- Don't know: **28**%

- Yes: **40**%
- No: **21**%
- Don't know: **38**%

Those responses diverge in an interesting way from what local government CIOs told CDG in our most recent annual Digital Cities Survey. The survey found that local government CIOs consider IoT an important element in their strategic plans.[1]

A set of in-depth interviews with 12 government officials that CDG conducted as part of its research for this report revealed another interesting fact about network planning and IoT: When IT officials do think about the impact that IoT will make on their networks, they are particularly concerned about the security implications of this technology.

Network planners at government organizations face many unknowns. One of those unknowns is the effect that IoT will have on the network as a proliferation of "things"— from simple sensors to "smart" equipment and appliances — vastly increases data traffic and creates many more data entry points on government networks. Most network planners in governments have yet to make plans to accommodate IoT. But they understand that they will soon have to make provisions for the new technology, and those plans must include a special emphasis on security.

Produced by:

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. The Center conducts e.Republic's annual Digital Cities and Counties Surveys; the biennial Digital States Survey; and a wide range of custom research projects. **www.centerdigitalgov.com**

For:

Spectrum ENTERPRISE

Spectrum Enterprise, a part of Charter Communications, is a national provider of scalable, fiber-based technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions, including Internet access, Ethernet and Managed Network Services, Voice and TV solutions, Managed Application, Cloud Infrastructure and Managed Hosting Services. Our industry-leading team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs.

For more information, visit: **enterprise.spectrum.com**

SE-GV-RR001