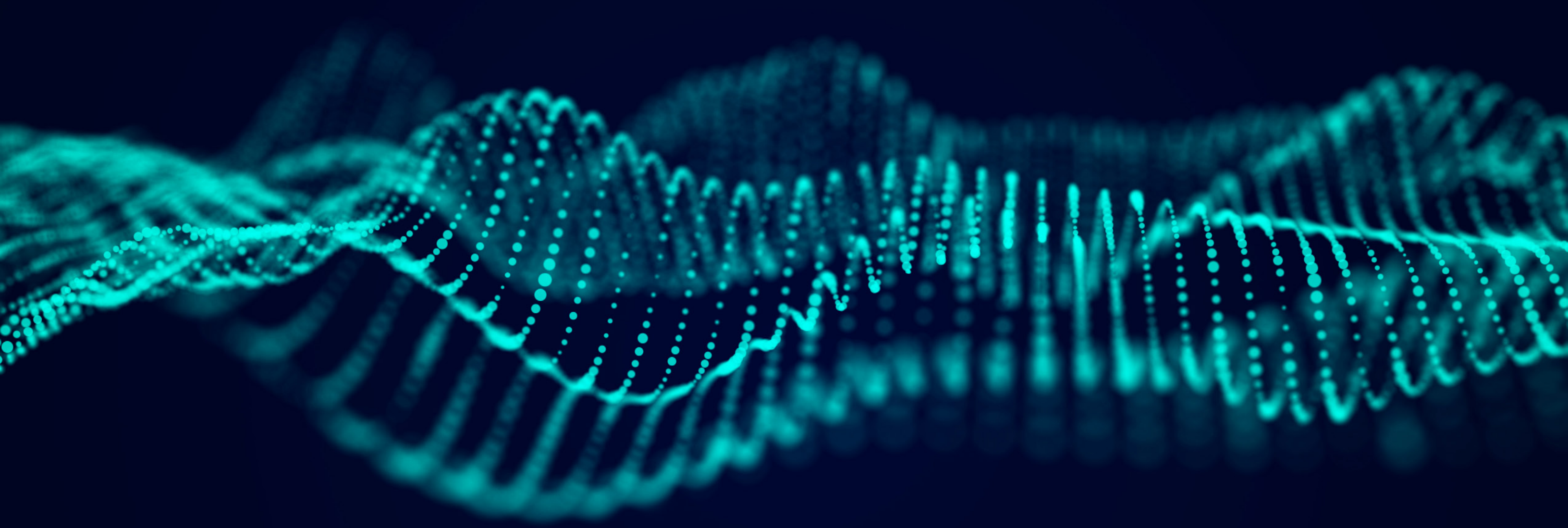
A CENTER FOR DIGITAL GOVERNMENT RESEARCH SURVEY

Future-Proofing Cybersecurity for Government and Education

For small and mid-sized organizations, the new hybrid work environment poses significant challenges.



Government and education IT officials consistently name cybersecurity as their No. 1 concern. Cybersecurity became a more urgent priority as the COVID-19 pandemic forced many employees to work from home. Even as the pandemic wanes, a large number of agencies and schools will likely keep at least some of their operations remote over the long term. Many public employees enjoy the convenience of a telework option.[1] And organizations see remote work as an opportunity not only to reduce costs, but also to broaden the talent pool of potential hires.[2]

Often, government and education IT professionals point to human error as the major threat to cybersecurity. With more employees taking government-owned devices home, IT leaders need to ensure employees are educated on cyber-safety. They also need to implement new security measures, such as multi-factor authentication and encryption, to protect data and networks in a hybrid work environment.

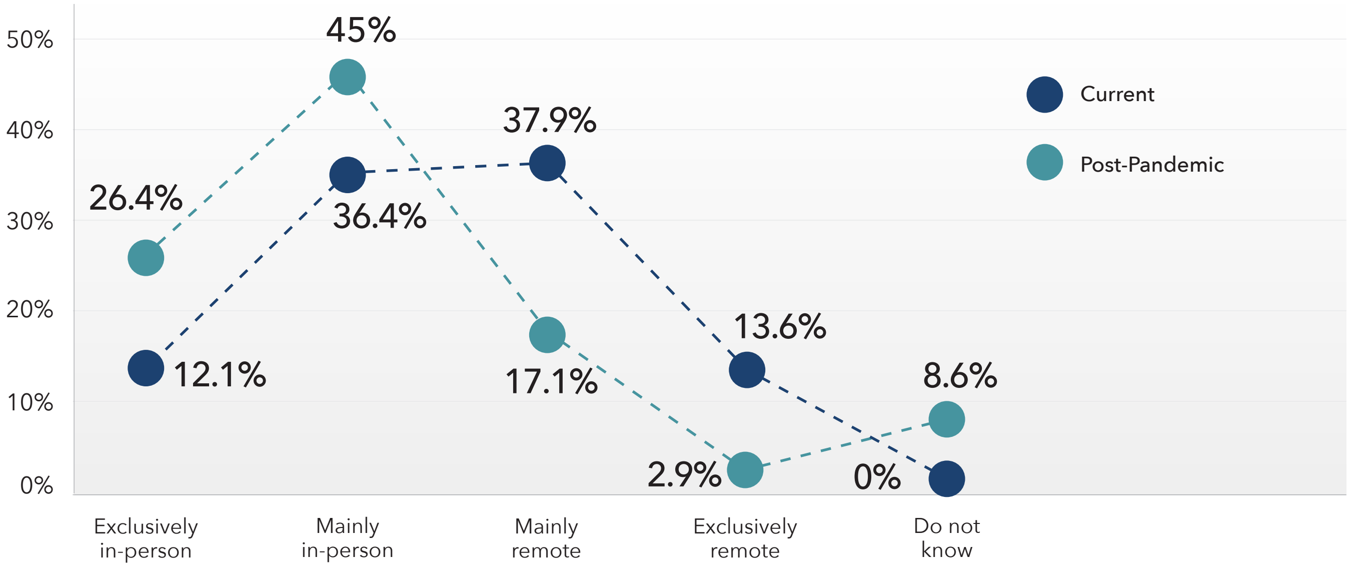
These challenges are particularly daunting for small and mid-sized local jurisdictions, which don't have the same IT budgets or capabilities as their larger counterparts.

To better understand the cybersecurity challenges facing state and local governments and education systems, and to explore recent trends in these organizations' security strategies, in February 2021 the Center for Digital Government (CDG) surveyed 125 state and local government and education leaders from across the country on the topic of cybersecurity.

The pandemic has changed the work environment.

More than half of respondents report that during the pandemic, their organizations have been working either entirely (13.6 percent) or mainly (37.8 percent) from remote locations. While the end of the pandemic will bring many employees back to the office, nearly 20 percent of respondents say employees will continue to work entirely or mainly from remote locations, and another 17.1 percent expect their organizations to support at least some remote work.

How is your organization currently working and how does your organization plan to work after the COVID-19 pandemic?

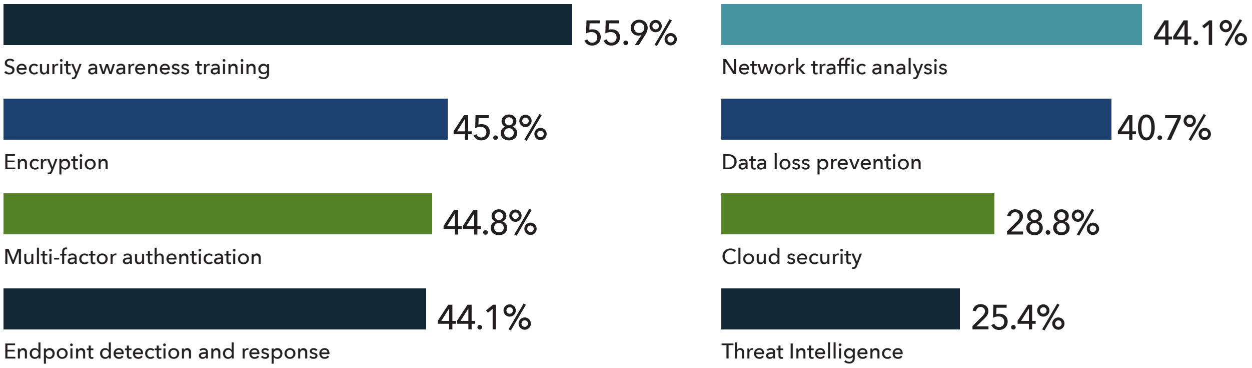


State and local governments and education systems currently employ a broad range of cybersecurity solutions.

The pandemic hastened trends such as remote work and digital service delivery that have vastly expanded the cyber-environment organizations must secure. Other trends, including increased mobile access and an interconnected Internet of Things (IoT), will expand that environment exponentially.

To meet the needs of securing this new landscape, governments and education systems are adopting a wide array of security technologies and initiatives. Beyond baseline endpoint protection, survey respondents say the security solutions most likely to be employed include security awareness training (55.9 percent), encryption (47.9 percent), multi-factor authentication (44.8 percent), and endpoint detection and response (44.1 percent).

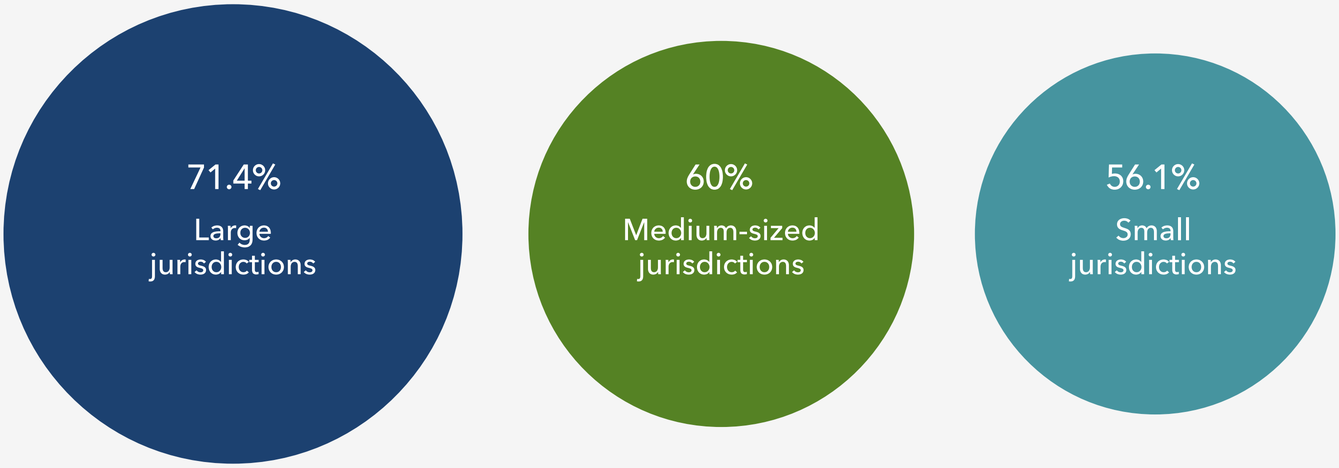
Which of the following cybersecurity solutions does your organization currently employ? (Please select all that apply.)



Not surprisingly, large and medium-sized jurisdictions have implemented more comprehensive cybersecurity solutions than small jurisdictions.

More than half of respondents – 53.4 percent – come from jurisdictions or educational entities with small populations. That means states with fewer than 8.25 million, counties with fewer than 200,000 or cities with fewer than 100,000 residents. Among educational entities, those are colleges or universities with fewer than 5,000, K-12 districts with fewer than 2,500 or K-12 schools with fewer than 500 students.

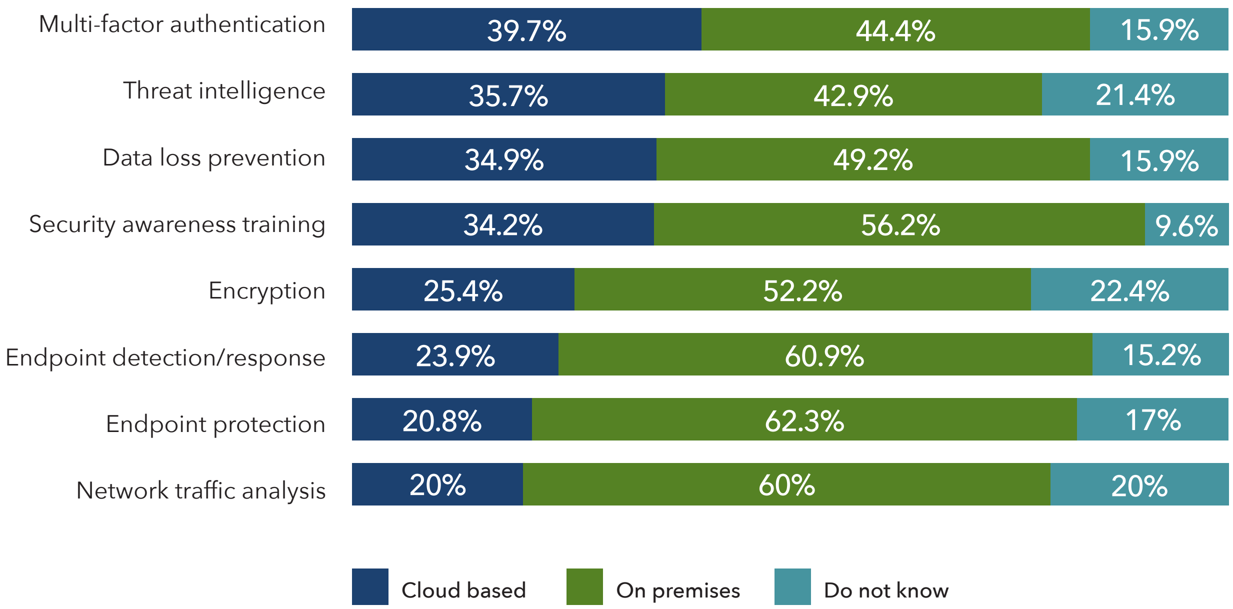
Generally speaking, the smaller the jurisdiction is, the less likely it is to have adopted comprehensive cybersecurity measures. For example, smaller jurisdictions are less likely to have implemented multi-factor authentication:



While government organizations still often utilize on-premises cybersecurity solutions, they often deploy the most popular solutions in the cloud.

One-third or more of respondents reported they have implemented security awareness training, encryption, data loss prevention or multi-factor authentication in the cloud.

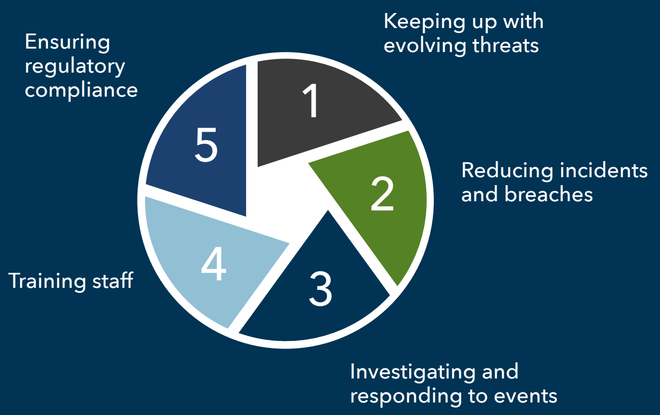
Where are these security solutions currently deployed or managed?



As security threats evolve, government IT departments are hard-pressed to keep up.

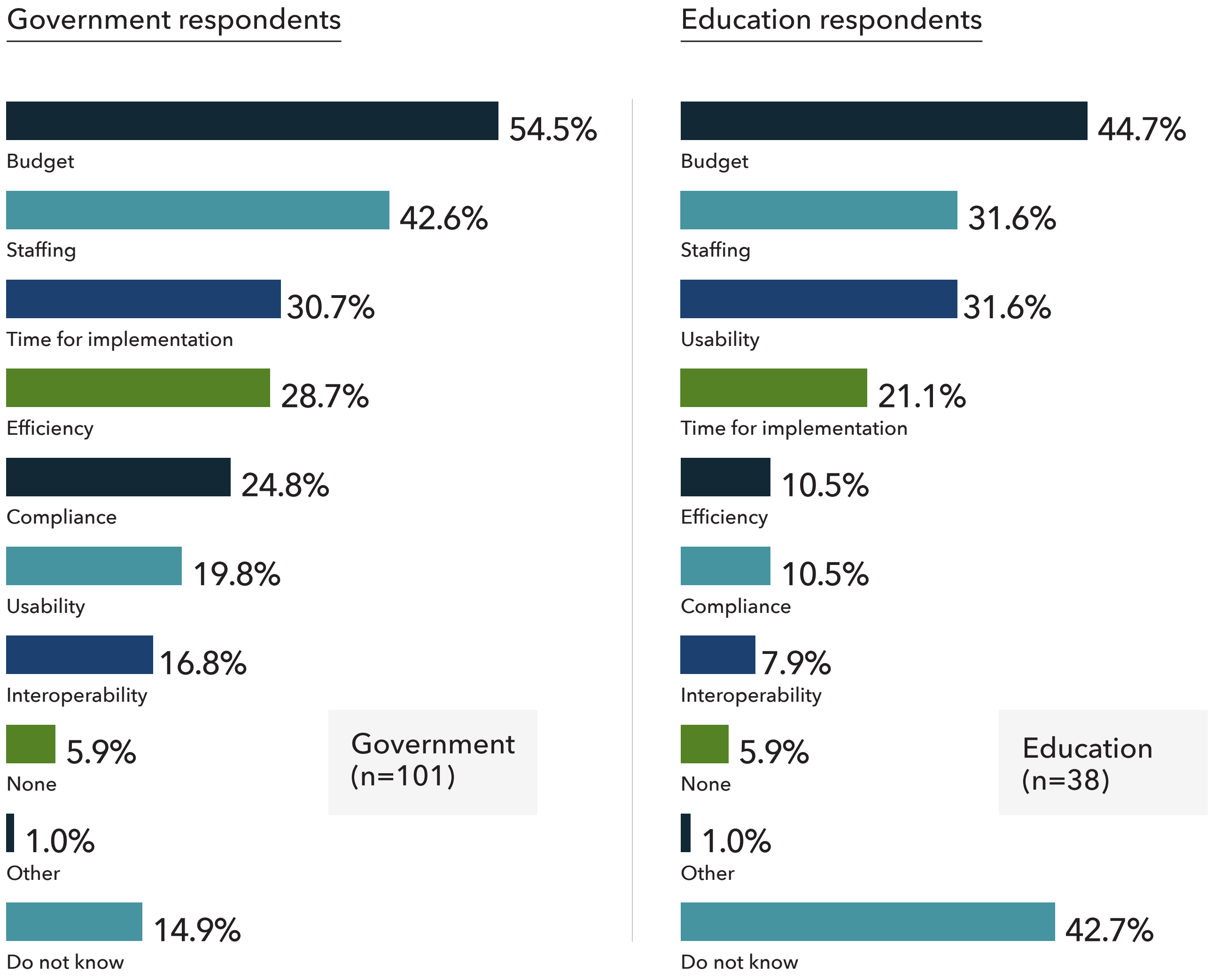
Staying on top of evolving threats has emerged as the top priority for IT officials as they work to improve cybersecurity at their organizations. The second-most important priority is reducing incidents and breaches. Respondents overall put less emphasis on staff training and regulatory compliance. However, training is a larger concern for respondents who are agency executives or C-level leaders; they ranked training number two in their list of priorities.

Rank in priority order your top priorities for improving cybersecurity.



Many organizations may lack the resources needed to achieve these primary goals. More than half of respondents from government and nearly half from education say that budget concerns are likely to impact their cybersecurity programs in 2021. Staffing is also a major issue for both groups: 42.6 percent of government leaders and 31.6 percent of leaders in education cite it as a major concern.

Which of the following cybersecurity challenges are likely to impact your cybersecurity program in 2021? (Please select all that apply.)



Government respondents

Education respondents

But few of those resource-strapped organizations currently get help from third-party partners.

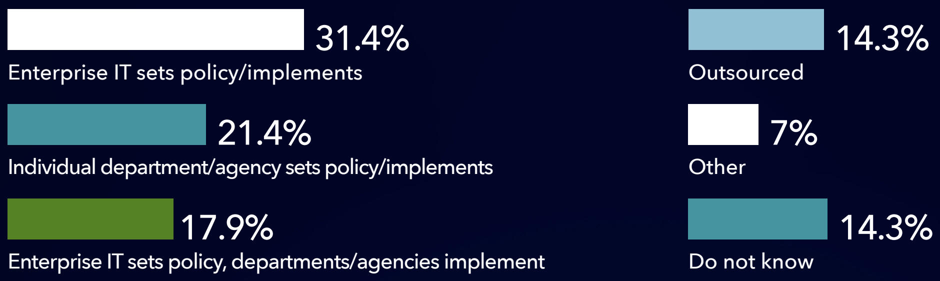
Only a small portion of organizations in the survey, 14.3 percent, have sought to supplement their resources by outsourcing cybersecurity administration. Outsourcing is particularly rare among states, where just 5.3 percent report they use this strategy. It is also uncommon among educational entities; only 7.9 percent of respondents in K-12 or higher education are outsourcing their cybersecurity.

Given the urgency of cybersecurity, and the ongoing challenges posed by budgets and staffing, more public sector institutions are likely to turn to third-party experts for help in the future. But recent high-profile events have triggered fears about IT outsourcing. One example is the 2020 attack on the IT services provider SolarWinds, which spread through that company's system to its clients. Another example is a series of attacks on Microsoft Exchange servers in 2021.

Many government leaders want assurances they can trust their vendors to safeguard their networks and data. The 2020 CDG Digital States, Counties and Cities surveys found 40 percent of respondents want greater visibility into their IT supply chain networks.

Government leaders may also want to rely on vendor partners to develop incident response plans that include the supply chain network to ensure vulnerable data is properly protected.

How does your organization handle cybersecurity administration?

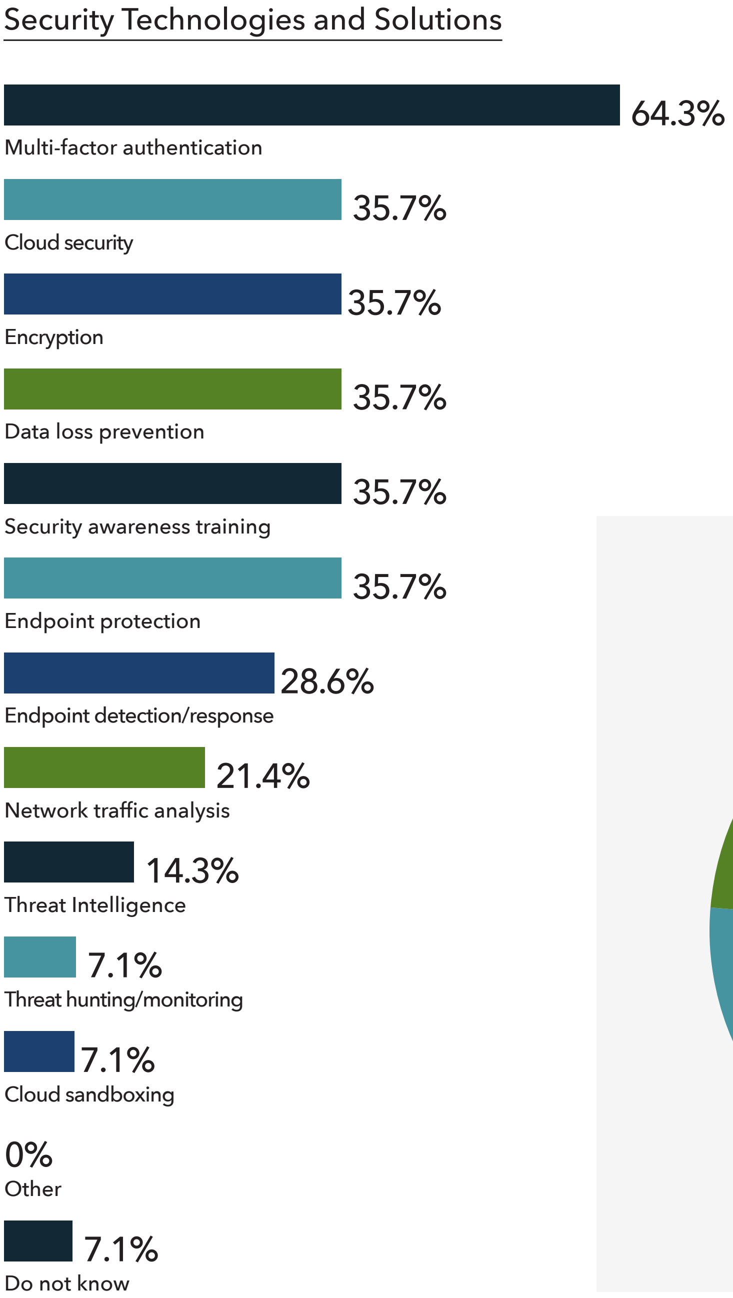


Government leaders want to know they can trust vendors to safeguard their networks and data.

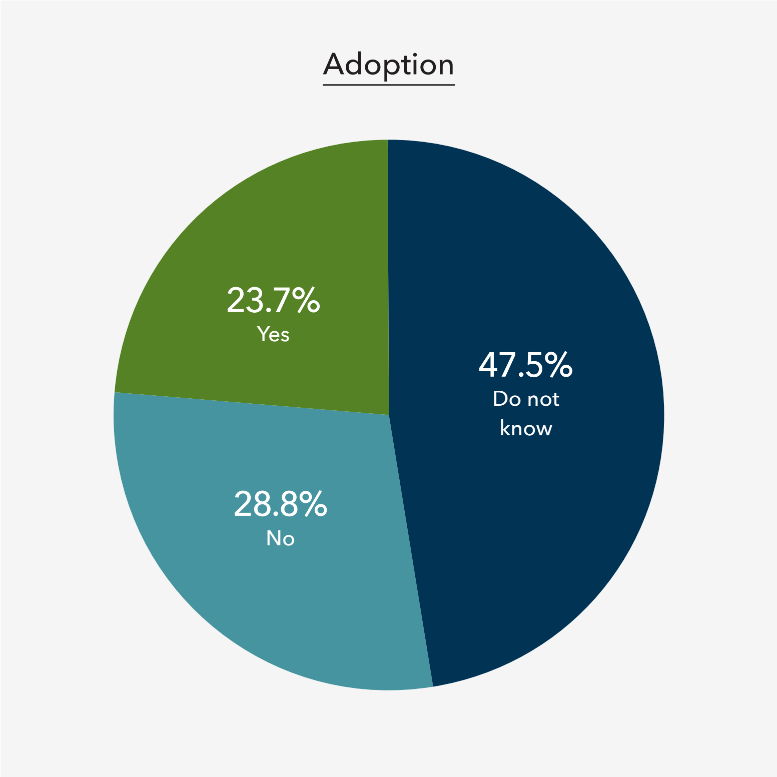
Governments plan to adopt or refresh security solutions in the coming year.

About a quarter of survey respondents say their organizations plan to adopt or refresh cybersecurity technologies or solutions in the next 12 months. Among IT employees who report such plans, multi-factor authentication is at the top of the priority list: 64.3 percent of them plan to implement or refresh solutions in that category. Behind that, cloud security and encryption are among the next-most popular solutions, each cited by 35.7 percent of respondents.

Is your organization considering adopting or refreshing any security technologies or solutions in the next 12 months?



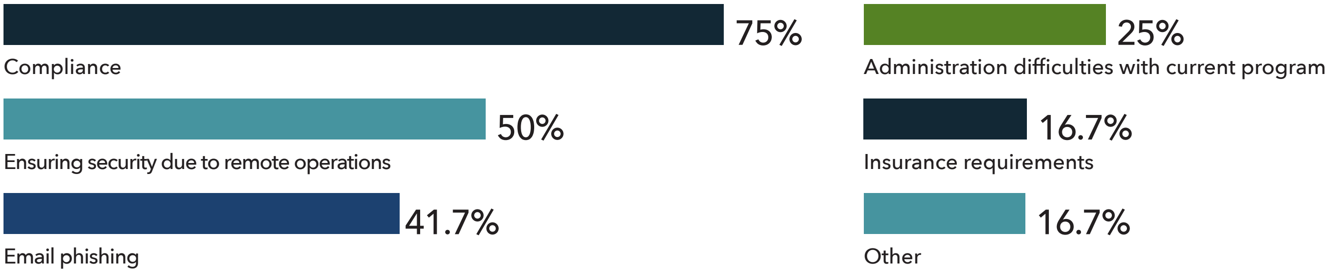
IT employees (n= 59)



For many, remote work has been an impetus for increased cybersecurity awareness training.

Although regulatory compliance is the biggest force driving government organizations to adopt or refresh their cybersecurity training programs, half of the respondents indicate that remote work is an important concern.

What are your top reasons for adopting or refreshing cybersecurity awareness within your organization?



IT leaders are pursuing cybersecurity strategies for a changing environment.

The pandemic created a new urgency for governments to strengthen their cybersecurity measures. Public sector organizations need a cybersecurity strategy that provides coverage seamlessly, whether employees are working from home, in the office or anywhere else.

Small and mid-sized local governments have unique cybersecurity challenges in this new hybrid remote work environment. These organizations don't have the same budgetary or staff resources as larger cities and states. To guard against potential attacks, it is important they partner with cybersecurity vendors that provide scalable on-premises and cloud solutions. An effective partner can provide critical solutions such as:

- **Endpoint security,** using multilayered technologies to balance performance, detection and false positives
- **Multi-factor authentication** to meet compliance requirements and help prevent data breaches
- **Cloud app security** to provide preventive protection against malware, spam and phishing attacks
- **Security awareness training** to empower employees with the knowledge and skills to help protect their organization's data and networks

In a hybrid environment, especially when some employees do their work on personally owned devices, it is especially important to implement cybersecurity solutions that work across multiple endpoints and operating systems. Solutions that allow IT staff to oversee the entire network, including workstations, servers and mobile devices in all locations, also provide advantages in a hybrid environment.

Governments challenged by budgetary constraints should look for trusted technology partners that offer strong, flexible solutions able to satisfy whatever needs arise.

The disruptions of the COVID pandemic led to skyrocketing numbers of new cyber-attacks. The FBI reported in mid-2020 that the number of complaints about crimes to their Cyber Division was up to as many as 4,000 a day – a 400 percent increase from before the pandemic.[3] Many of these specifically targeted state and local agencies.

As the United States continues to recover from the pandemic, small and mid-sized government organizations – many already struggling with constrained resources – must manage distributed environments while contending with an ever-evolving array of cybersecurity attacks.

Endnotes

1. https://www.governing.com/work/covid-19s-lessons-for-the-new-government-workplace.html
2. https://statetechmagazine.com/article/2021/02/how-will-remote-work-tools-help-government-recruitment
3. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

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. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com**

For:

ESET®

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.