How SLED organizations are fortifying cybersecurity and building an adaptable workforce

Insights from a leaders' roundtable: Have a seat at the table and learn more from real people tackling real challenges, brainstorming and sharing experiences.

LUMEN®

Table of Contents

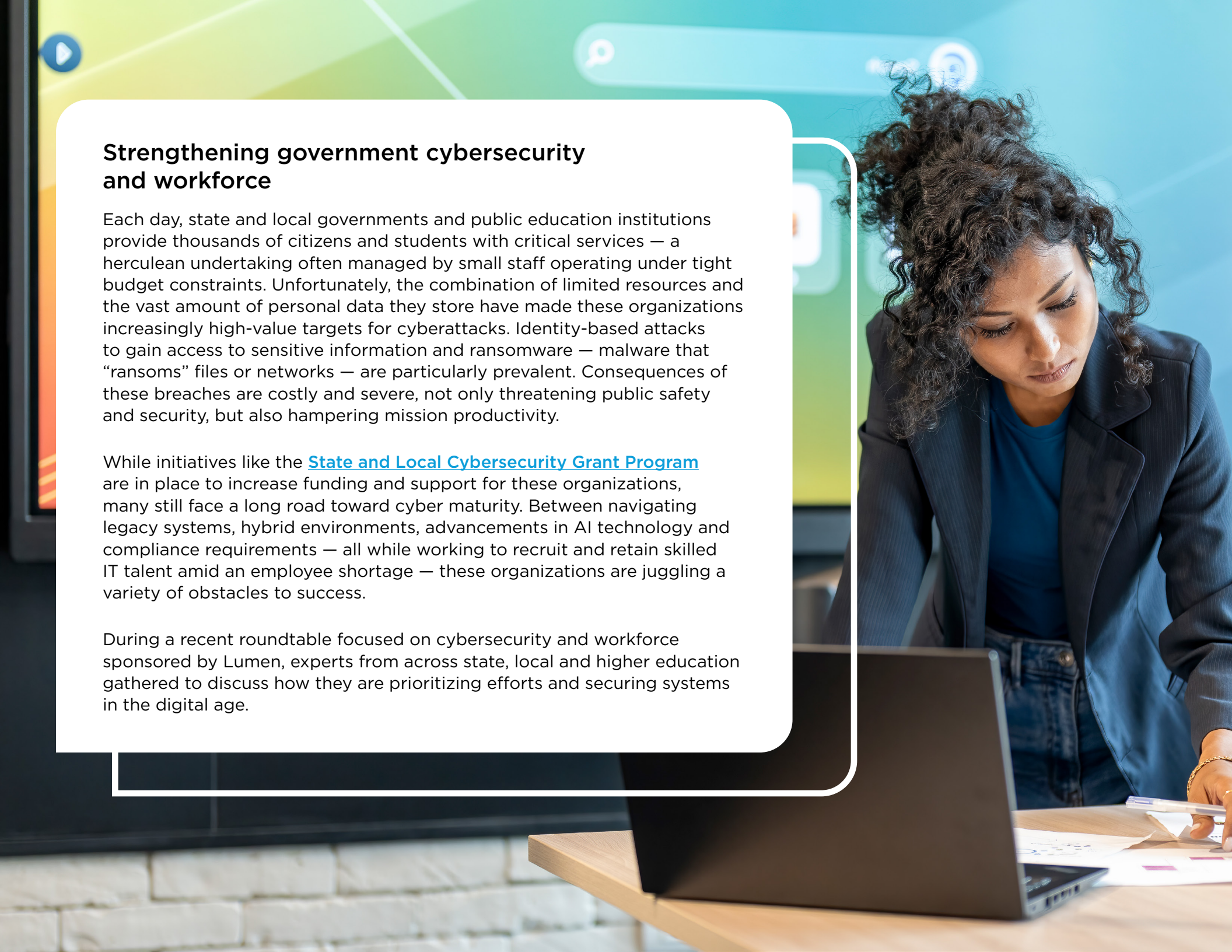
LUMEN®

Strengthening government cybersecurity and workforce

Each day, state and local governments and public education institutions provide thousands of citizens and students with critical services — a herculean undertaking often managed by small staff operating under tight budget constraints. Unfortunately, the combination of limited resources and the vast amount of personal data they store have made these organizations increasingly high-value targets for cyberattacks. Identity-based attacks to gain access to sensitive information and ransomware — malware that "ransoms" files or networks — are particularly prevalent. Consequences of these breaches are costly and severe, not only threatening public safety and security, but also hampering mission productivity.

While initiatives like the State and Local Cybersecurity Grant Program are in place to increase funding and support for these organizations, many still face a long road toward cyber maturity. Between navigating legacy systems, hybrid environments, advancements in AI technology and compliance requirements — all while working to recruit and retain skilled IT talent amid an employee shortage — these organizations are juggling a variety of obstacles to success.

During a recent roundtable focused on cybersecurity and workforce sponsored by Lumen, experts from across state, local and higher education gathered to discuss how they are prioritizing efforts and securing systems in the digital age.



CHAPTER 1

Understanding key drivers in cybersecurity

LUMEN®

The last several years have been transformative for government operations with the rise of cloud computing, the advent of new tools and capabilities, as well as the release of executive orders providing guidance on how to implement and secure these developments. Panelists highlighted that over the last 12-18 months, their organizations have been working to build cyber foundations and strengthen network security in accordance with changing times.

Modernizing systems and motivating staff

One local government IT official from a northeastern county with a population of approximately 60,000 explained that alongside a push to modernize systems and bolster endpoint security, her organization incorporates education and training to help end users to be more aware of cyberattacks in a more digitally focused environment.

"The next step would be looking at the other pieces and areas where we need to enhance security and continue with education and motivating staff, getting them interested in taking a look at the resources available," she said.

However, training alone isn't always enough, especially for IT teams that manage resources for thousands of people, like those in universities. A higher education official from a southwestern university of over 77,000 students noted that his team is upgrading security tools and software to provide more controls.

"We're changing up our security agents on all of our workstations, because in spite of all the mandatory training we do on our campus, we still have people who click on something and give a credit card number, then they get ransomware," he said. "So we don't really know how to circumvent that, other than put more measures in place to try to help them out."

> "The process that we're dealing with now is building the cyber risk program and building a more formalized cybersecurity program and maturing our processes."
>
> **— An IT official from a western city with a population of about 180,000**

Specialized cybersecurity teams

To ensure constant system oversight, some organizations are looking to hire employees or teams specifically dedicated to cybersecurity.

"The process that we're dealing with now is building the cyber risk program and building a more formalized cybersecurity program and maturing our processes," said an IT official from a western city with a population of about 180,000. "We were doing a lot of things ad hoc before, so we're spending the time to fill in those areas that we were overlooking."

Data governance

As government operations become increasingly data-driven, data management is a top priority for government leaders. Through proper data identification, classification

and governance, organizations can establish a strong data foundation that not only helps to effectively secure mission-critical information, but also drives accurate insights for actionable decision-making — and lays a necessary foundation for cutting-edge capabilities like AI.

"We have been spending a lot of time putting matrices together to actually score data correctly, to identify it correctly. It is definitely more challenging than I thought it was going to be," said a local government IT official from a western county of approximately 80,000. "At the end of the day, what we do and how we do it is always for a person or a group of people, so it's really about just capturing and protecting their information."

> "Who are you trusting on the other side? Who are you communicating with? And who are you now engaging and granting certain levels of access?"
>
> **— Vinod Brahmapuram, Senior Director, Security Sales, SLED Lumen**

Identity-based security

For all the benefit and flexibility hybrid environments bring, with assets now moved from on-premises data centers to the cloud, hackers have more of an opportunity to infiltrate environments. Non-malware attacks, in which threat actors use a stolen identity to pose as a different person, escalate their privileges to gain access to a confidential environment and launch an attack, are on the rise.

As a result, government organizations are looking to deploy zero trust security models and identity access management frameworks. Through processes like multi-factor authentication, entities can control privileges by requiring authorization and verification of each individual user before granting access.

"Awareness and training is useful, but it's not always about clicking the wrong link," said Vinod Brahmapuram, senior director of security sales for state and local government at Lumen. "Who are you trusting on the other side? Who are you communicating with? And who are you now engaging and granting certain levels of access?"

Asset management

Local government environments are growing more complex, encompassing both internal and external systems, such as student registration systems and benefit application portals. To have full visibility into their systems, many organizations are adopting tools that identify the location of their assets, monitor access and resolve potential weaknesses or gaps.

"You have these publicly available systems and internal systems, and so many other assets supporting the environment," explained Brahmapuram. "Getting a hold on your assets, understanding your internal and external vulnerabilities is a big area of investment right now."

CHAPTER 2

Reactive vs. proactive strategies

LUMEN®

Unfortunately, establishing a cybersecurity program to prevent attacks is often interrupted by the near-constant threat of the attacks themselves. A higher education official exemplified this challenge, stating that every hour, student-run and university websites experience numerous cyberattack attempts and, despite a skilled team of employees and work-study students, the organization is usually forced into a reactive state.

"When we look at the cumulative number of incoming attacks, those are a driving force for our cybersecurity right now," he said.

To combat the rapidly increasing attack rate, government entities are working to develop strategies for more proactive cybersecurity. One government cybersecurity leader stated that the goal for his program is to shift from "wildfire management to wildland management," building out an environment that is better equipped to handle cyber risks.

After a ransomware attack in 2021, a higher education official from a southwestern university with approximately 24,000 students noted that his organization had to completely reposition security from the ground up.

"All the preparation for something like that to happen is not preparation enough," he said. "For example, your disaster recovery is either outdated on paper in a binder or it's digital, and once you get hit with ransomware that's the first thing they go after."

Indeed, perhaps the most important part of a proactive strategy is training personnel in disaster recovery. Tabletop exercises in which teams test different simulated emergency situations can help individuals understand their roles and memorize procedures.

> "If you haven't tested your disaster recovery, you don't really have disaster recovery. If you haven't tested your security controls, you don't really have security controls."
>
> **— A local government cyber official from a southwestern city with a population of approximately 1.5 million**

"If you haven't tested your disaster recovery, you don't really have disaster recovery. If you haven't tested your security

controls, you don't really have security controls," said a local government cyber official from a southwestern city with a population of approximately 1.5 million. "Tabletops and other exercises where you get with your team to test these things and make sure they work the way you expect them to work, so that the first time you're doing this is not in the midst of a crisis, is hugely important."

Government hacks are a significant threat to national security, so several participants involve local emergency managers and national security organizations, such as state leaders, the National Guard or the Cybersecurity and Infrastructure Security Agency, in training exercises.

"Those things became quite popular when Russia was getting ready to attack Ukraine and the president sent a letter to all governors and asked, 'What is it that you can do should something happen? How are you prepared?' That really generated a lot of action," said Brahmapuram.

Moreover, don't underestimate the effect a cyberattack can have on employee well-being. The official whose organization fell prey to ransomware noted that a senior engineer on his team had a major anxiety attack after the incident, prompting his organization to include mental health recovery in disaster planning.

"Cyberattacks can almost give some people PTSD," he said. "We now have counseling and guidance as part of our disaster recovery plan."

CHAPTER 3

Artificial intelligence: New opportunities and threats

LUMEN®

InIn many ways, artificial intelligence is reshaping the government landscape — streamlining internal operations and allowing organizations to provide citizens and students with more efficient experiences. Although AI has been around for decades, as more accessible and affordable variations proliferate, the barrier to access is significantly shrinking. Now, adoption processes that would traditionally take years can happen almost immediately.

The excitement over new capabilities has led to a rush for government to adopt AI, but there are several key considerations before implementation. First and foremost, what goes in will come out — without trusted data and privacy oversight, AI cannot deliver trusted outputs. Additionally, one participant, who serves as a security official for a southeastern city of about 1.5 million people, stressed the importance of first establishing clear goals for the technology, as well as training employees in ethical use.

“Our big thing right now is education on how to properly interact with these models, understanding biases that could happen,” she said. “Here’s how to use this without dumping our data everywhere, but also understanding their use cases so that when they talk to vendors, they know what applications would be most useful, helping lead them from risk to reward.”

On the flip side, as government organizations grow more adept with AI, so do adversaries. With the advantage of expanded attack surfaces from hybrid and cloud environments, the technology allows threat actors to accelerate the volume and velocity of attacks.

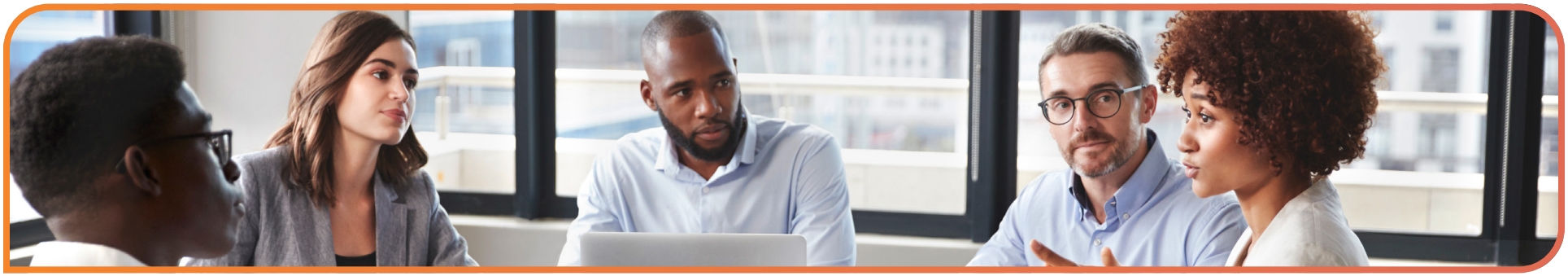
“If we look at the attack lifecycle from 20 years ago, hackers had to gain intelligence, collect the data, enter the environment slowly while concealing themselves to get the crown jewels — all of these things took time,” said Brahmapuram, noting that threat actors now have a much easier time launching attacks with AI, and can do so 90% faster than they used to.

“We have to be thoughtful and mindful of how we adopt AI, and at the same time, we need to start improving our defenses to be AI-ready, because it’s coming at the speed of light,” he said.

CHAPTER 4

It takes a village: Collaboration builds cyber resilience

LUMEN®



Partnerships — both interorganizational and external — can increase communication, eliminate silos and create transparency across different environments, ultimately lessening the chance of a successful cyberattack. Many roundtable participants highlighted their initiatives to build relationships with fire departments, public safety officials, police forces, as well as utility providers like water and electricity companies.

"Having these working relationships in place is really invaluable with regard to detecting events and kind of getting an early read on things that are happening across, not just your environment, but everybody's environment," said a government cybersecurity official, noting that these partnerships also allow larger organizations to support and guide smaller ones that may not have access to as many resources.

Additionally, the cybersecurity official shared that he participates in a forum that gives cyber operators across different entities a platform to share experiences, tools they're using and projects they're working on.

"We just let the actual guys on the ground doing the detections and responding to incidents talk to each other," he said. "We get all of these folks together and just let them have a powwow about all of the things that they're seeing and have an actual technical discussion about the things that are working or not working in their cybersecurity environments."

Knowledge sharing between government and industry is also crucial in shaping cyber strategies moving forward. Lumen, alongside other industry leaders like Google and Amazon, participates in the Joint Cyber Defense Collaborative, which focuses on creating awareness around present and emerging cybersecurity threats, as well as sharing best practices and new tools that benefit both sides.

"Some of the activities based on that collaboration are what is leading to what the U.S. Congress is funding," said Brahmapuram. "For example, the State and Local Cybersecurity Grant Program was based on some of those discussions — it's about creating that awareness, therefore the need and then the budget."

CHAPTER 5

A spotlight on training and workforce development

LUMEN®

Building a well-equipped cyber workforce is more critical than ever but finding and keeping top talent is no easy task amid a growing skills gap and worker shortage.

Equip current employees

Several attendees noted that their struggles to recruit new talent have led to increased efforts to grow current employee skill sets with regular re- and upskilling sessions. Cross-training employees to be adept in each other's roles is also key to improving continued productivity with limited staff and resources.

"I cross-train so everybody knows everybody else's job," said a higher-education official. "When you start sharing jobs across teams, it can help them feel more supported."

Offer opportunities to interns and students

Cybersecurity jobs are increasingly popular among college students, but limited opportunity and layoffs in the private sector opens a unique opportunity for government employers. One participant shared his pursuit to build a cyber team from the ground up by connecting with colleges to recruit and train student interns with the aim of eventually turning them into full time employees.

> "We're about 18 months in, and we've transitioned 40 student workers into full-time employees. We never thought we'd have that type of success, and our program is growing."
>
> **— A higher education official from a south-western university of over 77,000 students**

"I've had to find creative ways to try to staff up. I've been leveraging the ability to bring on interns so I can start to develop staff from scratch," he said. "It takes a little bit more to bring them up to speed, but they're eager to learn."

Meanwhile at the collegiate level, a higher education official highlighted a similar mutually beneficial initiative. With so many students interested in — and, in some cases, already highly skilled in — modern cyber practices, his university established a program that offers to train students in cybersecurity, then join their team after graduation.

"We're about 18 months in, and we've transitioned 40 student workers into full-time employees," he said. "We never thought we'd have that type of success, and our program is growing."

Keep pace with the private sector

Amid competition with industry, one participant noted that government organizations must position themselves and their offerings differently to attract talent.

“We’re public servants, and doing things to protect the greater good is a selling point for our careers that we probably don’t leverage as much as we can,” he said.

Additionally, the COVID-19 pandemic caused many organizations to digitize operations, introducing opportunities for remote or hybrid work — a desirable job quality to new talent. With the right policies and infrastructure to ensure software and hardware can process remote workflows securely, governments can offer remote or hybrid work options to stand out to a younger workforce.

“We’re looking into the hybrid environment to cater to all the younger folks and attract talent so that they have that flexibility, and not the rigid schedule of having to come into the office,” said one government cyber leader. “It’s so hard to get people into the building, we have to have that flexibility in order to show that we are a competitor with the private industry.”

Preventative measures create stronger, happier future for cyber employees and networks

As cybersecurity continues to evolve, it is imperative for government organizations to ensure employee health and happiness in a field where burnout is prevalent.

“I recommend a litmus test for five days out of seven days a week: Are you smiling at the end of the day?” said Brahmapuram. “That is a litmus test for burnout to measure how you are feeling. You have to take care of yourself, that’s when other things are going to be fine.”

While employees try to make the most of limited resources and even more limited budgets, Lumen’s expert recommends prioritizing investment in preventative cybersecurity measures to reduce the manual burden on detection and response, and build a more resilient environment overall.

“Let’s say you have $10. Spend no less than $6 on prevention, $3 on detection, and $1 on anything to do with incident management and response,” Brahmapuram said. “The way we are positioned based on staffing challenges, the more we should put into preventative measures, understanding your assets, and knowing where your vulnerabilities are.”

Learn more about how Lumen Technologies can help your organization strengthen cybersecurity.

About Lumen

Lumen connects the world. We are dedicated to furthering human progress through technology by connecting people, data and applications-quickly, securely and effortlessly. From metro connectivity to long-haul data transport to our edge cloud, security and managed service capabilities, we meet our customers' needs today and as they build for tomorrow.

866-352-0291 | lumen.com | info@lumen.com

LUMEN®