

SECURITY FOR THE NETWORK OF THE FUTURE

AT&T Public Sector



government
technology



02	Introduction
04	Protecting Data in an Ever-Expanding Network
06	Fighting New Threats from Home and Abroad
08	Training Up: How One Program is Leading the Workforce of the Future
09	Helping to Keep Elections Safe
12	Confronting the Human Factor
14	Conclusion: The New Cybersecurity

Photos courtesy of Shutterstock.com and iStock.com

Today's cybersecurity

challenges are truly unprecedented. Governments are creating and storing more information than ever before, including sensitive internal records as well as the personal data of their constituents. They're charged with the security of an ever-shifting mix of desktop hardware and mobile devices; on-premises servers and cloud storage; and traditional software, apps and third-party platforms. Agencies everywhere—especially at the state and local level—are constantly bombarded by attempted hacks and other cyberthreats through ransomware and malware. Election systems and other vital networks are under attack by state-sponsored enemies with more funding, organized support and technical sophistication than any time in history.

All of that was prior to a global pandemic, which redistributed millions of state and local workers and drove agencies to adapt to new work-from-home policies overnight. The disruption of COVID-19 exposed networks to new threats and vulnerabilities. As the edge of the network moved from the office

to employees' kitchen tables, cybersecurity leaders confronted challenges to maintain security in a world of home computers and personal wireless networks.

"All of these factors have conspired to make cybersecurity a more herculean task than ever," says AT&T Cybersecurity Director Kim Bilderback. "With many organizations forced to move to an entirely remote workforce, the pandemic redefined the definition of an organization's computer system. And cyberattackers have taken advantage of this to deploy their malware, challenging traditional models used for network security."

Security has been a major concern among public CIOs for years; cybersecurity remained the top priority for state technology leaders for the seventh year running in the National Association of State Chief Information Officers' (NASCIO's) annual survey released at the end of 2019.¹ It is also an issue that impacts the business sector, of course, with numerous high-profile data breaches in recent years of retail companies, credit agencies, banks and other financial institutions. And hackers have successfully targeted many

federal agencies, including the Defense Information Systems Agency in 2019 and the Office of Personnel Management in 2015, believed to be the largest breach in U.S. government history.²

But as the threat landscape has evolved, hackers have increasingly trained their sights on state and local government. According to one industry estimate, two-thirds of ransomware attacks in the first six months of 2019 targeted state and local agencies.³

“Governments are challenged to keep up,” says Kevin Miller, an AT&T sales executive who supports states and localities. “Some governments do have a robust cybersecurity posture. They have the right policies and procedures in place, the security tools they need, and the budget and staffing resources to meet the task at hand. But I would say that’s about 5 percent of jurisdictions. The other 95 percent need support.”

Network security has never been more important, or more challenging. As governments work with the private sector to build out new technologies, including 5G and the Internet of Things (IoT), public sector cybersecurity will be even more imperative. To highly secure the network of the future requires a better understanding of cybersecurity threats and a new way of thinking about security solutions. This guide will show you what steps you can take today to help protect the network of tomorrow.



Smarter Networks are Designed to be Safer Networks

The same factors that are redefining the network are also creating new ways to help protect it. Software-defined networking (SDN) allows organizations to manage and monitor their networks with comprehensive solutions that are more efficient, highly secure and more resilient than traditional decentralized hardware systems.

This network of the future is better at protecting itself, repairing itself and reacting to disruptive conditions, and can do so at a much faster speed than any human intervention. These capabilities are going to be critically important to state and local governments in an evolving work and threat environment.

“As more and more of us need access across the environment—from home to office to cloud, from various devices—we need tools that provide a holistic approach to security,” says Miller. “Cloud-type security tools offer instant scalability and access from a variety of different environments, and they help protect users in the network as close to their endpoint as possible.”

In other words, governments need a security profile that follows the same shape as their changing networks, says Pete Balles, an AT&T cybersecurity representative who works with state and local agencies. “What we’re seeing is that networking topology and cybersecurity tools are combining. SDN creates an atmosphere where you don’t have to stack appliances in a data center and protect them behind a firewall with content filtering. Instead, you can enable those same functions in the cloud. You make security part of the network itself.”

In addition to providing a more comprehensive security posture across the entire network, SDN and cloud-based tools deliver other cybersecurity benefits:

Agility: Cloud security offers greater flexibility than traditional physical approaches, allowing organizations to implement universal, updated solutions on the fly and instantly scale them across the enterprise.

Automation: Centralized, virtualized networks are better equipped to help detect and fight threats automatically and react in near real-time. Cyberthreats are coming faster and constantly changing—security responses have to be automated to keep pace.

Smarter focus: Greater automation and artificial intelligence (AI) technology means network architecture is actually learning from previous incidents and working to help mitigate future attacks. That frees up IT leaders to focus on strategic responses to more serious threats from bad actors.

Resilience: SDN and cloud-based networks allow for greater visibility into an organization’s networking environment, making it easier to monitor and detect potential threats—and respond to them fast. And 5G technology will enable “network slicing”—running multiple, isolated virtual networks on the same architecture, limiting access to those who need it and helping contain any breaches that do occur.



Protecting Data in an Ever-Expanding Network

Just as crooks rob banks because that's where the money is, "attackers target state and local governments because that's where the data is," says AT&T's Bilderback.

In today's information marketplace, data is money. And public entities are a veritable treasure trove of citizen data. That includes personally identifiable information (PII) such as Social Security numbers, birth dates, addresses and driver's license numbers, along with health records, payroll information, credit card data, court records and more.

These valuable pieces of information make government agencies rich targets. In addition, states and localities often rely on legacy systems, and they don't have the same cyber defense budget or staff resources as private sector companies.

"The criminals aren't going after specific people's data," says AT&T's Miller. "They just want the most data they can get. The more data they have, the more they can monetize it."

A user may need to access the information from her work computer or a mobile device—or perhaps even her personal laptop at home. "There's been this huge growth not only in the data that's being collected but where the data is being stored," Miller says.

Operationally, governments have had to expand their networks to stay effective.

"But it becomes a challenge because you've effectively increased your attack surface, and you've expanded it exponentially across the number of devices that now have access to the network," Miller adds.

Other factors are rapidly expanding that attack surface

“You have to make sure the entire ecosystem is highly secure. If a small city or town goes down, so does the state.”

– Kristin Judge, CEO and Founder, Cybercrime Support Network

even further. The pandemic instantly redrew the security perimeter for every jurisdiction in the country, requiring remote access for millions of workers and adding an untold number of new devices to the network. And that shift is only a precursor to the transformation ahead, as the continued rollout of smart-city technologies and 5G networks will enable a vast array of connected sensors and endpoints to be brought online.

“5G and the IoT are game-changers,” says Bilderback. “The number of devices that can be connected to 5G versus 4G is revolutionary.”

Safeguarding citizen information also extends to third-party apps and vendor technologies. States and cities rely on private industry for a growing number of services, such as toll road concessions. Those companies often maintain sensitive citizen data as well. Recently, for example, a company that sells “smart” parking meters and parking-enforcement technology to cities around the world was

the victim of a ransomware attack that exposed not only the company’s own employee records, but its contracts with cities and garage vendors, as well as bank information and credit card numbers for people who had paid to park using its products.⁴

And it’s not enough to consider only your own jurisdiction’s network. In an increasingly connected world, forward-thinking security professionals know they must take their peers and other levels of government into account.

“You have to make sure the entire ecosystem is highly secure. If a small city or town goes down, so does the state,” says Kristin Judge, a national cybersecurity expert and the CEO and founder of the Cybercrime Support Network. She notes that Michigan, where she lives, has embraced a collaborative approach, including the state’s innovative CISO-as-a-service initiative, which offers cybersecurity help to smaller cities and counties throughout the state.

Smart Strategies for a Growing Network

Changes in technology are rapidly redefining what networks look like and how to help protect them. Here are some emerging best practices for governments.

Know your network. Governments may not always have the most current view of their network infrastructure, let alone how it may change in the future.

“Just knowing what you have on your network is critical,” says Trent Redden, AT&T’s director of public sector cybersecurity solutions. “One good-sized U.S. city we worked with thought it had about 5,500 endpoints on its network. After just a 24-hour assessment, we found it had over 15,000.”

Rethink your access. Not everyone requires access to the entire enterprise. With an increasingly mobile and remote workforce, governments must focus on providing users access only to the information they need.

“We have effectively put everything behind a network segmentation zone, and we have developed an adaptive architecture where the closer you get to sensitive data, the more security checks come into play,” says Irvine, Calif., Chief Information Security Officer Deepak Lakhiani. “Network zoning has become even more crucial and we are implementing no

cross-talking between zones and denying if it’s not necessary.”

Take a holistic security approach.

Government security solutions are often a patchwork of firewalls, antivirus software and other legacy tools. Conduct a risk posture assessment and create a comprehensive strategy to address your needs. Cloud-native security tools can offer instant scalability and access from a variety of different environments.

Prepare for a connected future. The evolution of 5G and IoT-connected devices “is going to change the paradigm for cybersecurity best practices,” says Bilderback. “We’re going to have to rely on better endpoint security, whether that’s better encryption or another solution.”

Consider your other entity relationships. A comprehensive network security plan can’t just focus on your own jurisdiction’s systems. It must also include private data storage vendors you work with and other companies that carry out government functions. Your plan should include the networks of other levels of government you interact with, and it may even include your employees’ home Wi-Fi networks. Require that all entities that have contact with your network have the same security standards you do.



Fighting New Threats from Home and Abroad

Governments face dangerous new enemies in their efforts to maintain network security. On one front are nation-state actors looking to disrupt American elections and other systems, including physical infrastructure. Meanwhile, increasingly sophisticated criminal enterprises—both overseas and here at home—are threatening state and local systems with ransomware and other crippling attacks.

“Fifteen years ago, you had this classic stereotype of a lone hacker sitting in his basement, deviously trying to break into systems mostly just for bragging rights,” says AT&T’s Bilderback. “That era is over. As cybercrime evolved, hacking became big business for criminal enterprises. It also

opened the eyes of nation-states that cyberattacks could become another weapon in their arsenal for warfare.”

Nation-state attempts to meddle in American elections have been well documented. But these bad actors aren’t just targeting elections. They want to hack into state and local networks to steal technological and intellectual property. Even more insidious is the idea that cyberattackers could infiltrate critical physical infrastructure in the U.S. such as energy grids, transit systems and dams. The federal government has consistently said that specific nations are engaged in those efforts. With the advent of IoT-connected street sensors, water meters, electricity meters, traffic lights, video cameras and more,



securing control systems for physical infrastructure will become an even greater challenge in the years to come.

“There is a very real and present danger in these critical infrastructures,” says Oklahoma CISO Matt Singleton. “As you’re starting to bring on more devices that feed into the network, you’re just creating additional compromise locations.” In general, he says, “nation-state actors are much more advanced, with much greater capabilities. It’s a very different adversary.”

In addition to those threats from abroad, governments in the U.S. have increasingly been targeted by criminal organizations seeking to extort them for money. Much of this criminal activity comes from overseas, as hackers know it may be harder to find and prosecute them if they’re in a foreign country. But many

“Nation-state actors are much more advanced, with much greater capabilities. It’s a very different adversary.”

- Matt Singleton, CISO, Oklahoma

of these attacks come from domestic cybercriminals as well. In either case, these hackers are fueling a meteoric increase in ransomware attacks against U.S. governments. States, counties and municipalities suffered an unprecedented barrage of at least 162 ransomware attacks in 2019. The full picture is far worse: According to one industry report, ransomware attacks in 2019 impacted at least 966 U.S. public agencies, healthcare providers, higher education institutions and

school districts, at a potential cost of more than \$7.5 billion.⁵ These attacks, which can lock users out of a network for days or weeks, don’t just cost money. They shut down 911 services. They force hospitals to cancel surgical procedures and redirect emergency patients. They prevent courts from processing cases. They disable critical police functions like background checks and surveillance systems.

High-profile attacks in Baltimore, Atlanta, New Orleans and elsewhere have made

national headlines.⁶ But as the incidents have proliferated, they’ve also targeted smaller localities—and demanded staggeringly high payouts. Jackson County, Ga., paid hackers \$400,000 in 2019 to unlock its files after an attack.⁷ Riviera Beach, Fla., paid out \$600,000; less than a week later, another small town in the state, Lake City, paid \$460,000 after its systems were knocked offline.⁸ And attacks are evolving into more coordinated assaults: One Friday in August 2019 saw a simultaneous attack of 22 small towns in Texas.⁹

How can states and localities help protect their networks against these growing threats? The key, says Singleton, is a layered framework of security solutions that protects you from mundane malware and allows you to learn from previous attacks. That way, you can focus instead on advanced threats from more sophisticated attackers.

“Ultimately, we’re trying to get to the point where I don’t care about [smaller] attacks anymore, because the architecture is strong enough and smart enough to learn from previous attacks. That allows me to carve out the white noise and let the technology and the processes handle that. And it lets me focus my people on those uncommon threats,” he says.

Smart Skills for New Challenges

Today’s technology leaders need new capabilities and soft skills to combat tomorrow’s evolving threats.

Technical acumen. It goes without saying that CIOs and CISOs must have a deep understanding of technology. But cyberthreats have grown more complex, and so have the tools to fight them. “This job is far more technically oriented than how it’s felt in the past,” says Oklahoma’s Singleton. “You need to understand how different technologies work and how they work with each other.”

An open mind. Two of the most important capabilities for tomorrow’s tech leaders? Objectivity and humility, says Singleton. “You’re going to get stories and data from multiple sources. You need to be able to step back and scrutinize it to ensure there aren’t biases that are being read into it.” And check your ego at the door: “As soon as you feel like you know what’s going on, you will be corrected.”

A natural curiosity. Now more than ever, cybersecurity officials must have an inherent interest in a wide range of current events. Staying on top of the news—from geopolitics to pandemics to financial turmoil—is a key part of staying prepared.

Ability to talk to elected leaders. Technologists must be able to make their case for ROI to lawmakers and budget directors outside of IT. They need to show how their team helps other departments do their job.

“Approach this as a risk-management issue,” says Judge of the Cybercrime Support Network. “Cybersecurity is not a technology issue when you’re sitting in an elected office. It’s a public policy, public health and national security issue.”

Ability to tell your story. Ironically, the more effective your IT team is at stopping cyberattacks, the less most people will hear about it. Figure out how to convey your successes to the right people. Judge recalls one city CISO who sent a report to the mayor every Friday with a list of all the attacks that had been thwarted that week. She noted, “He was able to make the case about just how many threats they’re up against. You’ve got to put it in terms other people can understand.”

Training Up: How One Program is Leading the Workforce of the Future



Protecting the network of the future isn't just about technology. It's about making sure the next generation of IT workers has the right cybersecurity skills for the jobs in today's marketplace. NPower, an innovative nonprofit, has been focused on doing just that, while also providing new opportunities to a critically underserved community—U.S. military veterans and their spouses and families.

Since its founding in New York City 20 years ago, NPower has trained more than 5,200 veterans and young people from underserved communities. With locations now in several other cities—including Baltimore, Detroit, St. Louis, San Jose, and multiple places in New York and New Jersey—NPower is providing more individuals with critical workforce skills in tech fundamentals, cybersecurity and cloud computing. One especially noteworthy venture is NPower's Dallas location, which has been in operation since 2013 and provides advanced training for veterans and their families in the area of cybersecurity.

"NPower is an organization that aligns with AT&T's skills building strategy for our nation's heroes," says Roman Smith, Director-Corporate Social Responsibility at AT&T, which recently announced an enhanced relationship with NPower. "Our relationship with NPower supports veterans and their families with opportunities to upskill their education and align their experience with digital careers of the future."

AT&T has provided financial support to NPower for the past several years. All of NPower's programs are completely free for participants; the nonprofit is supported by corporate donations, philanthropic foundations, individual donors and government entities. The Dallas program receives some state funding from the Texas Veterans Commission. Now the company is doubling down on its commitment to the cybersecurity program, joining other corporations in working directly with NPower to hone its curriculum so graduates learn the exact skills they need for IT security jobs.

There are plenty of cybersecurity certification programs out there. What sets NPower apart, in addition to its focus on veterans and their families, is how comprehensive it is. Students receive 18 weeks of in-class instruction, followed by a 12-week internship and, in some cases, a six-month cybersecurity apprenticeship. The holistic curriculum includes specific tech skills as well as broader topics involving policy and governance, research, data science and cyber ethics. There's a strong focus on soft skills as well, with extensive training on interviews and personal presentation, time management, resumes and LinkedIn™ profiles, and professional networking. NPower even provides students with a social support manager to help mitigate any personal challenges—such as housing, family issues, financial hardships or

healthcare needs—that might prevent them from continuing their education.

"Honestly, it's more comprehensive support than most college students receive," says Patrick Cohen, NPower's Vice President for Strategic Partnerships. "It's a real soup-to-nuts approach, from recruitment to internships to placements and apprenticeships, and then the alumni network and the social capital they're exposed to during the program and after they graduate."

Another defining aspect of the NPower program is the intensely close involvement of corporations like AT&T to continually refine the coursework, giving students a skillset that's attuned to shifting marketplace needs.

"Obviously, technology constantly changes. And so do the skills, roles and job titles," Cohen says. "So we want to make sure we're really aligned with the market and we're agile about evolving our curriculum." That's the opposite of many training programs, he notes. "We look at it as a combination of understanding the needs of our target population plus the availability of entry-level tech jobs that we're training for. We review the available jobs and then work backwards."

It's a valuable partnership that goes far beyond corporate altruism, says AT&T Cybersecurity Training Director Rick Stiffler. The company can support a successful nonprofit that's upskilling

national heroes—veterans and their families—while also developing a pool of cybersecurity professionals to meet public and private sector hiring needs.

"There's both a social return and a business return for us," says Stiffler. AT&T's close involvement even allows students to train on actual tech platforms, rather than simulators or publicly available tools that may be outdated. "They're working hands-on with a product that's in the marketplace right now, getting real-world experience that will allow them to start working immediately when they walk into their new roles."

For program alumnus Ray Genova, NPower proved to be a valuable rung on his career ladder. "It helped me market myself," he says, noting that NPower worked with him to receive an internship and, later, a full-time job. "The connections I made and the networking I've gotten to do—it really helped me with job placement."

An Iraq War veteran who received a Purple Heart for being wounded in combat, Genova had struggled with finding a career after he left the military. But today he works as an instructor at MyComputerCareer, a national IT training program. That's thanks in large part to NPower, he says. "NPower put their trust in me, and they invested a lot in me. They really helped me get where I am today."

[Visit us for more information about the program.](#)

Helping to Keep Elections Safe

On the morning of Good Friday, April 19, 2019, officials in Potter County, Texas, arrived at work to discover their computers had been infected by a malicious virus. The county was set to begin early voting in a local election that Monday, and the attack threatened to derail the vote. As IT workers scrambled to assess the damage, county election leaders were told to prepare for the worst.

But the worst didn't happen. The elections department immediately began executing its emergency plan, a comprehensive document based on an assessment that included strategic workarounds for communicating with polling sites, the public and the Texas secretary of state's office. The department was in the process of obtaining a firewall, laptops and other things recommended when the event occurred. But

because vulnerabilities were known as a result of the assessment, the department was prepared. Voting was able to start on schedule Monday morning, and the election went off without a hitch.

That was all thanks to an innovative Election Security Assessment Program that had been rolled out in the state. Using Help America Vote Act (HAVA) funds, Texas in 2018 began working with each of its 254 counties to enhance election security measures. The program includes a full accounting of every county's election processes, fiscal controls, software and hardware. The county receives a risk assessment with recommendations about how to prioritize its needs. Other state and federal funds are then available for technology upgrades. Potter County underwent its assessment in January 2019, received its report in February and began implementing the



recommendations in March, a month before the cyberattack.

“We did it just in time,” Potter County Elections Administrator Melynn Huntley told a newspaper.¹⁰ “It saved an election.”

No cybersecurity issue has received more attention in recent years than election security. Attempts to influence the 2016 presidential election galvanized much of the American public and many elected leaders to focus on election security as a signal issue of national security. In 2018 and 2020, Congress appropriated a total of more than \$800 million in HAVA grants for states to upgrade and protect election systems.¹¹

Election attacks weren’t limited to disinformation campaigns on social media. They also included direct attempts by foreign adversaries to infiltrate election systems across the country. The FBI and the Department of Homeland Security have said they have direct evidence that cyber actors “conducted online research and reconnaissance to identify vulnerable databases, usernames and passwords” in at least 40 states in 2016; the investigators said they assume that all 50 states were targeted for exploitation.¹² In August of that year, just weeks before the election, foreign military intelligence launched a cyberattack on at least one U.S. voting software supplier and sent spearphishing

“It’s important to remember that the election isn’t just one day, it’s an entire process.”

- Keith Ingram, Elections Director, Texas

emails to more than 120 local election officials in Florida. Two Florida counties were successfully infiltrated.¹³

Attacks like these aren’t necessarily aimed at changing vote totals.

“They’re trying to affect public trust in the whole system,” says AT&T’s Gene Moore, who is leading the implementation of the Election Security Assessment Program in Texas. “The bad actors want to shift public perception so that the people don’t have faith in the integrity of their vote.”

The intense focus on shoring up election systems is undoubtedly a good thing, says Texas Elections Director Keith Ingram. But he worries it has led to a perception problem.

“Since 2016 and the concern about foreign interference, there has been a pronounced emphasis in the media about voting systems being susceptible to manipulation,” he says. “But in my experience, that’s the part that I worry the least about. I think it’s the least susceptible.”

Much more important, Ingram says, is highly securing all the other aspects of the

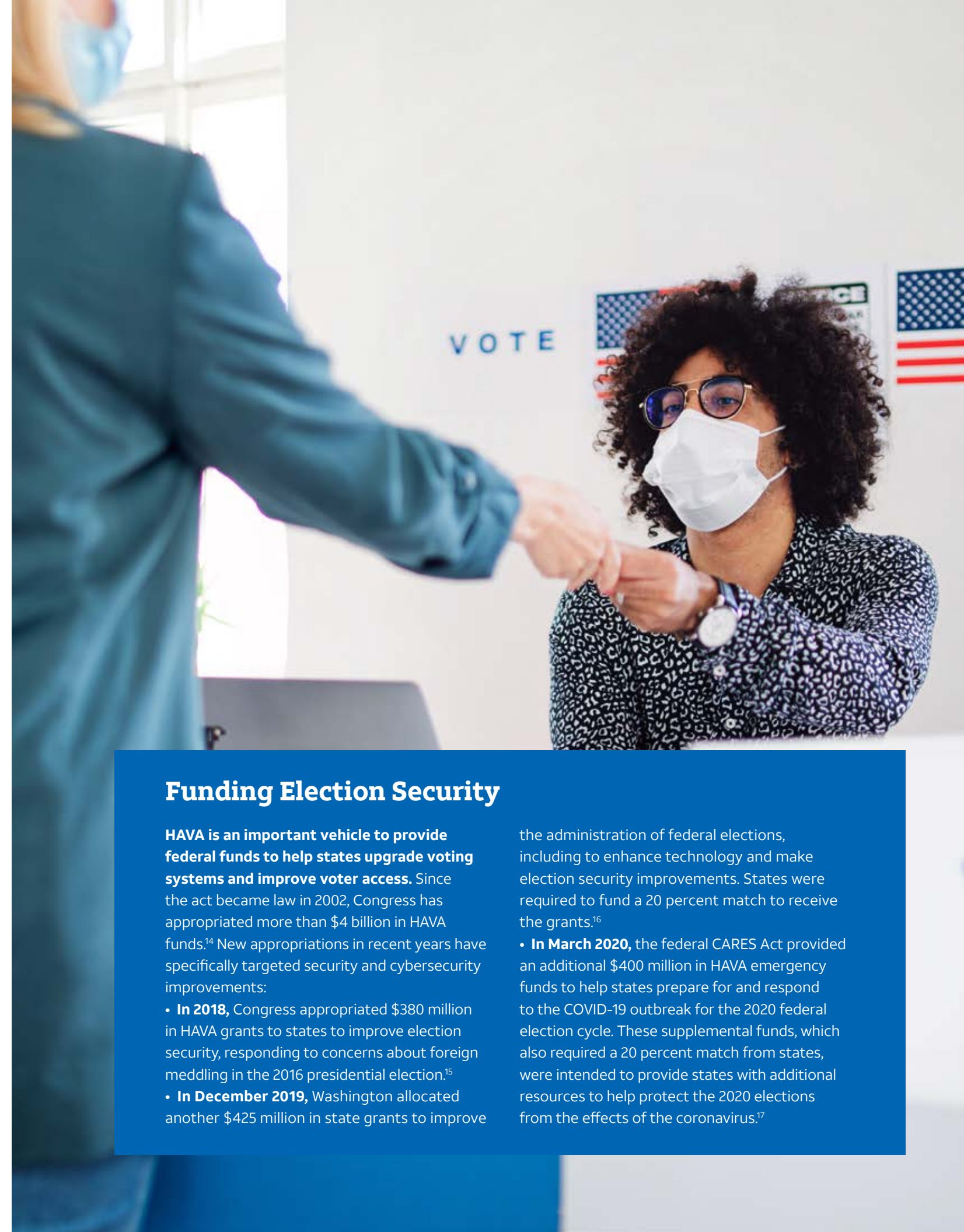
election management process. Voter registration databases, electronic poll books, campaign finance records, methods for reporting county vote totals to the state, and each election department’s own network and computers are all more valuable targets. And unlike the actual voting machines themselves, those systems all must be connected to the internet.

“It’s important to remember that the election isn’t just one day, it’s an entire process,” says Ingram. “So that’s where our focus has been.”

That’s also been the focus in Los Angeles County, which has engaged in its own initiative over the past few years to strengthen election security. The nation’s largest voting jurisdiction, L.A. County has 5.2 million registered voters—more than 42 states.

“Security has to be holistic,” says Aman Bhullar, the CIO for the L.A. County Registrar-Recorder/Clerk’s Office. “We had to step back and look at the whole picture.”

That meant security upgrades for election infrastructure and endpoints, but it also meant rethinking



Funding Election Security

HAVA is an important vehicle to provide federal funds to help states upgrade voting systems and improve voter access. Since the act became law in 2002, Congress has appropriated more than \$4 billion in HAVA funds.¹⁴ New appropriations in recent years have specifically targeted security and cybersecurity improvements:

- **In 2018**, Congress appropriated \$380 million in HAVA grants to states to improve election security, responding to concerns about foreign meddling in the 2016 presidential election.¹⁵
- **In December 2019**, Washington allocated another \$425 million in state grants to improve

the administration of federal elections, including to enhance technology and make election security improvements. States were required to fund a 20 percent match to receive the grants.¹⁶

• **In March 2020**, the federal CARES Act provided an additional \$400 million in HAVA emergency funds to help states prepare for and respond to the COVID-19 outbreak for the 2020 federal election cycle. These supplemental funds, which also required a 20 percent match from states, were intended to provide states with additional resources to help protect the 2020 elections from the effects of the coronavirus.¹⁷

policy and governance, looking at risk and compliance, improving identity management, expanding training for users and developing strategies for combating misinformation on social media.

Bhullar's office worked with AT&T to conduct a risk assessment of its baseline security posture. Then it set about improving it. The team pulled in best practices from established cybersecurity

frameworks from places like the National Institute of Standards and Technology (NIST) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

"But there wasn't an exact model for us to follow," says Bhullar. "There was nothing parallel to what we are and how we wanted to establish our cybersecurity program. So we built it ourselves."

One important move, which Bhullar instituted

in April 2019, was actually bringing the AT&T consultants into the Registrar-Recorder's offices, allowing them to physically work alongside the county team.

"That was very new and very different from how the county normally operates," says Janet Ifekwunigwe, the AT&T strategic lead for the initiative. "It created this sense of synergy, and it allowed us to walk down the hall and

have a conversation, or run upstairs and grab someone for 10 minutes. That was a really big piece for us."

"Los Angeles County elections are much more protected now than they were two years ago," says Bhullar. But he plans to continue conducting risk assessments on an annual or biennial basis. "The threats will never stop evolving, and you must be able to continually evolve as well."

Indeed, the single biggest challenge with election security is inaction, says Moore in Texas. "We've been talking about election security for years. But most counties still don't think an attack will happen to them. You need to take action. Make yourself stronger today than you were yesterday. The threat is real, and the bad guys are just getting smarter, faster and better funded."

Smart Strategies to Help Safeguard Elections

Election security concerns are at an all-time high. Here are some ways to help safeguard voting.

Make a plan and write it down. The most common failure in an elections office is a lack of documentation and repeatable processes.

"Walk through your whole process and ask tough questions," says AT&T Client Representative Patrick Robinson. "Play devil's advocate. What if there's a fire? What if you lose power on election day? What if you're hacked? For every problem, articulate a solution. And now you've got a playbook."

Assess your current risk. Many jurisdictions may not have the same in-depth assessment capabilities as Los Angeles County or the state of Texas. But there may be HAVA funds available for you to conduct one on your own. Additionally, the Department of Homeland Security provides vulnerability reviews at no cost.

Protect your system. Most big counties have segregated their elections office from the rest of their network. But in many smaller and more rural counties, the systems are "still completely co-mingled," says Moore. Separating elections infrastructure helps keeps it safe in case a virus hits the rest of the county.

Think beyond election day. The risk of a hack at polling sites is extremely low. Focus on highly securing your entire elections management process, including voter registration databases and your elections office system. Texas, for example, is instituting multifactor authentication for all its county election endpoints. It's also piloting a security software that's behavior-based rather than signature-based. Instead of relying on passwords for access, the new platform can better sense when a user starts behaving differently and can flag the suspicious behavior.

Recognize your role in managing disinformation.

Unfortunately, part of protecting modern elections means combating false and misleading information online.

"We live in an overheated environment where disinformation can get a foothold and cause trouble," says Texas' Ingram. "That's actually what worries me most of all in the entire election process." He uses tools to stay on top of trending posts, and fervently scans social media for any inaccurate information that needs to be corrected or taken down.

Collaborate with your peers. Numerous resources are available to help improve your election security. The NIST and MS-ISAC frameworks are widely recognized standards. Texas has published its own 34-page best practices guide on the secretary of state's office website.¹⁸ Los Angeles County and other places that have improved security welcome the opportunity to share their learnings with counterparts in other jurisdictions.





Confronting the Human Factor

The most heavily fortified castle in the world can't keep out the enemy if someone on the inside opens the door and hands them a key. Helping to protect the network of the future isn't just about building defenses around your hardware, software and the cloud. It's about engaging and educating your employees and users.

"We know 80 percent of all cyber breaches today are from an internal perspective," says AT&T's Trent Redden. "Most

employees today are still not trained as to what to look for, whether that's via email, texts or physical on-site attempts."

Almost every successful ransomware attack or malware infection occurs when an unsuspecting employee clicks on the wrong link or unwittingly provides credentials to the wrong website. Hackers prey on trust, and phishing emails and scam sites have grown increasingly sophisticated and convincing in recent years.

The employee education gap is the single most pressing issue today, says AT&T's Bilderback. "If I had one dollar to spend on cybersecurity," he says, "it would be on user awareness training."

Addressing the human element has become even more crucial in the age of the coronavirus. Any crisis that causes confusion is seen by cybercriminals as an opportunity to exploit users' trust. But the massive disruption of the workforce

has made it especially difficult to guard against phishing attempts and other scams. Remote employees may be more likely to let their guard down, and more willing to open an email or click on a link without verifying it first. In late April 2020, Google reported that it was identifying more than 240 million coronavirus-related spam messages per day, and more than 18 million malware and phishing emails related to the pandemic each day.

Smart Strategies for User Awareness

Human error is the single biggest threat to network security. Addressing it requires better training and tighter limits on access.

Outline your goals. Before implementing any new employee training initiatives, take a step back and define your broader cybersecurity plan. Then align your training with it.

"The best training model is the one that aligns with your procedures and policies," says AT&T's Miller. "If you don't have those in place, a training program will not work."

Develop the right program. Find a comprehensive training model that educates your employees about high-risk behaviors and equips them with the information they need to help protect themselves and the network. Proper training isn't about checking off a list of do's and don'ts. It's about helping employees create new behaviors and better habits around staying highly secure.

Train and train again. Mandatory annual trainings are good; twice-a-year trainings are better. Beyond that, find ways to engage employees in an ongoing conversation about cyber hygiene, as Lakhiani has done in Irvine with his weekly newsletters. Frequent communication helps provide that cybersecurity remains a top-of-mind concern for everyone.

Adopt a zero-trust model. Even the best education programs can only go so far. A zero-trust approach treats all users as potential threats and prevents access to data and resources until a user can be verified. Multifactor authentication and other tools can help make your systems mistake-proof.

Empower employees. Humans may be the weakest link in the cybersecurity chain, but they can also be one of your strongest assets. Help employees understand the essential role they play in your overall security posture.

"Employees are the firewall," says AT&T's Balles. "From the top C-level executive down to the guy taking the trash out, if they have an email or credentials, they're part of the whole solution to any threats from the outside."

One “notable” effort, Google said, specifically targeted U.S. government employees through their personal email accounts with phishing messages posing as COVID-related updates or coupons from fast-food chains.¹⁹

Even before the coronavirus, some forward-thinking tech leaders were making user awareness a centerpiece of their cybersecurity strategies. Lakhiani, the Irvine, Calif., CISO, has transitioned employee education to incorporate an ongoing focus on digital health. “We have weekly emails where we talk about good digital health practices and how to recognize malicious communications versus legitimate ones.”

“If I had one dollar to spend on cybersecurity, it would be on user awareness training.”

- Kim Bilderback, Cybersecurity Director, AT&T

Lakhiani’s campaign includes standard tips about complex passwords, hovering over a link before you click on it and verifying all requests before providing any personal information. But he also focuses more broadly on improving employees’ own security posture.

“What are you doing to protect your own social

presence? How many applications do you have running in the background right now, quietly collecting information about you? What’s your browser health? Do you even know how many plug-ins and add-ons you have? That’s the level of education we’re trying to push right now,” he explains.

Education campaigns are important, but they have some limits, says Judge of the Cybercrime Support Network. IT officials should also put tools in place that prevent mistakes in the first place.

“I’ve been doing education and awareness for a long time,” Judge says. “And unless you sit someone down and really show them how to fix things, how to add security, it’s not going to be as successful as if it was built in.”

Security features that are baked into products, such as two-factor authentication, are extremely effective, she says. “We can’t just rely on the human user to opt-in to security. We have to build it in.”



Coming Together to Fight Cybercrime

States and localities don’t worry just about potential threats to their own networks. They also have a role to play in protecting citizens and businesses’ online activities and helping them recover when they’ve been the victim of cybercrime or online fraud. But without a standardized cybercrime reporting structure, it can be difficult for government entities to exchange information about cybercrime that could help apprehend criminals.

That’s the idea behind the Cybercrime Support Network (CSN), a public-private-nonprofit collaboration founded in 2017 by Kristin Judge to work with federal, state and local law enforcement and consumer protection agencies to help businesses and consumers affected by cybercrime. A former county commissioner in Michigan, Judge later worked at the Center for Internet Security, where she helped connect state and local governments to federal cybersecurity resources. She then served as the director of government affairs at the National Cyber Security Alliance, where she worked with a number of federal agencies, private sector groups and other stakeholders to help educate businesses and consumers about the need to protect themselves online.

CSN has launched a number of efforts, including:

FraudSupport.org – CSN created this first-of-its-kind database with guidance on

how to “report, recover and reinforce,” as the site says, following a cybercrime. The group is working with law enforcement agencies across the country to raise awareness about this important resource for cybercrime victims.

Cybercrime Hotline – Using funds from the Department of Justice Office for Victims of Crime and the Victims of Crime Act, CSN is piloting a nationwide hotline for cybercrime victims using states’ existing 211 call/chat/text networks. CSN has trained 211 referral specialists to assist victims, and the program is already being piloted in several states.

National Cybercrime Incident Reporting Program – CSN is currently working with the Department of Homeland Security’s Cybersecurity Infrastructure Security Agency (CISA) to develop this standardized cybercrime reporting and information sharing structure. This uniform reporting mechanism will enable state and local authorities to capture threats impacting consumers and small and midsize businesses (SMBs) and will equip government entities and law enforcement with real-time, integrated and operational cybercrime data to help combat cybersecurity risks.

Learn more about these and other resources at cybercrimesupport.org.

Conclusion: The New Cybersecurity

Cybersecurity is changing. Securing the network of the future requires holistic solutions that protect you at every step from endpoints to servers to the cloud. You must be able to adapt to evolving threats and changing network perimeters that can shift on a daily basis. You have to engage employees to help improve their own security intelligence quotient.

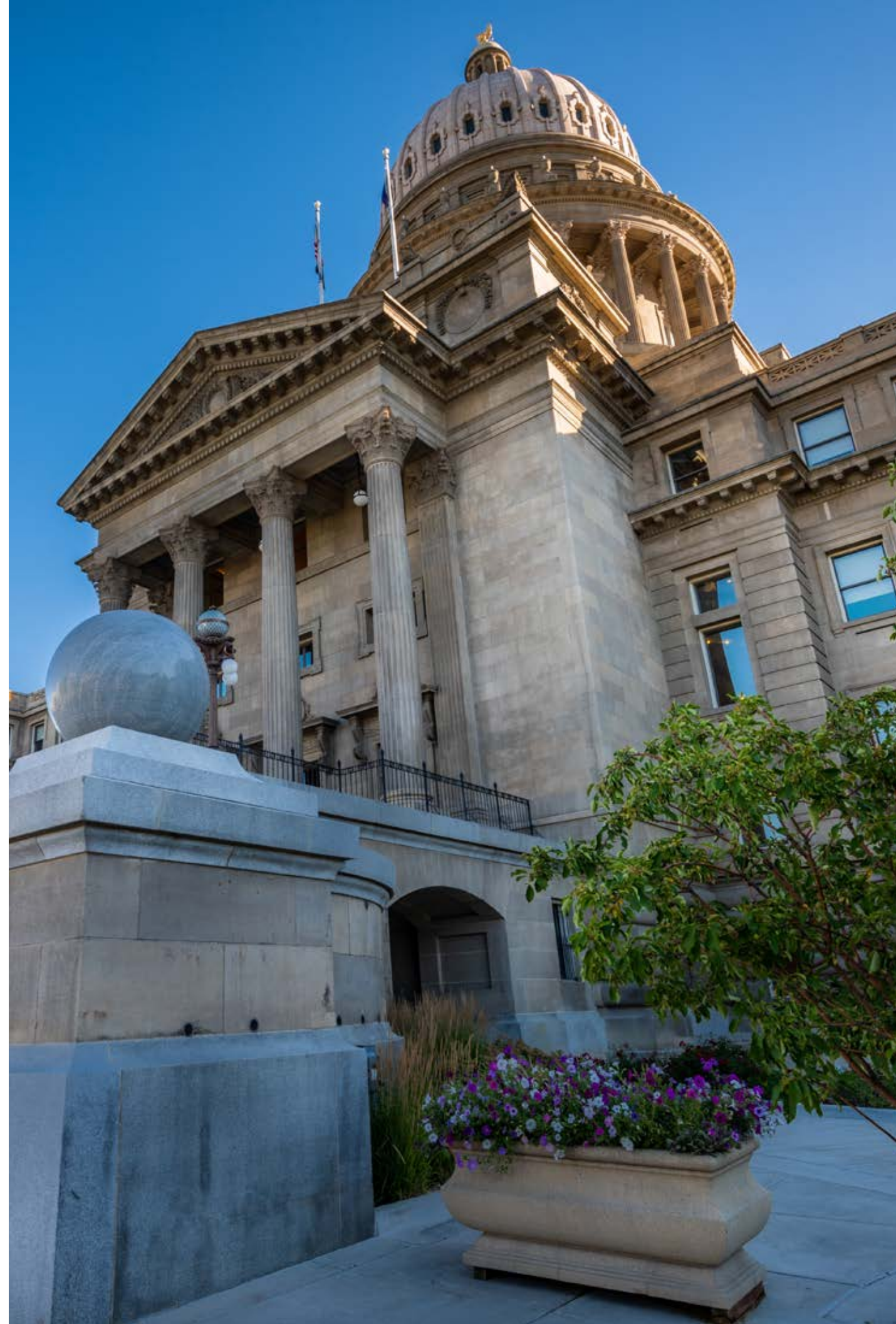
But the single most important aspect of security is simply understanding that you're a target. Recognize the fact that you will get breached at some point. Antivirus tools and anti-ransomware solutions are important parts of preparedness, but the new cybersecurity isn't just about building the strongest fortress you can. It's about managing and mitigating the impact of attacks when they inevitably occur. It's about resilience.

Begin by assessing your risks and developing a comprehensive cybersecurity framework for your organization, and then let

that guide you in prioritizing your needs. Treat your vendors as trusted knowledge consultants, not just a source for new products.

You cannot meet this challenge on your own. Reach out to your peers in other jurisdictions and collaborate with other levels of government. Exchange as much real-time information as possible and share the lessons you learn with each other. When you don't have the skills you need on your team, utilize the expertise of private sector partners. According to AT&T's Bilderback, research shows 62 percent of state and local entities still try to handle all their cybersecurity needs in-house, making it much harder to stay on top of the latest threats and the newest ways to thwart them.

Above all, know that we're in this together. "We like to say that there are two types of organizations in this world," says Balles of AT&T. "Those that have been hacked, and those that don't know they've been hacked."



Endnotes:

1. <https://www.nascio.org/wp-content/uploads/2019/11/2019StateCIOSurvey.pdf>
2. <https://techcrunch.com/2020/02/20/defense-agency-disa-breach/>
3. <https://www.npr.org/2020/02/17/806729389/behind-the-ransomware-attack-on-palm-beach-county-elections-in-2016>
4. <https://statescoop.com/smart-parking-meter-vendor-data-stolen-ransomware-attack/>
5. <https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/>
6. <https://www.zdnet.com/article/new-orleans-hit-by-ransomware-city-employees-told-to-turn-off-computers/>
7. <https://www.11alive.com/article/news/local/jackson-county-ransomware-attack/85-b02f15b5-b7f6-42e4-a64e-e28cc2f89ec3>
8. <https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html>
9. <https://www.nytimes.com/2019/08/20/us/texas-ransomware.html>
10. <http://dashboard.mazsystems.com/webreader/62052?page=14>
11. <https://www.eac.gov/news/2018/03/29/us-election-assistance-commission-to-administer-380-million-in-2018-hava-election-security-funds>
12. <https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/>
13. <https://www.tallahassee.com/story/news/local/state/2020/02/25/russian-hacking-floridas-election-system-what-we-know-four-years-later/4555126002/>
14. [https://ballotpedia.org/Help_America_Vote_Act_\(HAVA\)_of_2002](https://ballotpedia.org/Help_America_Vote_Act_(HAVA)_of_2002)
15. <https://www.eac.gov/payments-and-grants/election-security-funds>
16. <https://www.eac.gov/payments-and-grants/election-security-funds>
17. <https://www.eac.gov/payments-and-grants/2020-cares-act-grants>
18. <https://www.sos.state.tx.us/elections/forms/election-security-best-practices.pdf>
19. <https://www.cnet.com/news/hackers-are-targeting-us-government-workers-with-covid-19-scams-offering-free-fast-food/>



Our first name has always been American, but today you know us as AT&T. We're investing billions into the economy, providing quality jobs to over 200,000 people in the U.S. alone. We're supporting the veterans who make our country stronger and providing disaster relief support to those who need it the most. By bringing together solutions that help protect, serve and connect—committed AT&T professionals are working with the public sector to transform the business of government. No company is more invested in America's future than AT&T.

att.com/publicsector



Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

govtech.com