

Solutions for
state and local
government.

PLUS:

Leading the Charge

Get to know five state
and local CISOs.

Is the Virtual

Office Secure?

*The hidden threats
lurking behind the
shift to remote work.*



Cyberdata Dive
Survey data on
security strategy.



Risk Management
How safe are IT
subcontractors?

Faster Smarter Safer



A government executive's guide to understanding the **network of the future** and its role in transformative change.

Get your copy at
bit.ly/GovFuture



COVER STORY

18 / Locking Down the Virtual Office

Tech leaders grapple with the cybersecurity implications of a massive shift to telework that's lasting longer than anyone expected.

40 / Security in Profile

Five state and local CISOs on what it takes to keep government safe in 2020.

DEPARTMENTS

46 / Risks in the Chain

Securing subcontractors in as-a-service IT agreements is an ongoing challenge for state governments.

48 / Amplifying the Message

What does it take to be good at cybersecurity on social media?

INFOGRAPHIC

50 / Cyberstrategy in Numbers

A visual look at where state and local government stand on cyber.

COLUMNS

4 Point of View

When cyberthreats collide.

7 Data Points

Amid COVID-19, no-touch government services are the way forward.

10 Four Questions

New Jersey courts CISO Sajed Naseem on keeping justice secure.

54 Cybersecurity Strategies

The case for hiring hackers — and pirates.

56 CIO Street View

Local security often requires assistance from above.

NEWS

6 govtech.com/extra

Updates from *Government Technology's* daily online news service.

14 Big Picture

Takeaways from the 2020 Digital Counties Survey.

55 CIO Central

Career changes across tech-driven roles in state and local government.

58 Spectrum

More research, more science, more technology.

IN OUR NEXT ISSUE:

2020 in Review

GT reflects on a year for the books.

Who, What, Where

Recapping 12 months of career transitions.

Digital Cities

A look at the cities that are leading the way with tech.



When Cyberthreats Collide

As a pandemic sweeps the globe, the U.S. is in the throes of campaign season. The most high-profile race, of course, is the presidential election, set against the backdrop of an economy struggling to recover while clashes between those at opposite ends of the political spectrum in cities easily meet the threshold for domestic “unrest.”

And large-scale controversy, increasingly, brings bad actors in cyberspace looking to capitalize. After all, cybercrime is perpetrated by opportunists looking for the simplest path to success. Take, for example, the cascade of fraudulent unemployment claims targeting the billions of dollars in CARES Act funding flowing to states from the federal government earlier this year as COVID-19 decimated entire sectors of the economy. According to cybersecurity company Agari, one Nigeria-based group used stolen personal information to take advantage of abbreviated validation periods brought on by the emergency circumstances of the pandemic. Work is ongoing to recover the hundreds of millions of dollars that were stolen.

And as Nov. 3 nears, experts are pointing to a perfect storm of vulnerabilities to American election infrastructure. *Government Technology* has extensively covered the rise of ransomware over the past few years, documenting devastating attacks on school districts, cities, state agencies and more. In August, authorities from the federal Cybersecurity Infrastructure Security Agency and the FBI sounded the ransomware alarm as it relates to voter registration databases.

And as we saw in 2016, an attack doesn't have to be technically successful to cause chaos. Myriad news reports documented the fact that foreign adversaries breached voter databases in states across the country. In Illinois, attackers accessed the personal data of more than 75,000 voters.

But state elections officials insist that voter data was not altered, nor could it have been.

“We know where they got in and we know what the permissions were once you broke into that area,” Matt Dietrick, State Board of Elections spokesperson, told *The Chicago Tribune*. “It wouldn't have allowed you to change or edit or delete any data.”

But the breach did shake the public's confidence in election systems more generally. And despite broad agreement from cybersecurity officials that tampering with actual vote counts is incredibly unlikely, lingering doubts from the public are harder to overcome.

The decentralized nature of elections in this country helps guard against threats, since it's more difficult to orchestrate a large-scale attack against so many distributed targets. And elections officials across the country have been diligently working to secure every aspect of the voting process, to preserve the integrity of this most fundamental aspect of our democracy. It requires constant vigilance. But resources are scarce and levels of preparedness vary widely.

“We look at each and every system and process, no matter if it is seen as less risky or not,” Aman Bhullar, CIO of the Los Angeles County Registrar-Recorder/County Clerk, told *GT* recently. “Even a system as simple as email is very important during an election. We look at every threat vector as an opportunity to harden our systems [and] processes so that there is no way an attacker has an advantage.”

Elections officials should use every available resource — and there's ample evidence that they are — to ensure U.S. elections infrastructure is as impenetrable as possible. This includes lining up the right private-sector partners and heeding best practices guidance from organizations like the EI-ISAC, the Elections Infrastructure organization of the Information Sharing and Analysis Center. The future of fair elections depends on it. **GT**

Publisher: Alan Cox, alanc@erepublic.com
EDITORIAL
Editor: Noelle Knell, nknell@govtech.com
Managing Editor: Lauren Harrison, lharrison@govtech.com
Web Editor & Photographer: Eyragon Eidam, eeidam@govtech.com
Chief Copy Editor: Miriam Jones, mjones@govtech.com
Copy Editor: Kate Albrecht, kcalbrecht@govtech.com
Contributing Editor: Tod Newcombe, tnewcombe@govtech.com
Associate Editor, Data & Business: Ben Miller, bmiller@govtech.com
Assistant News Editor: Zack Quaintance, zquaintance@govtech.com
Staff Writers: Skip Descant, sdescant@govtech.com
 Jed Pressgrove, jpressgrove@govtech.com
 Lucas Ropek, lropek@govtech.com
 Andrew Westrope, awestrope@govtech.com
 Priscilla Christopher, David Rath, prath@govtech.com
 Andi Wong, awong@govtech.com

DESIGN
Chief Design Officer: Kelly Martinelli, kmartinelli@govtech.com
Senior Designer Custom: Crystal Hopson, chopson@govtech.com
Production Director: Stephan Widmaier, swidm@govtech.com
Production Manager: production@govtech.com

PUBLISHING
VPs OF STRATEGIC ACCOUNTS:
 Kim Frame, kframe@govtech.com
 Shelley Ballard, sballard@govtech.com
SALES DIRECTORS:
 Melissa Sellers, msellers@govtech.com
 Karen Hardison, khardison@govtech.com
 Lara Roebbelen, lroebbelen@govtech.com
 Carmen Besirevic, cbesirevic@govtech.com
 Lynn Gallagher, lgallagher@govtech.com
 Kelly Schieding, kschieding@govtech.com
ACCOUNT EXECUTIVES:
 Rebecca Regrut, rregrut@govtech.com
 Joelle Tell, jtell@govtech.com
 Kristi Leko, kleko@govtech.com
 Mark Androvich, mandrovich@govtech.com
BUS. DEV. MANAGER:
 Sheryl Winter, swinter@govtech.com
 Brittany Hopkins Siebel, bsiebel@govtech.com
INSIDE SALES:
 Paul Dangberg, pauld@govtech.com
 Katrina Wheeler, kwheeler@govtech.com
 Dana Kansa, dkansa@govtech.com
SALES ADMINISTRATORS:
 Jane Mandel, jmandel@govtech.com
 Lien Largent, llargent@govtech.com
 Sharon Penny, spenny@govtech.com
 Tara Holm, tholm@erepublic.com
 Janaya Day, jday@erepublic.com
Event Sales Operations Mgr: Alison Del Real, adelreal@govtech.com
Chief Customer Success Officer: Arlene Boeger, aboeger@govtech.com
Dir. of Content Studio: Jeana Bigham, jibigham@govtech.com
Dir. of Digital Marketing: Zach Presnall, zpresnall@govtech.com
Web Advertising Mgr: Adam Fowler, afowler@govtech.com
Subscription Coord.: Eenie Yang, subscriptions@govtech.com

CORPORATE
CEO: Dennis McKenna, dmckenna@govtech.com
President: Cathilea Robinett, crobinett@govtech.com
CAO: Lisa Harney, lharney@govtech.com
CFO: Paul Harney, pharney@govtech.com
Executive VP: Alan Cox, alanc@govtech.com
Chief Content Officer: Paul W. Taylor, ptaylor@govtech.com
Dep. Chief Content Off.: Steve Towns, stowns@govtech.com
VP Research: Joe Morris, jmorris@govtech.com

Government Technology is published by eRepublic Inc. Copyright 2020 by eRepublic Inc. All rights reserved. *Government Technology* is a registered trademark of eRepublic Inc. Opinions expressed by writers are not necessarily those of the publisher or editors.

Article submissions should be sent to the attention of the Managing Editor. Reprints of all articles in this issue and past issues are available (500 minimum). Please direct inquiries for reprints and licensing to Wright's Media: (877) 652-5295, sales@wrightsmedia.com.

Subscription Information: Requests for subscriptions may be directed to Subscription Coordinator by phone or fax to the numbers below. You can also subscribe online at www.govtech.com.

100 Blue Ravine Rd. Folsom, CA 95630
 Phone: (916) 932-1300 Fax: (916) 932-1470

Printed in the USA

Coming in November
A Government Technology Magazine

SPECIAL ISSUE

gt

✓ FUTURE READY

Exploring what
the future looks
like now.

This issue will explore:

- ✓ The Evolution of Smart Cities
- ✓ The Future of Work
- ✓ Tech and Rural America

Plus a look at Futurists and Forward Thinkers for their predictions on the biggest tech and trends that will reshape life, and government, over the next decade.

**Can't wait
until November?**

Discover Future Ready
tactics, COVID-19 resources,
and actionable best practices at
govtech.com/futureready

SPONSORED BY



Google Cloud



Trending Up?

Unemployment has made headlines since the onset of the COVID-19 pandemic earlier this year, but public-sector employment continues to make steady gains, growing at a rate of 1.4 percent between June and July, about on pace with the rest of the economy. However, a report from the National Association of Counties noted that those numbers were seasonally adjusted and may not reflect the reality of the pandemic's effect.

TEST DRIVE

California drivers who are interested in electric vehicles but aren't quite ready to make the commitment can take advantage of a new EV subscription service from AAA of Northern California, Nevada and Utah and Electrify America. The all-inclusive short-term lease includes maintenance, insurance, roadside assistance and a Level 1 charger that can be plugged into any 120-volt three-prong outlet, and is designed to help remove some of the barriers to EV driving.



Biz Beat

As protestors have called for rethinking how the American policing system works, one tech company has been working with about 400 law enforcement agencies since 2006 to help departments identify "problem officers." LEFTA Systems takes data that's often still kept in paper records and brings it together so that supervisors can track officer behavior. However, it would still fall on the police departments to respond to the tech's findings.



WHO SAYS?

"Our curbs and streets are still crying out for regulation."

govtech.com/quoteoctober2020

MOST READ STORIES ONLINE:

House Bill Could Mean Billions for State, Local IT

FCC Approves Amazon's \$10B Plan for Satellite Internet

Amazon Web Services Has Hired Four Former State CIOs

FAA Announces Drone Line-of-Sight Waiver for Public Safety

Cities Lose the Legal Battle Against FCC 5G Policies

Bipartisan House Bill Proposes \$50M for Election Security

2

The number of days it took Buffalo, N.Y., to stand up its remote 311 call center.

1^K

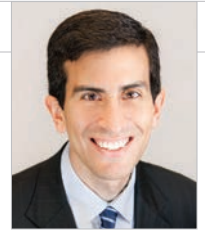
The number of polling places where Los Angeles County residents will be voting on Election Day.

128

The number of traffic signals that will be connected to a new monitoring system to improve transit safety and efficiency in Valdosta, Ga.

49^M

The number of interactions between citizens and government in New York state in three months thanks to the COVID-19 Technology SWAT Team.



Touchless Government

From digitizing paper forms to implementing facial recognition, no-contact government services are the way forward.

To prevent the spread of COVID-19, many organizations are dramatically rethinking their operations to ensure physical distancing, from professional sports leagues creating quarantine bubbles for their players to the music and film industries offering performances at drive-in theaters. As the global pandemic stretches into the fall with no clear end in sight, public-sector agencies must similarly wrestle with how to safely reopen government operations while protecting the health and safety of government employees and citizens. Achieving this will require government leaders to focus on a new objective: using technology to design a touchless future.

Part of the solution will entail shifting more government operations online. Government employees should be able to telework if they can perform their tasks remotely, and agencies need to continue to invest in the IT resources, including moving to the cloud, and training to allow them to do so securely and effectively. In addition, government agencies should migrate more services online to both reduce the need for face-to-face interactions and increase efficiency and convenience. For example,

government agencies should use the pandemic to finally replace all paper forms with digital ones and upgrade outdated online services to mobile-friendly ones.

But government cannot achieve a touchless, or limited-touch, future through online services alone. In addition,

“GOVERNMENT CANNOT ACHIEVE A TOUCHLESS, OR LIMITED-TOUCH, FUTURE THROUGH ONLINE SERVICES ALONE.

agencies should consider the myriad ways technology can reduce face-to-face interactions when people must leave their homes. In this regard, other sectors offer many early examples of the possibilities. For example, restaurants are offering no-contact delivery, hotels are offering no-contact check-in, and airports are offering no-contact security screening and bag drop.

Consider some of the possibilities for government:

- Facial recognition technology can integrate with automated gates to quickly check the identification of workers and visitors to government buildings without the need for direct contact with security guards and to reduce crowding at entrances.
- Thermal cameras can detect elevated body temperatures in real time, quickly screening individuals for COVID-19 symptoms. Manually taking the temperature of individuals exposes people to more physical contact and can be a slow and tedious process.
- Automated speed and red-light camera enforcement can bring down the number of traffic accidents and injuries while also reducing the need for police officers to make traffic stops.
- Mobile payment technology can enable residents to pay for city services, from parking to pet licenses,

from their mobile devices without touching any foreign surfaces.

- Self-service kiosks with speech recognition can allow individuals to access city information and services while eliminating the need for multiple users to share the same touchscreen.
- Autonomous disinfection robots can sanitize public spaces and other government-operated facilities without exposing janitorial staff to potential infection.
- Autonomous delivery drones can reduce face-to-face contact while distributing small packages.
- Smart building features, from lights that turn on automatically to hand washing stations with automatic sensors, can both reduce the spread of germs and increase efficiency.

Touchless government is not something many agencies have planned or prepared for, but it is an emerging opportunity that will require agencies to become more familiar with automation, sensors, robotics and analytics. Gaining greater experience with these technologies will help them not only address immediate health concerns during the pandemic, but also boost productivity, all while gaining important expertise that will serve these agencies well as they continue to leverage technology to improve government services in the future. **dt**

Daniel Castro is the vice president of the Information Technology and Innovation Foundation (ITIF) and director of the Center for Data Innovation. Before joining ITIF, he worked at the Government Accountability Office where he audited IT security and management controls.

Becoming a Future-Ready, Digital Government

An enterprise content services platform helps government transform processes, continue business operations and enhance service delivery in times of disruption.

STREAMLINING OPERATIONS AND DRIVING INNOVATION

As state and local government leaders continue to respond to COVID-19 and prepare for what is next, they understand the importance of technology that allows employees to work remotely and provide digital services to citizens. Yet moving work processes and citizen services online is just the first step. To meet constituent expectations of an uninterrupted digital experience and unlock the benefits of technology, governments must continue to embrace digital transformation.

Many public sector leaders recognize that a modern content services platform (CSP) is a key technology to make this change. In a Center for Digital Government (CDG) survey, more than two-thirds of respondents said a CSP will help their agency or department improve productivity and enhance the delivery of essential citizen services.

With all documents and data stored in a central repository and managed by a CSP, an agency benefits from stronger data security. Employees have secure access to the digital documents and workflows they need, whether working in the office, in the field or from home.

WHAT IS A CSP?

The role of a CSP is to centralize, modernize and automate how a government manages its information and associated workflows. Laserfiche describes a CSP as an evolution of enterprise content management, which represents a major shift in how organizations get work done and operationalize content. For governments, content services focus on solving multiple business process challenges with integrated solutions to modernize citizen services, increase productivity and enhance collaboration.

With all documents and data stored in a central repository and managed by a CSP, an agency benefits from stronger data security. Employees have secure access to the digital documents and workflows they need, whether working in the office, in the field or from home.

By implementing a CSP as an enterprise-wide system, a government agency can:

- Transform mission-critical service delivery
- Enhance the citizen engagement and experience
- Manage and operationalize information with strong security and access controls
- Maximize agency resources with seamless integration with core government systems

Government agencies are finding a great value in flexible solutions to meet dynamic and unpredictable demands for services, especially in a time of uncertainty. CSP characteristics like interoperability will help them better prepare for the next disruption or community emergency response.

HOW GOVERNMENTS RESPONDED TO THE PANDEMIC

Numerous government agencies have used a CSP for COVID-19 response in ways that can be adapted for future emergencies and community needs.

For example, Cowlitz County, Wash., created a business process to obtain daily status information from local long-term care facilities about their supply of personal protective equipment (PPE) and testing capacity. The process saves time by eliminating daily calls by a county employee and allows the incident management team to easily see status and trends on a data dashboard. Another recently implemented process allows constituents to submit noncompliance inquiries with stay-at-home and other public health orders, reducing the burden on the 911 center previously inundated with requests.

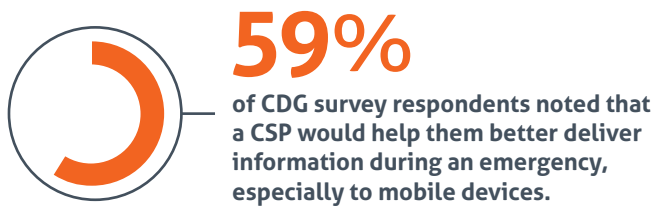
In the tourism-oriented town of Silverthorne, Colo., leaders allocated funds for emergency grants when small businesses were negatively impacted during the pandemic-related shutdown. Silverthorne staff were able to automate the entire application process and award grants to 92 businesses in two weeks.

Agencies throughout Oneida County, N.Y., are using a CSP platform to identify needs and provide assistance to keep the community safe and healthy. For example, one process helps IT staff determine the readiness and resource needs of remote

employees. In the health department, employees use a form to collect test data and contact COVID-positive citizens to provide advice and assistance. And at the county planning department, staff gather input from local businesses on revenue impact and employment levels as well as reopening plans.

But the COVID-19 pandemic is far from the only emergency that has or will disrupt government agencies. When Hawaii County, Hawaii, experienced a prolonged volcano eruption, residents and visitors needed an easy way to obtain up-to-date, official information. By using its CSP, the county was able to present relevant and timely information to keep their communities safe.

Fifty-nine percent of CDG survey respondents noted that a CSP would help them better deliver information during an emergency, especially to mobile devices.



TODAY'S LANDSCAPE FOR A FUTURE-READY, DIGITAL GOVERNMENT

In some jurisdictions, a solution for electronic document management or automated processes may already exist in a few departments or agencies. But a CSP offers greater

impact when it is implemented enterprise-wide because it facilitates collaboration, preserves records integrity, and balances efficiency with security. Benefits include:

- Opportunities for broad and continuing efficiency gains, cost savings and citizen service improvements
- Flexibility for rapid response to unpredictable constituent needs and fast-changing conditions
- Ability to deploy and scale processes to more departments, users, operations and citizen services
- Data collection, communication and collaboration tools that are already in place and familiar to users before a disruption or emergency occurs

In the CDG survey, respondents cited improved interoperability, enhanced citizen and employee experiences, and optimized costs as their top reasons for adopting a CSP by the end of 2021. All these factors will benefit both routine and emergency government operations.

THE WAY FORWARD: A CATALYST FOR DIGITAL TRANSFORMATION

The COVID-19 crisis has emphasized the need for governments to modernize service delivery, rethink digital strategies and digitally transform operations to prepare for the next big disruption. A CSP is at the center of this modernization, enabling the continuity and adaptability that will keep government working and ready to serve, no matter what the future holds.

This paper was produced by the Center for Digital Government Content Studio, with input from Laserfiche.

Where to Find the Funding

To cover the costs of a CSP, consider these tips.

Tip #1. Review CARES Act funding based on implementing a CSP for long-term telework and expanded online service delivery.

Tip #2. Look across all budgets for expenditures planned before the pandemic that can now be redirected to an enterprise-wide CSP.

Tip #3. Ask for help and insights from a trusted partner when building the business case that can justify a CSP solution as a priority for limited IT budgets.

Sample factors to make a strong business case:

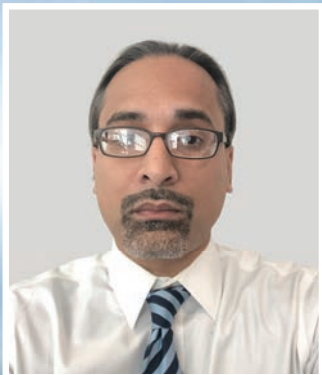
- Cost savings for paper supplies, storage cabinets and facilities, and processing when converting to digital forms and documents, especially for information capture
- Higher levels of readiness and resiliency for internal operations and public services
- Improvements in mission-critical processes that streamline operations in normal times and support business continuity during disruptive events

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: **Laserfiche®**

Laserfiche enables government agencies to innovate how they manage information, modernize processes and enhance the citizen experience. Leading government organizations use Laserfiche's powerful workflows, electronic forms, document management, Department of Defense 5015.2-certified records management and analytics to transform service delivery. To learn more about government solutions from Laserfiche, visit: <https://www.laserfiche.com/slg>.



Sajed Naseem

Chief Information Security Officer, New Jersey Courts

Sajed Naseem handles cybersecurity for the New Jersey Courts, a centralized system that had 750 networks and about 50,000 devices before COVID-19. Naseem, who is also a cybersecurity professor at St. John's University in Queens, N.Y., has responded to new challenges since the system went virtual this year and added home networks and activities to its list of concerns.

1 How do you promote cybersecurity awareness in a remote context?

We definitely have cybersecurity awareness, but we also have what I call cybersecurity readiness and performance. To me, awareness is knowing something, and readiness and performance is having the right amount of knowledge and the right amount of training to be able to act on a problem.

We actually measured cybersecurity readiness and performance of our staff for many years beforehand. This is unique. We weren't talking about it, but we wanted to know the knowledge, behavior and attitude of our employees. We measured that mathematically.

One of the steps we've been taking is looking at the high-profile users — someone who doesn't have the right amount of knowledge about phishing — and asking, can we monitor them differently? Can we act on them differently?

2 What might keep you up at night at this point?

It goes back to an engineering problem. To me everything is about

defining things in a big-picture format, then acting on it with an engineering mindset and then training the operational teams to be able to deal with it.

To directly answer your question, I want to make sure that those actions by the operational teams are directly in line with the way that we've engineered the systems. Did the overnight operational teams know how to act on a particular engineering rule that we've created? We've seen so far that they know how to do that, but it's an ongoing situation.

Our court could be down if ransomware hits. We've made engineering directly related to ransomware, because we've seen places like Atlanta, Baltimore, Albany and Quebec that were basically missing the right engineering to be able to deal with these threats.

3 Has the pandemic taught you anything new about cybersecurity?

This has been a major learning situation, not just learning in academic terms but in terms of practical mindsets.

We've even seen a mindset change with our users. I always go back to this in

cybersecurity: If the end user is talking, I listen. I'll go to people who may not be engineers, and I'll talk to them: How do they view cybersecurity awareness month? How do they view working from home?


It's been interesting during this period. We've seen a lot of users at different levels of the organization reaching out who would've never reached out to me earlier with cybersecurity questions. It could be questions like, "How do I keep my computer safe for my kid?" or, "What threats do I need to be aware of on the Internet?"

There's a mindset change there, so I think we're all learning.

4 Are there any additional equity concerns as court proceedings go virtual?

We have several courts here: Supreme Court, Superior Court, Appellate Court and Tax Court. The Supreme Court had several committees during this COVID-19 period. I was part of pretty much all of them, and they were related to technology, cybersecurity and providing justice. There was even a new one recently that was getting into a key topic, the security of judges' personal information online, which is a major threat to them.

One of the key questions that was posed to me was, what are the disparities? Once you came into the physical court, you had a judge, a jury, a certain background. Now you're sitting behind a Zoom session or whatever you have, a virtual image. What are the things at home that could lead to disparities in terms of the judge judging you?

If, let's say, you had red paint in the background, or a lot of noise, does that affect the way that your judgment comes out? If you're in a court case and you're always No. 1 on the screen, does that change the way that the judge may rule on your case because you're always in the forefront? These are things that we never had to deal with before and that we will be studying and understanding for many, many years. And I don't think that's going in reverse. Now there's a new area; we saw a court case out of the U.K. where someone had doctored audio for a child custody case, so deepfakes. This is all part of the world now. 

— Jed Pressgrove, Staff Writer

Successfully Navigating 2020 Required Not Just Being Prepared, Agencies Had to Be FUTURE **READY**

This year, in partnership with Google Cloud, we're recognizing five state and local government agencies that demonstrated what it means to be Future Ready by leveraging innovative technologies, processes, and leadership.



This month,
we're recognizing
Los Angeles County,
California as a
**2020 Future Ready
Award Winner.** A few
highlights of how
L.A. County prepared
for the future:

- ✓ Establishing a **\$10 million-dollar technology innovation fund** for new multidepartment technology programs.
- ✓ The development of an **enterprise IT strategy** for over 200 business units and IT professionals across 37 departments.
- ✓ Deploying a **\$20 million-dollar legacy technology modernization fund**.
- ✓ Leveraging **artificial intelligence and machine learning** in new mission-critical social services areas, including tackling homelessness.

CENTER FOR
DIGITAL
GOVERNMENT



Read more about L.A. County's story and
the other Future Ready Award winners at
govtech.com/futureready/awards

State of Illinois: Using AI to help residents impacted by COVID-19 receive unemployment benefits

The Illinois Department of Employment Security is using Contact Center AI to rapidly deploy virtual agents to help more than 1 million citizens who lost their jobs to file unemployment claims.

Google Cloud results

- The state of Illinois anticipates an estimated annual savings of \$100M based on an initial analysis of IDES's virtual agent data
- Virtual agents handle more than 140,000 phone and web inquiries per day
- Phone virtual agent answers 40,000 after-hours calls per night
- Illinois residents can get help to file their unemployment claims faster
- Contact Center AI web and phone virtual agents each deployed in just two weeks

When the COVID-19 virus spread throughout the US, it devastated the job market, driving millions of Americans into unemployment within weeks. State governments across the country suddenly faced an unprecedented surge in unemployment benefits claims.

In the state of Illinois, the number of COVID-19-related unemployment claims submitted between March 1 and May 9, 2020, totaled 1,076,461, which is nearly 11.5 times the number of claims the department processed during the same period in 2019.

For the Illinois Department of Employment Security (IDES), which administers the state's unemployment benefits, this led to a deluge of phone calls and web inquiries from residents. The surge was compounded by the state's shelter-in-place order, which prohibited residents from visiting IDES offices to file their claims in person.

"Because of COVID-19, our constituents were unable to walk into a state office, so the increase in web and phone inquiries was astronomical," said Jennifer Ricker, Acting Assistant Secretary for the Illinois Department of Innovation and Technology (DoIT). Illinois DoIT is responsible for

Virtual agents help hundreds of thousands get unemployment benefits

providing technology, innovation, and telecommunications services to all Illinois state agencies.

Contact Center AI virtual agents assist human staff

As overburdened IDES contact center agents strained to answer phone calls and respond to web inquiries, constituents contacting the agency for unemployment assistance waited for hours on the phone, or simply didn't get through. Realizing the urgency of the problem, Illinois mobilized a cross-functional response team to find and deploy a solution fast.

The state of Illinois chose Contact Center AI, a conversational AI solution from Google Cloud. Contact Center AI uses artificial intelligence to enable rich conversational experiences between virtual agents and customers through chat and over the phone.

"The automated virtual agents have acted like a force multiplier for IDES's support agents, in terms of processing and responding to unemployment benefits requests."

—Jennifer Ricker, Acting Assistant Secretary,
Illinois Department of Innovation & Technology

Advertisement

Working with Google Cloud, Ricker and her team developed a three-phase plan to deploy Contact Center AI virtual agents on the IDES website and through the agency's phone system. In phase one, the Contact Center AI virtual agents were designed to answer frequently asked questions regarding constituents' unemployment claims.

Three Google Cloud partners played key roles in designing and deploying the solution. Quantiphi, which specializes in applied AI and machine learning, helped launch the web virtual agent; and Presidio, a digital transformation IT solution provider, assisted with the phone agent. Additionally, the team used Cisco Contact Center AI APIs to connect the Dialogflow bot to IDES's Cisco contact center and communications system.

Contact Center AI quickly augments legacy technology

It took only two weeks to deploy each virtual agent—for a total rollout time of four weeks. In addition to quickly integrating Contact Center AI with existing technology, the DoIT team was also helping state employees transition to remote work due to COVID-19.

"We not only faced very tight timelines to launch the Contact Center AI virtual agents, but we also had to integrate with legacy technology while helping our employees as they transitioned to working from home," said Brandon Ragle, Chief of Enterprise Applications for the Illinois Department of Innovation and Technology.

IDES completed phase one in mid-April when they launched their web virtual agent and phase two in late April when their phone virtual agent started answering after-hours phone calls. Phase three will connect the phone and web virtual agents to IDES's backend systems to handle more complex requests, such as password resets, inquiries about check claim status, and changes to constituent records.

"The ease with which our teams were able to quickly integrate Contact Center AI on our legacy technology was a pleasant surprise," Ricker added.

Virtual agents help thousands file unemployment claims

As the economic impact of COVID-19 reverberated across Illinois, IDES's website traffic spiked from 50,000 page views per day to millions.

Fortunately, IDES's newly deployed virtual contact center agents provided immediate help. IDES reports that the phone virtual agent consistently processes an average of 40,000 constituent phone calls per night. And the web chat-bot interacts with upwards of 100,000 constituents a day.

By absorbing these constituent inquiries, Contact Center AI is helping many thousands of Illinois residents get im-

"Don't fear the unknown. We've had to push ourselves through some internal processes, and we're generally very cautious with our contact centers, but working with Google Cloud has been a great experience."

—Dale Walters, Chief of Network Operations,
Illinois Department of Innovation & Technology

portant information on their unemployment claims quickly. It's also alleviating the demand on IDES's human agents to answer common and repetitive questions, enabling them to focus on more complex cases.

As Ricker put it, "The automated virtual agents have acted like a force multiplier for IDES's support agents, in terms of processing and responding to unemployment benefits requests."

Momentum for digital transformation and omnichannel support

IDES's successful rollout of Contact Center AI is helping the agency achieve their immediate priority, which is ensuring Illinois residents get their unemployment benefits quickly in a time of crisis.

According to IDES, the web virtual agent answered 3.2 million inquiries in its first two weeks, helping them pay unemployment benefits in a timely manner to 99.99% of claimants. Seventy-five percent of claimants received their first payment within two weeks. And the project's success is creating positive ripple effects in other areas too.

For one, with virtual agents now assisting more than 100,000 constituents a day, the DoIT team is thinking more seriously about how they can serve constituents in an omnichannel way.

"The benefits we're seeing with the web and phone virtual agents has really led us to think in a more omnichannel manner, as opposed to viewing each of these channels as separate and independent," said Ricker.

The team's ability to quickly integrate Contact Center AI with their legacy technology stack—without any major snags—has also added momentum to the DoIT's digital transformation efforts.

Visit govtech.com/futureready for more news and insights on using cloud to reimagine government operations and services.

The Digital Life of Counties

2020 has been a transformational year for gov tech, and the nation's more than 3,000 counties are on the front lines of pandemic response, working toward providing consistent services to citizens using increasingly digital means. Here are some highlights from the 2020 Digital Counties Survey from *Government Technology's* sister organization, the Center for Digital Government. For complete coverage on all 53 winners across population categories, visit govtech.com/digitalcounties2020.

They're No. 1

First-place finishers in each of five population categories (smallest to largest):

Mono County, Calif.

Arlington County, Va.

Chesterfield County, Va.

Ventura County, Calif.

Los Angeles County, Calif.

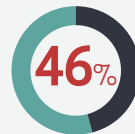
Citizen Experience: Most Widely Used Tools



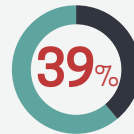
SOCIAL MEDIA



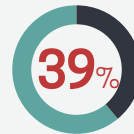
ACCESSIBILITY



TEXT MESSAGE



MOBILE APPS



RESPONSIVE DESIGN

On the Way



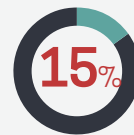
LIVE CHAT/
ONLINE HELP



SINGLE SIGN-ON



MESSAGING APPS



LOCATION SERVICES



TEXT MESSAGE

CIO Priorities

- 1 / **Cybersecurity**
- 2 / **Budget and Cost Control**
- 3 / **Citizen Engagement/
Experience**
- 4 / **Disaster Recovery/
Continuity of Operations**
- 5 / **Business Intelligence/
Analytics**

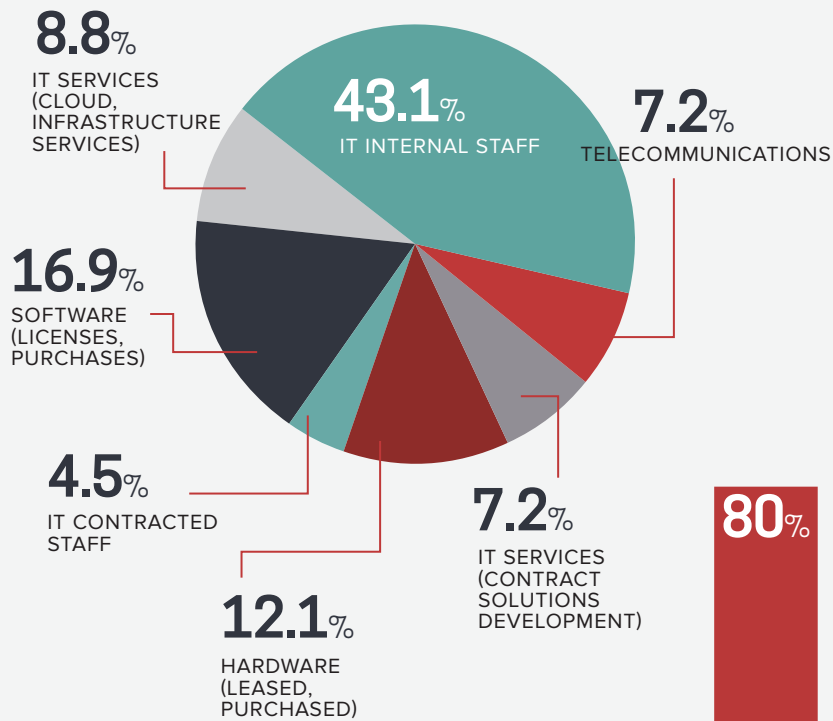
88%

of counties are gathering citizen feedback on customer experience channels and using it to make improvements.

Emerging Tech

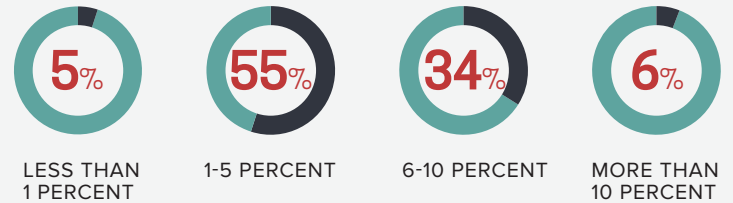
	IN USE	PLAN TO USE
Artificial Intelligence	24%	30%
Blockchain	3%	30%
Digital Assistants	13%	34%
Drones	39%	15%
Edge Computing	22%	21%
IoT	31%	16%

County IT Spending



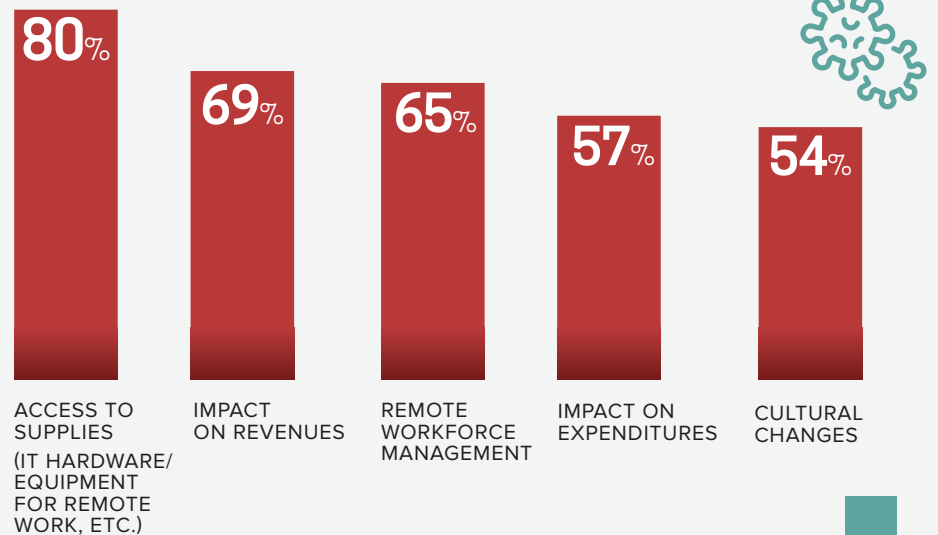
Supporting Cyber

Percentage of IT budget that goes toward cybersecurity:



Confronting COVID-19

Biggest challenges in pandemic response:



CENTER FOR
DIGITAL
GOVERNMENT

government
technology





Building a Better Way to Vote

Los Angeles has transformed its entire election system from the ground up.

Like most places in the United States, Los Angeles County's election system had long been plagued by inefficiencies, malfunctioning equipment and antiquated technology. But when L.A. first began confronting these challenges more than 10 years ago, it came up with an audacious plan: It would build its own election system from scratch.

Now, L.A. County's new "Voting Solutions for All People" initiative has transformed the way Angelenos vote. VSAP includes much-needed modernizations of voting machines and infrastructure throughout the county, but the overhaul isn't just about upgraded technology. It's a top-to-bottom reimagining of the entire voting process.

"People here had been voting the same way for 50 years," says Aman Bhullar, CIO for the L.A. County Registrar-Recorder/Clerk's Office, which oversees elections in the county. "Our system was on life support. We had to come up with a better way of doing things."

With 5.2 million registered voters, Los Angeles County is by far the biggest voting district in the United States — larger than 42 states. Its multilingual population and its sheer

size — 88 municipalities spread across more than 4,750 square miles — make it an especially challenging place to hold elections.¹

But voting in L.A. had remained essentially unchanged since the 1960s. "It was antiquated; it lacked flexibility and adaptability," says Bhullar. "It was a hindrance for the people who were trying to vote."

Los Angeles may be an extreme case, but its struggles with outdated voting technology are part of a widespread national problem. Despite some election modernization assistance from Congress — including more than \$4 billion in Help America Vote Act funds since 2002 — many jurisdictions still rely on decades-old voting technology. And many of the new machines that were implemented by states in the early 2000s are now themselves becoming obsolete. Indeed, as recently as 2019, 45 states were still using some voting equipment that is no longer manufactured,² forcing some election officials to root through used computer stores for compatible parts.

How Los Angeles Reimagined Voting

When Los Angeles officials started looking for a new solution, they

quickly realized there was nothing in the marketplace that would fit the county's needs.

"There was no system available that could actually scale to the volume that we deal with," Bhullar says. And in an industry where a small handful of vendors control the vast majority of the market, "there was little room for innovation," he adds. "So we thought, 'Let's create one ourselves.'"

They refocused around a new voter-centered approach. It began by outlining key principles around transparency, accessibility, privacy and options for voting. The county engaged a global design firm to reimagine the voter experience. Community representatives were involved every step of the way, including advisory committees made up of community-based organizations and technology experts. The county designed its own open source elections software and then approached manufacturers about building it into new touchscreen voting machines.

The county was always focused on three areas, says Bhullar. "It's people, processes and technology. Those three have to go hand-in-hand."

After several years of design and planning, the county was ready to begin

operationalizing VSAP. That's when it brought in AT&T to help implement various aspects of the project.

"As a system, VSAP had a lot of operational nuances that needed to be straightened out," Bhullar says.

The county had long maintained a relationship with AT&T, but it increased that collaboration to help make VSAP a reality.

"Bringing in AT&T helped us in many capacities, including streamlining our cybersecurity and network operations, as well as process improvement."

One key decision, which the county implemented in April 2019, was to assemble a program team, led by AT&T's consulting group and select subject matter experts from AT&T's security organization. The team was co-located with the Registrar Recorder which facilitated communication and helped protect the elections.

"That was very unique," says Janet Ifekwunigwe, the AT&T strategic lead for the initiative. "We felt like we were part of the organization, and that gave everyone a very different sense of responsibility to one another. It was an environment that allowed us to really collaborate as teammates."

That relationship also allowed AT&T to focus not only on its traditional strengths of connectivity and security, but also on things like technical staffing, asset management, mobile applications, site logistics, training and poll worker management.

"For AT&T, it was really about looking at every step of the election process to see how we can help support the county," Ifekwunigwe says.

It also speaks to the evolving roles between public and private organizations, says Bhullar. "I'm not looking for a vendor who can simply sell me products and services. I'm looking for a partner who can be there and stick it out with us in this journey and for a long term."

From 'Teething Issues' to a National Model

The county officially debuted its new system for California's presidential primary in March 2020. The new

touchscreen machines were easier to use, and voters received a printed copy of their ballot, allowing them to personally verify their vote had been properly recorded. The new devices were a major improvement in terms of accessibility: They offered ballots in 14 different languages, plus large-type and headphone options, and screens that could adjust for voters in wheelchairs.³

But L.A. didn't just change its voting technology; it changed voting itself. Utilizing new options available under state law, L.A. County expanded the voting period from 13 hours on a single day to 11 days over the course of a week and a half. It replaced its 4,800 precinct voting sites with nearly 1,000 voting centers — and voters could show up to cast their ballot wherever they wanted. Also for the first time, the county offered instant day-of registration for residents who wanted to vote.

All those changes resulted in some initial hiccups, including technical glitches and long lines at some polling places. But Bhullar likens those Super Tuesday problems to "teething issues," adding that, "in a huge rollout that touched the lives of millions of people, there were challenges that presented opportunities for us to learn from our mistakes."

The county immediately began assessing anything that had kept the election from running smoothly, and it implemented those lessons for subsequent elections, including eliminating some of its smallest election centers and redeploying those resources to other sites in higher-traffic

"People here had been voting the same way for 50 years. Our system was on life support. We had to come up with a better way of doing things."

Aman Bhullar, CIO, L.A. County Registrar-Recorder/Clerk's Office

parts of the county. The important thing, says Bhullar, is embracing the fact that it's an iterative process.

"We continue to evolve and learn," he says.

Most other voting districts in the country don't have the resources to do what L.A. did. But thanks to L.A., they don't have to.

"VSAP was intended to be used by other jurisdictions for the greater good," says Bhullar.

The county is making its open source code — and its experience and expertise — available for jurisdictions throughout the country to pick and choose what they need.

"They may not need 100 percent of VSAP. Maybe they just need a tabulation system. If they do, they can pretty much take ours and start running with it," Bhullar says.

Ultimately, as more communities start using the new platform, they could even help improve the system.

At the end of the day, it's about creating a process based on transparency and making it easier for each person to cast a ballot, Bhullar says. "More transparency and better access are good for the community, and good for democracy."

Endnotes

1. <https://www.fastcompany.com/3049203/voting-needs-a-serious-overhaul-and-la-might-have-the-solution>
2. <https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-where-we-stand-today>
3. <https://www.nbcnews.com/politics/2020-election/has-los-angeles-county-just-reinvented-voting-n1000761>





Locking Down the Virtual Office

Tech leaders grapple with the cybersecurity implications of a massive shift to telework that's lasting longer than anyone expected.

By David Rath

Jim Weaver, chief information officer of Washington state, refers to the pandemic as the state's new chief innovation officer. "It is demonstrating to agency leaders the transformative opportunities

that some technology tools bring to how business can be done as opposed to how it has always been done," he said.

One such innovation involved securely shifting thousands of state employees to working from home in March 2020 when Gov. Jay Inslee issued a stay-at-home order.

Washington was the first U.S. epicenter of COVID-19 in January, and as a member of Inslee's cabinet, Weaver had insight that a stay-at-home order was on the horizon. "We were able to scale up capacity and get ready for the onslaught that was coming. Overnight we shifted from fewer than 3,000 users to having 29,000 concurrent users on our VPN [virtual private network] at any given time," he recalled.

The remote work setup, which continues, has challenged Weaver's team to redouble educational efforts on cyber-hygiene and rethink how patching is done. Meanwhile, in a state with a decentralized IT framework, the complexity level increased because his office was in the process of changing VPN platforms, trying to move agencies to Microsoft Teams as a unified communication platform, and dealing with laptop supply shortages. Some employees took desktop computers from the office to set up at home, creating remote support and maintenance issues.

Although many state and local governments have been pleasantly surprised that they were able to rapidly shift a large percentage of their employees to remote work, many CIOs are losing sleep over increased cybersecurity threats.

"As we made the initial transition to remote work, a lot of the typical standard security controls were circumvented in the interest of expediency," explained Mark Weatherford, chief strategy officer for the National Cybersecurity Center. "Some of the things we might have taken a more measured approach to implementing

got swept away in the urgency to get things done. We went from one day having everyone in the office to a week later everybody working from home. For government agencies that weren't prepared to do that, whether it was having laptops available or remote capabilities available to everyone, there was a lot of work that had to be done over a short period of time."

If the workforce wasn't prepared to be mobile, IT teams would have to go in and tweak firewall rules and install VPNs, Weatherford said. "The danger would be that in the urgency of the moment, a lot of these security controls would be put on a checklist to get back to, but IT teams would feel they don't have time to do it right now. They are just going to open up these ports and protocols to allow people to work."

TELEWORKING WITHOUT A POLICY

Eric Romero, director of information services for Baton Rouge, La., was in a difficult position when the stay-at-home order was issued in March. His office had spent more than a year focused on tightening up security after several organizations in Louisiana, including New Orleans and the state government, had dealt with ransomware attacks. However, Baton Rouge had no official telework policy and very few laptops.

"We were scrounging around for laptops and other all-in-one computers we could possibly send home with key people," Romero remembers. "But sending someone home with a keyboard, mouse,

"The danger would be that in the urgency of the moment, a lot of these security controls would be put on a checklist to get back to, but IT teams would feel they don't have time to do it right now. They are just going to open up these ports and protocols to allow people to work."

desktop and a monitor and expecting them to connect it all to their network properly — that wouldn't have worked."

The idea of employees using their own computers was brought up, but cybersecurity concerns gave Romero pause. "I know it is possible, but we didn't have all the security measures in place that would allow that." The city ended up with about 100 laptops, and configured the VPN so that when employees connected, they would have remote access to their desktop computer on the network.

But that left many employees unable to work or coming into the office in shifts to get work done. And while governments in the region have experience determining who is an "essential worker" during emergencies like hurricanes, it gets more complex when the emergency extends into months. For example, clerks in accounting who pay bills may not be essential for the first week, but they are essential after a month has passed.

After two months, the stay-at-home order in Louisiana was lifted and people went back to work, but the virus was still present in the state, and as cases spiked, there was talk that another stay-at-home order might be necessary. "Quite honestly, we still don't have enough assets to accommodate everybody," Romero said.

John Gilligan, president and CEO of the Center for Internet Security (CIS), says that a government's experience of remote work during the pandemic depends largely on whether there had been a gradual migration to telework.

"Organizations that had a fairly robust telework program had the knowledge of what their technical approach would be to provide the connectivity and security. What they did not have was the capacity," he explained. "For the most part, I believe we will look back and say the changeover was dramatic, relatively seamless and painless, and a good example of cooperation between government



61%
of security and IT
leaders are concerned
about increased
cyberattacks targeting
remote workers.

SOURCE: CENTER FOR INTERNET SECURITY



Working from Home, Securely

Here are a few recommendations related to remote work from the Center for Internet Security's Resource Guide for Cybersecurity During the COVID-19 Pandemic:

PHISHING AND MALSPAM

Remind employees to be cautious when opening emails about COVID-19, especially those from outside the organization. They should exercise caution when entering credentials into a website, linked from an email, text message or social media account, or when downloading attachments.

CREDENTIAL STUFFING

It may have been necessary to make services available to employees remotely, without the time to secure accounts through multi-factor authentication (MFA). Along with securing accounts with MFA, employees should make sure all passwords are secure, and should never reuse passwords on different accounts.

REMOTE DESKTOP PROTOCOL TARGETING

An increase in the number of employees connecting remotely means an increase in the number of systems with the remote desktop port open and potentially being scanned. While your workforce needs to access systems remotely, limited and secure access by VPN can reduce the attack surface.

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

Downtime from an attack is even more detrimental with a remote workforce. A larger remote workforce can even act as an unintentional DDoS attack, simply because more users are trying to access services at the same time. To handle these possibilities, and ensure you are protected against DDoS attacks, have increased bandwidth allocations ready, temporarily disable unused services to allow for more bandwidth, and discourage your employees from streaming videos, music or other services through the VPN.

organizations and companies like Microsoft, Google and telecom companies.”

Nevertheless, a recent CIS survey found that 61 percent of security and IT leaders are concerned about an increase in cyberattacks targeting their employees working at home. “Whenever there is any disruption in the environment, there is a corresponding increase in attacks,” Gilligan said. “Having been a CIO, I am a little less comfortable when the employees pick up their laptops and are working from home because I have less control over the equipment they are using. When employees worked all within the same physical confines, there was a boundary around them, so the organization could fend off attacks. Now the boundary is in lots of people’s homes. It is a different technical issue. Over the next six months, CIS is going to focus on putting more emphasis on endpoint protection rather than boundary protection, and I think that is where the industry is going as well. For state and local government, the challenge is that the solutions have to be inexpensive, because the budgets are going to take a hit from the pandemic.”

In King County, Wash., CIO Tanya Hannah oversaw sending home approximately 5,500 of the county’s 15,000 employees in early March and is prepared to support them for the long haul. “We are not coming back to the office until at least January 2021,” she said. The county’s penetration of laptops or

tablets was at about 85 percent, and a number of workers have county-issued mobile phones, so from that perspective they were well prepared, but she does have heightened security concerns.

“Now you have endpoints all over the place,” Hannah said. “Individuals could be using unsecured networks, so I think the challenges around cyber and privacy and trying to understand your risk is even greater with remote employees.” It gets exacerbated depending on what kinds of tools you have and the work you are doing, she adds. For instance, users dealing with HIPAA privacy rules and protected health information must be sure not to use unsecure applications or communications tools without encryption.

When she became CIO two years ago, the county increased spending on cybersecurity by approximately 35 percent. “We are using Microsoft ADP and their information protection tools,” Hannah said. “The threats are always changing and we have legacy applications. In recent years we have seen an increasing number of attacks on state and local, and even federal entities. We probably don’t spend enough of what is required.”

WORKING FROM WALMART

Washington CIO Jim Weaver says that as much as his office thought it was prepared, patching and basic cyberhygiene issues arose. “Instead of having those internal endpoints and the normal way



we distributed those security patches, we now had to do that in an external fashion and in a way that does not cripple the capacity of our firewalls or VPN,” he said. “We try to do it during non-peak hours and have our users keep devices connected overnight to allow for downloading of those patches. We had to coordinate timing of those patches with agencies, so we weren’t having gigabytes pushed out at the same time across a multiplicity of agencies.”

Weaver says the readiness to work remotely in Washington state varied from agency to agency. Some were forward-thinking and had enough laptops for employees; other agencies did not have laptops and employees took their desktop PCs home and are leveraging virtual desktop infrastructure (VDI). In some cases employees are using their own devices and connecting in through the VPN into a VDI-type situation.

In addition, some employees in remote parts of the state have broadband connectivity issues. “In my own agency, I have one employee

who drives to a Walmart parking lot to connect,” Weaver said. “I love her dedication, but that is not the right answer. We are starting to enable workers like that to come back into the office. I don’t want somebody driving to Walmart to work.”

There are other management challenges around having a decentralized IT organization, he says. “In many cases we were all solving the same problem a multiplicity of times,” he added, “so we set up daily calls with IT leaders to issue guidance and best practices and to ask what we were doing that might be impacting them.” That was well received, he says, and five months into operating in this model, they are still holding those online meetings three times per week for 30 minutes.

IMPORTANCE OF PATCHING

Both Gilligan and Weatherford stress the importance of continuing to patch and monitor antivirus software during the pandemic. “Failing to keep up with patching during an emergency is short-term thinking that could have really long-term implications,” Weatherford said. “I consider patching and updating part of normal operations, and most security teams do as well. If you are not patching, you are leaving gaping holes.”

King County’s Hannah says there is no way her organization would pause its patching work. “That would be a big mistake,” she noted. “You have to think about all these legacy systems and the vulnerabilities with them.”


Patching was also initially an issue for the state of New Hampshire when it sent its employees home with their desktop computers in March. “When employees were in our offices, the network resources were more robust,” said New Hampshire Information Technology Department Commissioner Denis Goulet. “We had to make changes to the patching infrastructure so we could patch directly over the Internet rather than through the VPN. That was a challenge at first and we got a little behind on patching. We caught up after we moved our Microsoft patching off the VPN. We also did that with our trusted conference solutions like Webex so we didn’t have to go through the VPN for those.”

“Organizations that had a fairly robust telework program had the knowledge of what their technical approach would be to provide the connectivity and security. What they did not have was the capacity.”

Because it didn’t have laptops for its employees and didn’t want them to use their personal devices, New Hampshire encrypted the work desktops, purchased Wi-Fi cards for them and helped employees set them up at home. “We quickly upgraded our remote access infrastructure because like everybody else we had the ability to support many fewer connections than we anticipated connecting,” Goulet said. About 11,500 state employees use computers in New Hampshire, but before

the pandemic, remote access to the network topped out at 600, according to Goulet. “We are now doing 10 times that every day. It was a big change.”

Goulet said the fact that IT is centralized in New Hampshire made the switch to home easier. “The benefit is we had one remote access solution and one technology stack that went on the computers,” he explained.

The experience of the pandemic will require looking at cybersecurity and compliance through a different lens, Goulet noted. “We have to focus on it more in the remote context,” he said, adding that it may lead to business process transformation. As an example, he says, many employees felt they had to be able to print at home because they did in the office. “They thought they had to transfer that business process to home. For instance, in my department I have to sign off on all large purchases. Well, that was largely a manual process before we moved offsite. But now I am not going to print those out, sign them and send them back to somebody, so we went to a full electronic signature process. It is a lot faster and better.” 

draths@mac.com

29k
Washington state went from fewer than 3,000 users to 29,000 concurrent users of its virtual private network overnight.



INNOVATION IN GOVERNMENT®

Best of What's New in Cybersecurity

*Adapting to massive changes in the
risk landscape.*

- 2 Intro: An Inflection Point for Cybersecurity
- 4 Time to Reevaluate Security Practices
- 6 Building Resilience through Digital Risk Management
- 8 Confronting a New Threat Ecosystem
- 10 Remote Work Is Here to Stay
- 12 Addressing Evolving Application Threats
- 14 Taking Threat Detection and Response to the Next Level
- 16 Six Ways to Enhance Cybersecurity in a Post-Pandemic World

An Inflection Point for Cybersecurity

Now is the time to reassess security policies and strategies.

For security professionals, the COVID-19 pandemic represents something of a perfect storm.

First, the risk landscape exploded in a matter of days. State and local agencies — many with little telework experience or established policies — rapidly sent thousands of employees home to work remotely. Due to equipment shortages, these workers often used poorly secured personal devices and home networks to continue delivering vital government services. To connect remote employees to enterprise resources, agencies expanded their use of virtual private networks, increasing the chances of inappropriate network access or theft of access credentials.

The urgency of responding to the pandemic also pushed government organizations toward cloud-based solutions that could be quickly deployed to support remote meetings and collaboration, handle spiking unemployment claims, collect and analyze virus-related data, and provide other important functions. But, again, many of the agencies adopting emergency cloud solutions had little experience with the nuances of cloud security.

The bad guys, of course, weren't sitting on their hands. Sensing opportunity, hackers quickly shifted to COVID-related phishing schemes — impersonating agency leadership,

health officials and other authority figures to play on users' fears and anxieties.

Midyear reports from several security providers confirmed an alarming rise in cyberattack activity. Skybox Security found ransomware attacks had grown by 72 percent during the first half of 2020.¹ And Check Point Security said COVID-themed phishing attacks jumped from 5,000 per week in February to 200,000 a week in late April.²

Regaining Security Focus

As all this happened, security personnel and resources were stretched exceedingly thin. Many security teams were redeployed from operational tasks to urgent projects such as standing up new online services to help citizens apply for unemployment insurance benefits and other safety net programs.

"There was an awful lot of shifting of resources, which I think really depleted the energy of security teams," says Deb Snyder, who was CISO for New York State until January of this year. "COVID didn't completely change the game. Instead, it expanded the preexisting threat surface exponentially at a time when we were already dealing with significant risk."

Snyder and other security professionals say now is the time to reevaluate security tools, processes and strategies in light of these massive COVID-driven changes. Immediate steps include understanding and addressing situations where users may be storing sensitive data on insecure home computing devices, as well as dialing back remote access privileges to reduce the risk of inappropriate access or stolen user credentials.

"We know we deployed solutions without normal security planning considerations and took steps to get things up and running that were risky," Snyder says. "So, take steps now to review and strengthen security controls."

Moving Forward

Over the longer term, agencies must develop better monitoring capabilities that help them spot threat activity and potentially risky user behaviors. Most government agencies don't have the visibility they need into network traffic patterns and user habits. With many agencies planning to continue remote work options and expand digital services post-pandemic, gaining these capabilities is crucial for securing a new way of operating.

"Without this sort of visibility, you're flying blind — you can't make informed decisions,"



says Snyder. “In this new reality of virtual work and workplaces, we really need to study system activity and network traffic to develop a baseline. Then we can act flexibly and with agility when we see changes.”

Government organizations also must increase their sophistication around securing cloud services. Cloud solutions aren’t necessarily secure out of the box, she says. Agencies need to understand the security capabilities of cloud providers, as well as their own responsibilities around data protection and security configurations for cloud-based tools. And as governments rely more heavily on cloud, they’ll need to invest in cloud access broker services to manage and enforce security policies across multiple clouds.

Automation is the Answer

Finally, smart automation will be crucial to augment overwhelmed security staffs as they contend with a greatly expanded threat surface and cyber attacks that are growing more numerous and sophisticated.

Movement toward implementing smarter cybersecurity tools already is underway, according to the Center for Digital Government’s annual Digital Cities and Counties surveys. Fifty-eight percent of cities and 69 percent of counties responding to the 2019 surveys said they already use some form of artificial intelligence (AI) for cybersecurity. Another 37 percent of cities and 26 percent of counties said they plan to implement AI-powered cybersecurity tools in the future.

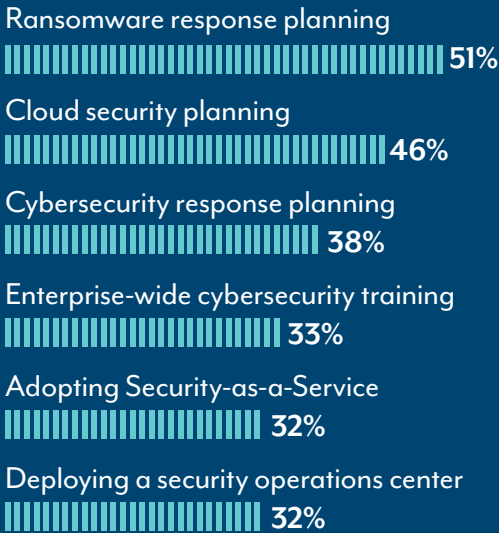
But Snyder argues more work needs to be done around automating government’s response to cyber threats.

“I believe this crisis is really a wake-up call for so many organizations that haven’t embraced the benefits of AI and automation tools that detect and process threat intelligence,” Snyder says. “Security teams need effective tools that reduce the noise, increase efficiency and apply contextualized threat information. In this environment, we need to automate threat detection and incident response as much as possible.”

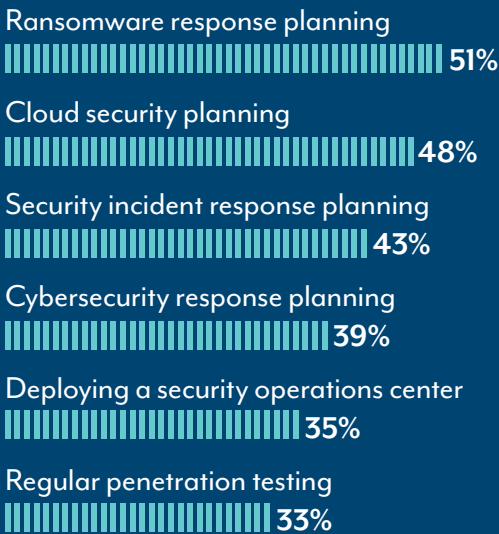
¹COVID-19 pandemic sparks 72% ransomware growth, mobile vulnerabilities grow 50%. *Security Magazine*. <https://www.securitymagazine.com/articles/92886-covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50>

²COVID-19 Has Given Hackers an Unfair Advantage, Experts Say. Govtech.com. <https://www.govtech.com/security/COVID-19-Has-Given-Hackers-an-Unfair-Advantage-Experts-Say.html>

Cybersecurity Priorities for Cities



Cybersecurity Priorities for Counties



Source: 2019 Digital Cities and Counties Surveys

Time to Reevaluate Security Practices



State and local government leaders pushed themselves to the limit to keep government operations afloat in the initial phase of the pandemic.

Sumit Sehgal, Chief Technology Strategist, U.S., for McAfee shares insights to help organizations prepare for the future.

Organizations moved quickly to adapt to the pandemic, adopting cloud-based technology and new approaches.

Now what?

After pivoting quickly to keep government functioning, agencies are reevaluating. They recognize the way they typically provide citizen services may be too expensive to run full native cloud and that cloud-enabled doesn't always equal lower costs. Labor is another consideration. Running a cloud-based Microsoft Azure instance for your data center is different than running a hardware-based instance. Staff might not even know what that looks like from a security operations perspective. At the macro level, the challenge isn't so much the technology or moving stuff to the cloud. It's looking at long-term costs, labor and expertise to determine whether the organization can afford to keep everything it has done in recent months running the way it is.

What threats and vulnerabilities currently dominate the state and local government landscape?

The threat issues with security hygiene and complex, aging IT infrastructures are largely the same as pre-pandemic, but the attack vectors have changed. Instead of attacks against the infrastructure, we see an increase in very sophisticated email and

voice phishing scams that are designed to harvest information. On the vulnerability side, organizations have moved complex IT infrastructure to the cloud without accounting very well for security. We're seeing a shift from traditional operating system and application vulnerabilities to cloud-related vulnerabilities. That's everything from identity to the way cloud applications are run to how access and attribution of data security occurs as it travels through that whole continuum.

How has the surge in remote work impacted cloud security?

It has forced people to look at security from the lens of cloud application security, data integration and interoperability. Besides confidentiality, they're investigating how they can frame their security architecture so that it's cloud native to begin with and applies things like identity management, privilege management and user behavior monitoring to the cloud world. The rapid shift to third-party security providers and cloud providers has caused some growing pains in terms of how people remotely access their applications, VPN or cloud. In some cases, applications that were running in the cloud don't work at scale from a security perspective. So, organizations must change their approach to protect citizen information.

How can organizations make the most of tools and approaches such as zero-trust architecture, adaptive security and user behavior analytics?

The bottom line is that even the best tool or approach will not fix a bad process. All the zero-trust technology in the world won't work if your identity and asset management processes give the system bad data. To fully utilize these approaches, agencies must look

honestly at their processes and what they're doing regarding hygiene, security practices and things like that. Organizations also need to determine what they want from these tools, whether the tools align with their best practices and overall security approach, and how these tools impact the way they perform existing processes.

How can state and local governments simplify regulatory compliance and governance related to data privacy?

I see the potential for security and privacy practitioners to come together to create a standardized language that bridges security and privacy — similar to MS-ISAC, the Multi-State Information Sharing and Analysis Center, where everybody uses the same language when a security incident occurs. Ideally, security and privacy teams would watch for — and notify their counterparts of — unusual behavior or incidents that may impact the other's domain. We need something like this because cloud applications and the future we're headed into don't provide the same visibility.

What strategies can organizations employ to move forward with modernization while addressing the urgencies of the pandemic?

Standards-based approaches such as the NIST Cybersecurity Framework or the MITRE ATT&CK framework can help on both the security side and the application architecture side. Multiple agencies can create a structure that lets them design services and other things in the same manner. When done appropriately, that eases the burden of customization and enables organizations to scale or improve functionality and the user experience for things like security and analytics applications, as well as infrastructure management.

Concerned with where your data goes in the cloud?

**Gain visibility and control
to protect data everywhere**

- Visibility
- Control
- Compliance
- Data Protection
- Threat Prevention
- Cloud-Native

MVISION Unified Cloud Edge protects data from device to cloud and prevents cloud-native threats that are invisible to the network. This creates a secure environment for the adoption of cloud services, enabling cloud access from any device and allowing ultimate productivity.

Learn more at www.mcafee.com/unifiedcloudege



Building Resilience through Digital Risk Management



*As organizations undergo digital transformation and increasingly depend on internet-connected devices, disruption occurs. With that disruption comes risk. **Steve Schmalz**, Field CTO for RSA's Federal Group, discusses digital risk management and key components of resilience.*

What's the biggest challenge of protecting an ever-expanding perimeter?

Visibility. That means knowing what's happening on your networks and who is doing what — regardless of the device or service being used. It means being able to monitor endpoints, keep track of logs, look for potential problems, ensure all policies are enforced and so on. The amount of real estate to be monitored keeps expanding. It's not just the number of things you have to look at, but the complexity of those new devices and the new ways of doing business.

Please discuss an integrated risk management approach to cybersecurity.

A core component of the NIST Cybersecurity Framework, which aligns with RSA's risk management approach, is visibility. You have to understand your cybersecurity posture — what controls you have in place and what threats are out there. Based on that analysis, you implement the ability to monitor that continuing state and identify the real threats to your organization. Some things are extremely important to protect and some aren't. As you identify threats and their targets, you can start calculating the risks and putting dollar amounts on them. Then you develop a plan

for modifying your existing controls and processes to meet those evolving threats and to reduce those risks. It's a continuous process of assessment and refinement that should be integrated across the entire organization, not just within cybersecurity.

What can cybersecurity leaders do to adapt their security operations centers (SOCs) to the changing landscape?

SOCs typically have monitored network traffic and endpoints. They are at the center of that visibility process we're talking about. It's critical that the modern SOC extends monitoring functionality out to the Internet of Things as well as cloud-based resources. Besides monitoring all of that real estate, the SOC itself should take advantage of any cloud infrastructure that is in place. As the COVID-19 pandemic evolves, SOC analysts must be able to access their tools and dig into incidents from a secure connection at home as easily as when they sit in a SOC. Without that, it's going to be hard to maintain a sound cybersecurity posture.

As multifactor authentication becomes a more important tool for workforce transformation, what do organizations need to consider?

Flexibility and usability are at the top of the list. It's important that you can provide the type of authentication that's most appropriate for the individual and the resources they're attempting to access. In addition, if authentication isn't simple to use, people will find a way to get around it. Workers often become your worst threat because even though their intentions are good, their hack can open up holes for malicious actors to follow.

How can organizations build resilience into their security strategies so they are best prepared for any disruption?

Planning ahead for how you'll address problems and putting contingency plans down on paper is an important risk management process. Organizations need good security workflows and a way to aggregate information about their networks, valuable resources and who is doing what in the organization. Then they need plans for triaging the most devastating risks first. It's impossible to think of every threat, but organizations can start by considering what types of incidents could interfere with critical capabilities and prevent them from completing their mission. With that information, organizations can put together contingency plans, even when they're not quite sure what potential threat might bring about that particular loss of functionality.

What are some unexpected consequences of the pandemic on security and risk management?

Initially, organizations were in a rush to find the appropriate way to extend the use of their existing authentication or access management technology to SOC staff and other people working from home. They got that low-hanging fruit to make things more secure, but now they're struggling to manage their SOC, do governance and keep security workflows in place. It's also more difficult to do some everyday security jobs. In terms of innovation, the pandemic accelerated the use of the cell phone as an authenticator. A lot of people were doing this already, but the pandemic certainly pushed this wave of mobile-centric access to sensitive resources.

Detect and respond to threats **your way**



With complete visibility, analytics and automated response

Tap into your full potential as a threat hunter with RSA NetWitness® Platform. Our industry-leading evolved SIEM and threat defense platform gives you all the capabilities you need to detect virtually any threat anywhere: end-to-end visibility across your entire IT infrastructure, advanced behavioral analytics and automated response. **Be the threat hunter you're meant to be.**

Go ahead.
Be you.

RSA

RSA
NETWITNESS®
PLATFORM

Learn more at rsa.com/publicsector

Confronting a New Threat Ecosystem



Jeremy Kennelly, manager of Mandiant Threat Intelligence for FireEye, talks about how government agencies can guard against new risks created by the massive shift to remote work.

What new vulnerabilities and attack vectors are emerging from the pandemic?

The pandemic significantly shifted the flow of network traffic within many organizations as their employees migrated to full-time use of VPN infrastructure instead of devices located within physically secure corporate buildings. This has implications for security monitoring, but also opens more avenues for employees to lose access to corporate assets. Beyond this, employees working from home or using personal devices may put sensitive corporate documents or systems at a higher risk.

How should organizations change their security approach to defend against these vulnerabilities?

This is a complex problem that requires defenders to understand how user computing habits have changed, and how those habits are likely to evolve in response to shifting work situations. Defenders must develop a baseline for what legitimate network traffic and application usage looks like — particularly now that many users are accessing systems differently or have adopted different work schedules — and they must use these insights to sharpen their ability to detect anomalous activity. Beyond this, strict network segmentation and the deployment of two-factor authentication on critical systems continue to be important security controls, even more so now that a higher proportion of employees may be working from home.

What can organizations do to filter the noise that comes from their security tools and focus on threats that matter?

Understanding your organization and where it fits into the threat ecosystem is probably among the most effective ways to grapple with this issue. In a purely introspective sense, it's important to understand your corporate network — you need to know which information assets, individuals and applications are likely to be targeted by attackers and then place a higher priority on security alerts and advisories that impact them. Organizations also can narrow the focus of their detection and threat-hunting efforts by understanding the specific attackers that are known to be interested in their industry and geography, and use this knowledge as a preliminary guide.

Even if organizations are getting high-quality, timely threat intelligence from threat feeds and services, how do they integrate that in a way that adds value and supports decision-making?

Organizations need to understand each of their threat intelligence sources contextually: How are they produced, what data sources were used to produce them and how are they intended to be used. This information helps you distinguish between threat intelligence sources that provide little operational or strategic value and those that describe impactful threat activity about which your organization might need to make serious decisions. If you are working with written intelligence products rather than simply indicator feeds, it's important to take the time to assess the implications of the intelligence and to think about how your organization can protect itself from the described threats. This can help you deploy controls in anticipation of credible future threats.

Many organizations use managed services to address in-house staffing and skills shortages. What advice do you have for organizations seeking to leverage additional support this way?

There are many factors that should go into an organization's decision to engage outside security experts. One of the first steps an organization should take is to fully assess and document exactly the type of support you need. This will be critical when you approach trusted security partners for help. The better your requirements, the better they can be met. Also, it's important to work with organizations that act as force multipliers and aren't simply providing head count. Ideally you can leverage a partner's historical information and expertise.

Please discuss security validation and why it should be a pillar of an organization's security strategy.

Security professionals have long been designing and deploying complex security architectures intended to protect their organizations against highly capable and evolving cyber threats. A common approach to validating the value of these security investments has been periodic vulnerability scanning or penetration testing — but both processes can only test for a subset of attack scenarios and may fail to emulate real intrusion activity. Using a security validation platform — particularly one that's designed to exactly mimic known attacker tactics, techniques and procedures — can provide organizations with an unprecedented level of visibility into the effectiveness of their controls. This can guide decisions around future security infrastructure investments, test the effectiveness of detection and response processes, and help organizations identify security blind spots.



BREACHES ARE INEVITABLE. BEING A HEADLINE ISN'T.

Secure your systems and manage your message with world-renown incident response services and cyber threat intelligence.

FireEye.com



Remote Work Is Here to Stay



MK Palmore, VP and Field CSO for Palo Alto Networks, discusses the threat landscape created by remote work and strategies for securing remote access now and in the future.

What types of adversarial activities warrant closer attention in government enterprises?

The threat landscape is extensive, and adversaries continue to be fairly successful in their attacks. Financially motivated criminals are responsible for the vast majority of intrusions; however, insider threats warrant extra focus because the number of successful insider attempts is increasing. The last thing you want is someone walking out with the keys to the kingdom and you not knowing it. In addition, credentials are a prime target of malicious activity. With proper credentials an adversary can gain access to an environment, evaluate the data there and then successfully exfiltrate valuable information.

How has remote work impacted cybersecurity?

Government employees went from operating with business-approved devices from business-approved locations through business-provided pipes to mostly remote access. That introduced a whole new set of problems in terms of securely accessing the business information they need on a day-to-day basis. In addition, the number of attack vectors grew exponentially. Most organizations adopted secure remote access solutions so their users could connect safely and to maintain operability. Now that organizations realize they can be

productive remotely, I think they'll maintain some portion of their secure remote access capability even when they return to more "normal" operations. With secure remote access, there's no limit to how they might be able to respond with agility to future challenges.

What overall strategy allows organizations to secure users, data, applications and other resources regardless of their location?

The secure access service edge (SASE) model lets organizations apply security no matter where their users, applications or services are located. It dictates that enterprise users need access to a variety of business resources and information. To maintain business operability and meet their missions, enterprises must figure out how to do that securely. Secure remote access — which includes secure connectivity, identity access management, access control, continuous validation of secure connectivity throughout an interaction and more — will be the mark of a functioning cybersecurity apparatus moving forward. The other component is being able to scale cybersecurity talent and resources to accommodate growth.

What challenges go along with using cloud-based security services?

We find the people responsible for configurations make the same mistakes in cloud environments that they make in on-premises environments. The cloud doesn't alleviate network defense of security; it makes it more difficult. With the shared security model, organizations must understand the responsibilities of the cloud provider and their own responsibilities to protect enterprise data. Understanding and managing those gaps

requires government security teams to get even more involved in terms of identifying security tools that might be helpful. And then, even though cloud providers offer cloud-native tools to help with these things, enterprises often need help with getting tools that are easily accessible, scalable and solve their business problems.

How can AI and machine learning help level the playing field against adversaries?

Given the tools available to adversaries, the frequency of automated attacks and the increasing complexity of our environments, there's no way to keep pace with the adversarial environment if AI and machine learning aren't baked into your appliances. With AI and ML, baseline data collection and rudimentary activities — for example, moving from one application to the next in order to gather information — can get done automatically; so by the time the data is teed up in front of a human, all of that time-intensive work has been boiled down to a decision that needs to be made: Do I need to investigate this further, escalate it or dismiss it?

What has the pandemic taught us about cybersecurity?

It's taught us that cybersecurity must be a component of existing technology investments and a baked-in additive to the technology advances that we hope to adopt in the future. Without security, those technology advances will always represent a potential vulnerability that adversaries will try to exploit. The pandemic also highlighted our reliance on digital information both for business reasons and as consumers. Folks absolutely must figure out a way to access that information securely as they plan their roadmaps for digital transformation.

Securely Connect and Scale Remote Workforces

With **Prisma™ Access**



paloalto[®]
NETWORKS



PRISMA[™]
BY PALO ALTO NETWORKS

paloaltonetworks.com/remote-security

Addressing Evolving Application Threats



Raymond Pompon,
Director of F5 Labs,
discusses the complexities of
protecting componentized
applications and digital
services and suggests ways
to stay ahead of today's
application threats.

How has application threat management become more challenging?

In the past, an organization would write a monolithic app, and a small group of programmers would write code and tie it to a database. Now, with the shift to more componentized applications, multiple libraries and tiers may be added, different teams — with different approaches — will work on different components, and it's all glued together with APIs. All these moving parts create more insertion points for an attack and more things that can fail in unexpected ways. In addition, with the dispersal of apps across the organization, it's much more difficult to fully understand and control an application's security and operations.

What gaps exist between perceptions of application security and actual security?

There are a number. People assume if they've outsourced something, security is included. That's not always true. On the development side, organizations may put together a series of components that are secure and stable on their own, but when assembled into an app, they create new vulnerabilities. Also, different components may have varying levels of security, and the weakest link in the chain creates an opening for attack.

How have digital citizen services increased risk?

With the growth in digital services, many organizations are using the same sets of apps and libraries across the entire organization. Different departments use them in different ways, but they all tie together because they use the same user ID for log in. The user can use this login ID to access all the organization's digital services. While that's convenient for the user and seems secure, what happens if a bad actor compromises the ID on a lower-value service with weaker security requirements? Now that bad actor is in the system with a legitimate ID, and they can move sideways to potentially gain access to more valuable assets.

How can organizations ensure that only the right users access applications?

No matter who comes through the door, you have to verify everything about them and that verification must follow them through the system. Organizations can't just check a user's ID, give them a password and be done with it. It's a continuous process of authentication. When a user attempts to move from one part of a system to another — for example, if a person applies for unemployment insurance, but they logged in through a parking application — the organization may want to require additional authentication or scrutinize the user more deeply. Access is not all or nothing. There's a granular dial that you're turning up and down based on what a user is doing within the system.

What are adjuvants and how can they help cybersecurity teams be more effective?

In medicine, an adjuvant is a substance that enhances the effectiveness of the

main drug. In cybersecurity, adjuvants are people outside the security organization — they might be power users or have a special interest in security — who help fill gaps, act as liaisons, provide additional perspective and more. For example, adjuvants can share their knowledge of the organization's culture and processes to bring new cybersecurity hires up to speed more quickly. They can help roll out new concepts and policies. They can act as security evangelists and provide first-level support to end users within their group. And of course, they're also your recruiting pipeline. You can eventually bring them into your group when it's time to grow.

How can organizations "make the most" of a security incident?

Whether a security incident turns out to be a near miss or an actual breach, it provides an opportunity to learn how controls are failing and to find ways to fix them. Turning incidents into opportunities requires organizations to move away from blame. Often, the process is at fault, not the user. So it's about asking, in a very neutral way, "How do we fix that problem so we can react more effectively the next time?" You can actually get a lot of support when you say, "This is what happened; we identified these processes that could be tighter; and we'd like to change them in this way." And it doesn't always mean having to spend money. Sometimes it's just doing additional training or tweaking a configuration somewhere.



Cloud-native SaaS solutions for enhanced application delivery, security, and insight.



Robust Security

Your applications are automatically protected from multiple attack vectors with dynamic security options.



Cost-effective

Consumption-based pricing allows you to only pay for what you use.



Simplicity and speed

Easily provision and configure services within a few clicks.



Intuitive Interfaces

Manage services in an intuitive user interface or automate everything with declarative APIs.



Real-time visibility and analytics

Track performance, usage and billing with detailed reports and visualization tools.



Experience and support

Delivering 99.9 service guarantees with premium 24x7 support from experts with over 20 years of experience.

Learn more at: www.f5.com/products/ways-to-deploy/cloud-services

Taking Threat Detection and Response to the Next Level



*An expanding attack surface, massive volumes of event data and aggressive adversaries are stretching threat detection and response capabilities. **Barry Hensley**, chief threat intelligence officer for Secureworks, hones in on strategies to scale security initiatives.*

How has the pandemic changed risk management for state and local governments?

A lot of the change comes from having to support a large remote workforce. Regular system maintenance tasks like vulnerability scanning and software patching have changed dramatically. In the past, patching technologies assumed that systems were physically on the same network or would ultimately be connected via a virtual private network. As users' machines move off the network, they get scanned less often, if at all. Remote work and increasing reliance on SaaS have really highlighted the need for zero-trust networks, where services require not only a trusted user but also protection of the data viewed and saved from these services.

What are the keys to effective threat detection and response?

The first key is having sufficiently accurate detections so the security team doesn't develop alert fatigue from chasing false positives. This capability must be coupled with comprehensive visibility into the environments and data sets the organization is defending. Once the team can detect threats effectively, knowing how to respond in various threat scenarios is also critical. Incident response playbooks, reinforced with table-top exercises, are a great way to ensure teams understand

their roles, the actions they should take and who they should communicate with throughout the process. Experienced incident response teams can reduce the overall time of an incident; get the business up and running again faster; and advise on remediation of architecture, policies and controls to prevent future incidents.

How can machine learning (ML) complemented by human intelligence help organizations better manage threats?

No matter how good an ML algorithm is, the goal is never to replace humans. It's to augment our top-tier security analysts with the best that machine learning can provide. ML improves operational efficiency through various models. One, it greatly improves the scale of data you can process and the likelihood of greater consistency than a team of humans can reasonably produce. This often results in a reduction of false positives and improves detection by sifting through vast amounts of data and detecting known patterns of malicious behaviors. Two, ML can greatly help with security analyst workflow augmentation and automation by optimizing complex tasks. For example, it can reduce the number of alerts the Security Operations Center must process by removing easy-to-identify benign traffic coming from various security controls. Lastly, ML can learn from past human validated actions and then automate those decisions for future similar alerts.

Is it realistic for today's state or local government security organizations to retain their own internal threat research staff?

The costs associated with highly skilled threat researchers and the advanced tools they leverage are often beyond a state or local government's budget. A good compromise

is to partner with a Managed Security Service Provider (MSSP) that can leverage its economies of scale and infuse very deep and robust threat intelligence into its detection and response platforms. This allows organizations to focus on high-severity risks versus day-to-day incident investigation.

How can organizations optimize the effectiveness of managed security services?

It's important to ensure that the onsite team has workflows in place to consume the outputs from the MSSP. Using the case of managed threat detection services, for example, if the organization can't digest, draw insights from and act on what the MSSP detects, the value is lost. Second, the organization needs a dedicated direct liaison between the MSSP and the in-house team tasked with remediating threats and vulnerabilities. This improves responsiveness and accountability on both sides, and ensures that alerts are properly tracked from discovery to complete remediation.

You've led top cybersecurity organizations in the military and the private sector. What advice do you have for CISOs and other cybersecurity professionals as they lead through the pandemic and into the future?

As leaders, it's our job to ensure our team members have the appropriate resources to do their jobs and maintain their peak effectiveness. Especially now, we have to focus on innovative ways to maintain team cohesion and improve communications. In addition, it's important to encourage team members to be cognizant of work-life balance, both in terms of delineating between work and personal time as well as not letting work and professionalism slip when they are out of a more formal environment.

We're Revolutionizing Cybersecurity.

Secureworks combines machine learning with human intelligence to detect faster, respond smarter, and predict and prevent more threats altogether.

4,100

Customers in
50+ Countries

300+

Expert Security
Analysts, Researchers
and Responders

20+

Years of Attack
and Threat Actor
Group Data

Request a demo. Learn more at secureworks.com

Secureworks[®]

ISSUES TO WATCH

Deborah Snyder joined the New York State Office of Information Technology Services as deputy CISO in 2012, a position she held until being promoted to the state's top cybersecurity job in June 2017. As New York State's CISO, Snyder was responsible for setting policies for data security, vulnerability monitoring and cyber hygiene across one of the biggest state government organizations in the country. She retired from her state position in November 2019.

Snyder recently shared her thoughts on key steps state and local government agencies can take to improve cybersecurity in a post-pandemic environment.

1 Focus on immediate, actionable efforts to bolster security and assure resiliency. First, secure critical operational needs, including the mass shift to telecommuting and remote access. Then review and tighten security controls.

"Organizations that rushed to get people connected and working have told me security was relaxed or sidelined during that time," says Snyder. "Now is the time to revisit the security of those solutions. Go back and put the right controls in place and affirm you are protecting sensitive information in all places."

2 Reexamine and reevaluate. The technologies organizations put in place quickly during the pandemic might not be the technologies that will serve them best in the future.

"Look at your cyber strategy or strategic plans with new eyes. The lessons we learned from the pandemic response experience and challenges shouldn't be wasted. Ask tough questions about priorities and planned investments, and recalibrate those plans now to add value and address current and future risks and workplace realities," says Snyder.

3 Take advantage of new tools. The pandemic forced government leaders to think differently about how they work and how they secure their environments. Snyder recommends security leaders ask their teams and partners how



Deb Snyder: Six Ways to Enhance Cybersecurity in a Post-Pandemic World

to take advantage of new technologies to achieve long-term benefits and efficiencies, reduce operational costs and improve security.

"Think about the future workplace and focus on technologies that can improve security in that environment, including zero-trust strategies that restrict access or integrated solutions that enable better productivity," says Snyder. "Then, make sure you have essential end-to-end defensive measures in place. Automation is key. Leverage technologies that enable automated blocking, detection and response, and address advanced threats."

4 Consider new partnerships. Don't automatically rely on your old allies, recommends Snyder. Greater creativity and innovation are two positive outcomes of the pandemic. Look for forward-thinking partnerships that can help you address new challenges and gaps.

5 Plan with the new normal in mind. Consider remote work scenarios as the expected norm going forward. The workforce and the workplace may never go back to what they were. Most

organizations don't have contingency plans that fully reflect critical operational processes, requirements and alternatives. Examine your organization's business continuity and disaster recovery plans to make sure they work and are scalable and sustainable in this new environment.

"That includes everything from updating emergency contacts to testing realistic scenarios so you can understand where even the best thought-out plans might run aground," says Snyder.

6 Reconsider cyber insurance. Cyber insurance is designed to protect organizations from risk and is worth consideration. But before securing a cyber insurance policy, think carefully and holistically about your coverage and your organization's needs.

"No one size fits all," says Snyder. "All cyber insurance policies have deductibles, exclusions and exemptions. Be cautious and make sure your cyber insurance policy addresses your organizations' specific needs and that it will support you during a network security incident, a data breach or a pandemic."

2020

SPREADING BEST PRACTICES & SPURRING INNOVATION IN CHALLENGING TIMES.

DIGITAL GOVERNMENT
SUMMITS ARE GOING
VIRTUAL!

government
technology

ATTEND/SPONSOR:
govtech.com/events

Arizona
Arkansas
Bay Area
California
Chicago
Colorado
Connecticut
Florida
Georgia
Hawaii
Illinois
Indiana
Iowa
Kansas
Kentucky
Los Angeles
Maine
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Nevada
New Jersey
New York
New York City
North Carolina
Ohio
Oklahoma
Oregon
Pennsylvania
Tennessee
Texas
Utah
Virginia (COVITS)
Washington
Wisconsin



SECURITY

Five state and local CISOs on what it takes to keep government safe in 2020.

BY PRISCILLA CHRISTOPHER



N PROFILE

RANSOMWARE ATTACKS. MALWARE ATTACKS. PHISHING ATTACKS. DDOS ATTACKS.

While cybersecurity has long been a top priority for government IT leaders, the last two years in particular have made clear that a concerted effort to protect government data is paramount.

With an ever-growing need to protect information assets and secure infrastructure, the role of the chief information security officer has never been more critical to the ongoing effectiveness of government agencies and departments.

Government Technology spoke with five such state and local government CISOs. Here, they share their cybersecurity backgrounds and insights on the field.

Shirley Erp

Austin, Texas

WHEN SHIRLEY ERP JOINED Austin as its security chief, she did so with a desire to protect and serve. “As for my current position of CISO for the city of Austin, this provides yet another opportunity to serve my community and motivates me to do my best at protecting the city against cyber-threats, securing confidential information and adding value by further maturing the city’s cybersecurity program,” she said.

Erp’s path into technology and cybersecurity was influenced by her father, who was in security intelligence for the U.S. Air Force. This, combined with her aptitude for math and science, led to the pursuit of her first degree in computer science. After graduating, Erp started her career as a mainframe systems programmer and gravitated toward computer networks. “Later, when organizations started to adopt

the Internet for business transactions,” said Erp, “I had both the background and innate interest which allowed me to progress my career in cybersecurity.”

Having CISO experience in both the public and private sectors, she is well-poised to compare the two. “The role of the CISO is similar in that you must be both a business and technology leader,” Erp explained. “The difference for the public sector is it takes more time for change with legislative oversight, governance approvals, limited funding and budget cycles, as well as selection justifications and implementation coordination.”

Erp has only been with Austin since June 2020, but she has been doing something she enjoys: leading change to improve organizational security through priorities. One such project is the creation of an information security road map to further mature Austin’s cybersecurity program and capacities. “The road map,” Erp said, “will help guide the way for continuous improvement with planning initiatives that utilize the city of Austin’s established processes and budget cycles.”

While Erp enjoys serving her community, she’s well aware of the risks and challenges that come with digitization. “Attacks are getting more sophisticated, organizations are transforming to multi-cloud architectures, and the workforce is transitioning to remote work and bring-your-own-device — all of these things bring new challenges to the forefront,” Erp said. She believes that security must transform its protection of data as IT is transforming to meet tomorrow’s business needs.

Transformation to meet threats requires good CISO leadership. The ideal cybersecurity leader, according to Erp, “is a critical thinker who embraces the strategic vision, goals and objectives of the organization and builds relationships across the entity for improving security while balancing the business needs and customer service.”

Executives should not, however, only look to CISOs to improve security. “Security is not just a technology issue,” Erp said. “It is everyone’s responsibility, and it should be integrated into the organization’s culture and governance structure.”



Shannon Lawson

Phoenix

SHANNON LAWSON’S CAREER

began after college when he enlisted in the U.S. Navy, where he specialized in cryptology, which he says introduced him to “information and warfare.”

From there, he took on a variety of jobs with the Navy and National Security Agency, becoming a generalist in technology. He then left for the private sector, but after a few years returned to the Navy.

Years later, he became the inaugural CISO for Alaska. “I wanted a change from what I was doing and to be more hands-on, directly controlling an organization’s security program,” Lawson said.

In 2019, when his time with Alaska ended, Lawson transitioned to local work, taking on the role of Phoenix CISO. “Phoenix is the fifth-largest city, serving 1.7 million residents,” he said. “And we provide a wide variety of critical services to them. Water, for example, is a critical service.”

He views this role as a unique opportunity “because you have real issues that have to be solved right now,” Lawson explained. “What I like most is the wide variety of challenges. Here at the city, my team is really doing transformational change.” He credits city leadership for their ability to get things done.



Still, being a government CISO is not without its challenges. “The private sector,” he said, “is really good at eliminating liabilities and keeping assets that drive success. Culture, in the public sector, can be a liability.”

Lawson, however, has seen success in promoting a culture of security awareness in Phoenix. “For National Cybersecurity Awareness Month, approximately 15,000 employees completed training in 30 days,” he said.

For those interested in government cybersecurity leadership, Lawson notes the importance of a well-rounded background. First, “you need a resume that combines formal education and direct experience, as CISOs have now been accepted in the board room.” Next, formal certifications are key. “Not a lot,” Lawson cautioned, “but something to show you have passed a minimum standard of knowledge for a particular domain in security.” Finally, Lawson explained that “soft skills are just as important as hard skills.”

“Being CISO is a privilege, but it’s a long road there,” he said. “Plan properly. Be prepared to drink from a fire hose at the deep end of an empty pool. Communicate and enjoy the ride.”

David Allen

Georgia

DAVID ALLEN COMMISSIONED into the U.S. Army in 1995 after college. Upon completing his assignment, he returned to his home state of Georgia and worked in IT and project management roles for several years before joining the Georgia National Guard full time for nearly a decade.

During this time, Allen progressed professionally and held a few roles within the organization, including deputy chief information officer and a dual role of CIO and chief of cybersecurity.

Allen’s leadership experience in the Guard’s dual role specifically prepared him for his current cybersecurity position. “I was able to work on cybersecurity efforts



at the federal and state level, to include collaboration with my current organization. As a Guardsman, it also provided me the opportunity to learn crisis management skills that have benefited me greatly during incident response efforts,” he said.

Now CISO for the state, Allen reflected on his shift to state government from the military: “My whole career has been in service to my country, so it was a natural transition upon my military retirement,” he said. “I looked for an opportunity to continue to serve and found it at [the Georgia Technology Authority].”

Having some familiarity with GTA from his previous work, Allen took on the role with excitement in 2019, which remains over one year later.

However, Allen’s enthusiasm hasn’t clouded his ability to see the challenges of the CISO role. With an increasing number of cyberattacks and a mobile workforce due to COVID-19, he notes one significant challenge that CISOs are dealing with in this climate: “modifying the new normal, with things like working from home, and new technology to bring in so employees can safely operate.” This includes, Allen says, examining security in general.

Allen also acknowledges that to address recruitment and retention challenges, a leader should have an open mind when seeking cybersecurity talent. It will take different strengths

and different backgrounds, Allen explains, to fill available vacancies.

Such challenges indeed require effective CISO oversight. The ideal leader, according to Allen, should be strategic and operational; should have an appreciation for and an understanding of technology; and should be willing to gain new skills.

In all, since joining the state, he has seen progress on all fronts when it comes to cybersecurity priorities and initiatives, including workforce training and development and capabilities for incident response. “I’m really excited about where we’re trending in all things technology,” Allen said.

Stephanie Smith

Mecklenburg County, N.C.

WHEN STEPHANIE SMITH started her career years ago, she was aware of a gender gap that remains today: Women make up a small percentage of the U.S. technology and cybersecurity workforce — and an even smaller percentage hold leadership roles.

Smith was not deterred, however, from excelling in this male-dominated field. “It was a goal of mine, when I started 20 years ago, to get to that place of



leadership,” she said. Over the years, Smith indeed reached that place through roles at various public and private organizations, including CIO at a North Carolina health-care organization, and now CISO for Mecklenburg County, N.C.

“When the opportunity presented itself to serve Mecklenburg County, I was excited,” she said. “It’s a big role with a lot of responsibility, but the benefit of doing something meaningful is big for me.”

As county CISO, where she serves approximately 1 million residents, Smith has a responsibility to educate others, particularly fellow employees, about technology and security. “For me personally, it’s not just about the latest and greatest technology. It’s about helping people change their mindset about technology and using it securely,” she said. She also credits the team she’s built, who share her “passion for public service and technology.”

A top priority for Smith and her team has been transitioning employees to remote work effectively and securely due to COVID-19. She said they “purchased new equipment to be mobile, trained new employees and put technology in place to monitor and respond.”

The shift to remote work has been a priority amid the pandemic, but Smith remains attentive to other cybersecurity risks and challenges, like user behavior and education, regulatory compliance, business emails and phishing, and ransomware attacks. Local governments, she said, are particularly being targeted by ransomware demands, and “must step up to keep up.”

If Smith had to characterize the ideal cybersecurity leader in government, it would be someone who is passionate about service. “For the government specifically,” she said, “I think you have to have a passion for giving back to the community.” According to Smith, the ideal leader also has a strong background in compliance and an understanding of why rules and regulations matter in keeping data secure.

Moving forward, Smith would like to see more women in the field. “I encourage more females to take a look at cybersecurity, and those in STEM programs to continue their passion.”



Andy Hanks

Montana

WHEN ANDY HANKS DECIDED to find a position that would allow him to make a meaningful impact using his technical, security and business experience, he did not have his sights set on the public sector. That said, he has no regrets. “I was not specifically looking for a job in state government, but when I saw the state of Montana CISO job, I knew it was exactly what I wanted to do,” he said.

Hanks, who started programming at 13 years old, began as a mainframe programmer at IBM after earning a computer science degree. In this role, he worked in technology on the Y2K program.

But as he constantly saw “security from multiple domain perspectives and leadership levels,” he wanted to transition. After hearing from a hiring manager about cybersecurity, its complexity and its growing importance, he made the move — and advanced professionally.

What attracted Hanks to his current role was the state’s mission: “to protect citizen’s data.”

“As a state employee,” Hanks said, “my customer is my family, my friends and my neighbors. I only need to look around at the people I see in the restaurants, bars and parks to be reminded of the importance of our mission.”

While he enjoys the meaningful contribution he makes to his state and its citizens, he remains knowledgeable about present and future challenges that can affect it. “Cybercriminals ransoming our citizens’ data, nation-states attacking our elections, unfunded mandates stretching tight budgets and emerging technology outpacing our ability to protect,” he said. However, the biggest threat, he explains, is the lack of talent. “The United States currently has a shortage of 500,000 cybersecurity workers,” Hanks noted. “Educating and hiring the next generation of cybersecurity workers should be a priority at the local, state and national levels.”

It is a top priority for Hanks and his team. “In Montana, we are focused on multiple initiatives to retain and recruit highly skilled cybersecurity staff, to increase diversity so we can match the diverse perspectives of our attackers and approach complex problems from multiple viewpoints, to build a workforce talent pipeline by partnering with K-12, college and university education institutions, the military, and the nonsecurity workforce looking to retrain into cybersecurity.”

Altogether, public-sector CISOs must have a background of expertise and experience to handle such challenges. “CISOs don’t need to be experts in business and security and technology,” Hanks said. “They just need to be experts in balancing the perspectives of all three.” 

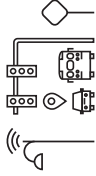
christopher.priscilla@yahoo.com

Building a platform for smarter government

Citizens, business owners and internal employees have higher expectations for state and local governments than ever before, but government organizations can struggle to meet them. State and local agencies need smarter technology and operations to be as productive, efficient and innovative as possible.

Verizon Wireless solutions work together to establish a smart government ecosystem which connects infrastructure, people and intelligence. And Verizon Wireless makes it easier and more cost-effective to implement smart government tools by making these solutions available through the National Association of State Procurement Officials (NASPO) ValuePoint® cooperative purchasing contract.

See how you can start on your journey to a smarter government:



Smart infrastructure

Intelligent Lighting

Lower operational costs and improve public safety by managing, monitoring and controlling street lighting remotely.

Traffic Data Services

Use deidentified cellular network records to analyze historical and up-to-the-minute population movement to minimize congestion and plan development.

Parking Optimization

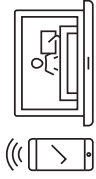
Optimize parking for additional revenue and reduce congestion.

Telematics Fleet Tracking and Management

Track vehicles, optimize routing and control costs.

ThingSpace (IoT management)

Simplify development and management of your Internet of Things (IoT)/machine-to-machine devices.



Smart communications

One Talk

Use a single phone number across mobile and desk phones so staff can be reached regardless of their location or the device they're using.

Push to Talk Plus

Just push a button to connect instantly and securely with one or many.

Digital Signage

Target public safety messages, raise awareness and engage citizens and visitors.

NetMotion (Mobile VPN)

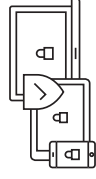
Make sure mobile employees can connect to applications reliably wherever they are – even when coverage is spotty.

GoCanvas

Replace paper forms with mobile apps to simplify data collection, streamline operations and boost productivity.

Field Force Manager

Help mobile teams stay in touch and on track; simplify workforce administration.



Smart mobile security

Verizon Mobile Device Management (MDM)

Track and manage all the mobile devices and operating systems connecting to your network from a single unified portal.

MobileIron

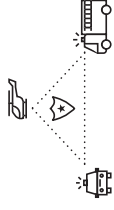
Become truly mobile with a foundation to manage standards-based security across the mobile-cloud ecosystem.

IBM MaaS360

Simplify how you manage mobile devices, applications, security, data and connectivity.

Samsung Knox

Use the industry's latest mobile devices to increase productivity, enhance collaboration and strengthen device security.



Smart response

Intrepid Networks

Help shorten response times and improve safety.

Public Safety Applications

Verizon's extensive ecosystem of public safety apps includes smart solutions related to response connectivity and prioritization (e.g., Responder Private Core), response operations (e.g., OneTalk, Push to Talk and Intrepid Networks), and response devices and equipment (e.g., Fleet Management).

For more information, visit verizon.com/naspo



Risks in the Chain

Securing subcontractors in as-a-service IT agreements is an ongoing challenge for state governments.

By **Lucas Ropek** / Staff Writer

The global marketplace makes it possible for easy transactions between public and private entities worldwide, but validating the security of those transactions isn't always so easy.

With supply chains that span multiple continents, often involving dozens of companies and products, regulation of cyber controls for public-sector IT contractors isn't a straightforward task. Pair this with the fact that cybercriminals and foreign intelligence agencies have increasingly honed their capacities to infiltrate and compromise organizations, and you have a unique security landscape that governments have yet to satisfyingly address.

At the federal level, the U.S. has worked hard to establish certification standards like the governmentwide Federal Risk and Authorization Management Program (FedRAMP), which was created to assess and authorize cloud service providers

working with federal agencies. At the same time, organizations like the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) have been deployed to continually assess risk and promote secure practices throughout the federal bureaucracy.

State and local governments, however, lag behind. While they are increasingly taking cues from federal agencies on supply chain risk awareness, the resources to act on that awareness are slim. Indeed, for smaller public agencies whose IT departments frequently find themselves deficient in funding and manpower, the idea of comprehensive supply chain audits is about as realistic as municipally funded moon landings.

"Certifying and evaluating suppliers is a huge undertaking and one that most states are not equipped to do," said Dugan Petty, former Oregon CIO. "Not even the

largest states have the capability to certify a supply chain or determine if hardware or software have malware built in," he said.

This problem has been complicated somewhat by broader shifts in the public sector's IT procurement process, said Steve Nichols, chief technology officer with the Georgia Technology Authority. As the CIO-as-broker model has come to replace the old owner/operator model, public agencies that previously procured and integrated all hardware or software themselves now frequently rely on the CIO to broker deals with system integrators. Integrators bring in whole suites of software from varied sources — increasing efficiency, but also the opportunity for intrusion.

"The software they [an integrator] bring or transfer might have a number of other third-party software packages already integrated into it (like a database or a Web server or an app server). Further, they might



for public agencies, cloud services often involve a number of different vendors in the same chain. Such vendors frequently have immense amounts of access to sensitive government data, making oversight of just how those vendors operate crucial.

“A SaaS solution might be built on top of a PaaS solution supported by another vendor and hosted in yet another vendor’s IaaS data center,” said Nichols, explaining that with all of these layered services and companies, the potential for proper oversight is difficult. Most worrying is the prospect of foreign intelligence agencies infiltrating supply chains to implant malware to conduct espionage and steal data.

Threats of this sort have been highly publicized in recent years. Huawei, the Chinese tech giant, has been in the headlines as an ongoing supply chain threat, but the problem hardly starts and stops with one company or nation-state. At the same time, NIST worries that “industrial spies/cybercriminals” are constantly on the hunt for opportunities to penetrate supply chains to gather information or exploit government data for financial gain. NIST also worries about the potential for organized crime groups to steal valuable government data, or terrorists to infiltrate systems to disable key services or wreak physical destruction through operational technology.

These threats, said Petty, can be especially vexing for state agencies because “no single authority” exists “that can take this on for the states. It has a complexity like other security issues because we have 50 different approaches all with individual state laws.”

Most of the solutions that do exist are some sort of auditing process, but these can be limited in scope and time consuming. In recent years, governments have frequently turned to certain certifications, such as a Statement on Standards of Attestation Engagement (SSAE-18 audit process), or even a FedRAMP certification — though these can be prohibitively expensive for vendors and can take up to a year to complete. More and more states are monitoring third-party access to their systems and data, said NASCIO’s Ward, requiring “some form of independent attestation” such as a SSAE-18 or a “Payment Card Industry

Data Security Standard (PCI DSS), and the like.” To the degree that this is affordable, governments should do it.


At the same time, said Ward, there are a number of more basic precautions that NASCIO recommends agencies take to protect themselves, including: “perform background verification checks on select high-risk, third-party employees; monitor and control third-party access to state systems and data; perform random spot checks of third parties’ sites; [and] engage an independent third party to assess the third parties’ capabilities.”

Nichols, meanwhile, has come up with a unique solution to supply chain risk management after GTA had a run-in with a potentially compromised vendor.

“This came up a couple of years ago with a vendor who got flagged by the federal government,” said Nichols. “We had some of that vendor’s product in use in our environment and went through a small project to find where we were using it and replace it and take them off the state contract. We realized that it would be a lot easier to deal with procurement and contractual issues if we had a standard on the books,” he said.

To make sure such an incident was less likely to happen in the future, Nichols researched and drafted a policy for GTA that would allow them to disqualify a supplier or product using a supply chain framework, basing it on NIST SP 800-161, which outlines supply chain risk management practices for federal agencies. It is one of the few examples of a state government imposing some sort of internal regulation to help secure the overall supply chain.

Nichols’ policy, which became effective in April, may be a step in the right direction — and a good model for state agencies that want to cut down on supply chain risk. Georgia’s policy asks agencies to integrate supply chain risk management into their overall risk management frameworks, while also giving agency officials an enforcement mechanism with the authority to reject certain suppliers if they have been deemed a security threat.

“This gives us an additional tool for dealing with problematic suppliers during a procurement or if we need to remove them from a contract,” said Nichols. 

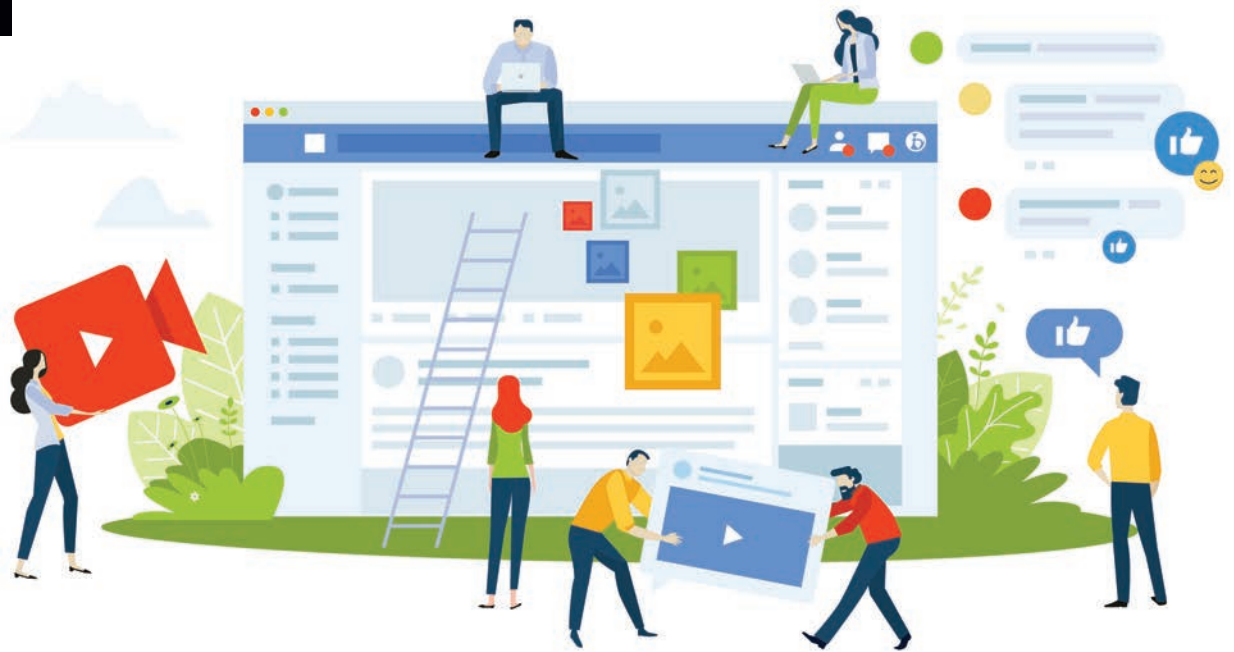
bring system or management software and hardware as part of that solution. All of those things are made and supported by other companies,” said Nichols.

Meredith Ward, director of research with NASCIO, said that data from her organization’s biannual cybersecurity survey shows there is some — though probably not enough — confidence in the security of government’s business partners.

“From this year’s study, we know that two-thirds of state CISOs are ‘somewhat confident’ that state information assets are protected from cyberthreats originating from business partners/vendors. However, one-quarter aren’t confident at all,” said Ward. “Some state CISOs have also cited that a lack of a third-party risk management program is a barrier their state faces to address cybersecurity challenges.”

Also adding to the problem is the rise in cloud procurement. While a useful resource

ilropek@govtech.com



Amplifying the Message

What does it take to be good at cybersecurity on social media?

A growing number of technology offices in state and local government have a public-facing role on social media. And many use their platforms to not only tell their department's story, but also to reinforce best practices when it comes to tech, and caution against prevalent cyberthreats to keep employees, businesses and citizens safe online. We caught up with the team at Minnesota IT Services (MNIT) to learn more about their social media efforts.

As far as social media, one external communications associate manages posts on Facebook, Twitter and LinkedIn, aided by in-house graphic design expertise as needed. The work is overseen by the agency's communications director.

Here's how Kendall Johnson of MNIT communications describes their social media strategy:



"It is important that digital accessibility is not an afterthought but included in every discussion so that the technology is available for the most amount of people." — @jay_wyant discusses an ever-present thread for "Tech Through the Decades". #a11y

"Minnesota IT Services (MNIT), the IT agency for the state's executive branch, mainly uses social media to inform the public of relevant IT projects, provide general cybersecurity information, and to highlight successful or compelling stories within the agency. We see our social media pages as a storytelling platform, where we create a person-centered narrative about the technology that connects Minnesotans to their state government.

"Our biggest campaign of the year is Cybersecurity Awareness Month in October. We create a theme for each week, generate content and graphics around that theme, and engage with the national campaign throughout the month. During that campaign, we also typically participate in a public event, which helps to tie our cybersecurity messages to people's everyday lives."



Cyber criminals are always looking for new ways to access data. Learn how to keep your information secure by staying on top of cybersecurity terms and cyber-attacks: <http://mn.gov/mnit/media/blog/index.jsp?id=38-407203>



MN.GOV

Cybersecurity and You

When it comes to cybersecurity, knowledge is power. We've broken down...



Password managers are a great resource and a security best practice!

A password manager will generate, retrieve, & keep track of long, random passwords under strong encryption. The best part is you only need to remember one password to access them all! #cybertip #CyberSafeMN

The agency closely measures the performance of its social media efforts, reporting out to leadership on a regular basis. Results inform the content and the timing of posts, helping to maximize engagement. Johnson reports the following growth in MNIT's social following over the past year: Facebook, 10 percent; Twitter, 9 percent; and LinkedIn, 57 percent. Timely, person-centered content, Johnson reports, sparks the most interest from followers.

ENSURING BUSINESS CONTINUITY IN TIMES OF CRISIS: A GAME PLAN FOR STATE AND LOCAL GOVERNMENTS

In this Q and A, **Herb Thompson, SLED strategist** at VMware, and **John Punzak, senior director of healthcare and SLED business development** at VMware, share how agencies can overcome their business continuity challenges to deliver a better constituent experience.



Herb Thompson



John Punzak

It's no longer business as usual for state and local governments. The COVID-19 pandemic has disrupted service delivery and led to significant loss of revenue. Business continuity has never been more important, and to strengthen these efforts, governments must empower the remote workforce, increase connectivity and enhance enterprise security.

What business continuity challenges have state and local governments faced since the pandemic began?

John: We've seen a three-phased approach throughout this crisis: reaction, adaptation and acceleration.

In phase one, the question was: "How do we respond to this and keep the business going?" For most agencies, that meant sending most employees home or to remote offices and setting up lines of communication.

As we move into phase two, agency leaders are looking at how to be more resilient, especially around enterprise security, because so many employees are working outside the firewall. Government agencies must consider how to scale to facilitate remote work because they typically have not been set up to manage that type of workload over the internet. At the same time, they are taking a significant hit to their capital budgets, but they may be able to enhance their operations with CARES Act funding.

In phase three, some state and local governments will accelerate digital-first initiatives and continue modernizing their legacy applications with the help of multiple cloud vendors. However, increasingly complex IT environments will bring new challenges.

How will the public sector's approach to networking and security need to evolve?

Herb: In some cases, state and local governments have gone from something like 500 remote users to 20,000 or 30,000 remote users. The old model of putting a moat around the data center only works when people are inside the perimeter. Going forward, governments will need to adopt zero-trust security networks to gain visibility into users and devices.

How can state and local governments best leverage the cloud to be more agile?

John: Three types of technologies will be beneficial for state and local governments: a digital workspace platform, an application development platform and a hybrid cloud infrastructure platform.

A digital workspace refers to the devices people use to access their work. With a digital workspace platform, it does not matter what device you use. Employees have easy, secure access to business applications. IT teams also can monitor and manage all devices coming into the network from a single place, which enhances security and network performance.

An application development platform can help prevent situations like unemployment insurance delays. Most states struggled to process benefits at scale because their applications were running on legacy systems. This is an opportune time to modernize and adopt cloud applications that can easily scale on Amazon, Azure or Google resources. An application development platform allows for this flexibility.

A hybrid cloud ties in nicely with this because many state and

local governments have virtual machines running on premises, but many have started moving those application workloads out to the big three hyper-scalers that I just mentioned, so they have the agility to scale on demand.

How can state and local governments balance budget considerations with technology modernization? Also, how can they ensure the solutions they adopted during the crisis continue to meet their needs?

Herb: My recommendation would be not to just procure individual point solutions but to look at IT security holistically. With revenues down, many agencies need to consider network, security and endpoint management and figure out how to leverage the cloud in a more unified way. This can help reduce total cost of ownership, eliminate duplicative products and point solutions, and improve security. By implementing a more encompassing single pane of glass management approach, you can also reduce support costs and other product costs.

What are some key considerations for state and local governments as they try to become more agile and responsive?

John: State and local governments must invest in future-proof infrastructure and technologies that will not quickly become obsolete. Investing in software, rather than hardware or an appliance, can help them integrate new capabilities as their business needs evolve. The mission of government is the same in the era of COVID-19. They still must deliver, but the way they deliver has changed.

Cyberstrategy in

It's a good time to be in the cybersecurity business. A recent survey of more than 500 leaders in local and state government yielded timely data on where priorities now lie relative to threat containment and overall strategy. Fielded in June, the survey was conducted by the Center for Digital Government,* in partnership with MS-ISAC (Multi-State Information Sharing and Analysis Center) and the EI-ISAC (Elections Infrastructure Information Sharing and Analysis Center).

WHO'S IN CHARGE?

This person oversees organizational cybersecurity:

||||| 46%
CIO/IT Director

||||| 26%
CISO

||||| 6%
No one has an assigned
cybersecurity role

||||| 6%
CTO or equivalent

||||| 4%
Third-party company

FOLLOW THE MONEY

A ranked list of where cybersecurity dollars go:

1 / Cybersecurity software and hardware

2 / Hardware/software backup
and redundancy

3 / Monitoring/reporting services

4 / Training, all employees

5 / Assessments and reviews

6 / Training, cybersecurity
and IT staff

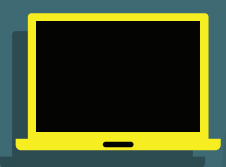
7 / Cybersecurity insurance

8 / Cyberthreat intelligence

9 / Incident response

*The Center for Digital Government is part of e.Republic, *Government Technology's* parent company.

Numbers

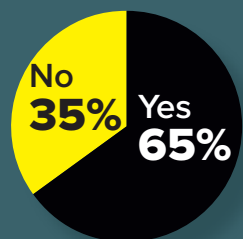


TRAINING THE TEAM

57% of counties annually train all employees on cybersecurity.

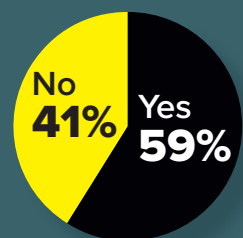
PROTECTING DATA

Do your cybersecurity policies protect data used by third-party partners?



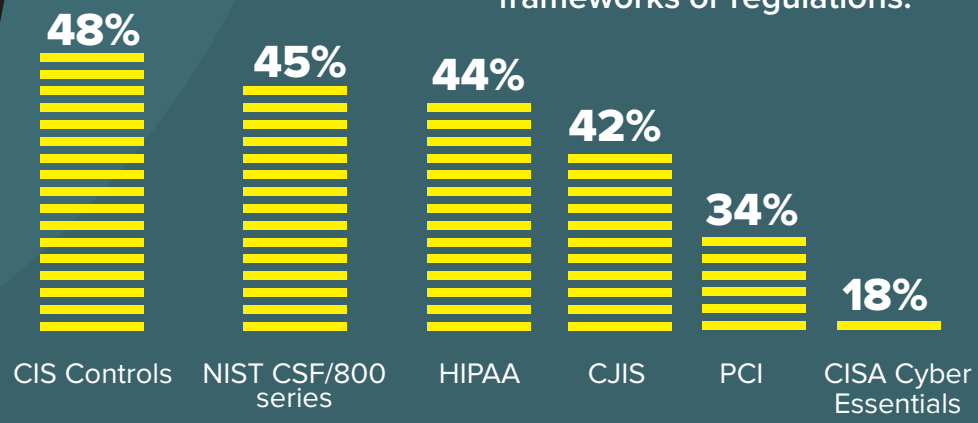
FRIENDS IN NEED

If another agency had a cybersecurity incident, could you help?



UNITING ON STANDARDS

The most commonly used cybersecurity frameworks or regulations:



Quick Action and Safe Storage Help New Orleans Recover from Ransomware Attack and Build a Strong Defense Against Future Threats

THE SECURITY ALERTS ARRIVED

early on Friday, Dec. 13, 2019: suspicious remote logins were occurring on the City of New Orleans' servers.

"The logins were coming from accounts I knew weren't being used at 5 a.m. That keyed us in that something bad was happening," says Bill Healy, the city's director of operations for information technology and innovation.

Aware of increasing ransomware attacks on cities across the country, the city's IT department wasted no time in responding.

"We took the most immediate and drastic actions we could to mitigate damage from the attack," says Kimberly LaGrue, the city's chief information officer.

At 11 a.m., the city began shutting off its Internet access. By 11:30 a.m., Internet connections for all of the data center's 470 servers and the thousands of virtual machines they contained had been completely shut down.

By isolating machines on a virtual network, investigators soon discovered the culprit: a variant of Ryuk malware, which has been used since 2018 to launch ransomware attacks on businesses, governments and hospitals. Researchers estimate the cost of Ryuk attacks in 2019 reached \$7.5 billion.

With Ryuk, as with other ransomware attacks, hackers break into an organization's network, usually by stealing an email account's login credentials in a phishing scam. They then use the compromised account to install and spread malware on the network. The malware encrypts data, making it impossible for workers to access systems and information they need. Attackers then demand payment, usually in Bitcoin, to release the data.

Thanks to the city's quick action, the New Orleans attackers didn't get far enough to make a ransom demand. Forensic analysis later revealed only one server had been completely encrypted. Several others had been partially encrypted when the city disrupted the attack by shutting off Internet access.

In the beginning, however, there was no way of knowing the extent of the damage. The city had to test and sanitize all of its data and find a safer place to store it. This served two purposes: to remove the current infection and to keep the hackers from later reinfecting the system — a growing trend in ransomware attacks. In the meantime, the city's more than 4,000 workers could no longer access mission-critical online tools and information.

MOVING TO SAFE STORAGE

New Orleans was faced with 50 terabytes of SQL data that it needed to analyze, sanitize and store. It set up a virtual local area network (VLAN) where it could isolate all servers. A monitoring service was used to determine which virtual machines on the servers — or files within those machines — were infected and had to be scrubbed. The scrubbed data then had to be moved to new, safe storage and backup systems while existing servers were still being patched and upgraded.

"We basically had to double our storage needs in order to recover," Healy says.

The city selected Pure Storage to supply the hardware and software for both primary and disaster recovery (DR) storage. Pure's storage system deduplicates all data stored on it, saving precious space for the city and allowing additional copies to be easily made and stored. The city

had previously run only its most important applications on its fastest storage, but with Pure Storage they could run far more — and faster. This helps city workers do their jobs more efficiently during normal operation and speed recovery time in the event of another attack.

"We have a platform that gives us a better and faster storage option. It makes us more comfortable with the response we are able to provide for our organization should there be another attack," LaGrue says.


Cyberattacks on municipalities have been on the rise for several years, a trend that has accelerated during the pandemic.

"Everything we hear in the industry tells us there has been an uptick in phishing attempts and malware attacks since COVID-19. The hacker community is exploiting vulnerabilities and preying on pandemic-related fears, and we have to be ready for them," says LaGrue.

Pure Storage's data snapshots are immutable, meaning hackers can't modify or delete them, and they even have an option that prevents these snapshots from being tampered with by a seemingly authorized administrator without first contacting Pure Storage. The city also worked with disaster recovery and data management firm Veeam, which provides additional protections to make backup data immutable.

"That means even if an attacker gets in and finds our backups, he or she can't do anything to them," Healy says.

Restoring data and moving it to a secure storage system quickly was the key to a swift recovery. With help from Pure Storage, the city's IT department set up the new storage platforms quickly and began data migration. Recovery and backup systems can take a long time for IT administrators to learn and deploy, but



city administrators found Pure Storage and Veeam simple to use.

“We needed the new system to be easy to learn and implement so that we could manage other parts of the recovery while building out the new storage,” LaGrue says. “The Pure Storage team provided a simple solution and gave us a wealth of cross-training and knowledge that helped us get it up and running quickly.”

RECOVERING AMID A PANDEMIC

In the midst of the city’s recovery efforts, the COVID-19 pandemic hit. While recovery efforts never stopped, the IT department had to shift its focus to providing a remote working environment for the city’s 4,000 workers.

“It delayed our recovery plan by about two months,” LaGrue says.

In addition, before going back online, the city added multiple new layers of network security.

“We could have had the network restored much quicker, but it wouldn’t have been nearly as secure,” Healy says.

Healy and LaGrue learned some important lessons while managing the attack, and have suggestions to help other governments avoid ransomware attacks or mitigate their damage:

“We were in a time crunch. We were very fortunate to have a solution that was simple and straightforward, so our engineers could start using it very quickly.”

Kimberly LaGrue, CIO, New Orleans

✓ **Know your organization’s disaster recovery plan** so you can move quickly to stop an attack. “Our IT team has been working on disaster recovery for years, and we knew what to do as soon as we detected the threat. It’s like knowing which exit to use during a fire drill,” LaGrue says.

✓ **Isolate traffic between nodes on the network.** “Granular management gives you a bit more control over traffic from bad actors,” Healy says.

✓ **Use a layered, multi-vendor approach to network security** to uncover more vulnerabilities and decrease the chances of another attack.

✓ **Use a secure, easy-to-deploy storage and backup system.** “It helps me sleep at night to know if our data is compromised, we can quickly retrieve it from a safe storage system,” LaGrue says.

Today, New Orleans has completed 80 percent of the work needed for

recovery. It is bringing the last of its legacy operations back online, and has distributed nearly all of the 500 new computers and laptops it needed to order when its old hardware couldn’t be configured to meet new security requirements. The city expects to achieve a full recovery by the first anniversary of the attack.

By providing efficient, secure and economical storage and backup systems, Pure Storage and Veeam accelerated New Orleans’ recovery and provided a stronger defense against future attacks. As a result, the city can now focus on achieving its other important objectives.

“Serving our community is our bottom line. By making efficient investments in storage and security, we can direct more funding to initiatives that help our citizens,” LaGrue says.

This paper was created by the Government Technology Content Studio, with input from Pure Storage and Veeam.



Pure transforms the government’s IT modernization journey by delivering a modern data experience that empowers agencies to run their operations as an automated, storage as-a-service model seamlessly across multiple clouds. One of the fastest-growing enterprise IT companies in history, Pure helps customers put data to use while reducing the complexity and expense of managing their infrastructure. www.purestorage.com/government



The importance of data has grown to drive every aspect of the digital business, and so has the need for solutions that can do far more than ensure its availability. Data protection must move to a higher state of intelligence and be able to anticipate needs and meet demand. Ensuring reliable backup, instant recovery and reuse of data requires an evolution in how data is managed. Leveraging intelligence to enable data to back up autonomously, migrate to the right location and secure itself. As the leader in availability, Veeam® is uniquely positioned to help customers along their journey to cloud data management. www.veeam.com/sled



The Case for Hiring Hackers

Look for character, passion and diversity when filling out your cybersecurity team.

About a decade ago I was sitting in a large auditorium listening to valedictorian speeches at my daughter's high school graduation ceremony. Most of the five-minute speeches seemed too long, with predictable thank-yous to parents and teachers, hopes and dreams, future service, etc.

But one bright young lady shocked everyone. "I've examined my options ... visited colleges ... taken my parents' money ... and have decided to buy a ship. I plan to live life as a pirate!" she declared.

Her passionate appeal to her classmates was to break the rules. Go the wrong way on one-way streets. Don't just reach for the stars — explore the universe. Live free or die. Don't let others define you. Follow your heart.

She received the only standing ovation.

But as a former National Security Agency employee, images of traitors and espionage filled my brain. I thought, "Hazards ahead!"

Nevertheless, a few years later, I realized that this 17-year-old was tapping into

something important. I read in *What Would Steve Jobs Do?* by Peter Sander that Jobs once proclaimed, "It's more fun to be a pirate than to join the Navy."

So why did Jobs seek to hire pirates?

"A pirate can function without a bureaucracy," Sander writes. "Pirates support one another and

support their leader in the accomplishment of a goal. A pirate can stay creative and on task in a difficult or hostile environment. A pirate can act independently and take intelligent risks, but always within the scope of the greater vision and the needs of the greater team."

Pros and Cons of a Pirate, and Hacker, Mentality

I've often heard similar statements made about "black hat" hackers. The desire is to hire people with an outside-the-box mentality. The sentiment is that hackers who like to break things, who steal things, also find new ways of accomplishing things. Hackers are professionally curious, and never say never. Talented hackers who understand the dark web and think like criminals are needed to stop the bad guys.

Which brings us to the elephant in the room with hiring pirates — and black hat hackers. Namely, their activities are generally illegal. They do not follow society's rules. Taken to the extreme, pirates and black hats might not even show up at the office at all.

But this leaves us with other questions like, how far do you let the pirates/hackers go? Could their illegal actions tarnish organizational reputations, lead to more insider threats and audit findings, or even bring fines, jail or bankruptcies?

This discussion leads to an inevitable question: Can you hire an ethical pirate? In security circles, many people call these

people "gray hat" hackers, with a foot in both the good and evil online worlds.


What Traits Should We Aspire to Hire?

There are no easy answers to these tough questions. Nevertheless, the importance of this topic cannot be underestimated. Every organization seeks to hire the best talent, but the greater goal is to build effective teams that work well together to deliver solutions, produce new innovative products and services, and build a culture of lasting success.

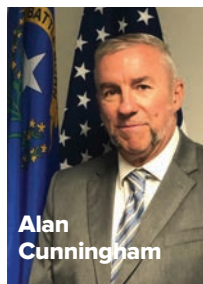
It is generally true that technology and security professionals who earn interviews have the minimum skills to fulfill the duties in the job descriptions, at least on paper. But how do we measure future potential and cultural fit? Beyond credentials and certifications, what traits should we be looking for?

My answer is to start with character. Is this person trustworthy? I'd rather hire a good security pro who has a great attitude, is trustworthy and is accountable than a great cyberexpert I don't trust.

Second, is the person passionate about the role, the organization and team success? You can't fake passion.

Third, hire for diversity of experiences and backgrounds on the team. I agree with Steve Jobs on this: "Recruit a diverse, well-traveled and highly skilled pirate, and they'll follow you anywhere." 

Daniel J. Lohrmann is the chief security officer and chief strategist at Security Mentor. He is an internationally recognized cybersecurity leader, technologist and author. From 2002 to 2014, Lohrmann led Michigan's award-winning technology and cybersecurity programs, serving as CSO, CTO and CISO.



New CIO Named in Nevada

Alan Cunningham was appointed to serve as chief information officer of Nevada after spending the past four years as head of cybersecurity for the Washoe County School District. He also brings private-sector security experience, as well as many years serving as an independent cybersecurity consultant. The Nevada CIO position was filled in an interim capacity since Michael Dietrich's departure in September 2019.

AWS Hires Four Former State CIOs

Amazon Web Services, the largest cloud services provider and a longtime vendor to government IT shops, has added at least four former state chief information officers to its ranks, three in the past year. **Craig Orgeron**, **Chuck Grindle** and **Morgan Reed**, formerly of Mississippi, Kentucky and Arizona, respectively, now work for the tech company, as does **Hardik Bhatt**, former head of Illinois IT, who has been with AWS since 2017.

Austin CIO Retires from City Service

After 10 years as head of the Communications and Technology Department in Austin, Texas, **Stephen Elkins**' last day with the city was Sept. 4. Prior to taking over as CIO, he was a city employee since 2004. A statement from the city manager indicated Elkins had taken a "promotional opportunity" outside of city government, and named Chris Stewart, CIO for Austin Water, as Elkins' interim replacement.

Innovation Officer Departs Sacramento

In early September, Sacramento, Calif., Chief Innovation Officer **Louis Stewart** left his role with the city, which he had held since May 2017. He will move on to work for private-sector company Nvidia. As of press time, Stewart's successor had not been named.



Longtime Delaware CIO Heads to Microsoft

After six years as head of IT in Delaware, **James Collins** announced he was stepping down from the public sector to take a job with Microsoft Consulting. In his time as CIO, Collins led a comprehensive cybersecurity modernization, led a rural broadband initiative and advocated for diversity in tech, among other accomplishments. Jason Clarke, chief operating officer for the Department of Technology and Information, will serve as acting CIO.



North Carolina Creates CTO Role

Longtime state employee **Dan Kempton** was named North Carolina's inaugural chief technology officer in late August. Kempton's previous roles include director of engineering and cloud services for the Department of Information Technology and CTO for the North Carolina Department of Revenue, as well as private-sector work at CAVU Corp. and Dell EMC.

Illinois CIO Steps Down

Ron Guerrier, who headed the Illinois Department of Innovation and Technology (DoIT) since March 2019, left state service in September. He previously had two decades of private-sector IT experience, although his next move had not been announced as of press time. Jennifer Ricker, assistant secretary of DoIT, will replace Guerrier in an acting capacity.



Securing the City

Local IT teams can take advantage of state and federal resources to boost their cyberposture.

The global pandemic has significantly raised the security stakes for CIOs, CISOs and IT decision-makers. Unfortunately, bad actors know well that our workforce is now more vulnerable due to the increase in the number of remote workers, many of whom have never worked anywhere other than in the office. IT teams are stretched thin due to COVID-19 as we work around the clock to support remote users and urgent digital transformation, and even assist with pressing community needs such as digital inclusion. Various budgets are under pressure as revenues have fallen dramatically, and many expenses have increased. This moment calls for us as technology leaders to conduct a thorough review of our cybersecurity posture.

One of the leading cybersecurity organizations available to government technology teams is the Center for Internet Security (CIS). Many people are familiar with the Multi-State Information Sharing and Analysis Center (MS-ISAC), one of CIS's key contributions. Another vital CIS program is its Top 20 Controls and Resources, a sort of cybersecurity version of Maslow's "hierarchy of needs" for IT security staff. The 20 controls are organized into three categories: Basic, Foundational and Organizational. This framework provides a terrific starting point and checklist to ensure best practices.

In the Basic category, IT teams should have full vision into all enterprise hardware and software. We've witnessed

both device and software sprawl over the past decade. We cannot keep our organization safe unless we have a complete inventory and accounting of our hardware and software. Are your technology assets logged, tagged and accurately assigned to staff? Do you utilize a mobile device management solution? Does your team employ a vulnerability scanner to search for weaknesses on at least a weekly basis? Are you leveraging automated software updates and patches where appropriate? Government agencies often lag behind the private sector on timely patching, and it is one of the best ways to harden our defenses.

“This moment calls for us as technology leaders to conduct a thorough review of our cybersecurity posture.

The Basic category also calls for a review of administrative privileges. Users and accounts with elevated permission levels offer an attractive target for hackers. Too much sharing of credentials and re-using passwords fosters a dangerous situation. Further, does your staff have a standardized, secure configuration for hardware and software systems? Are you running logging on all systems, and do the logs feed into a centralized system for review? Automation and AI can offer substantial improvements for teams already short staffed or underfunded.

The next group of CIS controls is the Foundational category, which includes recommended protections for email, data

and network devices. The controls provide guidance on email security, leveraging email security protocols to reduce spoofing and cyberattacks — especially critical these days. The controls also discuss automated port scanning and ensuring ports and protocols are only in use as business needs dictate. Another crucial element in this category is data protection. Does your organization have data governance practices in place? Has staff received appropriate training on HIPAA, CJIS and PCI compliance? These courses are often included with more extensive cybersecurity awareness training programs.

The third group of CIS controls is the Organizational category. In addition to a cybersecurity awareness program, are you actively running simulated phishing tests? Have you considered social engineering and vishing tests? Do you have an incident response plan? Do you know whom to contact the moment you confirm your organization faces a severe attack? We need to work closely with our emergency management partners, as a cyberattack is probably more likely these days than some other traditional hazards.

The overall scope and responsibility of cybersecurity operations can feel overwhelming and never-ending. However, many resources are available at the state, federal and nonprofit levels. Many services are subsidized or even free. There appears to be bipartisan support building in Washington for new funding for state and local cybersecurity needs. Now is a good time for us to collectively lobby our legislators to make this proposed funding a reality. **GT**

Luke Stowe is the CIO and interim director of administrative services for Evanston, Ill. One of *Government Technology's* Top 25 Doers, Dreamers and Drivers of 2018, he works to bridge the gap between technology and business practices.

OPTIMIZING EMPLOYEE SCHEDULING: HOW AI-DRIVEN ENTERPRISE OPEN SOURCE SOLUTIONS CAN EMPOWER HEALTH CARE ORGANIZATIONS



Employee scheduling is complex in every industry, but even more so in health care. The COVID-19 pandemic has exacerbated these challenges, as health care providers fall ill to the virus and are unable to work. To maximize resource availability and better manage schedules, hospitals and point-of-care centers can no longer rely solely on manual processes. Applying automation to decision-making is an impactful way to respond to existing and emerging scheduling complexity.

*In this interview, **Ben Cushing**, Field CTO of Federal Health at Red Hat, a leading provider of enterprise open source solutions for the public sector, shares how Applied AI-driven solutions can help hospitals optimize their business processes, streamline the scheduling processes and ultimately put providers in the best position to deliver quality care.*

What are the main challenges hospitals and point-of-care centers face when it comes to scheduling providers and maximizing their resources?

The obvious challenge right now is that people are sick. You have health care workers who are on the front lines of this crisis who are disproportionately affected. They're exposed more frequently, so they're more likely to become sick. That has created a lot of challenges. If resources aren't available to care for your patients, then that immediately puts a strain on your hospital.

The solutions health care organizations use for scheduling really vary. There are hundreds of scheduling applications available, but the irony is Microsoft Excel is probably the most popular scheduling tool in hospital systems throughout the

country. The complexity of scheduling is such that it requires flexibility in a product. In the case of Excel, its strength is its flexibility.

Despite its flexibility, how does Excel prevent hospitals and point-of-care centers from being more efficient when it comes to scheduling?

Excel easily adapts to the user, but the challenge is that on its own it's not capable of solving anything. It still requires cognition on the part of the scheduler. One of the challenges that has been exacerbated now is the need to schedule frequently. It takes time to put a schedule together. You need to think about the qualifications of the individuals who are going to be on the unit, the construction of the teams based on each person's skill set, whether certain providers are even available to work and their risk profile

when it comes to being placed on a COVID unit. It is important all these constraints are kept in mind when producing a schedule.

What technology capabilities do health care organizations need? How can AI, in particular, benefit them?

Applied AI, and specifically, automation of provider scheduling, is an opportunity to leverage powerful but small footprint technologies to solve existing health care problems. These solutions have wide application, from optimizing PPE distribution and availability to producing sophisticated planning for ramp up and down of expensive surgical capabilities. Coupled with existing APIs, an Applied AI system becomes an integrated part of the IT ecosystem and can solve for current and future crises.

Many hospitals and health care organizations are overstretched, especially now. How can they balance modernizing their technology with improving care delivery?

It really comes down to improving the experience for the provider so they can deliver better care. The role of IT systems is to assist, and not be an additional burden. Certain technologies, like clinical decision support, have the potential to transform health care, but are more risky to implement because they directly interface with patient care. However, technologies focused on optimizing scheduling for health care providers largely have been overlooked. There has been more focus on improving the patient experience — and rightfully so — but improving the experience of the people who provide care will enable them to deliver better care. Implementation of such a system ranges from out-of-the-box readiness to full integration with existing scheduling systems. Our Applied AI technology solutions are engineered to meet the hospital system where they are on their automation journey.



Red Hat

About Red Hat

The adoption of open principles helps the U.S. government start, accelerate, and improve the art of digital transformation—people, process, and technology. As the world's leading provider of enterprise open source solutions, Red Hat uses a community-powered approach to deliver reliable and high-performing Linux®, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500 and 100% of U.S. executive departments. As a strategic partner to cloud providers, systems integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future. Learn more at www.redhat.com/gov.



\$161B

In the U.S., 30 to 40 percent of food sold in grocery stores is wasted. That's about \$161 billion in wilted lettuce and expired milk that retailers can't sell. A handful of startups, like Shelf Engine, are using machine learning to help grocery store buyers better analyze the historic trends of their store to purchase goods more efficiently, thereby producing less waste. Shelf Engine reports that using its software to automate decision-making has increased stores' gross profits by 25 percent.

SOURCE: DIGITAL TRENDS



SAY CHEESE: After electric moped-share company Revel suspended service in New York City in July following accidents involving two customer deaths and one critical injury, the company modified its user agreement and resumed operations. Riders must now pass a 21-question in-app test that covers traffic laws and other safety requirements, and the moped will only turn on after a rider submits a selfie wearing a helmet. Revel has also imposed a stricter suspension policy for rule-breakers and an improved system for reporting bad behavior. SOURCE: THE VERGE



MASK UP: Wearing face masks in public has become part of daily life in the age of COVID-19, and while materials from medical masks to bandanas have proven to be effective against spreading the virus to one degree or another, a new gadget from LG is taking masking to the next level. The PuriCare Wearable Air Purifier is a personal air purifier for your face, with three fans and two HEPA filters designed to clean the air you breathe as you breathe it. While not necessarily designed to stop respiratory air transfer of coronavirus, LG claims breathing with the mask on is "effortless." SOURCE: ENGADGET

\$5M



An app that aims to gamify emergency preparedness closed a \$5 million seed round in August that will help it with its planned October launch. Harbor uses publicly available information from agencies like FEMA and USGS, plus building codes and land maps, to determine the particular risks of a user's location. The app makes a weekly preparedness checklist of tasks like checking smoke alarms or ensuring enough water is on hand so users can be ready for whatever disaster might occur.

SOURCE: TECHCRUNCH

Going Paperless in the Public Sector: How Agencies Can Ensure Business Continuity



*In an unpredictable scenario like the COVID-19 pandemic, citizens are more reliant than ever on services from state and local governments. What is not always as obvious in these situations is the same disruptions that challenge individuals also pose serious obstacles for government agencies — especially when it comes to business continuity. In the public sector, it's hard to get citizens the help they need if you can't efficiently process applications, gain approvals or collect signatures. In this Q&A, **Andrew Kok**, Regional Delivery Manager, Professional Services at DocuSign, discusses the challenges governments face in unexpected circumstances when they rely heavily on paper. He also explains how digitized processes help ensure operations remain running in difficult times.*

During an unplanned event, how do paper-heavy processes keep governments from carrying out their missions?

The biggest challenge is not being able to fulfill your obligations. Think of the people who lost their jobs in the wake of COVID-19 — they went for weeks without unemployment benefits because their states couldn't handle the deluge of claims. Think of the time it takes to process contracts, liability waivers and NDAs when an agency procures supplies and services for disaster response. You need to act quickly, but paper slows you down. On a smaller scale, what happens if there is a fire, and a room full of paper documents goes up in flames? Can the government continue business as usual without those records?

Paper also increases expenses. On average, it costs \$36 to conduct a paper transaction, including printing, copying, mailing, getting documents signed and other activities.¹ And that doesn't even include the cost of storage. For example, the state of North Dakota calculates it costs \$520.73 per year to maintain just one drawer in a five-drawer file cabinet.²

How do digital systems for document management help governments fulfill their missions during a crisis or unexpected scenario?

When you replace paper processes with digital ones, you can quickly get aid to the right people, direct supplies to the right places and make necessary payments. You can

also streamline internal processes. We have seen this during the current COVID-19 pandemic. With so many people working from home, something as simple as mail distribution has created serious delays. Someone must go to the office to collect the mail. Then it has to be distributed somehow so people can perform their jobs — sending invoices, getting approvals for payments, signing contracts. When you digitize those functions, employees can access the documents they need and complete their work from virtually anywhere.

If a government agency wants to eliminate paper processes, what are some good first steps?

It's best to start with the simple changes that bring benefits to as many people as possible and can be implemented quickly. Timecards are a good example of this. By digitizing that process you can eliminate the need for employees to fill out paper forms, pass them around for signatures and turn them in. Digitizing contracts also makes it much easier to procure items from vendors. On the citizen-facing side, digitizing unemployment claims would have a positive impact on many people, as would digitizing the process for obtaining various kinds of permits. In an emergency, you don't worry about creating the perfect scenario for digital adoption. By accomplishing a few quick wins, you can start building a foundation for future change.

DocuSign®

DocuSign helps organizations connect and automate how they prepare, sign, act on, and manage agreements. As part of the DocuSign Agreement Cloud, DocuSign offers eSignature, the world's #1 way to sign electronically on practically any device, from almost anywhere, at any time.

1. <https://c.environmentalpaper.org/> 2. <https://www.nd.gov/itd/services/records-management/cost-storing-paper>

A crack is a pothole waiting to happen.

Stop throwing resources and money into a perilous hole. With CentralSquare Enterprise Asset Management software, monitor your asset inventories — roads, water, sewer, fleet, waste, equipment and facilities — alongside associated work orders, maintenance requests, accounting and depreciation to prevent costly emergency repairs and remove dangerous hazards from your streets.

Learn more at centralsquare.com.



CENTRALSQUARE

FINANCE | COMMUNITY DEVELOPMENT | HUMAN CAPITAL MANAGEMENT | ENTERPRISE ASSET MANAGEMENT | UTILITIES