government technology™
gt
Solutions for state and local government.
OCTOBER/NOVEMBER 2021

INSIDE:

FAST FORWARD

THE BIGGEST THREATS SHAPING THE FUTURE OF CYBERSECURITY.

VOL 34 ISSUE 7 / A PUBLICATION OF e.REPUBLIC / GOVTECH.COM

VDGS

VIRTUAL DIGITAL GOVERNMENT SUMMITS

Spreading Best Practices & **Spurring Innovation.**

- Arizona
- Arkansas
- Bay Area
- California
- Chicago
- Colorado
- Connecticut
- Florida
- Georgia
- Hawaii
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Los Angeles
- Louisiana
- 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
- West Virginia
- Wisconsin

government technology

ATTEND/SPONSOR:
events.govtech.com

govtech.com

October/November 2021

CONTENTS

Vol 34 | Issue 7

COVER STORY

SHUTTERSTOCK.COM

Government Technology (ISSN# 1043-9668) is published monthly except February, May, August, and November by e.Republic Inc, 100 Blue Ravine Rd, Folsom, CA 95630. Periodical Postage Paid at Folsom, CA and additional offices. POSTMASTER: Send address changes to: Government Technology, 100 Blue Ravine Rd, Folsom, CA 95630. 916-932-1300.

COVER IMAGE: SHUTTERSTOCK.COM

SHUTTERSTOCK.COM

DEPARTMENT

COLUMNS

NEWS

IN OUR NEXT ISSUE:

Year in Review
Revisiting the stories that made 2021 a year for the books.

Now Hiring
Gov tech career moves from the past 12 months.

Let's Get Digital
Facts and figures from our annual Digital Cities Survey.

WWW.GOVTECH.COM

government technology

Publisher: **Alan Cox**, alanc@govtech.com

EDITORIAL

Editor: **Noelle Knell**, nknell@govtech.com
Managing Editor: **Lauren Harrison**, lharrison@govtech.com
Web Editor & Photographer: **Eyragon Eidam**, eeidam@govtech.com
Senior Copy Editor: **Kate Albrecht**, kalbrecht@govtech.com
Copy Editor: **Kali Tedrow**, ktedrow@govtech.com
Associate Editor: **Zack Quaintance**, zquaintance@govtech.com
Associate Editor, Data & Business: **Ben Miller**, bmiller@govtech.com
Managing Editor, Education: **Andrew Westrope**, awestrope@govtech.com
Assistant News Editor: **Jed Pressgrove**, jpressgrove@govtech.com
Staff Writers: **Skip Descant**, sdescant@govtech.com
Julia Edinger, jedinger@govtech.com
Katya Maruri, kmaruri@govtech.com
Jule Pattison-Gordon, jpgordon@govtech.com
Brandon Paykamian, bpaykamian@govtech.com
Thad Rueter, trueter@govtech.com
Contributors: **Pamela Marineau, Adam Stone**
Web Producer: **Andi Wong**, awong@govtech.com

DESIGN

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

PUBLISHING

Senior Vice President:
Kim Frame, kframe@govtech.com

Strategic Account Directors:
Carmen Besirevic, cbesirevic@govtech.com
Lisa Brown, lbrown@govtech.com
Katie Dunlap, kdunlap@govtech.com
Lynn Gallagher, lgallagher@govtech.com
Karen Hardison, khardison@govtech.com
Charles Hughes, chughes@govtech.com
Kristi Leko, kleko@govtech.com
Andrene Potts-Dierkes, apotts-dierkes@govtech.com
Rebecca Regrut, rregrut@govtech.com
Lara Roebbelen, lroebbelen@govtech.com
Kelly Schieding, kschieding@govtech.com

Bus. Dev. Manager:
Sheryl Winter, swinter@govtech.com

Director of SMB Sales:
Ron Avneri, dravneri@govtech.com

SMB Account Director:
Katrina Wheeler, kwheeler@govtech.com

SMB Account Managers
Dana Kansa, dkansa@govtech.com
Lisa Blackie, lblackie@govtech.com

Director of Sales Administration:
Jane Mandell, jmandell@govtech.com

Sales Administrators:
Janaya Day, jday@govtech.com
Ayesha Faiz, afaiz@govtech.com
Tara Holm, tholm@govtech.com
Lien Largent, llargent@govtech.com
Sharon Penny, spenny@govtech.com

Chief Customer Success Officer: **Arlene Boeger**, aboeger@govtech.com
Dir. of Content Studio: **Jeana Bigham**, jbigham@govtech.com
Dir. of Digital Marketing: **Zach Presnall**, zpresnall@govtech.com
Subscription Coord.: **Eenie Yang**, subscriptions@govtech.com

CORPORATE

Executive Chairman of the Board: **Dennis McKenna**, dmckenna@govtech.com
CEO: **Cathilea Robinett**, crobinett@govtech.com
CAO: **Lisa Harney**, lharney@govtech.com
CFO: **Paul Harney**, pharney@govtech.com
Executive VP: **Alan Cox**, alanc@govtech.com
Senior VP of Events: **Jack Mortimer**, jmortimer@govtech.com
Executive Editor: **Paul W. Taylor**, ptaylor@govtech.com
Chief Innovation Officer: **Dustin Haisler**, dhaisler@govtech.com

Government Technology is published by e.Republic Inc.

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.

e.Republic

By Noelle Knell / Editor

Are Ransom Bans the Answer?

There are nearly as many opinions on how to play defense against the ransomware threat as there are cybersecurity professionals. The prevailing thought early on seemed to be to never, ever pay a ransom. ("We don't negotiate with terrorists" comes to mind.) But that's easy for a remote expert to say, one who's not facing catastrophic disruption to their organization, not to mention the collateral damage to public confidence and reputation.

And while the actual impact of ransomware is difficult to quantify, one expert told *Stateline* that last year more than 110 state and local governments were hit. That number jumped to almost 1,700 for schools, colleges and universities.

As the threat evolved, there were rumblings, albeit quiet ones, that victims of ransomware should just pay the ransom. Maybe it's the most expedient way of putting the incident behind them? While some security experts were aghast at the suggestion, some agencies, particularly smaller, under-resourced ones, do make that decision when their backs are against the wall, vowing to beef up their defenses to keep from being hit again. The approach got validation, of sorts, from reports that oftentimes organizations spend way more money recovering from an attack than they would have paying the original demand from the hackers who infiltrated their systems.

One element of cybersecurity strategy that has gained ground alongside ransomware is cybersecurity insurance. While it does not replace the need for good cyber hygiene practices (keep those patches up to date, back up your data, etc.), many public agencies now purchase an insurance policy to help mitigate losses and add a layer of protection. *Government Technology*'s sister organization, the Center for Digital Government, reports that it's now more likely than not that cities, counties and states have cyber insurance policies. Our feature *Out of Reach?* (p. 30) looks at how the cybersecurity insurance market is changing to keep up with the growing threat.

But policymakers are also contemplating what should be done about ransomware. Legislators in multiple states have taken up proposals in the name of protecting citizen data that would ban victims from paying ransoms. The argument is that bans disincentivize the crime, sending would-be ransomware attackers to go pick on someone else.

It's encouraging that many of these proposals include funding to boost the cybersecurity posture of under-resourced governments to guard against attacks in the first place. And there are exceptions that are being incorporated into the discussion on bans, like utility companies and hospital systems, for example, where legislated bans could put lives and critical infrastructure at risk.

U.S. Energy Secretary Jennifer Granholm voiced support for ransom bans on *Meet the Press* recently, though she acknowledged uncertainty about whether the Biden administration was prepared to take a policy step in that direction.

"I think we need to send this strong message that paying a ransom only exacerbates and accelerates the problem. You are encouraging the bad actors," she said.

But the idea does not have universal support, based largely on the continued vulnerability of most public and private organizations to cyber threats like ransomware.

John Davis, retired U.S. Army major general and vice president of Palo Alto Networks, served as the co-chair of the Ransomware Task Force for the Institute for Security and Technology, which presented its ransomware framework earlier this year. Davis recently described the discussion among task force members (a broad coalition of international representatives from government, the private sector and academia) about ransomware payment bans as "the most contentious thing the task force debated."

Until the task force's key recommendations are implemented broadly, Davis explained that banning ransom payments is "impractical and potentially counterproductive."

"We're not there yet. We need to raise the maturity of the ecosystem that surrounds the problem itself," he concluded. But unlike bans on ransom payments, what's not contentious is pointing resources toward making the public sector a less vulnerable target. gt

Strengthening enterprise security in government with the cloud

The American Rescue Plan gives leaders an opportunity to invest in the future

As state and local governments make remote work a core part of their operations, increase digital service delivery, and look to expand broadband access, strengthening enterprise security will be critical. From 2017 to 2020, cyberattacks increased an average of 50 percent[1] and a recent study found that ransomware cost governments nearly $19 billion in recovery costs and downtime in 2020.[2] Fortunately, state and local governments have a prime opportunity to improve their security posture with cloud technologies and funding from the American Rescue Plan (ARP). This can help states and localities address security gaps and invest in robust, long-term security solutions.

In conjunction with Amazon Web Services (AWS), the Center for Digital Government (CDG) surveyed chief information officers (CIOs) and security professionals from state and local governments across the country to better understand their current security challenges and barriers preventing them from quickly moving to the cloud, and how cloud technologies can address these issues and strengthen their incident response strategies. The research shows how impactful the cloud can be in helping government organizations create an effective defense against today's evolving threats.

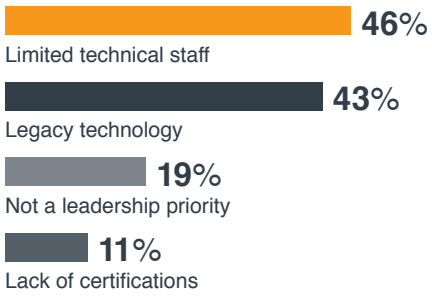
Modernizing security infrastructure in state and local government

State and local governments must modernize their security infrastructure to better protect the ever-growing volume of sensitive data they collect. Forty-three percent of CDG respondents said legacy technologies prevented their organizations from adopting the cloud more widely within their department or agency.

However, staffing constraints and lack of prioritization also play a role. Forty-six percent of CIOs and security practitioners said limited technical staff hindered cloud adoption within their organizations and 19 percent said the main obstacle was that their leadership team doesn't prioritize cloud security. Eleven percent of respondents also said a lack of certifications delayed cloud adoption.

When asked how they would rank their organization's current cybersecurity maturity, only 31 percent of security leaders and professionals said their cybersecurity threat model is established. Twenty-two percent said their organizations were currently building a policy around cybersecurity threats and 19 percent said they were currently implementing their cybersecurity threat model. What is even more telling is that 11 percent of respondents said their organizations had taken an ad-hoc approach and didn't have a threat model in place at all.

Top challenges in adopting the cloud



In a recent Government Technology and AWS webinar, Chuck Grindle, digital government practice leader for AWS, highly recommended state and local governments advance their cybersecurity maturity.

"Organizations have turned to the cloud to help secure and deliver infrastructure and applications to their constituents and workforce, but we also need to be mindful of cybersecurity risks and continue to evolve our security strategies to protect sensitive data," he said.

By accelerating cloud adoption — and leveraging available federal funding to make this critical investment — state and local governments can improve threat detection and incident response, and strengthen their long-term security posture.

The power of the cloud

Cloud security benefits governments in several ways. The cloud helps government organizations expand their information technology (IT) capacity, alleviating one of their biggest pain points of limited technical personnel and a lack of certifications among their staff. Cloud security solutions can also integrate artificial intelligence (AI) and machine learning (ML) capabilities that help automate threat detection and incident response. These solutions provide the scalability, flexibility, and agility governments need to respond to security events.

Retired General Keith Alexander, founder, chairman, and co-CEO of IronNet Cybersecurity — a Collective Defense and network detection and response platform, and AWS Advanced Technology Partner — said although state and local governments can develop security solutions in-house, partnering with a cloud service provider can be more cost effective and allow them to accelerate security modernization.

"The problem I see today for all state and local governments is how do you build the IT infrastructure you need? And the answer is running it yourself is often very expensive. The cloud is an extremely valuable way for governments to advance their IT services," Alexander said.

Moving to the cloud can increase application and system reliability and redundancy for government organizations, according to Alexander. It also enables all levels of government to work more collaboratively to take a holistic or whole-of-state approach to cybersecurity or adopt what Alexander and IronNet refer to as Collective Defense.

Grindle said that although the COVID-19 pandemic has been a catalyst for governments to accelerate cloud adoption, leadership is still important as these organizations navigate their cloud journey. As governments consider moving more of their applications and systems to the cloud, they must be strategic about assessing risks in their environment and identifying the right solutions that will effectively address these risks. This way, they can make sure any federal funding they receive is used in the best way possible.

Once state and local governments perform this due diligence, they should look for a cloud partner who offers solutions with built-in security and privacy controls that align with leading cybersecurity frameworks, such as NIST 800-53.3 The right partner should also offer a robust range of services, including serverless computing platforms that allow organizations to run code without provisioning or managing servers and low-code and no-code development tools that streamline application development and deployment. These solutions can also minimize attack vectors without significantly increasing technology burdens or costs for government agencies.

State and local governments are expected to face an estimated $225 billion budget shortfall in the coming year — even with pandemic-related federal aid.[4] As they contend with increased budget uncertainty, they can leverage available federal funding to address their security risks.

"The ARP is an opportunity for leaders within state and local government to shore up their security posture and position their organizations for the future," Grindle said. For more information about AWS, please **contact us**.

This piece was developed and written by the Government Technology *Content Studio, with information and input from AWS.*

Endnotes
1. https://gcn.com/articles/2020/09/04/cyberattacks-state-local-government-climbing.aspx?m=1
2. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/
3. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
4. https://thehill.com/policy/finance/economy/535452-states-local-governments-face-225-billion-budget-shortfall-study

MAXIMIZING EFFICIENCIES AND SECURING THE ENTERPRISE

Maria Thompson, Leader Cybersecurity, AWS, underscores: "State and local governments need to look at multiple streams to fund cybersecurity initiatives outside of traditional state funding paths. The American Rescue Plan, mentioned within this article, is a great opportunity and one of many government funding options available."

The pandemic created situations where many organizations increased their use of cloud services to ensure continuity of mission-critical services. This shift impacted security teams that were budget strapped and under resourced. These teams now had to contend with hybrid cloud infrastructures, remote endpoints, and a more complex security monitoring requirement. Asset visibility, compliance, and continuous monitoring was and still remains a challenge. This can be complex but is achievable by embracing the opportunities that secure cloud services can offer. Capabilities like automation can greatly reduce the workload for those organizations with a low security head count.

> "Capabilities like automation can greatly reduce the workload for those organizations with a low security head count."
>
> *Maria Thompson, Leader, Cybersecurity, Amazon Web Services*

A May 2020 Government Accountability Office audit report identified 24 states that estimated spending between $43.8 million to $67 million during FY 2016 through 2018 on security audits. These states also estimated upwards of 500 hours expended on a single federal assessment. These audits impact the efficiency and ability of security teams to prioritize current threats and risks to their environment.

In summary, state and local government teams need to maximize efficiencies across their increased areas of responsibility. "My goal at AWS is to work with organizations to establish a secure cloud strategy, which includes leveraging existing toolsets for hybrid environments, and building automation and orchestration into the infrastructure where possible," says Thompson.

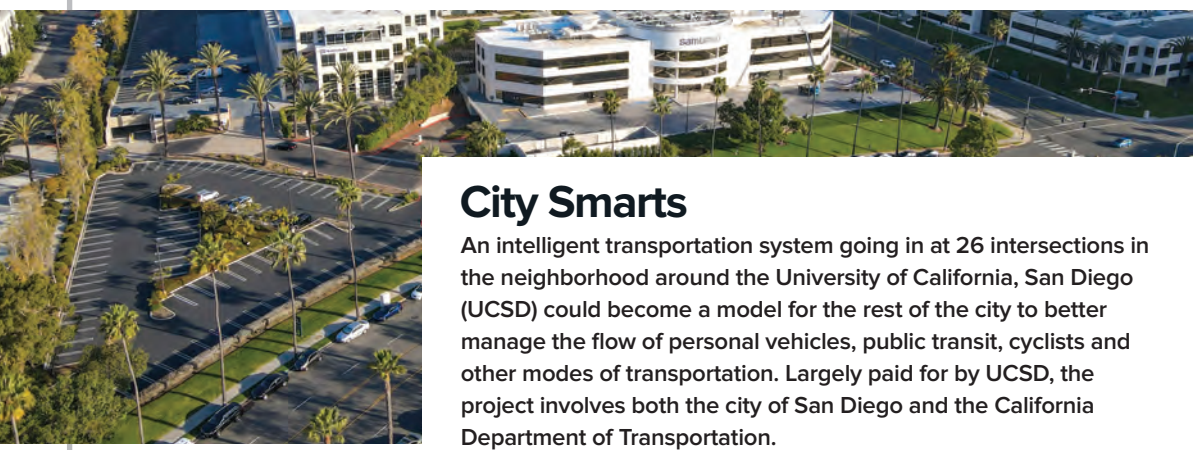
Numerous states have deployed cloud solutions that may fall within ARP funding streams such as cybersecurity. Visit our ARP microsite to learn more: https://www.govtech.com/aws-arp-rescue

PRODUCED BY: government technology

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

FOR: aws

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation across the globe. With AWS, you only pay for what you use, with no up-front physical infrastructure expenses or long-term commitments. To learn more, visit **aws.amazon.com/stateandlocal/digital-government.**



City Smarts

An intelligent transportation system going in at 26 intersections in the neighborhood around the University of California, San Diego (UCSD) could become a model for the rest of the city to better manage the flow of personal vehicles, public transit, cyclists and other modes of transportation. Largely paid for by UCSD, the project involves both the city of San Diego and the California Department of Transportation.

FINDING FAKES

A bill establishing a National Deepfake and Digital Provenance Task Force was unanimously approved by the U.S. Senate Committee on Homeland Security and Governmental Affairs Aug. 4. The task force would include representatives from the federal government, higher education, and private and nonprofit organizations, and would develop policy and strategies for controlling the malicious use of modified audiovisual content designed to deceive audiences.

Biz Beat

Citizen engagement firm Granicus added to its portfolio with the acquisition of GovQA, a startup focusing on public records request workflows. Granicus CEO Mark Hynes said a lack of trust between governments and citizens paired with an increase in records requests means the move will strengthen the company's platform to offer unified services for communities. Earlier this year, Granicus purchased gov tech startups OpenCities and Bang the Table.

WHO SAYS?

"Net neutrality is a national thing, not a state thing. However, if Congress can't address this issue, then we aren't going to sit back."

govtech.com/quoteoctober2021

MOST READ STORIES ONLINE:

- Florida Moves Forward With Digital Driver's Licenses and IDs
- Terabytes of Deleted Case Data Forces Dallas PD to Revise Policy
- Here's What's in the Bipartisan Infrastructure Spending Bill
- Texas Law Will Block IT Contracts With Some Foreign Vendors
- Labor Dept. to Push Out $500M to Combat UI Fraud, Boost Equity
- Fairfax, Va., Uncovers History With Multispectral Imaging

tech/**bytes**

90%

The rate commuter rail ridership declined in some areas during COVID-19.

2K

The number of hours graduates of an IT job training program at Northern Virginia Community College, in partnership with AT&T, need to earn certifications for tech and security work.

$8.5M

The amount of new funding raised this summer by Champ Titles, a startup aiming to use blockchain to change the vehicle title business.

28%

The percent increase in open cyber-security positions in Idaho in 2020, according to the state's Department of Commerce Director Tom Kealey.

 By Stephen Goldsmith

Get Out the Map

Realizing the untapped potential of Georgia's highway infrastructure with GIS.

Andrew Heath, state traffic engineer for the Georgia Department of Transportation (GDOT), opens our conversation with an intriguing mix of futurism and pragmatism. His view of the power of GIS to transform his department's work comes through loudly as he envisions a future where all GDOT assets, from guardrails to traffic lights to exit signs, are entered into a GIS-based asset management system.

Heath then refocuses on the critical opportunity to build a safer, more sustainable future. In his opinion, building a safer transportation system requires him to experiment with emerging technologies. His view of that future involves a much safer commute, where the state helps provide data in cars to drivers that, combined with connected vehicles, keep drivers safe and public safety personnel informed.

To achieve this grand vision, Heath understands that he must rethink optimal use of GDOT's right-of-way assets. One challenge for his department is identifying and procuring the best viable new solutions, which of course often results in a cycle that takes so long that new solutions or iterations may have emerged by the time it is deployed. To address this issue, Heath needed some outside support.

In 2014, then-Georgia Gov. Nathan Deal dedicated a portion of Interstate 85 (I-85) in Troup County to Ray Anderson, the former CEO of carpet tile producer Interface, who was famous for his dedication to environmental sustainability. After the official dedication, Harriet Langford, Anderson's daughter, had an unfortunate realization — her late father, once known as the "Greenest CEO in America," now had his name on an 18-mile stretch of transportation infrastructure, a major contributor of CO2 emissions. She then dedicated herself to carrying on her father's legacy. In 2015, she founded The Ray, a 501c(3) nonprofit committed to exploring new innovations that can advance sustainability, as well as public safety goals in transportation.

The Ray and the state started their work in 2015 with the very highway named after Langford's father. Today, The Ray "is the premier living laboratory and testbed for transportation innovation" according to Laura Rogers, deputy director for The Ray. Rogers went on to highlight more than a dozen projects the organization has spearheaded along I-85 that "demonstrate how these roadsides, which are severely underutilized assets, can be put to greater use."

The Ray works with GDOT to test new technologies and solutions in a live environment to maximize the potential of transportation infrastructure. One of the tools being explored to understand the untapped potential of highway infrastructure is GIS.

The Ray recently helped to develop a "right-of-way solar mapping tool" that assesses regulatory and environmental conditions in order to determine optimal locations to install solar arrays along the highway. This provides a comprehensive view of protected lands and habitats, as well as proximity to city centers, railroads, and energy transmission and distribution lines. The platform also has digital elevation and surface models that help to anticipate tree canopy coverage, the nature of the surface and elevation levels. It also includes digital twin capabilities to measure societal impacts of solar installation before a project reaches the planning stage of development. All of these layers are used to determine suitability for clean energy generation at different locations.

The same tool is also being used to identify solar energy generation opportunities. According to Allie Kelly, executive director for The Ray, this includes "solar canopies over parking lots, solar attached to parking decks or solar on rooftops." She also highlighted opportunities for infrastructure to expand the electricity grid for clean energy generation opportunities.

Beyond that, Rogers intends to leverage the tool to understand where they can plant vegetation for carbon sequestration or address land erosion for stormwater management. Also, with significant farmlands along Georgia's highways, she hopes to be able to conduct studies to determine where they can develop pollinator habitats to help agricultural farmers keep their crops alive and healthy.

With infrastructure spending increasing, local and state governments have a once-in-a-lifetime opportunity to rebuild America's infrastructure for the better. Creative partnerships with third parties like The Ray, a willingness to try new technologies and a comprehensive spatial inventory will chart a path to the future. GT

Matt Leger, a research assistant for the Innovations in Government Program at the Ash Center, contributed to this column.

Stephen Goldsmith is a professor at Harvard Kennedy School and director of the Innovations in Government Program and Data-Smart City Solutions. The former mayor of Indianapolis, his latest book is *The Responsive City: Engaging Communities through Data-Smart Governance.*

SEEING THE BIG PICTURE

How one agency increased visibility and security across a complex IT environment

Public agencies must be able to identify every device on their networks because any endpoint is a potential attack vector. The experience of the New York City School Construction Authority illustrates how agencies are addressing this, thanks to advances in agentless device security.

Agentless technologies help agencies effectively monitor devices, flag anomalies and manage risk throughout their environments without creating disruption. Agentless tools have emerged because conventional approaches using agents force organizations to install and manage software on servers and endpoints that consume system resources and may cause applications to crash. Public agencies running mission-critical, real-time applications cannot take that chance.

Moreover, many networked devices, especially in the IoT realm, can't support conventional security agents. So while security agents remain appropriate for certain types of devices, agentless technologies enable comprehensive endpoint security that fills agent-related gaps.

The best agentless device security platforms operate passively, using advanced algorithms and expansive databases to reveal anomalous behavior on any connected device, regardless of its operating system.

Securing Network Endpoints

The New York City School Construction Authority had a lot to work through when it decided to deploy an agentless device security platform. The authority builds 10 to 12 schools per year in a school district comprising more than 1,800 buildings and 1,500 current projects. It stores digital data on building designs, financial records, vendor contracts and personal information that requires strong protection.

"A critical factor for us is making sure none of that information slips out of our hands," says Manny Innamorato, chief information officer with the construction authority, which typically runs 200 to 400 active job sites.

The authority is digitizing its data and work processes to reduce paperwork, streamline communications and help employees get their work done in any location. This is essential because half of the authority's workforce typically operates from temporary job sites on construction projects that last anywhere from six months to five years.

The authority's 1,300 employees use about 3,000 devices, Innamorato says. Each work site has two to eight employees who also share the authority's network with vendors, subcontractors and potentially unauthorized users. This poses distinct security challenges — identifying all the devices on the agency's network and making sure they are authorized to be there.

Agentless discovery tools revealed how much the agency was missing. "We've gone from what we thought was about 3,000 devices to about 9,500 to 10,000 devices as of today, which includes IoT and other transitory devices," Innamorato says.

Where are they all coming from? For starters, the wireless connectivity systems in nearby vehicles often try to link automatically with construction site Wi-Fi networks. Work sites also attract people trying to secure free wireless

> "We've gone from what we thought was about **3,000 devices to about 9,500 to 10,000 devices as of today,** which includes IoT and other transitory devices.
>
> *Manny Innamorato, Chief Information Officer, New York City School Construction Authority*

access. And summer interns may try to play online games on authority time.

Moreover, connected devices have disparate applications, security patches, firmware updates and operating systems. How to make sense of all these variables? That's where agentless device security tools prove their worth.

Implementing an Agentless Solution

Getting an agentless device security platform up and running does not have to be complex or time consuming. "We've never really experienced a tool that was so simple to deploy in this agentless way," Innamorato says. "It was essentially just, turn it on and we interfaced it with Azure, with VMware and with other equipment. That was really easy for us to do."

The New York City School Construction Authority partnered with Armis, which provides an agentless device security platform that is hosted in the cloud and delivered through a software-as-a-service model. The platform features a dashboard that provides crucial data about each connected device and all the software and firmware contained within it.

System administrators can perform granular searches of IT environments, sorting by device type and operating system. Alerting policies tell them about any anomalies that signal potential breaches or malware.

Learning algorithms monitor the devices and their recent behaviors. Armis software correlates this data with massive databases containing real-time insight on devices, software, firmware and vulnerabilities, and threats. These features deliver a single point of truth for the entire device ecosystem.

An agentless system implemented properly enables public agencies like the School Construction Authority to assess critical infrastructure and model potential threats, according to Sumit Sehgal, strategic product marketing director for Armis.

"You can't secure what you don't know you have," Sehgal says. "I recommend an approach that allows you to collect baseline information about the devices on your network and how they function in your environment for your specific use case, so you understand what the importance is from a business criticality perspective."

Agency IT leaders must be able to place every device in the context of its interactions within the environment. That means getting solid, reliable data on whether a device is up to date, behaving normally, and communicating properly with upstream and downstream devices.

After the agentless platform establishes a baseline of device visibility and behavior, IT leaders can zero in on their top priorities, such as compliance, system uptime, revenue and service management. "That will help you better secure your environment," Sehgal says, "and it will help you learn what it takes to operationalize the technology and work with your partners."

Results: Better Visibility and Security

The Armis agentless device security platform reveals every device on the School Construction Authority's network, providing complete visibility that enhances overall security and enables strategic planning.

The platform helps answer questions such as how long the device has been on the network and whether it should be there in the first place. "When we first turned on the solution, we started picking up vehicles parked out in front of the building that were trying to attach to our Wi-Fi," Innamorato says. "That was very enlightening to see."

He adds: "Not only do I see the devices, I know the software they have on them. I know the patch levels; I understand the operating system."

Software development is a key component of the School Construction Authority's IT operations — about a third of the staff does operations and customer support. The agentless device security platform pulls insights from these user groups. "We can take a product and really push it down into more of those customer support areas, whether it's cell phone support or desktop support," Innamorato says. "We've pushed the intelligence down to where people are actually maintaining the device systems."

> **"Not only do I see the devices, I know the software they have on them. I know the patch levels; I understand the operating system.**
>
> *Manny Innamorato, Chief Information Officer, New York City School Construction Authority*

The system also reveals whether devices have the construction authority's mobile apps installed on them, and it shows potential vulnerabilities. Data from the devices helps with forming plans to maintain firmware versions on printers, for example. "We now have a much better handle on what those workloads look like," Innamorato says.

Ultimately, comprehensive visibility enables Innamorato and his team to prioritize security threats, matching attention with the criticality of the infrastructure.

"It's helping us to really get a handle on who's on our network today, who's on our guest network and who's temporarily there," Innamorato says. "It gives us a better way to see what's happening at all times and to understand the holes in our infrastructure."

This piece was developed and written by the Government Technology *Content Studio, with information and input from Armis.*

Produced by: government technology

For: ARMIS

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

Armis® is the leading unified asset visibility & security platform designed to address the new threat landscape created by connected devices. Fortune 1000 companies trust our real-time continuous, and agentless protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

Liza Massey

CIO, Marin County, Calif.

Marin County, Calif., CIO Liza Massey has served as a tech leader for a long list of state and local government agencies in California, including Los Angeles and San Francisco. Her resume also includes stints as the leader of a nonprofit tech organization as well as the founder of a private consulting firm. All of this makes Massey an ideal leader for Marin's ongoing work to foster equity with tech, efforts that involve a number of cross-sector collaborations. GT *recently spoke with Massey about the push for equity, community involvement and why it's all so important.*

1 How is Marin County using tech in the service of racial equity?

Marin County has been addressing racial equity in two ways. We've had a data-driven dashboard for some time that includes tracking racial demographics for county employees. We use that to analyze, report and identify where we need to take action to address racial inequities in our workforce. Now, our digital and data teams are working with the Marin County racial equity officer to create a public website. Part of that will be a dashboard, and the purpose of the website and dashboard will be to aggregate data that allows analysis of racial equity in a variety of areas, not just county government employees.

The other initiative is Digital Marin, a county-funded cross-sector project with the goal to create a digital infrastructure strategic plan. We want universally accessible, affordable, reliable, resilient broadband throughout Marin — for everyone. We have taken special efforts to ensure Marin's underserved areas are represented in the needs assessment and the planning process.

2 How are members of affected communities participating in these processes?

Getting community members involved is critical. We've found that, especially with the Digital Marin project, community advocates have to step up and lead the effort; it's the best way to ensure success. One of the guiding principles for us has been that we want to work with the communities. We don't want to assume what they need.

3 Are there other jurisdictions that served as models for fostering racial equity?

Closest to home, the city of San Rafael, which is in Marin County, started a digital equity effort in its Canal neighborhood. It really set a model for partnering with community advocates, but also business stepped in; so did government, schools and nonprofits. We even had private donors writing big checks. Other projects then really followed that model.

Then there are certainly jurisdictions across California that are all doing the same thing. But you can look all over. Memphis has deployed great broadband infrastructure to provide broadband to their citizens. You can look at Philadelphia and their smart city efforts. The way they approached it and developed their plan is something I've looked to as we've developed our plan, but we are doing it differently. We took it all together, and then looked at our community and determined how we need to do it.

4 Why is digital equity so important for Marin?

Equity has been on Marin County's agenda, and there have been actions toward it for some time. The unrest that occurred last year around racial justice really accelerated and showed the importance of it, and I think we're not the only government that felt that way. The Digital Marin project was conceived and funded prior to last year's unrest, and it always had the goal of broadband for all and addressing the digital divide.

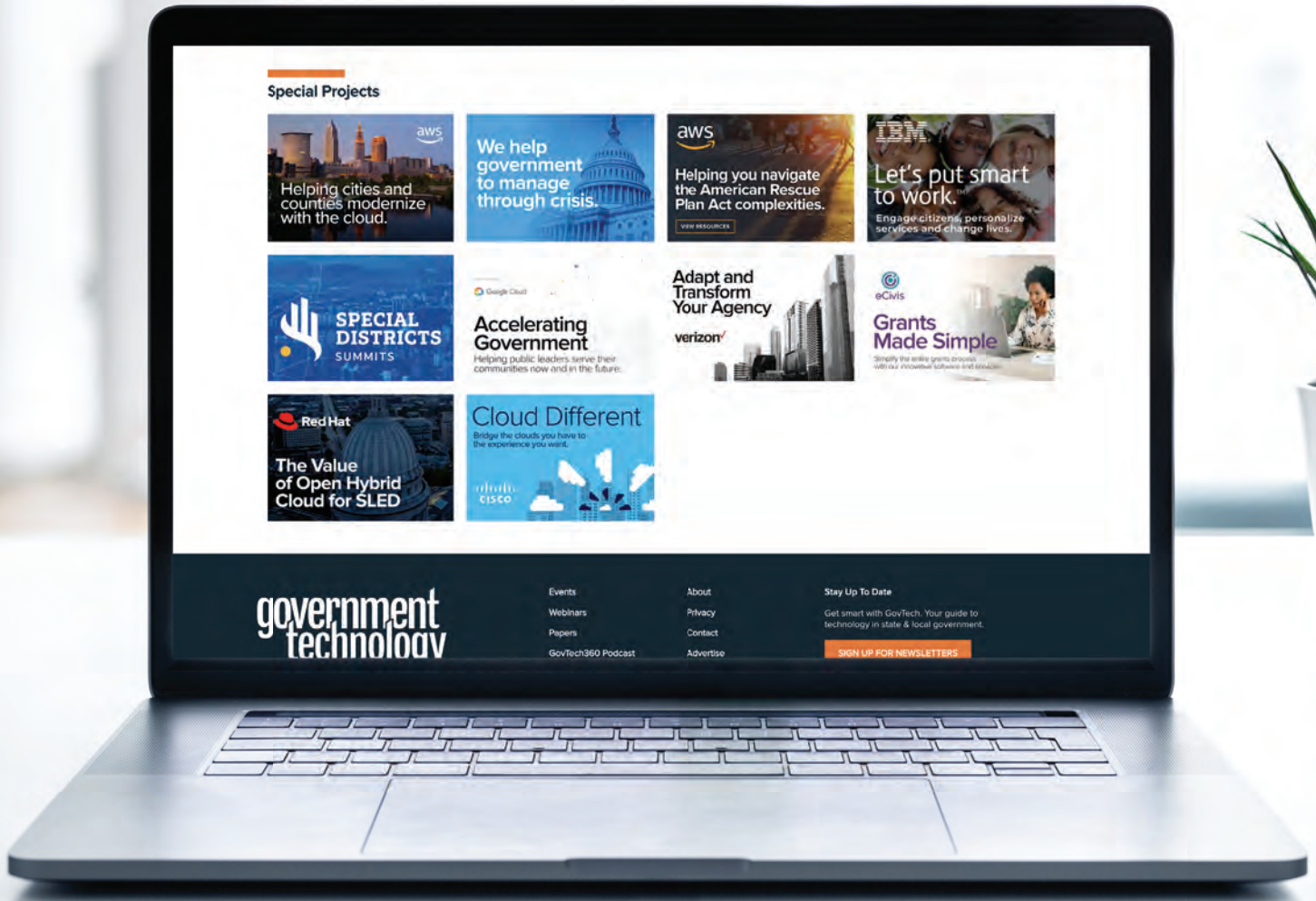
We know the digital divide disproportionately affects people of color. During our needs assessment, we also identified another group that disproportionately experiences the digital divide, and that is older adults. Older adults are the fastest growing demographic in Marin County, so without targeted efforts by the project, we could have 70,000 people in that group experiencing the digital divide. We've looked at the numbers, and we're making a targeted effort to work with representatives of that community. We included them in the needs assessment, but we really need to make sure that we're adequately addressing their needs. GT

— Zack Quaintance, Associate Editor

Take a deeper dive into

government technology

Scroll down to view our Special Projects:
www.govtech.com



A CENTER FOR DIGITAL GOVERNMENT ISSUE BRIEF

CENTER FOR DIGITAL GOVERNMENT

THE CONSTITUENT-CENTRIC EXPERIENCE

From Airports to City Halls, Reimagining the Constituent Experience for the Post-Pandemic Era

As state and local governments look ahead to a post-pandemic future, they're responding to the evolving needs and demands of their constituents. Residents want government service delivery that's fast, convenient and predictable, and they want a digital experience that's as easy and seamless as what they're accustomed to from leading private sector companies.

Agencies across the country have made "improving constituent experience" a top priority, and one important part of achieving that is adopting virtual queuing solutions. With advanced queuing software, constituents can place themselves in line virtually, receive up-to-the-minute information about wait times and then be notified when it's their turn. These solutions not only offer a user experience that's seamless and safe, they also represent a powerful management tool to streamline workflows and reduce bottlenecks.

"Waiting in line, obviously it's a pain point that has existed forever," says Michael Twersky, co-founder and CEO of Whyline, a software company that helps organizations overcome queueing challenges and bottlenecks with smart-scheduling technology. The company's public sector partners include municipal agencies in Providence, R.I.; Lincoln, Neb.; and Seattle, Wash.; as well as large global cities such as Buenos Aires. Whyline also serves numerous companies in the private sector, including multinational banks, Fortune 500 retailers and premiere health facilities. "Folks have acclimated to waiting in line over the years because, historically speaking, there was no viable solution," Twersky says.

That's changing, especially now as agencies assess their plans for post-pandemic service delivery. A wide range of public agencies — from DMVs and permitting offices to schools and public health facilities — are already leveraging smart-scheduling platforms to transform the way they do business.

The right virtual queuing solution can ease their digital transition and help agencies of all kinds innovate for the hybrid, constituent-focused government of the future.

Today's most advanced smart-scheduling platforms are agile and flexible enough to support any organization. Two public agencies that could not be more different — the municipal court of Irving, Texas, and the Seattle-Tacoma International Airport — show the transformational power of virtual queuing, and how any state or local organization can leverage this innovative technology to iterate and improve the way it serves the community.

Irving, Texas: How a Local Agency Eliminated Waiting in Line

Like other local government entities throughout the country, the municipal court system in Irving, a bustling Dallas suburb with more than 240,000 residents struggled with long wait times and a negative public perception.

"Anytime you traditionally think of a court, you think, 'I'm going to wait,'" says Irving Municipal Court Manager Jennifer Bozorgnia. "You have scheduled dockets; you have times

you're supposed to appear. It's all a very formalized process."

When the pandemic hit, the court adopted a virtual queuing solution to process court participants safely and effectively. Rather than waiting months or years to launch, which can be typical of many IT efforts in the public sector, Irving worked with the team at Whyline to launch the new system in just six weeks.

With the new scheduling system, Irving court professionals can place participants in a virtual queue, letting them know exactly when it's their turn to enter the building for their scheduled appointment. It's also more efficient for court employees: Because a participant can upload all necessary documents prior to their appointment, court officials can read and review all documents ahead of time. The system can even be used to direct court participants to those court processes that can be completed entirely online, saving them from ever having to come into the court in person.

That's why the court is planning to expand its use of the platform even after the pandemic subsides.

"It saves time not only for the person who has to come to court, but also for our prosecutors, our judges, our clerks," save Bozorgnia. "It saves them all time."

Seattle-Tacoma International: How an Airport Transformed the Passenger Experience

Lengthy security lines have long been a frustration for airport travelers and personnel alike. And just as in all other aspects of government, the pandemic has altered customer expectations about the airport experience.

One facility, the Seattle-Tacoma International Airport (SEA), is using virtual queuing to seamlessly transition to meet these changing expectations. Under an innovative new pilot program known as SEA Spot Saver, passengers can use their smartphones to schedule a spot in the TSA line in advance. With these digital reservations, travelers can place themselves in a virtual queue and skip the long lines for security screening.

The technology is "transformational," says SEA Manager of Innovation and Systems Todd VanGerpen.

"Airports are always looking to improve their service level, and virtual queuing is probably one of the most important elements we can look forward to in the future," VanGerpen says.

Nearly 95 percent of users in the first month of the program said they were satisfied with the experience. Six out of 10 travelers report spending more money in the airport: By giving passengers more opportunities to grab a latte, linger over a glass of wine or pick up a magazine, Spot Saver helps increase the bottom line for airport vendors.

In addition to improving the customer experience, Spot Saver provides airport officials with meaningful data they can use to adjust screening appointments based on demand. The airport has already expanded the pilot program to additional checkpoints and will be rolling it out to more passengers.

Six out of 10
travelers report spending more money in the airport.

Nearly 95%
of users in the first month of the program said they were satisfied with the experience.

There are longer-term potential benefits as well. If an airport does not have to turn over a large portion of its terminal to accommodate TSA lines, it could redesign those areas to be more useful and more pleasant for passengers. Indeed, virtual queuing could one day be applied to several other aspects of the entire airport experience, including check-in, ticketing and baggage claim, as well as providing accessible options for passengers with reduced mobility.

These two government entities are markedly different. One is a municipal court system in a small city; the other is a massive international airport. But as these use cases demonstrate, smart-queuing solutions can be successfully deployed in virtually any government office, workplace or public space where congestion or inconvenience is an issue. As agencies everywhere focus on serving the new needs of their constituents in the post-pandemic environment, virtual queuing will play a vital role in evolving the constituent experience to make it faster, safer, more convenient and more efficient.

This paper was written and produced by the Center for Digital Government, with information and input from Whyline.

Produced by: CENTER FOR DIGITAL GOVERNMENT

For: whyline

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**.

Whyline was founded to create better, more efficient experiences through the use of virtual queues, dynamic appointment scheduling, and digital capacity management solutions. Currently supporting both governments and the private sector globally, Whyline empowers people everywhere to skip the line and let the software wait on their behalf. **www.whyline.com**

FAST FORWARD

BY JULE PATTISON-GORDON

TWO DECADES IN CYBER

From spam to 'Cyber Pearl Harbor,' experts trace the evolution of IT security from 2010 to the present day and consider what the future might hold.

Just over a decade ago in 2010, state and local agencies were breaking their dependences on desktop computers and paper-based processes, and embracing mobile technologies like smartphones, laptops and even the brand-new iPad. Governments kept an eye on the dangerous side of digital, too. As cyber criminals became more sophisticated, the Obama White House introduced the U.S. Cyber Command within the Department of Defense and states across the country started adding a new chief to their payroll: chief information security officer.

Now in 2021, cybersecurity has become a national — and international — focus, with ransomware attacks hitting consumers at the gas pump and the supermarket. Increasingly ubiquitous technologies like artificial intelligence, the cloud and IoT are reshaping the threat and defense landscape.

Government Technology caught up with cybersecurity experts about how the past decade shaped our present cybersecurity picture and what the next 10 years may bring.

CASHING IN

Hackers in the early 2000s may have been largely aiming to boost their reputations, experiment with technology and cause disruptions, according to security software firm Sophos. But ensuing years introduced new motivations, and the 2010s saw cyber criminals increasingly realize their vast potential to make money, Pennsylvania CISO Erik Avakian told *GovTech*.

Hackers in the mid-2000s and early 2010s used botnets to power massive pharmacy spam campaigns that tried to sell recipients what were often counterfeit or illicit goods, according to Sophos. But criminals' business models then advanced to tactics like stealing and selling personally identifiable information (PII) online.

"We've seen a shift from simple hacking to the monetization of information and data," Avakian explained. "[As] they realized they could gain profit from it, we saw this shift from just hacking to stealing data where they can post online and sell it for profit."

Ever-more popular ransomware attacks see malicious actors encrypt victims' data and hold files locked until the targeted

SHUTTERSTOCK.COM

parties pay up. Cyber criminals recently have graduated to "double extortion" in which they seek payment twice — first to unencrypt the stolen files, and second to refrain from publishing them.

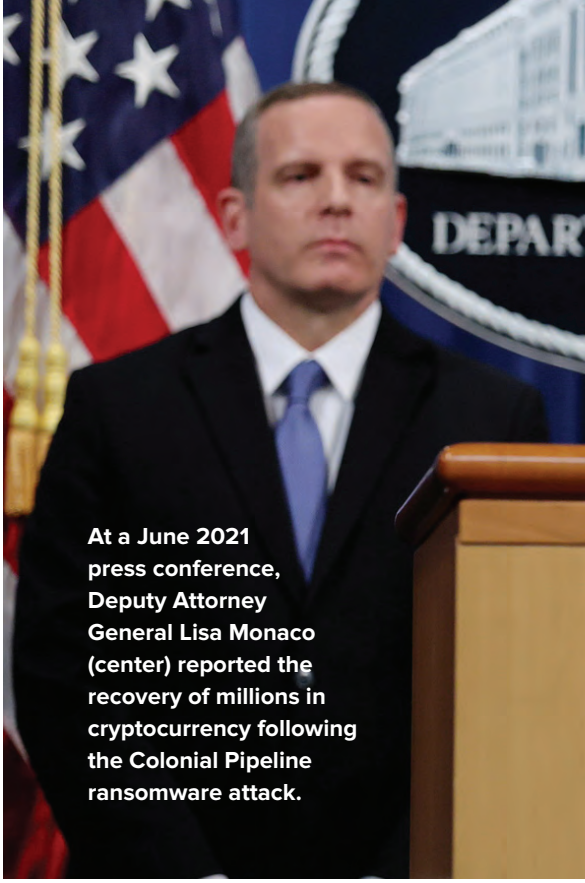
Bad actors may view the public sector as a particularly tempting victim, because agencies' efforts to be transparent to constituents also let hackers identify which ones have desirable information, said Mark Weatherford, CISO for risk management company AlertEnterprise. His former roles include serving as California and Colorado state CISO and Obama administration deputy undersecretary for cybersecurity.

"Because so much information is public, and publicly available, it may be a little easier for bad guys to figure out where, how and when they can target state and local government organizations" compared to large private organizations, Weatherford said.

The past couple years have seen ransomware rise to new heights of disruption, taking cities and critical infrastructure offline. Atlanta city personnel and residents became unable to use a variety of digital government services following a 2018 attack, and 2021 saw ransomware threaten critical infrastructure operators like Colonial Pipeline.

Hackers also seized greater opportunities for social engineering as the 2020 COVID-19 outbreak prompted so many societal activities to shift online, from business to education and shopping. Criminals unleashed a flurry of phishing attempts and other attacks against residents, local agencies, health care and school facilities and private targets in efforts to trick victims during the confusing transition and exploit weaknesses in digital systems not designed for such high-volume use.

Political goals — not just profit — have also become a frequent driver of cyber intrusions conducted by foreign nation-states and domestic hacktivists, Avakian said. 2016 saw Russian hackers strive to undermine the election, and the same year also brought several instances of ideologically motivated hacks that downed government websites or leaked their data. A North Carolina law prohibiting transgender residents from using bathrooms matching their gender identities and Baton Rouge, La., police's fatal shooting of Alton Sterling both triggered retaliatory hackings, to name just a couple of examples.



At a June 2021 press conference, Deputy Attorney General Lisa Monaco (center) reported the recovery of millions in cryptocurrency following the Colonial Pipeline ransomware attack.

THREATS ON ALL SIDES

The past decade taught public officials that threats can come from all angles. The 2013 Adobe breach compromised a trusted brand and demonstrated the necessity of software security, Deb Snyder, former New York CISO, told *GovTech*. The SolarWinds hack — which spread malware to the IT company's clients through infected software patches — has underscored this point, putting "supply chain security" on everyone's lips, as well. California CISO Vitaliy Panych told *GovTech* that his state is currently heightening attention on third- and fourth-party risks, which come from vendors (and vendors' vendors) of everything from IT to legal services.

The field of potential adversaries has widened as well, with cyber crimes no longer the exclusive realm of tech-savvy perpetrators. Attackers now create and sell their malware to other parties seeking to wield high-tech

A DECADE IN CYBER INCIDENTS

2011
Sony is breached, exposing the personally identifiable information of 77 million users, in one of the world's biggest attacks at the time.

2013
Edward Snowden's disclosure of the NSA's massive, covert cyber surveillance alerts the world to new forms of digital privacy and security concerns. Some organizations see this leak by a federal contractor as a wake-up call about the risk of insider threats to the confidential information they hold.

2015
The Office of Personnel Management suffers a breach that exposes sensitive personal information and security clearance files on 22.1 million people in an espionage attack attributed to Chinese state actors. Officials worry that China may use the information to unmask undercover operatives.

2016
Russian actors attempting to sway the elections hack into emails from the Democratic National Committee and Hillary Clinton campaign and share them with WikiLeaks. They also penetrate state voter registration databases. The events spur negative media coverage of the Clinton campaign and trigger concerns over the security of elections.

2017
Credit reporting agency Equifax is breached, exposing personally identifiable information on 147 million people. Roughly 45 percent of the U.S. population is impacted.

ADOBE STOCK

attacks, opening the doors to a wider array of perpetrators, Panych said.

"It's no longer where there are sophisticated adversary elements that have sophisticated knowledge," Panych said. "It's more widespread, horizontally, where your common criminal element can pick up hacking tools and start targeting organizations."

Organizations have also turned their focus inward. Edward Snowden's 2013 exposure of NSA's mass espionage program shocked U.S. citizens and the world with its revelations. But Snyder said that for many agencies, it also delivered a second message: that their sensitive information can be put at risk by contractors and other insiders, and thus emphasized the importance of tightly controlled account privileges.

Major attacks in recent years have taken cybersecurity from an abstract idea to something that impacts the general public's daily lives. A breach of Sony in 2011 revealed details on 77 million customers, alerting organizations to the seriousness of data protection, Snyder said. Public pressure intensified as the 2017 Equifax breach exposed 147 million residents' data, while 2021 ransomware attacks on JBS and Colonial Pipeline hit people at the pump and the dinner table.

Equifax's 2017 compromise and "Experian being hit again in 2020 and exposing credit scores for nearly every U.S. citizen ... started the rise in public ire and public expectation of 'why aren't organizations taking care of our data and what punishment should they suffer when those kinds of things happen?'" Snyder said.

If public pressure wasn't enough to put government on alert, the 2015 Office of Personnel Management breach and 2016 Democratic National Committee hacks revealed just how seriously cyber criminals will go after government.

Constituents increasingly expect government to keep its troves of resident information private, and Europe's General Data Protection Regulation (GDPR) drove forward thinking in the space by offering a model. States like California responded with their own data privacy legislation two years later. Panych said recognition of the growing importance of data is prompting California to seek to ensure that, going forward, its technology adoptions and practices include privacy considerations.

STATES GET SERIOUS

States have responded to the growing sophistication and visibility of digital threats by elevating cybersecurity to an enterprisewide concern and mindset.

States and localities increasingly incorporate cybersecurity recovery into their emergency response planning — alongside terrorism and natural disaster plans, said Avakian. Many agencies are now adopting emerging best practices and strategies like zero-trust authentication in which they require every user and device to verify itself for each interaction, and adoption of technologies that have privacy and security incorporated into the designs, Panych said.

Across the nation, state CISOs now have the ear of key decision-makers.

"Ten years ago, for me to get time or an audience with the legislature [as state

2018

Atlanta internal and external digital systems and devices are crippled by a ransomware attack, as cyber extortionists perfect their techniques. At the time it's deemed the most expensive and extensive cyber disruption to hit a city. A similarly scaled ransomware attack on Baltimore followed in 2019.

2020

IT solutions provider SolarWinds sends out a software patch, not knowing it includes malware from Russian-based actors. The hackers access systems of customers — including government agencies and leading cybersecurity companies. Organizations realize security gaps at third-party suppliers can also bring significant risk.

2021

Colonial Pipeline and JBS pause operations after being hit by ransomware, in separate incidents that disrupt residents' daily lives and spark fears over the vulnerability of critical infrastructure to cyber attack. The incidents down the nation's largest refined oil pipeline and the supplier of about one-fifth of its meat, respectively.

CISO] was almost impossible," Weatherford said. "But today, CISOs are routinely meeting with legislators or briefing legislative players at the beginning of every session."

But despite the increased visibility of cyber leaders within government, states and localities still grapple with legacy technologies and historical technological underinvestment that leaves them open to cyber attack.

Ransomware perpetrators often launch automated mass attacks in indiscriminate attempts to penetrate wide swathes of organizations — and school districts' and local governments' antiquated defenses are especially likely to fall, Center for Internet Security (CIS) President and CEO John Gilligan told *GovTech*.

Agencies struggle both to obtain enough resources and also to know how to use them most impactfully. Organizations need to prioritize evaluating their cyber positions and maturities so they can see where to best invest available dollars, Avakian said. Greater visibility into their networks, data collection and storage practices, and user behavior also are essential to helping identify vulnerabilities and differentiate between normal and suspicious behaviors, Snyder said.

Still, some resources are becoming scarcer. Agencies that traditionally relied on cyber insurance to assist their recoveries also are seeing prices rise

VISITGRANDFORKS.COM

The North Dakota Joint-Cybersecurity Operations Command, part of the Grand Forks Air Base near Emerado, facilitates interstate intelligence sharing.

"Even over the past decade, email threats and phishing attacks are still predominant because people will be people. That's the common denominator, and as long as people are clicking on things they shouldn't be, the bad actors are finding ways to get in."

— possibly out of their reach, according to Dan Lohrmann, chief strategist and chief security officer for Security mentor, and former Michigan CSO and current *GovTech* columnist. (For more on cyber insurance, see *Out of Reach?*, p. 30.) Governments of all levels also struggle to recruit enough cyber specialists, with 36,000 federal, state and local positions currently unfilled, according to *The Washington Post*.

Snyder said agencies will need to establish more hiring pipelines, expand recruitment efforts to include candidates with nontraditional backgrounds and upskill existing staff. Departmentwide cyber awareness training will also be key to effective security, because humans remain one of the greatest chinks in defensive armor, Avakian said. Social engineering remains core to many attacks.

"Even over the past decade, email threats and phishing attacks are still predominant because people will be people," Avakian said. "That's the common denominator, and as long as people are clicking on things they shouldn't be, the bad actors are finding ways to get in."

CALLING ON PARTNERS

Partnerships are helping to bolster efforts. The CIS's Multi-State Information Sharing and Analysis Center (MS-ISAC), formally launched in 2003, provides assistance to supplement agencies' resources and has expanded its membership and offerings in the years since.

Gilligan emphasized the outsized impact of any such organizations capable of offering localities low-cost, easy-to-implement defensive tools that may not be perfect, but which are at least able to thwart run-of-the-mill threats most of the time. Third-party organizations like MS-ISAC also sidestep concerns over jurisdictional autonomy that can deter some states from turning to federal agencies for help, he said.

States are driving their own cross-border collaborations, too, including regional efforts like the North Dakota Joint-Cybersecurity Operations Command, which facilitates interstate intelligence sharing. Many states also work to share tools and build relationships with their local partners, sparing the localities from having to conduct their own procurements and ensuring they know who to call in case of an incident (for more on these jurisdictional partnerships, see *Whole of State*, p. 24).

FEDERAL RESPONSE

Federal efforts over the years have produced advancements like the National Institute of Standards and Technology's first cybersecurity framework in 2014, the Cybersecurity and Infrastructure Security Agency (CISA) in 2018 and the Cyberspace Solarium Commission report in 2020.

But in the wake of SolarWinds, Colonial Pipeline and JBS, the federal government is settling itself into a greater role. President Biden's May executive order signaled intent to deal seriously with cyber problems, and experts speaking with *GovTech* in July expressed tentative optimism that more action, including funding support, would follow.

Biden's order obligates federal agencies and their vendors to follow fairly basic cybersecurity best practices — which is, nonetheless, an improvement, Snyder said. She and others highlighted the need for the White House to press forward with additional measures.

State and local governments need recurring, long- and medium-term funding streams to maintain strong cyber postures — not just one-off grants, Lohrmann said. Gilligan suggested providing federal dollars to more ISACs beyond just the MS-ISAC

so those groups can avoid charging membership dues that block participation from localities with slim budgets.

Some such change may come, with an August national infrastructure proposal delivering $1 billion over four years to state, local and tribal governments for upgrading their software and hardware against cyber attacks. It also could bring more cohesion to national cybersecurity policies and greater information sharing across agencies by budgeting $21 million to the newly launched Office of the National Cyber Director. Cyber experts applauded the 2021 appointment of Chris Inglis, a former deputy director of the National Security Agency, to the post, while waiting to see if he would get sufficient funding to be impactful.

FUTURE READY?

As they eye the next decade, states need to employ emerging strategies and technologies to detect, deflect and mitigate threats. Artificial intelligence applications, particularly machine learning and predictive analytics, will increasingly help departments detect potential threats and amplify staff efforts, Avakian said. Organizations are already improving their post-attack analysis to better understand the kinds of defenses that could stave off future attempts, according to Gilligan, and more agencies are adopting zero trust and context-informed security analysis, said Panych.

The shift to remote work has also enabled states to draw upon experts from around the U.S. — and even around the world — for cyber projects, expanding recruitment abilities, said Lohrmann.

Ransomware, social engineering and "commoditized threats" that see criminals buy PII and malware from other criminals are unlikely to go away soon, and compromised IoT devices may become an increasing risk.

Additionally, foreign nation-states that have been unable to compete with the U.S. in traditional military might are finding that cyber attacks put them on more even offensive footing and are unlikely to back away, said Lohrmann. This adds pressure to ongoing efforts to establish rules of cyber warfare and aggression. In June 2021, Biden told Russia that 16 certain critical infrastructure sectors should be off-limits to hacking, and NATO said this year that it would consider military response to cyber attacks.

The past decade has shown malicious actors continually raising the stakes. Practitioners fear that attacks may eventually progress from disrupting essential infrastructure to actively destroying it. The World Economic Forum has warned that nations should anticipate a massive, society-changing cyber incident, with impact on the scale of the COVID-19 pandemic.

"There are a lot of people that are predicting that we're going to have a major incident, whether that's the Internet going down for 10 days, or power grids all go down," or some other worst-case scenario, Lohrmann said. Such an event coming to pass would redefine how organizations and society view cybersecurity.

"You're also going to see a different paradigm with cybersecurity following that," Lohrmann said, "because organizations that are hit with major ransomware, or a major cyber attack, tend to act a lot differently than ones that haven't."

jpgordon@govtech.com

A FRAMEWORK TO FOLLOW

States and localities often refer to federal guidelines when measuring their cybersecurity posture and planning for improvements to reduce vulnerabilities. President Biden's May 2021 executive order, therefore, may offer hints as to where cybersecurity is headed around the country. Here are some of its components:

INCIDENT REPORTING. Requires — and contractually permits — federal software vendors to report cyber incidents to agency clients and, often, CISA.

MODERNIZING DEFENSES. Requires federal agencies to follow cyber hygiene practices like zero trust and multifactor authentication, create plans to protect sensitive data, and encourages the adoption of secure cloud services.

SUPPLY CHAIN SECURITY. Federal contractors selling — and federal agencies buying — software that performs critical functions will have to ensure products meet certain security requirements and are used in secure ways.

- ☑ NIST will outline a Software Bill of Materials for vendors to provide, helping attest to secure development.
- ☑ Vendors will be encouraged to voluntarily put labels on consumer IoT offerings that attest to the security of the devices and their development processes.

CYBERSECURITY SAFETY REVIEW BOARD. A public- and private-sector group will be created to investigate major cyber incidents, threats, vulnerabilities and responses.

STANDARDIZED CYBER RESPONSE PLAYBOOK. A common (but flexible) cyber incident and vulnerability response playbook will be created for all federal agencies to follow. It will include standard definitions of key cyber terms.

INCIDENT, VULNERABILITY DETECTION. Agencies will improve efforts to catch issues early and provide CISA with data. CISA will report on its efforts to hunt threats on agency networks without interrupting their operations or getting their permission first.

INVESTIGATION AND RESPONSE. Federal agencies and IT service providers will need to collect and maintain federal IT system and network logs and provide them to CISA and the FBI as needed to support their handling of cyber incidents and risks.

A CENTER FOR DIGITAL GOVERNMENT ISSUE BRIEF

CENTER FOR DIGITAL GOVERNMENT

How Local Governments Can **Get Ahead** of Their Threat Opponents

Agencies of all sizes, in every discipline, and at all levels of government have at least one thing in common: they're facing a large and growing cybersecurity threat landscape. Government entities are vulnerable to a multitude of attacks, including hacking, ransomware and distributed denial-of-service.

Many agencies are simply unprepared to defend themselves against these assaults on their own. There are two important questions organizations need to address: How do they know when they need help, and how can they determine the best cybersecurity partner? Once agencies have selected a partner, a key to success is knowing how to measure the value added from such a relationship.

Organizations are Under Attack

The cybersecurity attack surface has grown considerably in recent years, and government agencies are among the biggest targets of bad actors.

Many employees continue to work from home at least part of the time, as the hybrid work model becomes more common. Oftentimes workers use their own devices rather than those sanctioned by the IT department. The lack of visibility and sufficient security on devices or network connections gives attackers new opportunities to penetrate systems.

Incidents such as ransomware and distributed denial-of-service are on the rise. Workers and managers are also increasingly vulnerable to phishing and malware attacks. Furthermore, the shift to cloud services can give cybercriminals additional opportunities to gain access to systems and data.

"Information could be leaked that is proprietary or sensitive, involves financial information or contains content that a threat actor could use for identity theft," says Rex Johnson, director and practice leader of cybersecurity consulting services at Computer Aid Inc. (CAI). "That's a large area of risk for an agency to mitigate."

Defenses are Lacking

Even as they face this array of threats, a lot of government agencies that operate with limited budgets and resources are simply not prepared to defend themselves against increasingly sophisticated attacks.

Many public sector organizations at the local level do not have the budget to create sufficient security teams and invest in the latest tools to detect and stop attacks. Agencies must compete for cybersecurity talent against private sector businesses that in many cases have more resources.

Government entities are vulnerable to a multitude of attacks, including hacking, ransomware and distributed denial-of-service.

"With over 300,000 open cybersecurity jobs nationwide, many smaller agencies do not have mature cybersecurity programs in place," says Frank Ury, senior client executive at CAI and a director of the Santa Margarita Water District Board in Rancho Santa Margarita, Calif. "Bad actors recognize these agencies' vulnerability, and therefore are likely to make them targets for attack."

What's particularly concerning is attackers can be present within agency systems for a substantial amount of time before they are detected. This gives them the opportunity to learn about vulnerabilities and enables them to gain access to and steal more data.

Even among agencies with adequate security programs, there is oftentimes a sense of complacency about security.

"But every agency is vulnerable, regardless of the financial resources," Ury says.

How to Know When Help is Needed

Agencies need to conduct an honest assessment of their existing security programs and be on the alert for signs they need to bring in outside expertise to bolster their defenses.

One of the best ways to determine if an organization needs help to address cyber risk is to conduct a readiness or current-state assessment, Johnson says. With such an assessment, a government agency can identify what it is doing well and where it needs help.

"Make sure it's an objective assessment from someone who's qualified to understand their business and how government works," Johnson says.

Aside from an assessment, a sure-fire way to know that assistance is needed is a steady increase in the frequency of attacks such as ransomware. This is a clear sign that the current security program — tools as well as procedures — may be failing to protect systems and data.

The lack of a coherent incident response plan or procedures for dealing with breaches is another indicator of a need for improvement.

Choosing the Right Partner

Once a government organization determines that it needs outside expertise for help with securing its infrastructure, it must decide which partner is the best fit.

One important attribute of a service provider is extensive experience, not only in cybersecurity but in the particular areas in which the agency is focused. For example, if a government entity is involved in healthcare services, the partner should have knowledge of healthcare issues, regulations, threats, etc.

The ability to customize services is also vital. An agency needs a partner that can provide exactly what it needs in the way of protection. This includes understanding the specific systems the agency has in place and the potential security issues and vulnerabilities.

"Even though there are security frameworks, there really is no cookie-cutter approach to cybersecurity," Johnson says. "Organizations need to consider their operational needs and how to protect their most critical information and assets. It is not the same for everyone."

Organizations can't just assume a security partner will deliver on all its promises and provide the expected value from the relationship.

Of course, the partner also needs to meet the budget requirements of the agency. This is especially important for small, local agencies with limited resources.

Getting the Most Value from a Partnership

Organizations can't just assume a security partner will deliver on all its promises and provide the expected value from the relationship.

A partner should be willing and able to sit down with agency leadership, as well as IT and security executives, and discuss security strategy and how to build a roadmap to carry out the strategy over a given time period, Ury says.

Priorities should be set, so the most pressing risks are addressed first and less important issues are dealt with at a later time. This way, agencies can deal with and mitigate the truly urgent risks right away rather than use up resources on multiple projects at the same time.

An agency and its partner should create and implement a cybersecurity strategy within the context of the budget requirements of the agency. If all goes well with a security partnership, the agency should be able to significantly increase its level of cybersecurity maturity over time.

This paper was written and produced by the Center for Digital Government, with information and input from CAI.

CLICK HERE to arrange a meeting with CAI cybersecurity experts. Or, you can reach Rex via email at Rex.Johnson@cai.io.

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: CAI®

About Rex Johnson, Director and Practice Leader — Cybersecurity
Rex has over 30 years of senior level management experience encompassing IT, cybersecurity, privacy, digital forensics and analysis, and enterprise risk management. He is a frequent speaker on cybersecurity addressing national and international audiences with Gartner, Secure World, and the Information Systems Audit and Control Association.

About CAI
CAI is a leading business technology services firm committed to helping private and public organizations drive value, improve productivity, and enhance customer experience. The firm specializes in digital transformation services, including application management, strategy and consulting, intelligent automation, contingent workforce solutions, IT service management and business analytics. **CLICK HERE** to learn more about CAI.

Whole of State

Governments are embracing a larger role in collective cybersecurity. Here's what that looks like on the ground.

BY ADAM STONE

When the Colorado Department of Transportation got hit by a ransomware attack, state IT leaders called for backup, bringing to the table the cyber expertise of the National Guard and the crisis-response skills of the state's emergency management office.

"They came in and created a battle plan: Here are the five things that we are focusing on," said Colorado's CISO at the time, Deb Blyth. (Blyth has since returned to the private sector.) "They helped us really get organized around what resources we were allocating to each thing, rather than just chasing every little blip and anomaly all over the network."

In the present, escalated threat environment, experts agree, no one should be going it alone.

"With a dramatic uptick in ransomware attacks across the country, governors, state chief information officers and state government executives are designing and implementing programs to strengthen local partnerships in cybersecurity," according to a recent report from the National Association of State Chief Information Officers (NASCIO).

This "whole of state" approach helps governmental entities to leverage their combined resources and expertise.

With an emphasis on partnering, state IT leaders can deliver high-impact tools to local jurisdictions. "State governments are increasingly providing services to county and municipal governments, including endpoint protection, shared service agreements for cyber defensive tools, incident response, and statewide cybersecurity awareness and training," NASCIO reports.

At the city and county levels, the pooling of resources is proving an effective means of staying ahead in an increasingly volatile cyber environment.

What does whole-of-state cyber look like on the ground?

We asked state and local IT leaders to share their best practices.

NYC CYBER COMMAND

At the New York City Cyber Command, Senior Advisor Mitch Herckis can't imagine approaching the present situation with anything less than an all-hands-on-deck mentality.

"Cyber crime affects everyone, it impacts the entirety of the city, and that means we can't be secure in isolation," he said. "The more resilient we all are, the better off we'll all be. For New York City to be the most cyber-resilient city in the world, that requires us all to be aware of the threat and to have the tools necessary to defend ourselves."

With that in mind, Herckis and his team have taken steps to ensure that ordinary citizens are aligned in the fight. To that end, the NYC Secure App delivers free, real-time protection to users' mobile phones. The app has been downloaded more than 200,000 times.

"It will alert you to unsecure Wi-Fi networks or unsafe apps on Android systems — the things that people experience in their daily lives that could impact their digital safety," he said.

Cyber Command also has teamed with the nonprofit community by partnering with Quad9, a free service that replaces the default Internet service provider or enterprise domain name server configuration. Together they've worked to secure some 3,000 public Wi-Fi access points across the city.

"If someone's connecting to these, it will block known malicious sites, ensuring people aren't steered to places that are intended to hurt them," Herckis said. "It's a way of trying to protect residents when they're utilizing public infrastructure to connect to the Internet."

Small businesses also play a key role in Herckis' whole-of-state vision.

He has teamed with the city's small-business services office to deliver basic cyber hygiene information to the business community. "We wanted to give them things that they could apply to their own businesses: small steps that they could take to be more secure," he said.

Getting public participation in a shared cyber mission has its challenges. The problem seems so big, and individuals may have a hard time understanding how they personally can help in the fight. Herckis tries to keep the messaging simple and tangible.

"People quickly become overwhelmed by the scope of the problem. So what can be done? You can show them the small steps that can be taken to significantly improve their security, rather than focusing on the big, scary problem," he said.

At the same time, NYC Cyber Command also partners with larger public and private entities, from the police department to critical infrastructure operators, in order to coordinate cyber preparedness and response. "We need all of that coordination," Herckis said. "We'll all be stronger if we're working together as a community of cyber defenders."

UNEVEN PLAYING FIELD

"Some have cybersecurity teams that have funding, that have good security programs – and then some have nothing. They may have no IT staff, no security personnel, no funding, no security program. There is a huge pendulum swing between the haves and the have-nots."

YORK COUNTY, VA.

In York County, Va., one high-profile cooperative effort has the IT department working with the Department of Elections to push out basic guidance to all jurisdictions.

"I'm on the advisory board for that effort to create a set of standards for all the jurisdictions involved with elections: Here are the best practices of what everybody needs to be doing," said Deputy Director of Information Technology Timothy Wyatt.

The team is pushing out processes and procedures, describing administrative controls and modeling system security plans. "For a lot of these smaller and even medium-sized jurisdictions, these are all new concepts," Wyatt said. "They're not sure how to tackle it, where to start."

With a population of 68,000, York isn't the biggest county in the state, but Wyatt said his team still has valuable know-how it can share with other counties looking to bolster their cyber efforts.

"This isn't the private sector, we're not in competition with each other," he said. "We're all one family, and we're all about helping the citizens. They may live in your county, but maybe they work over in one of those other jurisdictions. The more we help each other, the better it is for everyone."

There's precedent for this approach: A whole-of-state cyber strategy mirrors similar efforts in public safety. "We do police software hosting for a neighboring city. We have a regional 911 system with various other cities and jurisdictions," Wyatt said. "If it's good for the community, we embrace that very readily."

Looking beyond the elections initiative, Wyatt's team has also engaged in direct efforts to enlist citizens and the business community in the cyber fight. He's worked with a regional development center for small businesses to deliver cyber basics, and has shared similar information directly with small businesses.

> "Overall, we have to take a collective stance to try to fight against the wave of cyber hackers and everything else. We have to share resources. We have to collaborate and work as a team."

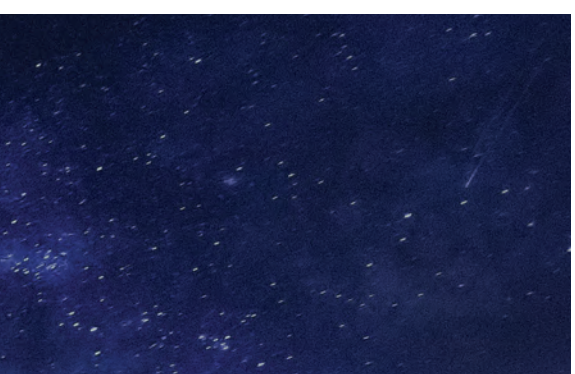
Wyatt has found he can build strong partnerships by making the message personal.

"We focus on what they care about, what's important to them," he said. "For businesses, their reputation with their customers is critical. If they get hacked or they leak data, it could lead to the loss of their brand, the loss of customer confidence."

He's reached out to citizens as well, for example with information about securing personal information online. Here, the best route seems to be the gentle touch. "I'm not here to tell you what to do or what not to do," he said. "I'm here to educate on how risky a certain activity may be. Then you choose how risky or how safe you want to be. I just want to give you the tools and the knowledge."

All these efforts — the outreach to individuals and businesses, as well as the intra-governmental push — help to drive a stronger countywide cyber environment. To Wyatt, this seems the only sensible approach to an ever-expanding problem.

"Overall, we have to take a collective stance to try to fight against the wave of cyber hackers and everything else," he said. "We have to share resources. We have to collaborate and work as a team."



COLORADO

There's often profound inequality among local jurisdictions when it comes to cybersecurity capabilities.

"Some have cybersecurity teams that have funding, that have good security programs — and then some have nothing," said former Colorado CISO Deb Blyth. "They may have no IT staff, no security personnel, no funding, no security program. There is a huge pendulum swing between the haves and the have-nots."

From a statewide perspective, it's imperative to find means to close that gap. That includes taking cooperative steps to share information and insights. "The local governments provide critical services to their communities," Blyth said. "We can't just leave them out to dry."

At present there is no formal mechanism for driving a whole-of-state approach in Colorado, but it's coming. The Governor's Office of Information Technology, the Secretary of State's Office, emergency management officials and others are all working to define the rules of the road for a formal collaborative approach.

> "The local governments provide critical services to their communities. We can't just leave them out to dry."

"We would like folks from across state and local government to be able to sign up, to self-select in order to become incident responders. We would give them some consistent training and then have agreements in place so that when someone calls us, we can all help," Blyth said.

Details have yet to be worked out. There are jurisdictional questions: Will the effort reside in the Governor's Office of Information Technology, or elsewhere? And how will it be funded?

"One challenge has to do with statutory authority," Blyth said. "Right now, no one is really in charge of cybersecurity standards at an overarching policy level. Each local government is sort of in charge of their own domain."

In the long term, jurisdiction will have to be made explicit.

Then there are the budgetary questions. Blyth doesn't want to create an unfunded mandate — telling jurisdictions how to conduct their cyber efforts without giving them adequate means. One possibility is for a state entity to aggregate homeland security funds that are designated for cyber defense. By pooling those resources, the state could potentially get bigger bang for the buck, sharing common solution sets among multiple local entities.

That's just one possible approach. State-level officials and local leaders are still working out potential funding schemes, which will eventually be brought to the Legislature. The goal is to have a formal plan in place by summer 2022.

If this vision comes to fruition, it could change the nature of cyber response across state and local authorities.

"It would mean we could be less about responding to emergencies, and instead be more proactive," Blyth said. "Right now, we've got 60 people from a state and local perspective who share cybersecurity threat intelligence information across the state. But there are about 3,000 local governments in Colorado. We can improve the cybersecurity landscape significantly, if we can just get more participation."

The 2018 ransomware attack on the state's Department of Transportation helped to prove the point. By collaborating with others, the IT team was able to have a state of emergency declared around that incident — the first time that had ever been done for a cyber breach.

"That gave me access to the Colorado National Guard. It gave me funding and resources that I needed to recover," Blyth said. "The Guard, they are cyber-trained warriors. They are really good at finding the holes in the environment, creating a battle plan, getting systems back online. We had great success with that approach at the state level, and now we want to replicate it at the local level."

NORTH CAROLINA

In North Carolina, three county and town CIOs are spearheading an effort to drive greater collaboration around cybersecurity issues. The North Carolina Local Government Information Systems Association (NCLGISA) has assembled an "IT strike team" led by Rowan County CIO Randy Cress, Henderson County CIO Mark Seelenbacher and Scott Clark, CIO in the town of Fuquay-Varina.

The CIOs agree that a cooperative approach is the best way to ensure an adequate defensive posture across disparate state and local entities, where the availability of skills and resources can vary widely.

"Especially during cyber events, there's a lack of resources around incident response," Cress said. "It requires a diverse skill set, and the whole-of-state approach is what brings together all those resources."

The effort here involves the state IT department, the emergency management agency, the National Guard and law enforcement, including the FBI and others. In addition, the Center for Public Technology at the University of North Carolina School of Government plays a leading role in coordinating efforts.

State legislation requires local governments to report all cyber attacks to the state Department of Information Technology, which works with the North Carolina National Guard and the emergency management agency to coordinate the response.

In practice, that initial report sets the wheels in motion, with key players huddling to assess the scale of the issue. "We start with a scoping call to assess the impact on the agency," Seelenbacher said. "All relevant responders will work to determine the total impact of the event."

These formal conclaves have given rise to a strong peer-to-peer network, through which local cyber pros are able to pool their intellectual capital. "At the local level there's always someone who knows that they can contact the strike team," Seelenbacher said. "Even if they don't know [who] to call up to at the state level, they at least get to us."

Clark described an incident in which all these pieces came together: a ransomware attack on a North Carolina city. The local emergency management team was already active in support of COVID-19 needs, and the strike force was able to leverage that presence to help drive the response.

"Especially during cyber events, there's a lack of resources around incident response. It requires a diverse skill set, and the whole-of-state approach is what brings together all those resources."

"Emergency management helped run the incident. They were basically the incident commander, while the IT staff got all the resources focused on the job at hand and repairing. It was a very good model of interagency and interdepartmental support," he said. "Working together, they were able to rebuild the system, and it is in better shape now than it was before."

As a result of that event, the local CIO has now stepped up to share his expertise with others who may find themselves under attack. "It shows how this can be a real win-win," Clark said. "We threw all these resources at it, and now he's giving back to the community and helping others that had the misfortune of having a cyber attack. It shows how this approach helps improve the state as a whole." gt

adam.stone@newsroom42.com

A CENTER FOR DIGITAL GOVERNMENT Q&A

DIGITAL STATES PERFORMANCE INSTITUTE

The Bridge Builders:
Government and Education Affairs

CIOs and technology leaders are inundated with both immediate and long-term issues to resolve, often with too few resources. What can we learn from past experiences and from experts on the front line? In this interview, Michael Esolda, SHI's National Director of Government and Education Affairs (GEA), shares his vision for amplifying the role that technology solutions providers play in creating connected, thriving communities and discusses how GEA teams are game changers in the industry.

Q After serving more than 30 years as a public servant and government official, what has surprised you about working on "the other side?"

After retiring as CIO for the Woodbridge Township Municipal Government, School District and Police in New Jersey, I joined SHI in early 2020. In March, everything became simultaneously critically important and urgent, especially keeping students connected to learning and communities seamlessly functioning. What surprised me most was realizing how much we — CIOs, local and state leaders, and technology providers — need each other. Technology was the thread that kept society from unraveling! People from disparate backgrounds and situations came together to rapidly achieve vital solutions for our communities.

Q What do you want CIOs, CTOs and government leaders to know about technology solutions providers?

It's important to know that those of us dedicated to public sector are devoted to helping leaders and community members stay connected; to improving the communities we live and work in through technology; and to facilitating success for our public leaders. We're not just trying to sell for the sake of selling. We genuinely care.

Now more than ever, technology solutions providers offer strategic partnerships and proactively design innovative ways to improve the health of our communities.

Within our GEA team, we're designing ways to ensure diversity, equity and inclusion are at the forefront of educational efforts and public health and safety initiatives. E-sports is a great example of how we're pushing the boundaries of what it means for a student to participate in K-12 sports — no matter their physical ability.

Q What's on the horizon that state and local government officials should be considering?

Future successes depend on what we are providing our students today. Good school systems are the backbone of economic development and an engaged citizenry.

If I were still a CIO, I'd be looking with great interest to legitimize esports within my school districts, support the Girls Power Tech program in partnership with Cisco, and provide guidance to higher education cybersecurity and career-focused tech programs within local high schools.

Q How can state and local governments optimize technology to ensure an engaged citizenry?

We must be relentless in the pursuit of digital equity for all residents — from WiFi-connected school buses to MiFi devices, and from technology hardware refreshes to secure networking — accessibility to technology is foundational.

In addition, we need to think of GEA teams as robust partners who help build bridges among the key players. We facilitate federal funding at all levels of government and education and grants applications; we sit on national panels with other decision-makers; and we listen reverently to end users to understand what they need and how to be better. Being open to leveraging technology providers and, specifically, their government and education affairs teams as consultants and technology connoisseurs, would be the simplest, most efficient thing technology leaders can do to ensure optimization.

SHI's Government & Education Affairs

With deep and diverse government knowledge, SHI's GEA team helps educate and inform Account Executives and Government Leaders about public sector policies and technology innovations to enhance relationships; to grow opportunities; and to increase technology success for end-users in our communities.

Because each of member of the GEA team has served in a public sector leadership position, they are able to leverage a vast network of other IT leaders to contribute to Public Sector solutions and connectivity.

For more information, please visit: SHI.com
And to learn more about Michael Esolda, please connect with him on linkedin: https://www.linkedin.com/in/michaelesolda/

Out of Reach?

Cybersecurity insurance is becoming harder to get, and some insurers are backing out of the market altogether. Where does that leave government?

BY PAMELA MARTINEAU

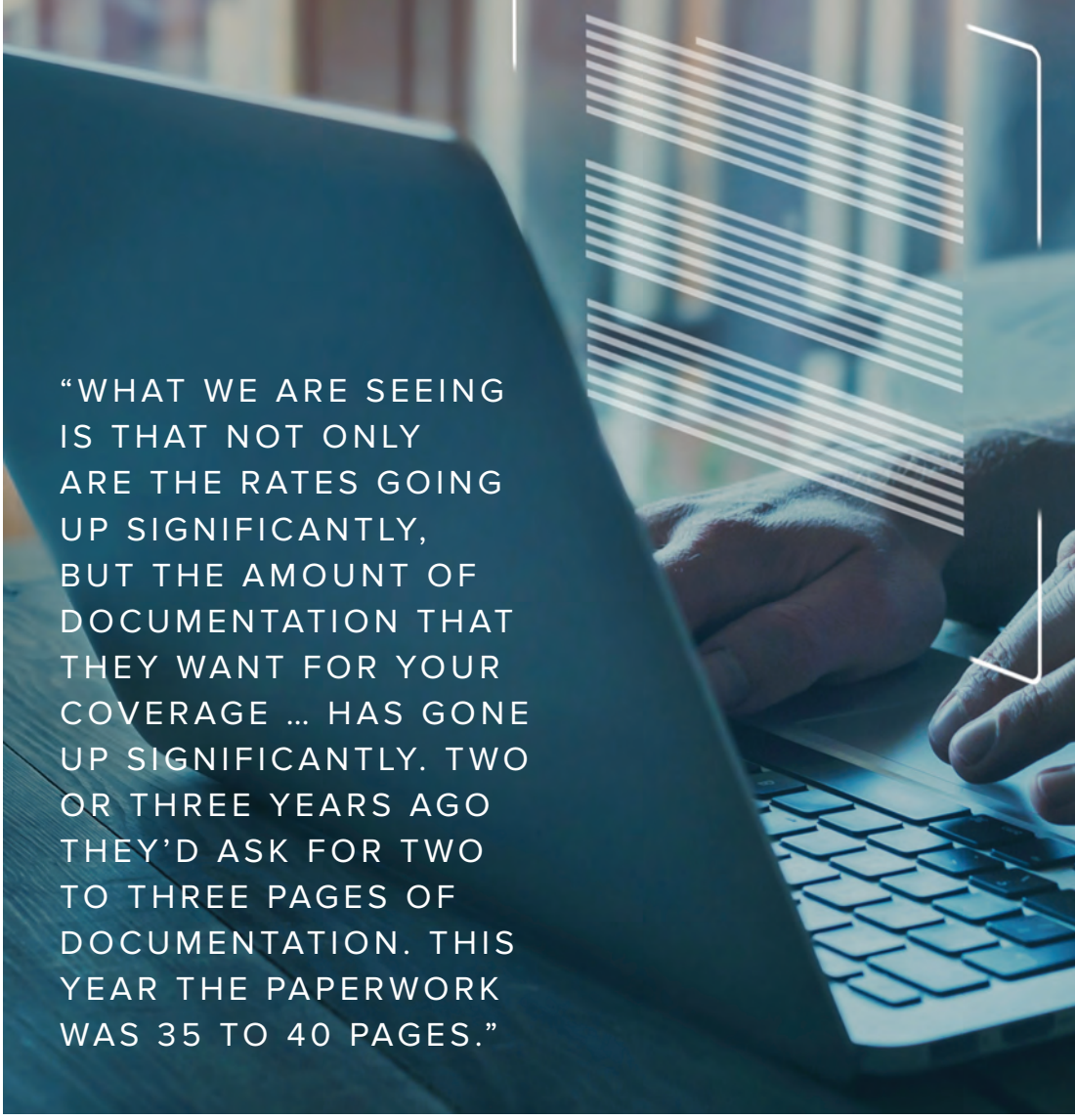
SHUTTERSTOCK.COM

Cyber attacks: They've shut down government agencies, global companies and even a gas pipeline that serves nearly half the population along the East Coast of the United States. Experts say the attacks are growing in number and severity and that governments and businesses need to make it a priority to guard — and insure themselves — against them.

But as cyber attacks and ransom demands grow, cybersecurity insurance is becoming increasingly expensive for the insured and the insurer. The upward trajectory in cost has some experts wondering if the cybersecurity insurance market will remain economically viable. Local and state government officials wonder too, but many believe the cost of not having cybersecurity insurance is incalculable, making their jurisdictions vulnerable to extreme losses in capital, human health and safety, not to mention reputation.

In this ever-evolving cybersecurity landscape, insurers are asking much more of their clients in terms of staff training and technological safeguards. And looming over the shifting insurance market is a philosophical question: Do larger policies incentivize bad actors to increase their attacks and ransoms because they know governments have insurance policies and can pay large ransoms? Yes, say some experts, but not having insurance is a risk government simply cannot take.

"I think it is critical coverage for our world today ...," said Mike Volk, vice president of Cyber Risk Solutions at PSA Insurance and Financial Services. "It is becoming necessary to operate."



"WHAT WE ARE SEEING IS THAT NOT ONLY ARE THE RATES GOING UP SIGNIFICANTLY, BUT THE AMOUNT OF DOCUMENTATION THAT THEY WANT FOR YOUR COVERAGE ... HAS GONE UP SIGNIFICANTLY. TWO OR THREE YEARS AGO THEY'D ASK FOR TWO TO THREE PAGES OF DOCUMENTATION. THIS YEAR THE PAPERWORK WAS 35 TO 40 PAGES."

WHAT IS CYBERSECURITY INSURANCE?

On the most basic level, cybersecurity insurance covers the liability and costs incurred by an entity as a result of a cyber attack. The policies can cover not just the losses of the insured, but sometimes the policyholders' customers as well. And if an attacker demands ransom to release stolen data or unlock a system, policies often pay these costs as well.

As cyber attacks have evolved to a new level of sophistication in recent years, many cybersecurity insurance policies have added core services. Many policies offer negotiators to interact with attackers. Often, these negotiators are able to bargain ransoms down or convince attackers to release some data before they release all of it, as a way to show they are acting in good faith. Policies also often provide a team of forensic experts to come in and study the nature of the breach, its depth and its breadth.

"They also will look at what was stolen," added Volk. "I've seen initial ransoms that were high and then were negotiated down when forensics realized the extent of the attack."

Policies that cover third parties impacted by an attack offer post-attack services such as sending letters, or calling or emailing customers or other users of a breached system, to inform them that their data has been compromised. Legal support and reimbursement for interruption of business also are often covered.

Some coverage plans send experts out to local and state governments to conduct tabletop emergency activities in which they simulate an attack and guide clients through the process of response. They also develop cyber attack response plans with clients that enumerate, step-by-step, the actions to take after an attack.

MORE EXPENSIVE, HARDER TO GET

Cybersecurity insurance experts and government officials alike report that cyber attacks are increasing and, as a result, policy premiums are going up. Underwriters also are asking much more of potential clients in terms of information on the application and training of staff.

SHUTTERSTOCK.COM

One of the problems in the cybersecurity insurance space is that there is no reliable data on the number of cyber attacks. No central clearinghouse tracks the events, and some businesses don't report them. Governments, however, are more likely to report them due to their mandates for transparency, but the attacks still aren't tracked globally. The lack of data makes it difficult for insurers to calculate risk. But anecdotally, experts and government officials report nearly unanimously that the attacks have increased dramatically.

"There is a sense of urgency ... a recognition [by local governments] that this is a big problem and a growing problem," said Brian Nussbaum, assistant professor in the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany.

"Attacks are increasing," said Alan R. Shark, executive director of the Public Technology Institute. "The pandemic was a wake-up call ... with the more remote workforce, people were unwittingly clicking on things they shouldn't have. ... In the remote environment, not everyone had the best practices in place."

And growing threats means a growing price tag for insurance. According to a 2021 Government Accountability Office (GAO) report on cyber insurance, a recent survey of insurance brokers revealed that more than half of their clients saw price increases in cyber policies of 10 to 30 percent in late 2020. Industry sources also told the GAO that insurers are reducing coverage limits for some industry sectors, including health care and education.

Shark worries that the upward trajectory in attacks, and subsequently insurance premiums, will make cybersecurity insurance unsustainable for both the insurer and the insured.

"Some [insurers] are getting out of the business," said Shark. "Some are upping the requirements to get coverage and upping the premiums."

Phil Bates, chief information security officer for the state of Utah, has seen the increase in premiums firsthand.

"The premiums have gone up quite a bit in the last year and we have heard from other states that their premiums were going up too and their coverage was going down," said Bates. "Now there is a higher deductible than we had before and that is pretty much across the board."

Alan R. Shark of the Public Technology Institute said more and costlier attacks are shrinking the cyber insurance market.

"TODAY ... THERE ARE SOME CYBER INSURANCE COMPANIES SAYING, 'YOU KNOW WHAT? THIS IS WAY TOO EXPENSIVE. WE ARE GOING TO STICK TO TRADITIONAL LINES OF INSURANCE.'"

Despite the increased cost, Bates says there is still great value in having a policy in place. "But if the cost keeps going up, we are going to have to look for other solutions because it is not feasible for governments to afford them [the policies]," he added.

According to Bates, some states are informally discussing moving to a self-insurance program where they would pool their resources with other agencies within their states to cover costs of attacks and possibly even ransoms.

"As you see costs go up, people will get more creative," Bates added.

Peter Miller, chief security officer for Orange County, Fla., says the underwriting requirements to obtain cybersecurity insurance have exploded in recent years and now resemble one of the many audits he is required to undertake each year. Miller says the dramatic increase in documentation demands occurred in 2020.

"What we are seeing is that not only are the rates going up significantly, but the amount of documentation that they want for your coverage ... has gone up significantly," said Miller. "Two or three years ago they'd ask for two to three pages of documentation. This year the paperwork was 35 to 40 pages. ... They go into a lot of detail."

Miller says insurers want to know what kind of cyber awareness programs

governments have in place, and if they don't have one, insurers want one implemented. Some insurers will offer to do the training. Orange County purchased a training module to educate staff about phishing attacks, which are the No. 1 vector for cyber attacks in his county, according to Miller. The program sends out fake phishing scams via email. If an employee clicks on the fake phishing link, they are automatically redirected to an educational module that instructs them on the dangers and types of phishing scams. Days or weeks after they have completed the module, they will be sent another fake link. If they click on the fake link again, they must repeat the training module.

Miller also said cyber intrusion events — instances of phishing emails or other attempted breaches of the system — have increased dramatically in the last six months.

"In the last six months I have seen more activity than in the last 10 years," he said. "It is definitely interesting times."

Some recent cyber attacks against local and state governments have been stunning in their breadth and ransom demands. CISOs and insurers across the nation have taken note.

Shark, the executive director of the Public Technology Institute, says the increase in ransoms and the sophistication of the attacks is dramatically shifting the market. Insurers have gained more control in calling the shots on what local and state governments need to do to get the policies and how they must react in the event of an attack. Often, insurers will demand that jurisdictions call them first to notify them of the breach — before state attorneys general offices or other law enforcement. And some insurers are running a cost benefit analysis and getting out of the cyber market altogether.

"Today ... there are some cyber insurance companies saying, 'You know what? This is way too expensive. We are going to stick to traditional lines of insurance,'" said Shark. "Others are upping the requirements and the premiums."

According to a report by Chainalysis Insights, a cryptocurrency blog, in 2020, total cyber ransoms paid by victims reached $350 million, a 311 percent increase over the previous year (most cyber ransom demands are made in cryptocurrency). Chainalysis also expects these ransoms to rise.

Shark says despite the increase in premiums, cybersecurity insurance is still a good idea for local and state governments.

"But does it make governments a target?" he asked.

"IT SEEMS TO BE THE CONSENSUS OF PEOPLE IN THIS SPACE THAT RANSOMS HAVE GONE UP IN PART BECAUSE OF CYBER INSURANCE. BUT ARE THEY GOING UP BECAUSE IT IS CLEARER AND CLEARER HOW DISRUPTIVE RANSOM ATTACKS CAN BE? IT IS HARD TO PULL THESE THINGS APART."

DOES INSURANCE INCREASE ATTACKS?

Shark is not alone in asking whether cybersecurity insurance incentivizes bad actors to launch more attacks and ask for larger ransoms because they know governments have the coverage and can pony up for the ransom.

"It seems to be the consensus of people in this space that ransoms have gone up in part because of cyber insurance," said Nussbaum, of the University of Albany. "But are they going up because it is clearer and clearer how disruptive ransom attacks can be? It is hard to pull these things apart."

To guard against higher ransoms, Volk, of PSA Insurance and Financial Services, advises businesses and local governments not to share their insurance limits.

"If a criminal knows your limits, they know where to start the negotiation," said Volk.

Shark says recent trends in legislation could put another damper on the cybersecurity insurance industry. Three states are weighing legislation that would ban local governments from paying cyber ransoms, even if they are funded through an insurance company. The proposed laws seek to decrease ransom attacks by taking the paying of ransoms off the table. Shark says the bills would strip insurers of the power to decide whether paying the ransom is more cost effective than paying for the local government to restore the system.

"If this is successful and local governments were banned from paying a ransom, this would really hurt or destroy the cyber insurance market," said Shark. "If that local government is prohibited from paying a ransomware fee, then the insurance company has its hands tied. They'll say, 'This market is not for us. ... We are out of here when it comes to the public sector.'

"It has an enormous chance of backfiring and reversing the very things these well-intentioned laws are trying to do."

Miller, of Orange County, believes cybersecurity insurance does entice bad actors to launch cyber attacks. He cites as evidence what he calls a "weird" analogy of some overseas companies buying ransom insurance in the event an employee is kidnapped.

"What happens then is they are kidnapped because these people know they work for a company and there is a policy and they will be guaranteed money," said Miller.

Still, Miller, other local government officials and many cybersecurity experts maintain that having a cyber insurance policy is a necessary risk mitigation measure in the current climate. What's unclear is how the market will continue to shift in response to evolving threats. gt

pamelamartineau@yahoo.com

government technology

INNOVATION IN GOVERNMENT®

The Best of What's New in Artificial Intelligence and Machine Learning

States and localities ramp up efforts to automate tasks and become more data-driven.

carahsoft®

Kick-Started by the Pandemic, AI and ML Adoption Isn't Slowing Down

State and local governments are dramatically expanding their deployment of artificial intelligence (AI) and machine learning (ML), moving the use of these technologies from theoretical to practical.

Chatbots are one example. These tools gained a foothold in public sector contact centers during the COVID-19 pandemic as agencies and departments struggled to cope with unprecedented demand for unemployment insurance benefits and other social safety net services. Chatbots and intelligent agent technologies expanded contact center capacity and took pressure off human contact center agents by providing automated responses to routine questions.

In Colorado, for instance, a virtual agent system deployed by the state's Department of Labor and Employment in summer 2020 was expected to handle more than half of the traffic coming into the department's contact center. Like many state unemployment insurance programs, Colorado's was inundated by claims from residents who lost their jobs during the pandemic, resulting in long wait times and busy signals for those seeking help. At the height of the crisis, an average of 8,000 calls a day were going unanswered.

"We should not have that long of wait times, and the department knows that," said Colorado State Sen. Chris Hansen, who worked on a series of reforms to the state's unemployment system. "And the department has brought significant new resources to bear."

A National Trend

Similar activity is occurring across the nation.

About 34 percent of counties plan to implement new chatbot technology in the next 12 to 18 months, according to the Center for Digital Government's (CDG) annual Digital Counties Survey. Almost 40 percent of counties responding to the 2021 survey already had chatbot solutions in place and many of them intend to upgrade those systems within the next year and half.

The numbers are even higher for state agencies. More than 80 percent of states have chatbot technologies in place and about 40 percent plan to upgrade those systems in the near future, according to CDG's most recent Digital States Survey, conducted in late 2020. Among the states that haven't implemented chatbots yet, all intend to adopt the technology within 18 months.

"This whole concept of contactless customer service has become really important. That's a key driver," says Bob Woolley, former chief technical architect for the state of Utah who is now a CDG senior fellow.

Woolley saw the trend firsthand as a judge for the Digital States Survey.

"Of the states I reviewed, more than half had chatbot projects underway," he says. "And some of them were enterprise in scope — they were very big."

Security is another growing AI use case. More governments are using AI in the form of machine learning to scour system activity logs to detect suspicious behavior that may signal a cyberattack. Intelligent software can automate this task and perform it at a scale that's difficult for humans to match.

"States have been great at creating these massive logs of stuff, but they often don't have any idea what's in them," says Woolley. "They didn't have enough hard drive resources, didn't have the right tools and didn't have enough people to review them."

In most cases, governments aren't deploying AI tools themselves, adds Woolley. Instead, they're acquiring AI-powered cybersecurity capabilities through security service providers and chatbots through software-as-a-service arrangements.

"They're working with partners who have this expertise," says Woolley. "That's what all of our top-tier states are doing. They realize they don't have these skillsets in house."

Broader Deployment Challenges

Although states and localities are moving rapidly to take advantage of AI and ML, the first wave of deployments often focused on individual programs or tasks: chatbots, for example, that answer questions about unemployment insurance claims or help utility customers restore service.

Broader and deeper use of AI will require governments to rethink traditional data management policies and upskill IT teams.

"One of the key policy challenges is data should be shared by default," says Woolley. "We've been talking about that for years — but when you do it, good things really can happen."

Better data sharing is particularly important as governments attempt to use AI to understand and address complex issues like recidivism, which are shaped by a broad range of factors and may involve data from corrections, law enforcement, education, social services programs and more.

In addition, government IT teams will need to hone their skills around consulting with business agencies to understand their

requirements and apply effective AI solutions to those problems.

"IT organizations really need to be asking line-of-business leaders what kinds of information and insights they need to be effective. A lot of them aren't asking that question, so that's a big gap," says Woolley. "IT teams get locked into doing the same old, same old — but when you get into analytics, AI and ML, you really need to listen to what your customers need."

Poised for Growth

These and other barriers must be addressed as governments expand their use of AI and ML — and they clearly intend to use these powerful tools more frequently and in new ways.

More than 50 percent of state, city and county governments say they intend to upgrade their data analytics capabilities over the next 18 months, according to CDG surveys. In other words, AI activity kick-started by the pandemic shows no sign of slowing down.

"I expect the growth to increase dramatically," says Woolley. "Sometimes over the years, we've seen the adoption of technologies move slowly and then suddenly spike. This is one of those times."

Accelerating AI Adoption

Chatbots			
	Cities	**Counties**	**States**
Not using; plan to implement in 12-18 mo.	**37%**	**34%**	**17%**
In use	**15%**	**15%**	**44%**
In use; plan to upgrade in 12-18 mo.	**13%**	**25%**	**39%**
AI/ML for Cybersecurity			
Not using; plan to implement in 12-18 mo.	**23%**	**20%**	**28%**
In use	**23%**	**32%**	**28%**
In use; plan to upgrade in 12-18 mo.	**26%**	**29%**	**25%**
Business Intelligence/Data Analytics			
Not using; plan to implement in 12-18 mo.	**10%**	**7%**	**2%**
In use	**34%**	**33%**	**37%**
In use; plan to upgrade in 12-18 mo.	**55%**	**53%**	**59%**

Source: CDG Digital Cities, Counties and States Surveys

From Call Center to 'Experience' Center

In the contact center of the near future, information will be so readily and intuitively available that constituents can get most questions answered and applications processed without relying on agent-intensive processes. In this Q&A, ***Nathan Hamrick,*** *principal solution consultant for public sector at Genesys, discusses ways that organizations can use AI and intelligent automation to deliver a modern experience.*

What call center opportunities are top of mind for government IT and business leaders?

Self-service and automation are top of mind. A majority of calls that come into contact centers today are people looking for basic information, such as status updates or frequently asked questions. By using self-service and automation as their frontline, contact centers can focus their resources on callers who have issues or concerns that actually do require agent assistance. The overall result is shorter queues and happier customers.

How do AI and ML improve the user experience and streamline processes?

AI — and machine learning automation in particular — can increase the speed at which information is delivered, whether to the agent or customer. In our increasingly instant world, users expect information as soon as they ask for it. Making customers wait longer than necessary is a sure way to ensure a negative experience. By streamlining information — whether through bots on the customer-facing side or agent assistance tools internally — contact centers can present information in a timely fashion to both users and agents.

What technologies simplify the adoption of AI solutions?

Voicebots and chatbots are a great place to start. They're increasingly easy to develop and deploy, and they address the need for self-service. Bots typically utilize AI components like natural language understanding (NLU) and self-learning. NLU is a crucial component to voicebots in particular, because you don't want to frustrate customers by having them constantly repeat themselves to obtain the information they're looking for. With NLU, users simply state what's on their mind or what they need, and they have more of an open-ended conversation instead of being forced into a particular menu, as is typical in legacy interactive voice response applications.

Given employee retirements and high turnover, how are organizations using AI and ML to address gaps in subject matter expertise and institutional knowledge?

Agent assistance is a great example of how AI can improve both the agent experience and the customer experience. An agent assistance solution detects keywords within a spoken or written dialogue, and then uses those keywords to automatically present helpful information to the agent. In the case of new hires or agents who lack subject expertise, this type of solution not only saves time, it provides "training wheels" for the agent until they're up to speed. AI models like agent assistance can also learn from agent feedback. Agents basically agree or disagree with the information that the AI presents, which helps the AI solution continually refine what it provides based on the context.

How can call centers effectively integrate AI as they modernize?

My advice would be to start small. Although AI solutions are more user-friendly today, each has its own complexities. Starting small gives organizations time to learn the ins and outs of utilizing AI and familiarizes them with the benefits and pitfalls. That helps them develop a strategy to scale effectively in the future. FAQs are one example of a small start that can deliver a great impact. By putting FAQs on a chatbot, one of our customers reduced call volume for basic information by 75 percent. Having those FAQs also sets up contact centers for more advanced capabilities like intent monitoring, where the AI analyzes conversations and points out the questions customers might have.

How do you see contact center services evolving?

The better NLU engines get, the more automation we'll see. This ranges from simple self-service to more complex conversational transactions with customers. One major goal is to present an AI dialogue so well that the only way your customers can distinguish between an AI interaction and a human interaction is by the solution's explicit transparency about the nature of the interaction. An important clarification is that AI doesn't necessarily replace human agents. Rather it handles routine or repetitive information so human agents can focus on more nuanced and complex interactions with customers.

GENESYS™

Give your constituents

SUPER HUMAN SERVICE

Customer experience software to deliver on the promise of digital government

Learn more at
genesys.com/government

Why Wait? Simple Strategies Put AI and ML Within Reach

Organizations no longer need data scientists and customized applications to make an impact with AI. In this Q&A, ***Chris Haas****, strategic business executive for Google Cloud Public Sector, discusses how state and local agencies can use AI and ML to improve government services and make life easier for workers.*

What AI and ML opportunities are top of mind as governments navigate the future of work and service delivery?

There are many. One theme is using AI and ML services — things like translation, automated document processing and intelligent virtual agents — to make government services more accessible for everyone, including people who have disabilities, don't speak English or can't travel to facilities. Another theme is around applying AI and ML to become more efficient in things like processing documents, which can help organizations justify their programs and quantify their impact. Finally, there is a big benefit to using AI for things like predicting, identifying and mitigating potential cyberattacks — especially as remote work and digital services expand the attack surface.

How can AI and smart automation improve collaboration and productivity across teams?

The idea is to ease the mental load on workers and help them be as productive as possible by giving them things to stay on track and make work easier. For example, Gmail can automatically present a nudge asking email senders what they'd like to do if their email goes unanswered. Gmail's Smart Compose capabilities suggest how to complete sentences when users type an email or other document. More comprehensive solutions consolidate email, collaboration, document editing and other functions into a single unified workspace and then apply AI to predict and suggest which sets of documents a worker may need when they open the workspace.

Where else are technologies like AI and ML making an impact?

One of the biggest areas is in social services and benefit programs. Call centers were completely overwhelmed due to the pandemic, and our Contact Center AI product suite let them add hundreds of thousands of virtual agents overnight. Most of these programs also were using paper-based, manual document processing that couldn't keep up with the high volume of requests during the pandemic. Using Google Translate and Document AI to translate documents and automate document processing enhanced the speed and accuracy of processes these agencies perform day in and day out. AI also helps identify duplicate, improperly documented and fraudulent requests early in the process, which saves time and money.

How can organizations best take advantage of these technologies?

You don't have to be a data scientist or develop custom models to be effective. There are very good AI solutions that are purpose-built for specific use cases and don't require customization, such as our Vision AI. I would start there. A software engineer can do what's needed, and the solution will likely address a lot of the organization's needs. Over time, software engineers and others can expand their skillset to retrain custom models in lightweight ways for slightly different use cases the generalized AI doesn't accommodate. For example, Google Cloud's AutoML products can be used by non-data scientists to retrain our best-in-class AI models for more custom use cases. Just remember that the AI solution is only one part of a larger automated processing use case, and organizations need to plan for how AI is going to be incorporated into that bigger process so it can be used efficiently.

What should organizations consider as they adopt AI and ML?

AI is more accessible than ever before, but it still requires some expertise and a track record of generating real customer value. Pick partners that can meet your needs and demonstrate customer experience depth and breadth. As you implement AI, don't trust the AI straight away. Make sure that a human is always validating what the AI is doing before you build it into a full automated process. Once you trust the AI, you can start automating implementation.

How can leaders overcome cultural barriers when adopting these technologies?

The pandemic proved the impact AI can have in times of crisis. Don't slow down now. Instead, continuously modernize and apply the lessons your teams learn deeply into your culture. Then apply those same innovations across agencies using dedicated teams to continue quickly iterating through new applications of AI.

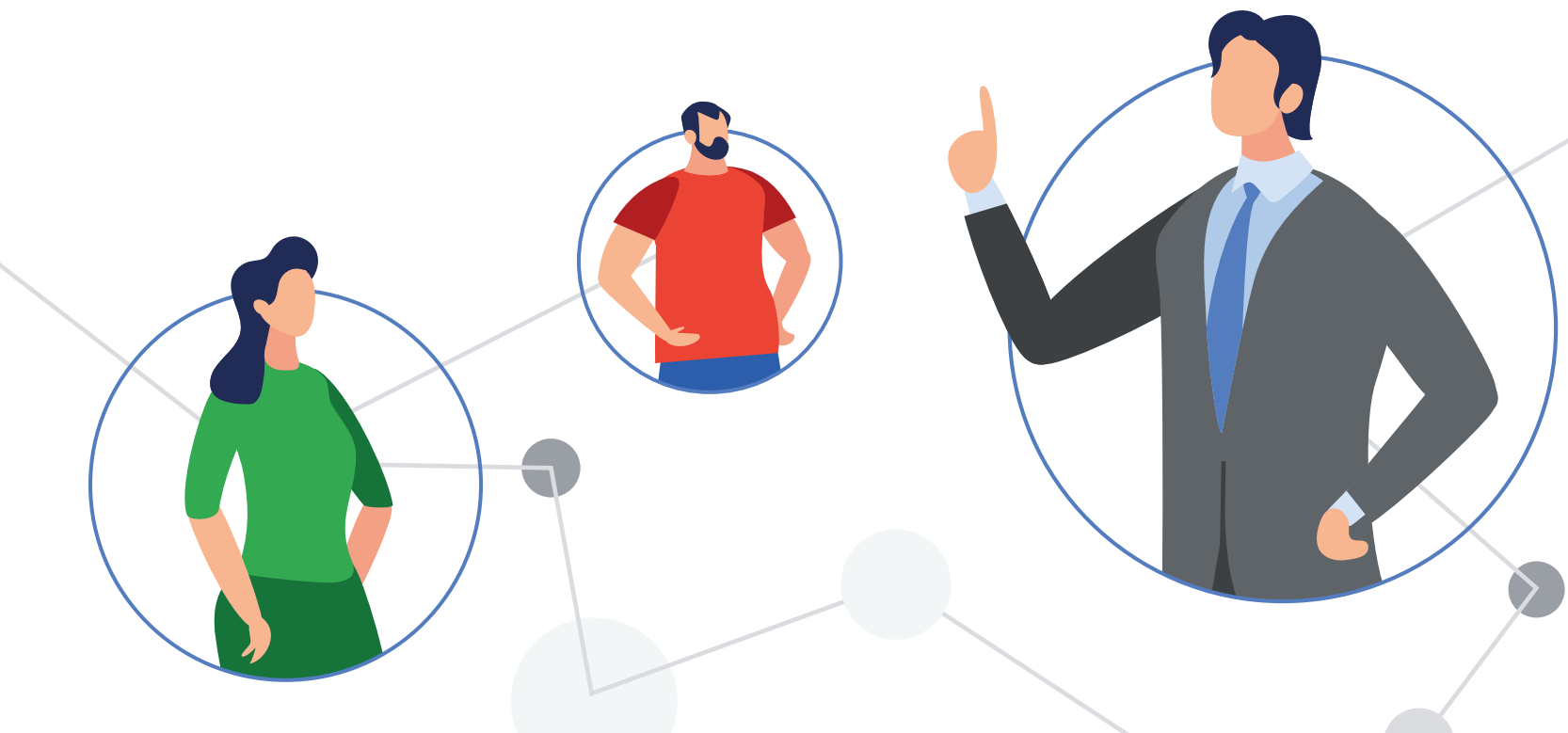
Learn more at **Carah.io/GovTech-AIML-Google**

Google Cloud

Public Sector Connect

Network and find reusable content, crowd-source innovations, and collaboration opportunities in this community exclusively for government and education employees.

Sign up here: carah.io/48185



Reducing Complexity and Preparing for Success

*Successful AI implementations start with laying the right foundation. **Timur Nersesov**, senior manager of professional services strategy at Cloudera, discusses key tactics to extract maximum value from AI and ML initiatives.*

How is the use of AI and ML evolving in state and local government?

State and local governments are just waking up to the possibilities of AI/ML. Use cases are emerging in areas like benefits administration, where states in particular have a ton of data, and in infrastructure management, where cities are using it to manage grids, networks and even traffic systems. Although many small pockets of creative work exist, there isn't yet a widespread rush to develop in the AI/ML area. Interestingly, some government organizations are in the midst of modernizing with enterprise and cloud systems, and their vendors are already building solutions with AI/ML capabilities in mind. So, in essence, a lot of organizations are building the infrastructure needed for AI/ML, even if that's not their main pursuit.

As organizations become more data-driven and automated, what hinders their ability to put data to work?

It's mainly the complexity of managing the data life cycle. Data consistency, cleanliness, formats, pipelines, storage, access and more have to be managed before you can use data to drive insights. That becomes a framing problem because when people get excited about AI, they're looking at the end result, which is the algorithms, dashboards, analytics and reporting. What gets lost is that all those capabilities are the output of an infrastructure. In reality, most of the technical debt around creating something like an effective ML application is the data infrastructure, not the data science.

How can an enterprise data cloud platform help organizations extract the full potential of AI, ML and RPA?

It comes down to efficiency. An enterprise platform typically uses a common standard that integrates data sources and manages data flow across the entire organization. That level of uniformity and simplicity is fundamental to efficiency. By creating a common standard, for example, it eliminates the complexity of managing multiple IT standards across the organization. The cloud also creates efficiency as it relates to storage and compute management. By outsourcing those functions, the organization taps into the economies of scale the cloud vendor can offer.

What tools and tactics help jump-start AI and ML projects?

The primary tactic is to take an enterprise view of the data pipeline. The data pipeline is where you will spend most of your energy and money in getting AI/ML ready, and it will determine the success of your data science program. This is where using an enterprise platform to manage the data pipeline comes in. It will simplify your data architecture, storage and management, and is much more efficient than having to manage multiple point solutions across the data life cycle. Another important consideration is the composition of the data science teams. Data science is a broad, multidisciplinary activity, so it's important to construct teams with breadth in mind.

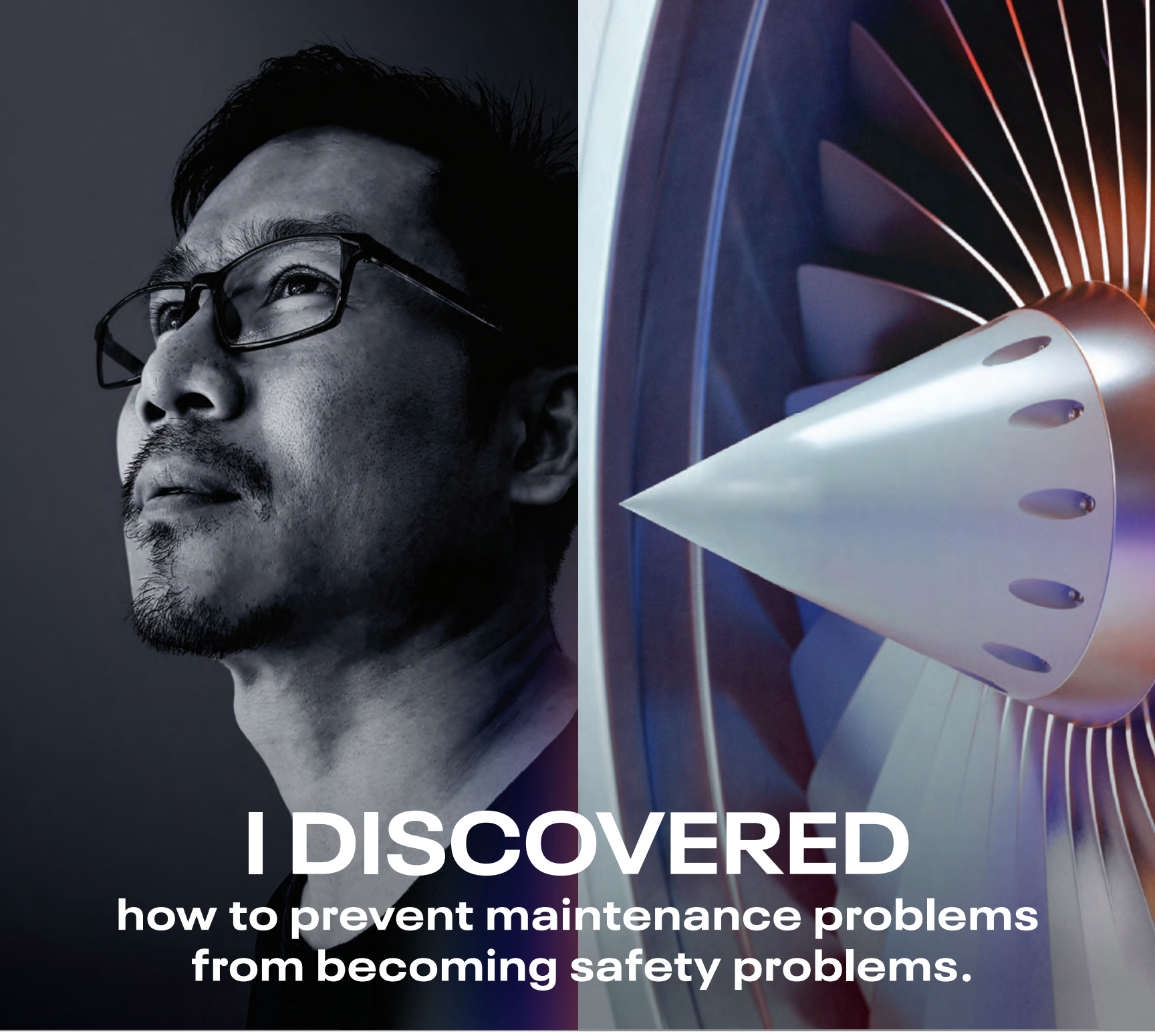
How should organizations address security and governance in data-driven, automated use cases?

Zero trust security is becoming a common expectation for managing access. The basic concept is that the network should not assume any user is trustworthy — regardless of whether they're outside the network or already in. Organizations using a zero trust approach implement access controls inside and outside the network. Another important tactic is to minimize the number of handoffs. In other words, simplify the network architecture. Nodes — and connections between those nodes — create complexity, and complexity leads to management challenges and greater risk.

How can organizations prepare for the cultural changes that come with these advanced technologies?

With AI, ML and process automation, organizations free up their human capital to do more sophisticated, creative and customer-facing work. However, many organizations miss this opportunity because they see the efficiency gain from these tools only as a way to replace human labor — and reduce cost — rather than a way to repurpose their talent. Any organization that effectively implements an AI, ML or RPA solution will have to deal sooner or later with the fact that it has made some labor redundant, and this will impact their culture. They need to consider how to team human labor with capabilities they've gained from automation. Once AI/ML is effectively introduced, it will change how the organization is run, which must be carefully considered by anyone who implements AI/ML.

Learn more at **Carah.io/GovTech-AIML-Cloudera**



It's not your data. It's how you use it. Whether pushing the envelope of aerospace design or delivering vaccines years ahead of schedule, harnessing data to transform your business requires the power of artificial intelligence and machine learning to translate complex sets of information into clear and actionable insights. Cloudera's enterprise data cloud platform accelerates data analytics at every stage of the data lifecycle, with security and governance built in, to make your hybrid cloud move your business.

Learn more at **cloudera.com/datamovesyou**

#cloudera.com/publicsector

CLOUDERA
Data That Moves You

Building a Human-Centered Foundation for Advanced Analytics

*In this Q&A, **Chuck Ellstrom**, vice president of sales for state and local government and education for Alteryx, discusses how organizations can transform the way they conduct key business operations with solutions that democratize analytics, automate key processes and upskill existing resources.*

What insights about government processes have emerged in the wake of recent upheavals?

COVID-19 and the public health crisis really highlighted the importance of data. Fast access to reliable data, along with analytics automation, has been fundamental to enabling state and local agencies to understand what is happening, plan their response with insight and accelerate service delivery. Unfortunately, some organizations found their legacy systems were not up to the task of automatically providing decision-makers with accurate, up-to-date data. In many cases, slow manual processes overwhelmed systems and jeopardized the delivery of key services.

How can organizations use data analytics, AI and ML to improve processes?

This starts with the capability to access data, verify the quality of the data and transform the data so it can be used in higher-level analytic processes. Without a unified ability to access, clean and prep data, AI and ML efforts stall. Organizations that build up their data analytic capabilities are more successful in applying predictive and prescriptive analytics, accelerating the use of AI and ML, and automating transaction-heavy processes using RPA.

What stages of maturity do organizations typically go through as they move toward true intelligent process automation?

There is no one-size-fits-all maturity road map, but organizations can achieve key milestones if they focus on building a strong analytics culture that will support their digital transformation and automation goals. These milestones include widening access to data and analytics and democratizing technology and automation with code-free building blocks, automating repetitive and complex analytic processes, scaling analytics across the organization and amplifying human output, and leveraging actionable insight to transform business outcomes and workforces.

What challenges typically stand in the way of progress within AI and ML programs?

Organizations often struggle to advance because of legacy processess. It's important to be open to new thinking and new methodologies to accelerate the maturation process. Many organizations also lack a solid grasp of their strengths and weaknesses regarding analytics. In addition, their processes may be hostage to old systems, data silos or poor alignment across enterprise teams. To address these issues, organizations often need to work first on breaking down traditional barriers between data scientists, IT, citizen data scientists, analysts and domain experts. One way to support this is via a unified, human-centered analytics platform. Such a platform augments human capability regardless of one's technical acumen, which allows everyone to take advantage of geospatial, predictive and ML-based analytic capabilities to collaborate, innovate and solve problems.

What tools and strategies can ease the way for AI and ML programs?

One key principle in the responsible AI framework is keeping humans in the loop, incorporating human judgment and accountability. Since the deployment of AI, there has been a significant delineation between "black-box" and "clear-box" AI. While AI and ML can be trained to perform many tasks without humans, these systems often operate in a black-box fashion, leaving it unclear as to how these machine-based decisions are made. By contrast, the leading unified analytics platforms provide clear-box insight into the results ML models are producing and how they're arriving at those results.

What types of use cases are emerging? Where can organizations get quick wins?

Any government business process that relies on data can benefit from greater levels of analytics automation through a unified platform. Finance teams can automate the manual preparation and blend process related to building pivot tables for spreadsheet analysis. Unemployment and benefits programs can quickly build AI and ML processes to ingest massive volumes of data; process this data with RPA; and use analytics automation to connect key business processes, verify enrollment eligibility, process payments and more. Counties can automate the analysis of COVID testing data for tens of thousands of tests to quickly verify that incoming data is complete and structured correctly. The use cases are practically endless.

Learn more at **Carah.io/GovTech-AIML-Alteryx**

alteryx

Make Breakthroughs That Matter

Drive mission-critical decisions with analytics automation

Learn More
alteryx.com

Getting the Most from a Next-Generation Contact Center Platform

*The AI technology needed for next-generation contact centers is available now. In this Q&A, **John Bastin**, vice president, industry strategy – government and education at Talkdesk, discusses important tools and tactics to empower contact center staff, improve constituent experience, and get the most out of AI and ML investments.*

What have the ongoing upheavals of the pandemic revealed about the customer experience in state and local government?

It's important to build an appropriate digital experience that is sensitive to users' needs and available on the communication channels they expect. However, the old ways of delivering services are not keeping up with the rapidly changing needs and expectations of residents. Many constituents were new to applying for benefits during the pandemic, and they didn't know how to go about it. When they did apply, they may not have received timely status updates. In addition, many systems could not scale to meet increased demand. Organizations today need to deliver services from wherever agents are — including at home — to anywhere constituents need them. With next-generation contact center capabilities, a constituent today can get around-the-clock support, for example, via AI-powered virtual agents that use natural language processing to provide assistance when human agents aren't available. AI also frees human agents to handle more complex and sensitive issues.

How can intelligent automation address contact center challenges and opportunities?

AI enables better automation that empowers end customers through high-quality self-service. AI-powered virtual assistants and agents can make self-service channels much more effective — not just for informational requests, but also for more complex transactions like understanding eligibility or checking claim status. Intelligent automation also makes human contact center agents more effective through agent assistance, which uses AI to suggest appropriate responses or provide contextual data about a customer. In addition, agent assistance and other forms of intelligent automation can help new agents become effective faster and ultimately deliver a better constituent experience.

What does an intelligent, end-to-end contact center solution encompass?

An intelligent end-to-end contact center solution integrates and incorporates AI and machine learning into all aspects of its platform to provide a frictionless user experience every step of the way. The best AI tools leverage cloud technology and data to deliver powerful support solutions and an incredible level of operational precision.

How does AI support remote contact center employees?

With the acceleration of work-from-home contact centers, supervisors are no longer able to "walk the halls" to check on the performance and engagement of their agents. AI tools fill this void. For example, AI-based compliance tools monitor audit logs, voice streams and text streams for moments when an agent may have inadvertently — or intentionally — stepped outside of bounds. Anomaly models help detect these moments and trigger alerts. AI-based assistants help new agents take on the expertise of veteran agents by listening to the voice stream and making next-best-action suggestions as agents interact with customers in their first weeks. AI-based quality management scans the interaction stream and does automatic evaluations so newer remote employees can get better faster.

What types of tools can make contact centers more equitable and inclusive for both callers and workers?

AI-powered real-time translation mediates conversations between people who speak different languages. AI-powered voices allow agents who are non-verbal to type their responses, which are then converted to speech for voice-only calls.

Which innovations should government contact centers lean into as they pursue AI and ML?

Virtual agents are a great place to start. They can save time for agencies and callers by automating repetitive work and assisting constituents who need help. But while AI has game-changing potential, AI systems are not perfect. Human-in-the-loop AI training can fill in the gaps that machines might miss. Using the no-code interface that is available on modern AI platforms, contact centers can easily leverage the subject matter expertise of in-house customer service experts to train and improve AI models. Organizations can also take advantage of tools that allow non-technical staff with domain or business expertise to make simple improvements. These tools reduce dependence on data scientists to program their machine learning models.

Learn more at **Carah.io/GovTech-AIML-Talkdesk**

talkdesk®

Leverage AI to build an experience that citizens love

Talkdesk is the modern cloud contact center solution that has the tools necessary to help your agency improve the citizen experience with artificial intelligence.

Visit us at talkdesk.com/GovEdu

Experience. A better way.

Reimagining Employment Systems

Using artificial intelligence to modernize employment systems and processes is a game-changer for both agencies and job seekers. ***Dan Hopkins****, vice president, applied AI & public sector with Eightfold AI, shares insight into how a unified talent intelligence platform helps redefine and optimize unemployment and re-employment processes.*

What employment challenges are keeping state and local government leaders up at night?

COVID-19 showed that existing systems are inadequate. Most of us have heard stories of states struggling to process unemployment claims and benefits. Systems and processes were overwhelmed. Equally important is what happens after an unemployment claim is processed. How do states or local agencies enable upskilling, reskilling and re-employment? Today we have a re-employment system that relies on displaced workers' ability to search and interpret vaguely worded job descriptions and to self-assess their own fit to roles. Anyone who has ever done a job search knows that this is a broken, frustrating and time-consuming process. Yet state benefits subsidize this inefficient system, paying millions of dollars weekly until their residents discover the right job. I think leaders are now realizing that if they can optimize the job matching system, they can quickly find people the right employment opportunities, which reduces time on unemployment and benefit obligations.

How can state and local governments use AI and automation to redefine and optimize their employment outcomes?

For the unemployed, finding a job is simply a search problem. It's not that there aren't any jobs out there. It's knowing which jobs are right for the individual. This is where AI can be a game-changer. By understanding what an individual is capable of through a deep understanding of their skills and capabilities, we can instantly surface the best jobs for them — even if they have never done the job before.

Why is it important to have a single talent intelligence platform to support re-employment?

A single platform is uniquely able to provide deep insights at scale. When you can use AI on one side to rationalize job requirements and on the other side to create a capabilities matrix of individual job seekers, you create some very powerful outcomes. So, a talent intelligence platform really becomes foundational to enabling a number of use cases such as dramatically reducing the time to re-employment, minimizing underemployment and reimagining learning and apprenticeship opportunities. And because AI is self-learning, a talent intelligence platform means these outcomes continually improve over time.

How can government organizations use deep learning or other AI processes to promote inclusion and diversity?

First, AI can guard against bias by masking the identity of an applicant to a hiring manager. This ensures a better analysis of candidates based on their merits, and it mitigates the unconscious bias of the reviewer. Second, AI can surface a candidate for consideration based on their potential. This becomes very powerful for promoting upward mobility. Often when hiring managers are determining fit, they only look at what a candidate has done in their past and they don't evaluate their potential. With AI suggesting candidates based on their capabilities and potential, job seekers get the break they need and the consideration they deserve.

Where should state and local governments start on the path to employment modernization?

Just start! The great thing about an AI talent intelligence platform is that you can stand it up very quickly and it will begin to learn from day one, creating even better outcomes over time. So, the faster you implement a system, the more insights and options you have when reimagining service delivery.

What's your vision for the future of government employment offices?

We believe that employment is the backbone of our society and that everyone deserves the right job. I think COVID-19 has forced state and local government leaders to take a hard look at their existing systems and realize that it's time for a change. There has been so much technical innovation over the last 10 years that government organizations can now implement powerful tools to help overcome employment and training barriers. A modern system that enables self-service, optimizes the job search, reduces time on unemployment, and reduces underemployment through upskilling and reskilling is in everyone's best interest.

Learn more at **Carah.io/GovTech-AIML-Eightfold**

Let's Get Future Ready

Build and Unlock the Potential of Your Workforce with Eightfold AI

Eightfold AI® delivers the Talent Intelligence Platform,™ the most effective way for organizations to retain top performers, assess the capability of their existing workforces, create upskilling and reskilling programs for employees, recruit top talent efficiently, and reach diversity goals.

eightfold.ai

Contact us | **888-325-8222** | **www.eightfold.ai**

ISSUES TO WATCH

AI In Government Is Poised to Grow

Successful use of chatbots and other AI technologies during the pandemic opened doors to wider adoption and more advanced use cases. CDG Senior Fellow **Bill Rials** provides a glimpse into immediate and near-term use cases. Rials, a former government IT executive who is now a professor and associate director of the Tulane University School of Professional Advancement IT and Cybersecurity Program, suggests how organizations can take full advantage of AI opportunities now and in the future.

Now that organizations have gotten their feet wet with AI technologies, do you foresee deeper use of AI?

Absolutely. Even if government agencies wanted to go back to the old normal, constituents wouldn't allow it. They've gotten a taste of what government can provide and now they expect things like automated delivery and self-service.

The top AI use case in government is chatbots that interface with constituents. They range in sophistication from simple decision-tree outputs to full AI/ML-powered intelligent platforms. We're also starting to see chatbots interfacing with government workers — for example to pass on institutional knowledge and subject matter expertise to new employees and others as they do their daily work.

As chatbots become more advanced, I expect the burden of learning to shift from the user to the chatbot. The chatbot will adapt the user interface based on what a citizen or employee wants. Taking that further, when organizations onboard new systems, users won't even perceive there's a new system. Minimizing the learning curve and making the user experience more intuitive will get users up to speed faster and encourage adoption of new technologies.

Where are the best opportunities for AI right now?

We're just starting to scratch the surface of what AI can do.

RPA. This technology provides an immediate opportunity. Government agencies have tons of repetitive minutiae and thousands of documents to process daily. RPA offloads those tasks so workers can focus on higher-level thinking. Low-code and no-code solutions allow even non-technical users to set up rules-based processes that automate repetitive work.

Internet of Things (IoT). Historically, many organizations have approached IoT deployments as technology projects rather than business projects that use IoT to achieve business outcomes. I expect increased use of IoT sensors once organizations realize that they provide valuable data for AI to use.

Edge computing. Edge computing has quickly become the decentralized complement to the centralized implementation of AI. I also see growth of AI at the edge. AI at the edge overcomes performance issues associated with data streams traveling back to a central processing unit and enables real-time decision-making based on data from latency-sensitive, resource-intensive devices like police body cameras or traffic monitors.

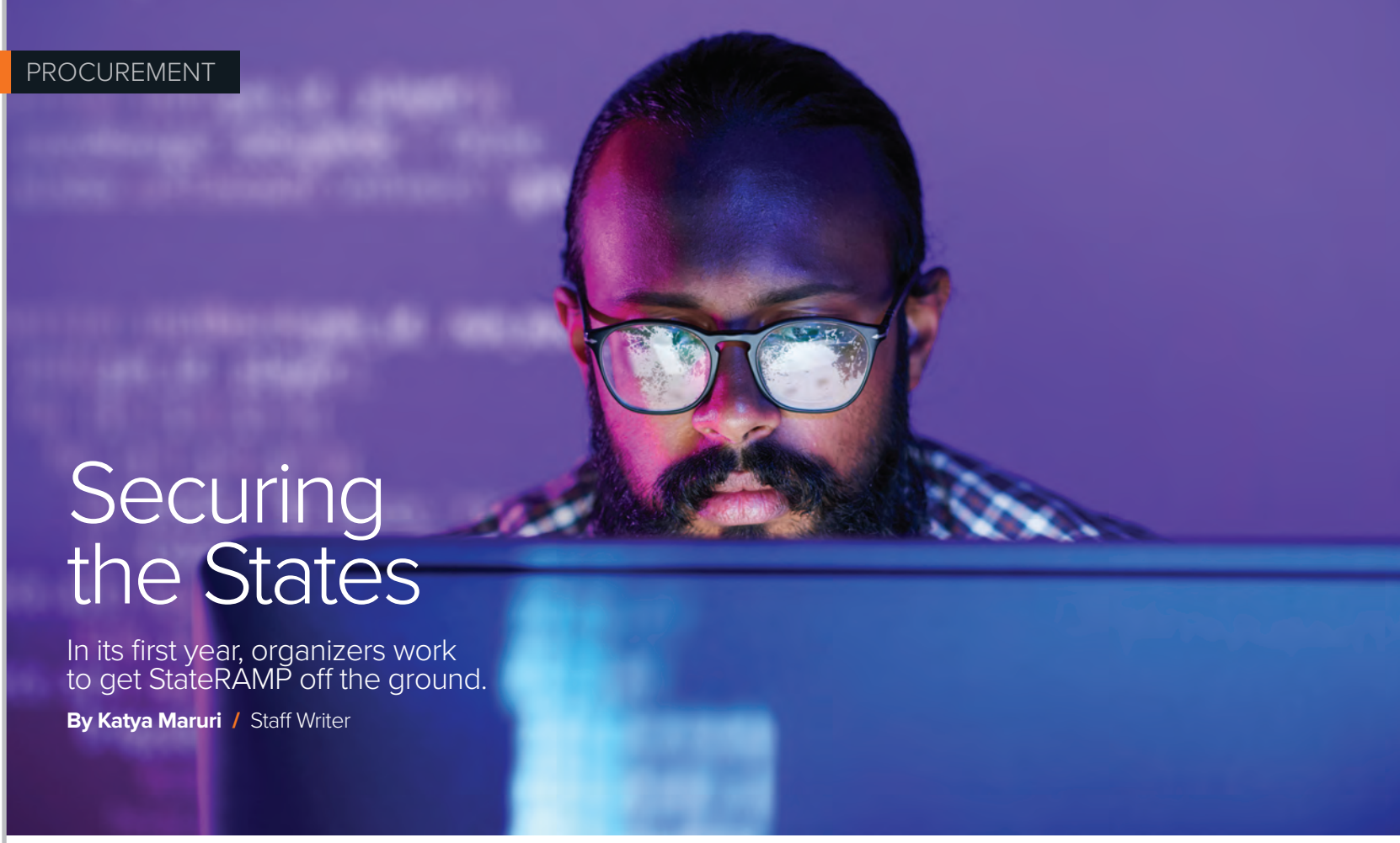
Digital twins. In the future, agencies will be able to use data from medical records, licenses, location logs and other systems to create a constituent's digital twin. With a clearer picture of the constituent's experience, organizations can make better decisions. Governments could even create a digital twin for an entire jurisdiction. This single-point visualization of cloud services, IoT sensors, data sets and other resources would help organizations understand how complex systems are connected. It could support scenario planning and modeling to help governments determine how to best use their technology.

Intelligent hubs. Many local governments have smart traffic lights and other devices distributed throughout their community — parking meters, charging stations, pollution sensors, digital signage, IoT sensors, Wi-Fi, 5G and more. There's an opportunity to create a single intelligent street pole that ties into all those data points to provide a one-stop shop. For example, when a person arrives for an appointment to get a building permit, a smart pole detects their presence and notifies the agency so the paperwork is ready when the person walks in.

What challenges will governments need to overcome to adopt AI more broadly?

The true value of AI only exists once we get past the issue of siloed, single-purpose solutions. The more data inputs that AI systems have, the more value they can provide. So siloed systems and silos of data ownership are the main limitations to expanding AI. We need to think about data governance and how we can implement AI into various systems. Once we address these issues, we can get to a central AI machine learning ecosystem that enables all kinds of situational awareness and user experiences for the greater good. And of course, all of this must be backed up by strong policies around data privacy and security and careful thinking about the trade-offs society wants to make between convenience and privacy.

SHUTTERSTOCK.COM



Securing the States

In its first year, organizers work to get StateRAMP off the ground.

By Katya Maruri / Staff Writer

The State Risk and Authorization Management Program, or StateRAMP, launched in early 2021 with the aim of solving a problem many governments are encountering in the pursuit of securing their systems: How can they be sure third-party vendors are meeting cybersecurity standards? Modeled on the Federal Risk and Authorization Management Program (FedRAMP), which offers pre-verification services for companies looking to contract with federal agencies, StateRAMP hopes to make it easier for both states and private companies to work together.

Since its inception, StateRAMP organizers have been working to get vendors certified in the program, as well as to get states to sign on to participate. The program's success hinges on getting both sides on board.

States Sign On

Arizona is currently in the process of participating in the StateRAMP pilot program, but it is not currently operational.

"Arizona has had an approach to reviewing cloud vendors for several years now," state CIO J.R. Sloan, also currently president of StateRAMP, said. "We labeled it AZRamp."

Under AZRamp, Sloan said vendors must provide documentation to show that they meet different thresholds relating to security and data protection. If a vendor meets these qualifications, they fill out a 30-question document and undergo a security assessment before being approved. However, one of the concerns the state had about AZRamp was the resources required to continuously monitor approved vendors. That made StateRAMP appealing.

"We joined StateRAMP's steering committee after seeing how their program was able to address the issues AZRamp did on a larger scale," Sloan explained.

Right now, the state is engaging in StateRAMP's pilot program and doing internal reviews to see how its cybersecurity efforts can be improved. Moving forward, Sloan said, the hope is that joining StateRAMP will create a centralized approach to working with its current 230 vendors and create room for other vendors to join.

Another goal is freeing up resources that AZRamp previously used to work on other projects.

"I am looking forward to this process," Sloan said. "Vendors will have a predictable understanding of what to expect when working with Arizona, and it will allow us to engage with vendors on an ongoing basis and maintain the state's data properly."

In Texas, the state is not directly using the program but will accept StateRAMP-certified vendors under its own certification program called TX-RAMP. State Senate Bill 475, passed in spring 2021, will require the Texas Department of Information Resources to certify vendors through TX-RAMP, with a fast track for vendors certified by FedRAMP and other states' RAMP programs. StateRAMP-approved vendors also qualify to be fast-tracked into TX-RAMP. However, that's the current extent of the state's use of the program.

"We are in the process of finalizing the development of the program," Texas Chief

Getting Certified

To be StateRAMP-certified, vendors must go through several steps. The first is to fill out an online membership application. The second step is to use a data classification tool to determine a vendor's security category (Category 1, 3 or 3+). Categories are determined by different data characteristics and corresponding security requirements ranging from nonprivate, generally accessible information to protected, personally identifiable information or classified data.

Once a category is assigned, a vendor must work with a third-party assessment organization to review their StateRAMP System Security Plan and other required documentation in order to provide a StateRAMP Readiness Assessment Report to the StateRAMP Project Management Office.

Costs

It costs $2,500 for the project management office to conduct a review for "Ready" status or $5,000 for an authorization review. After a vendor is approved, the annual membership fee is $500. Following that, continuous monitoring costs $5,000 per year.

Governments can join StateRAMP for free.

Information Security Officer Nancy Rainosek said. "It's a similar process where vendors will have to submit documentation and meet required security controls."

The major difference is that TX-RAMP's program will solely work with Texas-based vendors to ensure that small and medium-sized companies have the chance to engage with the state if the cost of joining StateRAMP is prohibitively expensive.

"The certification process under StateRAMP can be costly and time-consuming," Rainosek said. "Through TX-RAMP, there will be no charge to Texas-specific vendors that don't do business outside of the state."

She anticipates the program will be live in December.

As for other states signing onto StateRAMP, Teri Takai, vice president of e.Republic* and a member of the StateRAMP steering committee, said that understanding what the program can do along with the benefits it offers is key in widespread adoption.

"What I'm hearing is states are slowly getting an understanding of StateRAMP," Takai said. "They are beginning to understand that this can help them streamline procurement, and they won't have to go back and do multiple security assessments for each state. Instead, they would simply have to say they are StateRAMP-certified."

Another benefit is that vendors who are already FedRAMP-certified qualify to become StateRAMP-certified. If a FedRAMP-approved vendor wants to become StateRAMP-certified, they would have to show a prior 90 days of continuous monitoring and pay a fee to the StateRAMP Program Management Office to convert their documents to StateRAMP's templates.

Making It Work

As for vendors, Salesforce and Boomi, an IT service management company, are currently undergoing certification through StateRAMP.

According to Boomi's public-sector Chief Technology Officer Joseph Flynn, "one of the biggest benefits is that StateRAMP looks at security challenges more than we can and provides a common line among providers to work with states and creates a common language for procurement."

The barriers, Flynn said, are that it is a time-consuming process that requires a lot of resources and money. Another challenge, according to Paul Baltzell, vice president of strategy and business development for Salesforce, who also serves on the StateRAMP steering committee, is getting people on board since StateRAMP is relatively new.

"There has definitely been a lot of interest in states and vendors using StateRAMP," he explained. "But there have been a lot of questions from stakeholders in the vendor community, along with states."

However, despite these questions and having to undergo a rigorous process to become certified, Baltzell said, "StateRAMP allows vendors to become a true partner to states."

"We believe StateRAMP can be adapted to work in all 50 states," Leah McGrath, StateRAMP's executive director, said. "What makes this possible is that StateRAMP creates a common set of standards for vendors and states to follow."

"It also stands out from other certifications because it continuously monitors for cyber threats and allows vendors to go through the verification process one time and serve all states and local governments," McGrath said. gt

kmaruri@govtech.com

*e.Republic is Government Technology's parent company.

WITH AUTOMATION, ANSIBLE DRIVES CYBERSECURITY FOR STATE AND LOCAL GOVERNMENTS

With state and local IT teams stretched to the breaking point, cybersecurity initiatives risk being lost in the shuffle.

In this Q and A, Red Hat Business and Strategy Advisor Nick Lenaeus describes how an open-source approach to security automation can free up technology time and talent while improving cyber outcomes across the state and local government landscape.

Why do state and local governments struggle with cybersecurity?

Many critical applications in the public sector have been in service for multiple years — in some cases, a couple of decades. There are well-known vulnerabilities due to age, despite everyone's ongoing efforts to prevent access to those vulnerabilities.

For state and local government, these fragmented legacy technologies can introduce a lot of risk, as security was likely an add-on to the original systems. Ideally, security needs to start in the design and incubation phase and be part of how you build your infrastructure.

How does security automation help address this?

Automation is critically important as the average IT worker is tremendously overburdened. Security automation helps, especially for things like application development where organizations can automate the testing and scanning of code. Automation integrates security throughout the whole DevOps (development and IT operations) pipeline. You are automatically putting those safeguards into place and remaining compliant.

How does this approach support government-specific needs around privacy and compliance?

State and local governments can follow policies set by organizations like the National Institute of Standards and Technology (NIST) and the Defense Information Systems Agency (DISA). Agencies can implement security automation practices that follow these agency's standards, which is much more effective than trying to do this manually.

How does Ansible bring this to life?

Ansible helps bring DevSecOps to life in several ways. First, as an open-source innovator, Red Hat brings expertise and a shared sense of innovation to the table with our open-source work.

Second, there is the ongoing work with our partner community — including Cisco, VMware, Microsoft and Palo Alto. All these brand names are certifying their content with Ansible.

With network automation around your existing firewalls, and around your existing switching and routing and Wi-Fi infrastructure, you don't have to undo what you've already done with Ansible. For example, VMware and Microsoft both have a great hypervisor. Ansible talks directly to those hypervisors to automate their end-to-end workflows. That's the power of certified content.

What are some best practices for IT teams looking to implement security automation?

Start with the small, repetitive tasks. You can automate tasks like opening, updating and closing a ticket. People dislike that part of the job. By automating these repetitive and routine tasks, you can increase your team morale so they can focus on innovation.

As IT leaders, it's important to let people know they don't need to be scared of automation. The point isn't to automate you out of a job. It's to help you do the job better, and free you up from the most boring parts of that job.

UNIVERSITY OF IDAHO MIGRATES MAJOR SYSTEMS TO THE CLOUD IN JUST 14 WEEKS

The university has realized benefits around cost control, scalability and disaster recovery

The University of Idaho is Idaho's land-grant university, with almost 12,000 students, more than $113 million expended in research activities and two-thirds of undergraduates participating in hands-on research. Founded in 1889, the college is known for its agricultural, science and business programs, as well as for its setting in picturesque Moscow, Idaho.

Since 1993 the university relied on an on-premises Ellucian Banner system to run its student information, human resources and finance operations.

"Students, HR and finances are critical to us, so Ellucian Banner is our crown jewel," says Dave Lien, the university's Director of Technology Infrastructure and Innovation.

Though Ellucian Banner worked well, overhead costs, maintenance requirements and a lack of modern technological capabilities were a longtime concern for university officials. The university contemplated moving to the cloud in recent years to lower its costs, improve security and enhance scalability, but hadn't yet landed on the right solution.

"We knew a move to the cloud would bring a number of strategic advantages but we needed a mechanism by which we could do so and manage costs around Banner, the supporting Oracle software, and our computer and storage infrastructure," says Dan Ewart, the university's Vice President of Information Technology and Chief Information Officer.

When school officials reached out to Oracle, they discovered Oracle Cloud Infrastructure (OCI) could provide the university an easy path toward modernization and cost management.

Moving to OCI would also allow the university to dodge an imminent and expensive hardware refresh and take advantage of new services like intrusion detection and prevention.

Oracle representatives put together a bid to show university officials what they could potentially save over five years.

"The advantage Oracle brought over other cloud vendors was the licensing," adds Lien. "We would have spent more money on Oracle licensing running on other platforms. We looked at Ellucian's hosted Banner solution, but from a cost standpoint and an operational efficiency standpoint we saw the value of Oracle database in the cloud."

Another major hurdle was the university needed to move its Ellucian Banner environment to OCI quickly to accommodate contract and hardware replacement timelines while also addressing challenges presented by COVID-19. With most campus personnel working remotely, the migration would have to be carefully orchestrated from a distance.

“We feel so much more confident now knowing that our critical systems are running in multiple data centers in OCI and that the OCI environment has much more redundancy built into it than we could ever have achieved on our own. That really puts us at ease.”

Dave Lien, Director of Technology Infrastructure and Innovation, University of Idaho

After weighing its options, the University of Idaho committed to move Ellucian Banner to OCI and, at Oracle’s suggestion, recruited Astute Business Solutions to assist it with its swift migration.

A 14-Week Migration to OCI

Astute went to work quickly to create a clone of the university’s Ellucian Banner production environment in OCI that would not affect current systems or users. That enabled the university to kick the project off quickly and begin testing almost immediately.

“That saved so much time,” says Lien. “Before that we were worried we’d need to build out 60 new servers in OCI, re-install the applications and then move the data. But as we began working with Astute, it became clear they were very organized, they had done this before and they were adept at leading us through the project timeline.”

The university went live in 14 weeks, moving approximately 150 virtual machines and 24 databases to OCI.

“Great project management and great dedication of resources, both on the Astute and university’s side, enabled this to happen in three months,” says Randy Wood, Manager of Enterprise Applications. “This project was our biggest priority for those three months.”

“This was all-hands-on deck,” says Lien. “All of the university’s IT personnel were dedicated to making this happen, but we were led by Astute. The automation and tools Astute brought to the process were critical to getting this work done as quickly as we did.”

“In Astute we found more than a vendor with the technical and project management skills to deliver our needed outcomes — we found a trusted partner that became part of our team, helped deliver a successful migration and will continue to support our long-term success in OCI,” says Ewart.

Improving Performance, Security and DR

Since the University of Idaho completed its migration to OCI, it has realized benefits around cost control, availability and performance.

“Performance is better in OCI than it was on-premises,” says Lien. “It’s good knowing that the environment performs well, and we have the ability to easily increase performance as we need to. We were able to quickly add resources during our registration period and then remove those resources just as quickly so we only paid for what we needed while minimizing risk during this critical period.”

Improved security is another benefit. OCI natively enables database encryption, so the university’s data — both at rest and in motion — is fully encrypted. This is increasingly important as the number of cyberattacks on universities continues to rise.

Perhaps most critically, the move to OCI provides the University of Idaho with disaster recovery and business continuity benefits it couldn’t previously access.

“Before, we had two physical data centers with Ellucian Banner spread across them,” says Lien. “But we would have been significantly impacted by a major event like a power outage, ice storm or windstorm here in Moscow. We feel so much more confident now knowing that our critical systems are running in multiple data centers in OCI and that the OCI environment has much more redundancy built into it than we could ever have achieved on our own. That really puts us at ease.”

This piece was developed and written by the Government Technology Content Studio, with information and input from Oracle and Astute.

Produced by:

government technology

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

For:

ORACLE

The Oracle Cloud offers a complete suite of integrated applications for Sales, Service, Marketing, Human Resources, Finance, Supply Chain and Manufacturing, plus Highly Automated and Secure Generation 2 Infrastructure featuring the Oracle Autonomous Database. For more information visit **Oracle.com/stateandlocal**
#OracleGov360

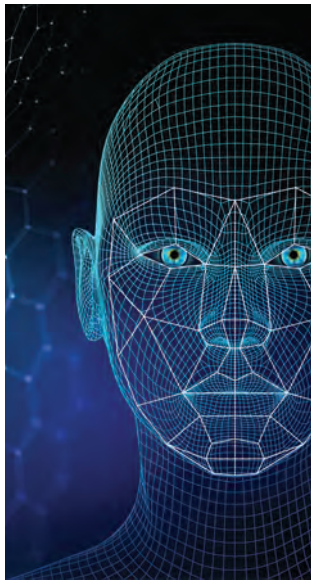
ASTUTE

Astute Business Solutions is a leading Oracle Cloud Partner, helping customers innovate, transform and modernize on Oracle Cloud. A premier Oracle partner for moving and improving PeopleSoft, Ellucian Banner, and VMware on Oracle Cloud Infrastructure, Astute is known for its customer-centric and tailored approach with clients in all industries. Committed to helping clients decrease TCO, improve performance, and modernize on Oracle Cloud Infrastructure, Astute offers innovative solutions for migrating and managing ERPs on Oracle Cloud, Cloud Analytics, Chatbots, Disaster Recovery, and more on the Oracle Marketplace.

IMAGE PROVIDED BY SHUTTERSTOCK.COM

spectrum

More research, more science, more technology.



MANHUNT:

In August, after 15 years on the run, a man was sentenced to four years in prison for scamming more than 20 people out of hundreds of thousands of dollars, according to the Justice Department. What finally brought his evasion to an end? Facial recognition. American Randy Levine, of Boca Raton, Fla., was picked up by a facial recognition system in Austria, where he tried to use an alias to open a bank account using a Mexican passport.

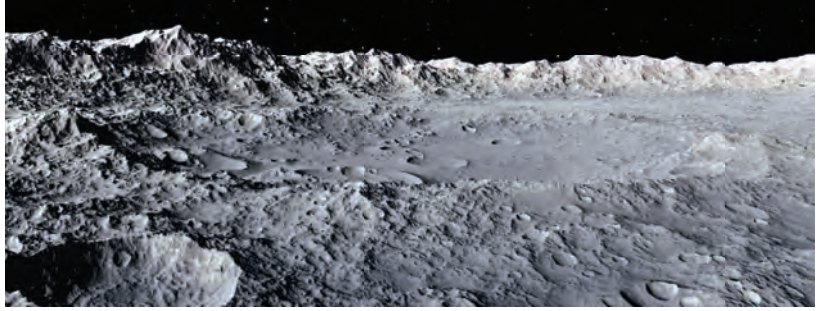
SOURCE: THE VERGE

Periscope Holdings, which uses AI solutions to help connect appropriate vendors to state and local government, was acquired in August for $207 million by mdf commerce, a procurement and supply chain tech company with a wide range of customers in both the public and private sectors. Periscope was notably behind Oregon's statewide procurement marketplace that launched in 2020. Mdf is a publicly traded global firm that took in $85 million in revenue last year. The deal is anticipated to be finalized in fiscal year 2022.

SOURCE: GOVTECH.COM

Moon Dust

A NASA resupply mission to the International Space Station this summer included some new equipment that could potentially make creating habitats on the moon or Mars a bit easier. The plan is for the Redwire Regolith Print project to work together with an existing 3D printer to make simulated regolith, or loose soil. The space station crew will then evaluate whether the material can withstand conditions outside Earth's atmosphere. If the idea works, in the future NASA may need to send fewer construction supplies to build structures on other planets. SOURCE: ENGADGET



SHUTTERSTOCK.COM

SHOPBIRD.CO

157%

That's how much the global e-bike market has grown year over year according to data from research firm Facts and Factors. The report also anticipates the market will be worth nearly $68 billion by 2026. The news came as micro-mobility company Bird began selling its e-bikes direct to consumers for $2,300 each.

SOURCE: FAST COMPANY

Send Spectrum ideas to Managing Editor Lauren Harrison, lharrison@govtech.com

government technology

To Strengthen Cybersecurity, Governments Need to Be Proactive

Ransomware attacks cost governments in the U.S. more than $18.9 billion in 2020.[1] Government agencies also face many other types of incursions that interrupt their operations, enable identity theft, increase expenses and cause other issues.

***Jared Pane,** senior lead solutions architect at Elastic in Mountain View, Calif., says that to avoid damaging attacks, state and local governments need to do more than merely react to cyber threats. In this Q and A, Pane shares his thoughts on how to enhance cybersecurity with a more proactive approach.*

What's the difference between taking a reactive or proactive approach to cybersecurity?

Due to competing priorities and resources constraints, many state and local governments wait for something to infiltrate the IT environment before they take countermeasures. They suffer a ransomware attack, or they detect a threat actor when it's already moving through the infrastructure. Cybersecurity solutions point out malicious activity they need to check out, but busy analysts and administrators can respond to only so many alerts. The rest can fall through the cracks, leaving systems vulnerable.

When you take a proactive approach, you don't wait for something bad to happen and then fix it. You keep bad things from occurring in the first place. Done right, proactive measures are simple for security teams to take on and are affordable.

What preventative measures should governments deploy?

Implement antivirus software or malware protection. Stay up to date on your patch management life cycle. Develop a comprehensive incident response plan. Implement a strong perimeter defense with security controls. Install a virtual private network (VPN) and implement a mobile device management tool that can track devices if they're lost or stolen. And use machine learning to spot anomalous patterns in network activity that human observers would never catch.

What are some solutions from Elastic that strongly support the proactive approach to cybersecurity?

More and more, we are seeing cyber intruders take hidden footholds on systems and move laterally through the network. Being proactive requires the ability to retain and look back at older data.

Elastic's "searchable snapshot" and "frozen tier" features let you retain large data volumes for years in a format that's immediately searchable. You don't need to go through the time-consuming process of rehydrating stored system activity data that has been migrated off into a non-searchable snapshot. Instead, that data is available immediately for audit or investigative purposes. You can also use stored data to compare current and past activity, helping you spot anomalies or malicious activity before it spreads throughout your data center. Besides helping you gain better insight into potential threats, these features can reduce costs. Elastic's technology allows you to ingest as much data as you'd like, but also allows you to retain your data on inexpensive media.

Elastic also helps you be proactive by automating and actioning routine cybersecurity tasks. For example, when you want to investigate network activity and hunt for threats, rather than build queries from scratch, you can use our Timeline feature in Elastic Security to design queries by dragging and dropping fields. Our Kabana Lens product lets you leverage drag-and-drop capabilities to quickly develop cybersecurity dashboards for use in a security operations center (SOC).

Do you have any final advice for state and local governments?

Create an incident response plan and security policy. Have a centralized SOC where you can collect all of your important data and proactively monitor as well as threat hunt. Backups are extremely important, especially as a defense against ransomware attacks. Instead of paying a ransom, you can roll back to the last available good timing of your system. All these measures, coupled with employee training and awareness, can help state and local governments head off cyber attacks before they have a chance to cause serious damage.

[1] https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

 Photo provided by Shutterstock.com

spectrum

More research, more science, more technology.

Every day on govtech.com, we explore a question about something new happening in the tech (and tech-adjacent) world. Here's a look at a few recent Questions of the Day. For more, visit govtech.com/QoD, or subscribe to our newsletter to get them daily in your inbox.

How can stand-up paddleboards be made more eco-friendly?

Answer: With old wind turbine blades.

While stand-up paddleboards (SUP) may be far more eco-friendly than gas-powered boats, the materials used to create them don't quite fit that bill. Most of them are difficult to separate from each other and recycle whenever the board eventually wears down or breaks.

Scientists are looking to an interesting source for a solution: old blades from wind turbines. A group from the Fraunhofer Institute for Wood Research and the Technische Universität Braunschweig has teamed up to build a new board filled with a lightweight foam made from materials like finely ground balsa wood harvested from old blades.

What insect inspired a self-righting drone?

Answer: Ladybugs.

If a fixed-wing drone survives a fall to the ground, it's still doomed if it happens to land upside down. The same cannot be said for beetles like ladybugs. That's because of their elytra, or the exterior red and black-spotted wings. If a ladybug lands upside down, it will use its elytra to balance and then right itself in no time.

A research team at the Laboratory of Intelligent Systems, Ecole Polytechnique Federale de Lausanne in Switzerland was inspired to create the same kind of advantage for fixed-wing drones. Lead by doctoral assistant Charalampos Vourtsis, the team developed a drone that mimics this technique using actuators and a set of artificial elytra.

"Similar to the insect, the artificial elytra feature degrees of freedom that allow them to reorient the vehicle if it flips over or lands upside down," Vourtsis said. They found that the drones were able to self-right themselves using a set of 17-centimeter elytra in every scenario except on a very steep incline and on grass and sand. The team also found that the elytra added non-negligible lift during flight, offsetting their weight.

What kind of weather is pizza weather?

Answer: Pizza Hut has set out to find the answer.

This summer, Pizza Hut confirmed that it is going to start trying to predict when you'll be in the mood for a pizza, and what kind, based on the weather. It's going to do this using artificial intelligence. The AI will, among other things, look at the weather in a certain location and compare it to what people are ordering in order to make predictions about what people will want when those weather conditions come around again.

According to Tristan Burns, Pizza Hut's global head of analytics, the weather is just one example of the kinds of things the AI will be looking at to make predictions on pizza preferences. It will also look at things like where they are and "ingest customer behavior and a little bit about who customers are." All in the service, of course, of making sure you know exactly what you want.

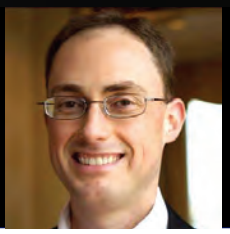
SHUTTERSTOCK.COM

A GOVERNMENT TECHNOLOGY Q&A

government technology

Protecting Citizen Data in a Zero-Trust World: Cybersecurity for State and Local Governments

Cybersecurity grows more challenging for government agencies every day and the sophistication of threats continues to rise. In this Q&A, Peter Romness, Cybersecurity Principal, US Public Sector CTO Office, Cisco Systems, and Steve Caimi, Public Sector Cybersecurity Specialist, Cisco, describe how zero-trust strategies can guide how leaders think about securing citizen data.



>>> We learned of a significant intrusion into federal systems at the end of 2020. What should state and local governments take away from this event?

Caimi: A lot of times, we think of cyber attacks coming from the outside, like nation-states, or from insider threats. But it is easy to lose sight of all the trusted relationships that state and local governments have with vendors, suppliers and service providers. We have known that trusted relationships and supply chains are ways organizations can be breached. This attack brought that to the surface.

Romness: For a long time, state and local governments focused on how they can protect their networks through technical means and by training their employees. There has always been the need to ask the same questions of their suppliers, and that has bubbled back to the top now.

>>> State and local governments rapidly shifted to remote work and digital service delivery last year. What will be the lasting impacts of these shifts on their overall cybersecurity posture?

Romness: Citizens are getting used to the idea of doing things online. The more state and local governments can accommodate that, the better they will look to their constituents. But they must think about how they are going to secure these services.

Caimi: When we talk about the basics of security – confidentiality, integrity and availability – all these things need to be the same regardless of where employees work or how citizens access government services. It is worth looking at new trends in cybersecurity, including zero trust.

>>> How do governments' best practices for cybersecurity need to change?

Romness: A colleague called zero trust a "lifestyle choice"– something that helps guide your decisions. When you start applying it to all the things happening in the world, it tends to fit very well.

Caimi: We all know there is not much of a perimeter anymore and we should not associate something being inside as being secure. But we must also secure things on a per-session basis – each time you access a network, you must prove yourself trustworthy with authentication and authorization. It must be dynamic.

When you look at the principles of zero trust against the backdrop of the cybersecurity challenges of today, there is a lot for governments to learn.

>>> What questions do government leaders need to ask their vendors and partners to ensure their systems are – and remain – secure?

Caimi: You want to get to the heart of how the organization protects its own data when you hand over a lot of important information about your agency.

Any technology in your environment is impacting citizen data. You have to understand how they build in security. Put the pressure on vendors and suppliers to be upfront with you about how they treat data and how they go about making things right when things go wrong.

Romness: Whenever you do business with a cybersecurity vendor, it is up to them to provide clear answers – even before you ask, they should be saying "this is our trust and security policy, and this is how we handle things." And they need to be a strong enough vendor to stand up when something happens.

cio central

Read full reports and breaking news about career changes across tech-driven roles in government at **govtech.com/people.**

Maryland Gov. Creates State Data, Privacy Officer Positions

Maryland established a pair of new roles aimed at improving data sharing, adding a state chief data officer and a state chief privacy officer. Gov. Larry Hogan created the roles via executive order, and the state is now undertaking a nationwide search to fill them. Each of these roles is expected to collaborate closely with Maryland CISO Chip Stewart.


Deborah Blyth

Colorado Opens Search for Next CISO as Blyth Departs

Colorado CISO **Deborah Blyth** has left the state, electing to rejoin the private sector. Blyth's last day with the state was Aug. 13. In the wake of her departure, the governor has named Chief Customer Officer William Chumley as interim CISO, taking on the job in addition to his current duties while the state conducts a search for a full-time replacement.


Eddie Kim


Ying Chan

San Jose, Calif., Adds Two New Deputy CIOs

San Jose, Calif., has hired two new technology executives to serve as deputies to Chief Information Officer Rob Lloyd. Those deputies are **Eddie Kim** — a veteran of the city IT shop, having served there in various positions for 15 years — and **Ying Chan,** who has more than three decades of experience spanning roles in both the public and private sectors. Kim will be San Jose's new deputy chief information officer for the IT Infrastructure and Operations Division, while Chan will oversee the city's Business Solutions section.

MANAGING SECURITY AND RISK ACROSS THE IT SUPPLY CHAIN: A Practical Approach

IT supply chain security is undergoing closer scrutiny as state and local government IT leaders grapple with ransomware, discover new vulnerabilities and confront the possibility of another SolarWinds type of attack. In the SolarWinds attack, an update in software created a backdoor for cybercriminals to enter systems and silently wreak havoc in many private sector firms as well as federal, state and local agencies. The massive attack is still under investigation, and recent reports indicate the perpetrators may have also turned cloud platforms and other vendors' products into potential attack vectors.[1]

The incident highlights the magnitude and complexity of managing risk in the IT supply chain, especially as government organizations increasingly rely on a multitude of third-party products and services to run their enterprises. Even if an organization implements rigorous controls to protect its systems and data from cybersecurity attacks, it may inherit vulnerabilities from third-party components.

The federal government has stepped up pressure on federal agencies to address IT supply chain risk, and a Cybersecurity and Infrastructure Agency (CISA) working group has issued guidelines for federal agencies to follow. Similar mandates are likely to emerge at the state and local government level. Proactive state and local government leaders can start now by incorporating processes and tools to identify, evaluate and mitigate the risk of IT supply chain threats. Doing so will lead to a more mature risk management approach that protects constituents, preserves trust in government services and ensures resilience.

Weak Links — Anywhere and Everywhere

An IT supply chain is a system of manufacturing and delivering components and products that enable digital operations and services. It starts with creating or procuring individual software (e.g., code) or hardware components (e.g., chips, routers or internet of things sensors), and then assembling components into a final product. It includes physical and digital transport; receipt and storage of components and products; and installation, management and disposal.

Today's IT supply chain ecosystems extend globally, with raw materials and parts coming from all over the world. When an organization engages with the supply chain, it may be interacting with one or many vendors (who also rely on multiple vendors and their subvendors) to obtain a single product or service. The more complex the product or service, the more complex the supply chain associated with it — and the more points of potential failure or risk.

Supply chain vulnerabilities may be introduced either intentionally or accidently. They frequently arise at the following points:

- **System development life cycle (SDLC),** including design, development and production. Many software developers are not trained to write secure code and may introduce vulnerabilities into their scripts. In addition, to save time, they may leverage blocks of legacy or open-source code that contain vulnerabilities.

- **Manufacture and deployment.** Malicious insiders may swap original parts for counterfeits or insert malware into systems at any point in the delivery process.

- **Maintenance and patching.** Unauthorized patches, legacy software and systems that are no longer supported by the original manufacturer, and maintenance performed by improperly trained staff can introduce vulnerabilities into a once airtight system — as can failure to patch known vulnerabilities.

- **Disposal or retirement.** If components are not properly retired, cybercriminals can steal intellectual property or personally identifiable information (PII) from them (e.g., by accessing files on a laptop that has not been properly "erased") or reverse engineer parts of the product to produce counterfeit copies.

Cybercriminals are constantly on the lookout for vulnerabilities and potential attack vendors throughout the supply chain. The move to remote work, where many employees are now using private home networks and their personal laptops and desktops, has expanded the attack surface and made organizations even more vulnerable.

"Security networks are only as strong as their most vulnerable point; it may only take one compromised system for a determined and skilled malicious hacker group to gain access. Conducting work over dispersed networks makes it harder to protect the network from threat actors," says George Duchak, chief information and innovation officer for the U.S. Defense Logistics Agency (DLA).

Best Practices for Maintaining a Secure and Resilient IT Supply Chain

The following practices help organizations strengthen the integrity, security and resilience of their IT supply chain.

Exercise good procurement hygiene

Any IT procurement decision is ultimately a security decision. When making procurement decisions, the lowest cost product isn't always the best investment in the long run. It's important to partner with reputable vendors who produce supplies and services that have been proven in the marketplace. These industry leaders have the expertise, rigor and resources to thoroughly vet their suppliers and workers, build in security by design and rapidly address emerging threats and vulnerabilities (e.g., via security patches). Regardless of the vendor, organizations should independently validate its security posture and continue to audit the vendor and its products over time.

> **"Security networks are only as strong as their most vulnerable point; it may only take one compromised system for a determined and skilled malicious hacker group to gain access."**
>
> *George Duchak, Chief Information and Innovation Officer, U.S. Defense Logistics Agency*

"Any agency or organization that plans to partner with a supplier of any size would be well-served by conducting a security audit of that partner prior to entering a contract or allowing any work to happen. Organizations could create a framework for evaluating and scoring a potential partner's security operations," says Duchak.

Leverage frameworks and guidance from CISA and other experts

A number of governmental bodies and industry working groups provide authoritative guidance on managing supply chain risks. While some of this guidance was specifically written for federal government agencies, cybersecurity and risk management leaders in state and local government can adapt these various models and recommendations to strengthen their risk posture. The CISA Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force advised CISA and its stakeholders on assessing and managing risks associated with the IT supply chain. Among other things, it publishes guidance on starting a basic supply chain risk management program, using qualified bidder lists, analyzing supplier threats and strengthening security posture. The Cyber Maturity Model Compliance (CMMC) framework — used by the Department of Defense — is also a useful model for verifying vendors have implemented appropriate cybersecurity practices and controls in the development and delivery of their products. Finally, the National Institute of Standards and Technology (NIST) 800 Series risk management framework describes computer security policies, procedures and guidelines.

INSTITUTIONALIZING SUPPLY CHAIN SECURITY

The U.S. Defense Logistics Agency (DLA) procures products and services on behalf of the U.S. military and other federal government organizations. It has nine global supply chains that acquire, store, distribute and dispose of these products. For its IT systems, DLA supports 54,000 devices globally and 194 software applications. Cyberattacks are a continuous threat. "Every organization today is, in essence, a tech company, and we are no exception," says Duchak.

While the range and number of components may be different in a state or local government, the essential challenges — and strategies to combat these challenges — are the same for any size government organization.

For the DLA, that strategy includes establishing an architecture that comprehensively addresses security via threat identification and risk prioritization; offensive and defensive risk-mitigation solutions; resilient supply chain operations; and prevention through detection, protection and defense. It also includes institutionalizing supply chain security across the enterprise.

"The bedrock initiative within this strategic focus area is integrating supply chain security into the agency's mission assurance portfolio and enterprise risk management framework. Developing a standardized, repeatable process to assess enterprise-wide supply chain vulnerabilities is the key essential task in making this happen," says Duchak.

Practice continuous diagnostics and mitigation

As part of its guidance on supply chain security, the National Counterintelligence and Security Center recommends that organizations maintain real-time awareness of the location and operational status of all assets; prioritize the critical systems, networks and information that require protection; and continuously monitor system data and network performance to quickly detect and respond to attempted attacks.[2] Automated scans, artificial intelligence, behavioral analysis, micro-virtualization and other advanced tools are critical components of diagnostics, detection and mitigation. For example, organizations can embed deep learning algorithms into laptops and other computer hardware to detect a zero-day or ransomware attack within microseconds, based on characteristics it shares with previously seen attacks. With micro-virtualization, organizations can quickly isolate application endpoints to contain phishing attempts and other attacks when users browse the internet or view untrusted documents.

Patch and update systems regularly

Human error, external and insider attacks, and system glitches are inevitable. Timely patching and system updates are critical to avoid breaches and downtime associated with these issues. Sixty percent of respondents in a Ponemon study said that a breach occurred because a patch was available for a known vulnerability but wasn't applied.[3] To avoid being a casualty of neglected patching, institute a formal patch management program that ensures patching policies are consistently enforced across the enterprise.

60% of respondents in a Ponemon study said that a breach occurred because a patch was available for a known vulnerability but wasn't applied.

Use data-centric protection

As state and local governments extend operations beyond their physical premises, firewalls, intrusion detection and other traditional controls cannot protect data. A data-centric approach focuses on protecting data rather than the devices or systems it travels on. It includes encryption to protect data at rest and in transit. It also includes multi-factor authentication (MFA) and zero-trust access control. MFA — also called strong authentication — requires a user to combine something they know with something they have in order to access a website or other resource. Beware of phone-based MFA — where a one-time passcode (OTP) is sent via a text message to a user's device. Although this method has become popular, it's vulnerable to interception because many carriers do not encrypt text messages.[4] Application-based and hardware-based MFA mechanisms are more secure. Zero-trust access control adds another level of data protection by limiting who has access to what.

"Risk mitigation will continue to be paramount for procurement leaders into the next decade. Leaders will need to leverage more sophisticated tools, triangulate information and data from more sources, and scan for risks in deeper parts of the supply chain than ever before."

George Duchak, Chief Information and Innovation Officer, U.S. Defense Logistics Agency

Modernize legacy equipment

In a 2020 NASCIO/Deloitte study, state CISOs identified legacy infrastructure and solutions as a top barrier to addressing emerging threats.[5] Legacy systems and software were not designed with security as a priority. In addition, it can be very difficult – if not impossible – to incorporate the encryption or zero-trust access control features that have become essential to modern security. Today's laptops, desktops, printers and other endpoint devices often have built-in mechanisms that make them inherently more secure. For example, industry-leading enterprise printers can detect and self-heal from malware, and they can be upgraded to incorporate new security features over time. With CARES Act funding available to be used by December 2021 and American Rescue Plan funds available to strengthen state and local infrastructure, now is an ideal time to modernize.

An Ongoing Practice Leads to Mature Risk Management

Protecting the IT supply chain is increasingly critical as digital technology pervades nearly every aspect of state and local government – from delivering constituent services and enabling back-office workflows to automating critical infrastructure operations. Managing cybersecurity and risk in the IT supply chain is an ongoing practice. To mature their cybersecurity and risk management posture, state and local government leaders need to incorporate criteria, processes and tools to identify, evaluate and mitigate the risk of supply chain threats.

"Risk mitigation will continue to be paramount for procurement leaders into the next decade. Leaders will need to leverage more sophisticated tools, triangulate information and data from more sources, and scan for risks in deeper parts of the supply chain than ever before," says Duchak.

Organizations can go a long way toward their goals by following the best practices recommended here and by private and public sector leaders.

This paper was written and produced by the Center for Digital Government, with information and input from HP.

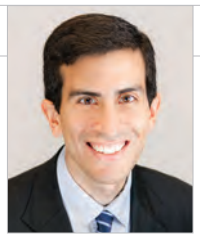
Endnotes:
1. Austin American Statesman. SolarWinds Close to Figuring Out How Cyberattack Occurred. January 2021. https://www.govtech.com/security/solarwinds-close-to-figuring-out-how-cyberattack-occurred.html
2. National Counterintelligence and Security Center. Supply Chain Risk Management:Reducing Threats to Key U.S. Supply Chains
3. Ponemon. Costs and Consequences of Gaps in Vulnerability Response. https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html
4. C. Cimpanu. ZDNet. Microsoft Urges Users to Stop Using Call and SMS-based Multi-Factor Authentication. November 2020. https://www.zdnet.com/article/microsoft-urges-users-to-stop-using-phone-based-multi-factor-authentication/
5. Deloitte-NASCIO. 2020 Deloitte-NASCIO Cybersecurity Study. https://www.nascio.org/wp-content/uploads/2020/10/2020-Deloitte-NASCIO-Cybersecurity-Study-1.pdf

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: hp

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. With the broadest technology portfolio spanning printing, personal systems, software, services and IT infrastructure, HP delivers solutions for customers' most complex challenges in every region of the world. More information about HP (NYSE: HPQ) is available at **www.hp.com**



What the Fax?

It's time to get fax machines out of government offices.

Faxes have mostly disappeared from the private sector, yet they have stubbornly remained a fixture for many government agencies. While public agencies are notorious for their slow rate of technological change, the failure to stop using this obsolete technology is one of the more egregious examples of this phenomenon. Given the apparent reluctance of many government agencies to fully relinquish their fax machines, state and local CIOs should set a firm date by which all agencies must stop using faxes.

While the precursors of today's fax machines trace their roots back to the 19th century, with early prototypes emerging not long after Samuel Morse invented the telegraph, it was not until the 1980s that organizations widely adopted fax technology. Most of the growth occurred because the technology matured: In 1974, it would take about six minutes to transmit a one-page document; a decade later, engineers had cut the transmission time down to less than 10 seconds. With these relatively fast speeds, sending faxes became the go-to solution for transmitting documents, especially the many forms that are the bread and butter of government data processing.

Today, fax numbers are still featured prominently on many government websites, but in many cases, these digits do not serve any clear purpose — they are the vestigial limbs from an older, less-evolved form of the agency. When people do use them, they are often the communication channel of last resort, a sign that something has already gone terribly wrong in delivering a government service. For example, one Virginia resident recently chronicled the absurd lengths she had to go through to obtain unemployment benefits — after attempts to resolve the issue in person, over the phone and online failed, she found herself having to track down a fax machine to send in her paperwork.

What is interesting about fax machines is that they are not hard to replace, so the excuses not to do so are extremely flimsy. The only real purpose of a fax machine is to send and receive paper documents. Unlike other outdated enterprise technologies that might be tightly integrated into existing back-office processes — think legacy COBOL systems — switching from receiving documents by fax to receiving scanned documents by email presents almost no real change in workflow and certainly more people have access to email at home and work than fax machines.

While email is a logical stepping stone for eliminating fax machines, it is often possible to make significant improvements in workflow through other upgrades. Typically the information contained in faxed documents must be transferred to some other system, often through a manual, inefficient and error-prone process. Replacing faxes with web-based forms allows agencies to collect information more efficiently. Indeed, early in the COVID-19 pandemic, many state health departments struggled to produce timely and accurate statistics about infection rates and deaths because their offices were flooded with faxes since they had not transitioned to an online reporting system.

Some government agencies have finally decided to pull the plug on fax machines — at least outside the United States. In March, the finance minister in Ontario, Canada, directed all of the province's agencies to eliminate their 1,500 fax lines by the end of the year. In June, Taro Kono, Japan's Minister for Administrative Reform and Regulatory Reform, issued an edict to all government ministries to stop using faxes by the end of the month. And earlier this year, the German government announced it would eliminate its approximately 8,000 fax machines.

It is past time for state and local governments to draw a line in the sand and similarly commit to eliminating fax machines. Not only will this save money — eliminating printing expenses, telephone service fees and maintenance costs — but it will also push agencies to further digitize their services and move toward web-based data collection that eliminates the need for scanning documents or manually re-entering data and makes it easier for individuals to submit information from their computers or mobile devices. Fax machines have served a valuable role over the past few decades, but the time has come to retire them to the dustbin of history.

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.

By Dan Lohrmann

Rethinking Cyber Talent

Hiring and retaining cyber professionals in state and local government has never been harder. Here are three strategies to help.

As I listen to state and local chief information security officers all over the country, there is no hesitancy in sharing what has been keeping them up at night during the summer and fall of 2021 — but it's not the answer that most business leaders expect.

Sure, ransomware, cyber threats, nation-state adversaries, patching systems, identity management, critical infrastructure protection, audit findings, budget woes, new risk management tools, security operations center improvements, tabletop exercises, zero-trust architectures, supply chain security and more are constantly on their minds.

Nevertheless, the winner is, to quote a recent conversation with a state CISO, "Vacancies! So many unfilled cyber positions. It's become a crisis. I've lost four of my top eight cybersecurity managers/experts this year alone. What can I do?"

No, these hiring and staff turnover problems are not new. We've been talking about attracting and maintaining cybersecurity talent in government for decades.

But a perfect storm of mounting cyber attacks, workforce shifts created by COVID-19, the growing global shortage of experienced cyber pros, and increasingly uncompetitive salary and benefit packages offered in the public sector have turned what was once a stream of concerns into a flood of problems with severe knock-on effects.

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.

One recent trend is the dramatic shift to working from home. Today, many organizations care less about where staff live, opening up out-of-state opportunities. The downside of this trend for state and local government employers is that they are no longer the only option (or perhaps employer of choice) in their area.

So if the cyber talent shortage is so dire, what can be done?

Redesign your hiring practices and pay scale for cybersecurity professionals. If you want to compete as an employer of choice in cybersecurity, it may be necessary to build a new career path and pay scale that is separate from other technology roles. For example, in order to compete with the private sector for cyber talent, the U.S. Department of Homeland Security (DHS) rolled out a new talent management and compensation system. The agency has seen great results, exceeding their hiring goals by more than 50 percent.

No doubt, DHS has advantages, including more resources than most government agencies, and yet many state and local governments can offer attractive options — like working from home — that are not available to three-letter federal agencies. Besides pay and benefits, recruitment should highlight career path options, a flexible work environment, local culture and security training opportunities.

Change what you are looking for and develop talent in house. Another attractive option is to grow your own team with technical expertise from other disciplines, such as system administrators, programmers, database experts and help desk professionals. Yes, degree mandates, certifications and/or other position requirements will likely need to be adjusted, but hiring passionate achievers with most of the required skills can still be effective. Consider building partnerships with local community colleges and universities to help attract interns and students in a win-win scenario.

Partner more with the private sector. When changing your hiring practices is a bridge too far, more security leaders are hiring contractors and/or bringing in managed service providers (MSPs) to run either part or all of their security programs. Indeed, the market has changed dramatically over the past few years, and now almost any technology or security function can be purchased as a service.

While this solution may seem like an obvious choice, you need to strengthen contract management skills on your team to ensure you get the right contract staff or MSP solution. Beware of vendors swapping in unqualified cyber pros after an initial "honeymoon period." Try to establish longer-term solutions and not just plug short-term holes.

Lasting government cyber solutions require looking beyond your organization. Building strategic relationships with other governments and nonprofit groups like the Multi-State Information Sharing and Analysis Center (MS-ISAC) can enable operational economies of scale. Finally, remember you can outsource the work, but not the responsibility. Whatever direction you take, you must become one team that works well together to enable the business of government.

Making government more resilient with cloud-based disaster recovery

State and local government agencies have a responsibility to protect their data, and the data of their citizens, to maintain trust and security. A strong disaster recovery strategy is an essential part of this effort. An effective solution — cloud-based disaster recovery — can help agencies achieve this goal while gaining operational efficiencies.

In this interview, **Alex Berkov,** manager of solutions architecture for CloudEndure Disaster Recovery, a leading cloud-based disaster recovery and business continuity solution offered by Amazon Web Services (AWS), shares the key benefits of moving disaster recovery to the cloud and how agencies can successfully make this transition.

How does cloud-based disaster recovery work, and how can agencies use this approach to protect their technology infrastructure?

Many state and local government agencies may not differentiate between backups and actual disaster recovery. A backup makes a copy of the data, whereas disaster recovery solutions not only protect your data, but also provide a method for recovering the application or workload.

Cloud-based disaster recovery allows agencies to quickly recover in the cloud, reduce downtime and data loss, and increase their resilience. A huge advantage is that agencies can typically recover in minutes without having to procure, manage, or operate a secondary site, such as an on-premises or colocation data center.

This approach also provides a unified solution to protect and recover databases and applications in case of disaster. Agencies can easily replicate their data — whether it is stored on physical, virtual, or cloud servers — in a separate environment at a lower cost.

What are the cost benefits?

The move to the cloud offers cost and operational benefits. The inherent approach of the cloud is you pay as you go. It's very easy to scale. With cloud-based disaster recovery, you don't need to provision or pay for duplicate hardware and software. Agencies can also leverage automation to reduce demands on IT staff. Less tangible is the reduced time to recovery agencies experience when events occur.

How does moving disaster recovery to the cloud also make it easier for agencies to test their environment?

The cloud provides on-demand capacity to test at any time, so you can run disaster recovery drills much more frequently. This gives organizations visibility into the frequency of testing, the ability to run tests more often, and opportunities to validate strategies ahead of issues. With cloud-based recovery, you can run more tests without impacting your users and your IT team doesn't need to spend weekends in a data center running drills. It all can be done remotely.

How can agencies migrate disaster recovery processes to the cloud?

Agencies can start off small, and review and categorize the requirements they have for various applications and workloads. Migrate the critical applications and workloads first, get them protected from a disaster, and test and validate them to ensure they operate in the cloud as expected.

Secondly, and even more importantly, when you move disaster recovery to the cloud, it doesn't interfere with existing methods. For example, if an agency is replicating [its data] in another data center or 'colo,' there is no disruption or conflict with the way they're doing business today. It really reduces complexity in shifting their disaster recovery strategy from on-premises to the cloud.

How can cloud-based disaster recovery accelerate the public sector's move to the cloud?

At AWS, one of the things we've seen with cloud disaster recovery is that it gives agencies the opportunity to dip their toe in the water to run and test their workloads in the cloud. Once they are ready from a knowledge and operational perspective, they can use solutions, such as CloudEndure Disaster Recovery, to fail over to the cloud and shift production workloads. It can be done over time. It's not an all-or-nothing approach.

aws

Amazon Web Services (AWS) Worldwide Public Sector helps state and local government customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation. Read the full paper on **https://govtech.com/cloudresiliency**.

GET INSIGHTS ON THE LATEST TRENDS.

Visit our websites to download helpful resources.

government technology

papers.govtech.com

GOVERNING
THE FUTURE OF STATES AND LOCALITIES

papers.governing.com