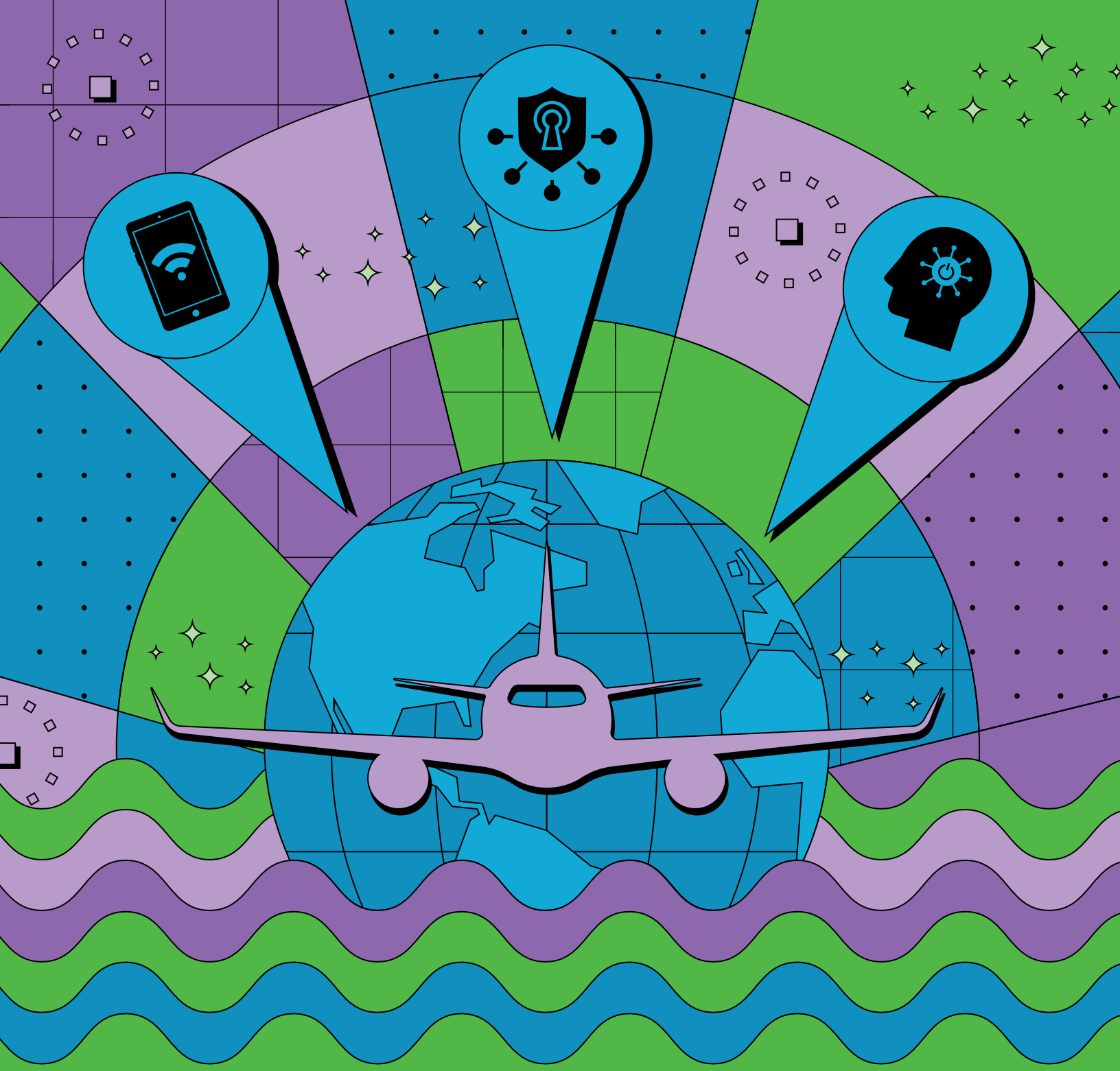


Going Places:
Priorities for State and Local Tech

govloop

carahsoft

Introduction

State and local agencies have a unique impact on constituents' quality of life, and the way people experience local services even can affect how they perceive government overall.

The objective of this guide is to provide actionable information for the public sector, especially regarding three areas of great state and local concern: AI, cybersecurity and data. Agency leaders discuss their recent priorities and achievements and their strategies through 2025 — for instance, demystifying AI, establishing whole-of-state cybersecurity and using data for more effective decision-making. They also share lessons learned, as leaders who have envisioned and implemented both small and large-scale government reforms.

In addition, we hear from industry experts regarding how technology can enhance user experiences. State and local governments have special responsibilities and opportunities. In this guide, we invite you to explore what's possible.

Table of Contents

3 Voices of the Community

7 AI Is Only Part of the Picture

11 Cybersecurity: A Menu of State Priorities

15 Better Communications Tops Data To-Do List

19 Lessons Learned From State and Local Experts

Expert Insights:

5 How to Protect Against Identity Threats
with Semperis

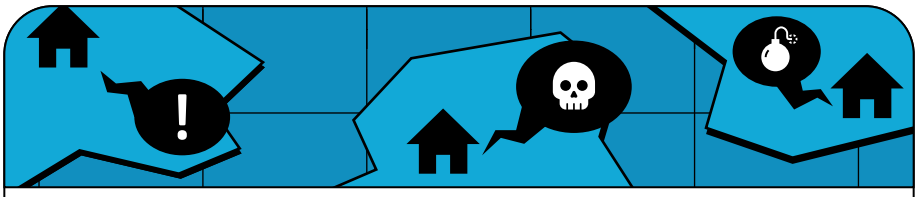
9 How SLED Can Secure OT, Critical Infrastructure
with Fortinet

13 Upskilling Your Workforce for GenAI
with Pluralsight

17 How Identity Drives Security in State & Local Government
with CyberArk

Voices of the Community

Sound bites that speak to top-of-mind issues in state and local government



Data

"We know, based on research, that approximately 4% of geography accounts for nearly half of all crime. We are taking a targeted, data-driven approach to narrow in on neighborhoods across the city that have historically been affected by violence during the summer months."

Cleveland Mayor Justin Bibb, announcing a new data-driven approach to combating violent crime

Workforce

"I do feel like we have a skill set deficit. Right now, we would look toward vendor partners. We have a few enterprising employees who seek out training on their own and on their own time, but their numbers are small compared to all the work we need to be doing."

Anonymous response to a National Association of State Chief Information Officers survey on the impact of GenAI on the state technology workforce

Cybersecurity

"There is a growing recognition at all levels of government that cybersecurity cannot be solely the responsibility of Information Technology (IT) professionals.... While much work has been done by state and local governments to implement stronger cybersecurity protocols and address vulnerabilities, sustained federal funding is critical to ensure continued momentum."

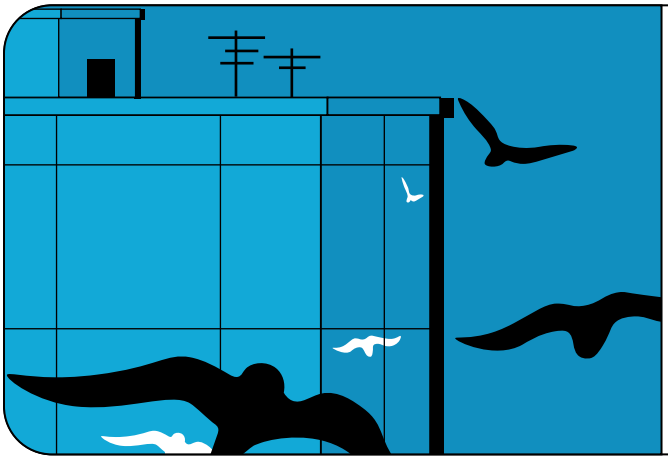
An open letter from **state and local government leaders** urging Congress to preserve the State and Local Cyber Security Grant Program



Critical Infrastructure

"We're entering a new and more dangerous phase, where nation-level adversaries are willing to significantly increase the stakes with destructive attacks on these vulnerable lifeline services."

The Institute for Security and Technology, announcing a new project called UnDisruptable27, which is focused on increased threats to critical infrastructure



Return to Office

"No one should have to come to work with birds flying all around."

Bobby Davis, Senior Adviser to District Council 33 in Philadelphia, arguing that the city's Municipal Services Building, home to a large bird population since remote work began, was not ready for city workers to return to the office

Accessibility

"As technologies — algorithmic and otherwise — continue to become incorporated into everyday life, and as people with disabilities interact with them more and more, disparate and problematic effects will only increase, both in frequency and in severity."

Report from the **Center for Democracy and Technology** on reducing disability bias in technology

Engagement

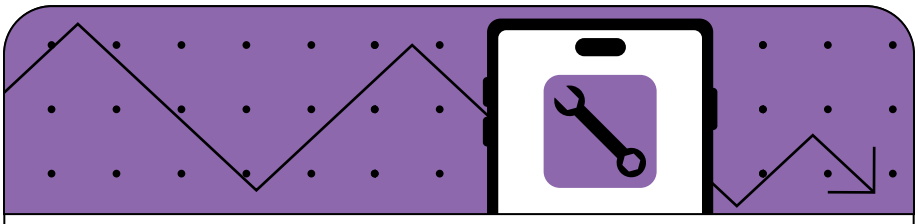
"One of the biggest things that the data indicated is the difference in the language used by business owners compared to the language used by agencies. We could write whatever we want on this site, but if owners aren't searching for it using the same terms we use, we've lost them."

Jessica Lax, New Jersey's Director of Business Experience, in a report by the Beeck Center for Social Impact and Innovation at Georgetown University

Modernization

"We have more than 40 projects at the idea phase and are awaiting funding, approvals, trained staff and procurement."

Response to a **National Association of State Technology Directors** survey



Digital Services

"The overdose crisis is relentless and the need for rapid overdose detection and response has never been more urgent. This [app] is going to be a powerful new tool in our toolbox to reduce overdoses in the county."

Scott Osiecki, CEO of the Alcohol, Drug Addiction and Mental Health Services Board of Cuyahoga County, Ohio, announcing an app that connects drug users with a companion who can assist during a crisis.



How to Protect Against Identity Threats

An interview with Alexandra Weaver, *Senior Solutions Architect, Semperis*

Identity-based cybersecurity threats are on the rise. The number of phishing attempts — the most common type of cyberattack — increased 62% from 2023 to 2024, for instance, and identity-related incidents have directly affected 84% of organizations this year, a 68% increase from 2023. What's more, identity breaches are often the first step to a larger cyberattack, and the public sector is a primary target.

Cybercriminals "are trying actively to hit and target governmental agencies to impact them negatively [and] take them down," said Alexandra Weaver with Semperis, which offers a comprehensive active directory security and recovery platform that protects hybrid environments from identity-based threats. Because state and local agencies are responsible for critical infrastructure, attacks can be disastrous for communities and constituents.

Protecting your active directory (AD) — the core identity system for most organizations — is critical. "Active directory holds the keys to your kingdom," said Weaver. "It is your source record of identity. Everything lies there..., and that's exactly what cybercriminals target."

Watch Your Environment

There are certain things you can do to keep your environment secure, explained Weaver. You can use a tiered administrative model, such as just-enough administration that limits how long someone can access a system and assigns exact permissions for specific tasks. You also can establish privileged access workstations and require multi-factor identification for administrative accounts, she said.

Weaver also recommends a layered security approach with network segmentation. Active directory administrators know they can't have a single point of failure, she said. "We can't just rely on one thing and one methodology."

Overall, Weaver emphasized the importance of having a plan. "It's not [just] important that people have a disaster recovery plan in place, it's actually critical if you want the operation of your business to survive."

Get to Know Your Solution

As you build your plan, an identity threat detection and response (ITDR) solution can help you efficiently monitor, detect and respond to threats, "cut[ting] weeks to days, days to hours, and hours to minutes," Weaver said.

You can test a solution in an isolated lab, evaluating what it provides to help you get up and running again after an incident. An effective solution should focus on what happened and on how, when, and where someone got into your environment. "You want to take the heavy lift out of the situation," said Weaver.

Semperis' Purple Knight tool helps administrators identify and remediate system vulnerabilities. There's also Forest Druid, a Semperis tool that allows agencies to define their most critical, Tier 0 assets and secure them, from the inside out, against identity attack paths, Weaver said. "So, that's a way in which you can really look down and lock down your permissions in AD," she added.

With identity threats growing each day, it's essential to practice recovery operations under non-emergency conditions, to see how well your incident response plan works. "Don't just draft it out," said Weaver. "Actually follow it [and] practice now while you're not under pressure."

semperis

semperis

ACTIVE DIRECTORY IS THE COMMON ATTACK TARGET

Protect Public Sector Organizations from Ransomware

Ransomware attacks against state and local governments, schools, and other public sector organizations are on the rise.



Sophos Report:

60%

of public sector organizations were hit by ransomware in the last year, up one-third from the previous year

Sophos Report:

75%

of public sector organizations had data encrypted the last year—one of the highest across sectors

IBM Cost of Data Breach Report:

1.37M

average cost for public organizations to remediate a ransomware attack

Gain control of public sector identity security

> I recommend Purple Knight for its ease of use—it's GUI-based, it gives you a quick report card, and gives you a good, easy checklist of things to start working on.
>
> Learn more →

Jim Shakespear

Director of IT Security, Southern Utah University

VIEW THE PURPLE KNIGHT REPORT

semperis.com

AI Is Only Part of the Picture

At the state and local level, adopting AI remains only one of a long list of IT priorities. Even when AI is near the top, data and systems often need updates to prepare for it.



Scot Barker, Chief Innovation Officer for Burlington, Vermont, carefully considers each AI application before using it. "I really have to dive into how I implement new technology on a limited budget," he said. "There's not a lot of room for me to say 'It will be cool to explore this.'"

The Journey So Far

In 2023, part of Barker's mission was to "demystify" AI for Burlington government colleagues. "I talk about the demystification, because it was a matter of setting people's minds at ease," he said. "If you've used a smart speaker, you've been using AI at some level. The 'Terminator' robots aren't around the corner."

In 2024, the task shifted to setting formal policy. "I don't think you can do AI without solid policy. How are you using it? How are you restricting your use? How are you annotating [it] when you've used it?" Barker asked.

He is also looking for applications where AI could have the most cost-effective impact. "We're exploring ways we can leverage robotic process automation," he said. For example, an automation could enter invoices into the accounting system rather than people typing them in by hand.

Beyond AI, Burlington is rolling out a new website that uses platform-as-a-service technology. Although that system will improve cybersecurity and accessibility and allow the site to adapt better to the device it's viewed on, there are trade-offs, Barker said. "The new site will definitely modernize the front end in terms of look and feel, but we're going to lose some functionality, some customization capability. It's change management."

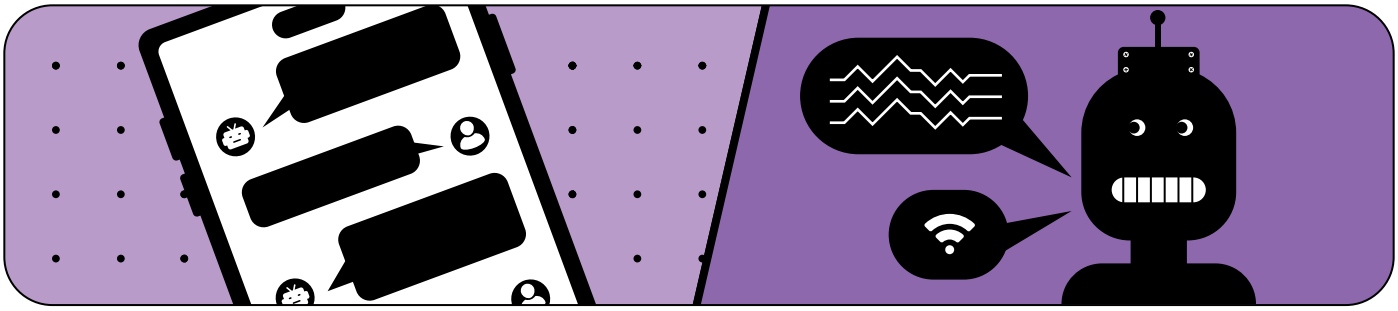
Guidance for Your AI Journey

In July 2024, the National Association of Counties published "AI County Compass: A Comprehensive Toolkit for Local Governance and Implementation of Artificial Intelligence" with the goal of enabling "county government leaders to recognize low-risk versus high-risk implementations of artificial intelligence (AI) and [generative AI] and address the risk and rewards that both bring to local government."

It covers four key themes:

- Prepare the workforce.
- Establish an ethical framework.
- Promote policy models.
- Enable responsible applications.

Along with recommendations on policy, ethics and workforce, it provides guidelines for evaluating use cases, regulations, and existing resources — and counsels robust data governance and cybersecurity.



On the Horizon

Barker is gaming out ways to integrate about eight terabytes of public records into an AI-driven chatbot that could answer sophisticated questions such as "Can you give me all the documentation for the Great Streets/ Main Streets project?"

Because digital records often contain multiple copies of documents, including outdated versions, Barker estimates that only about half that data is unique. Deduplication — winnowing out the extras without losing needed records — is a project that AI renders far more feasible. "And then we've got paper documents that go back forever," he added. "How do I digitize them? How do I make them part of the overall data repository?"

Barker is looking at how AI can help in other areas, too. For instance, the city's enterprise resource planning (ERP) system is also nearing the end of its useful life, Barker said, and "AI will certainly play a role in what our next ERP looks like."

Additionally, he's always aiming to boost cybersecurity. "If you ask your CIO what keeps him or her up at night and the first answer isn't cybersecurity, you probably have the wrong CIO," he said. "We've got a lot of new cyber initiatives going on over the next six to eight months."

But Barker knows these issues aren't unique to Burlington. "I don't think we're super outside the norm," he said. "A lot of people are in the same situation."

GenAI and Accessibility

"Revolutionizing Assistance: How States Can Improve Generative AI's Role in Disability Empowerment," a report by the National Association of State CIOs released in June 2024, provides an overview of where GenAI can advance accessibility — and where it still needs work.

The report incorporates the Department of Justice's guidelines for state and local governments to make webpages and mobile apps accessible, as well as findings from a University of Washington study on the use of GenAI among people with disabilities, and offers **four recommendations for implementing accessible AI.**

1 Engage all stakeholders when evaluating AI tools.

2 Cultivate inclusive datasets to combat AI bias.

3 Embrace transparency in developing AI tools.

4 Confront and navigate AI limitations.



How SLED Can Secure OT, Critical Infrastructure

An interview with Bryan Schneider, *Director, Public Sector, Fortinet*

In state and local governments, much of the operational technology (OT) that monitors and controls critical infrastructure is based on legacy technology. That presents a major challenge.

"Outdated OT systems were not originally designed with cybersecurity in mind. They may lack modern security features, and they are difficult to patch and update," said Bryan Schneider, with Fortinet. In light of rising sophistication among both profit-minded criminals and nation-state actors, this is a recipe for potential disaster.

In fact, a recent survey of WaterWorld and Wastewater Digest members found that 82% view cybersecurity risk as a threat to populations and public health.

SLED entities may struggle to impose greater security on their critical-infrastructure OT. "Upgrading to a modern solution creates complexity," Schneider said, noting that modern solutions "can be incompatible with these preexisting network technologies."

Key Steps

Nonetheless, SLED organizations can take steps to harden their OT.

Agencies must prioritize network visibility as part of their OT cyber strategy, focusing on segmentation between OT and more general IT environments in order to limit the potential impact of a cyber incident, Schneider said.

It's important, too, to "focus the entire organization around accelerating the digitization of the network — to shift the mindset to proactive controls," he said. "It starts with performing a cybersecurity threat assessment. [Organizations] can also dedicate a staff member with a title to focus on and address those complex issues."

Simplicity and Intelligence

As a cybersecurity company with 20-plus years of experience focused on network infrastructure management, Fortinet can help. "We can simplify everything on a single pane of glass, with tools that help deploy solutions efficiently and effectively," Schneider said.

Experts at Fortinet "can walk an agency through a range of security solutions," all delivered via a single platform — an approach that centralizes security and visibility across both IT and OT environments, he said.

"We can assist with network segmentation. Our firewalls can help isolate that OT network, limiting the attack surface and enforcing access controls," he said. "We can also assist with intelligence on the threats, to help detect and block those that are targeting OT environments and critical infrastructure."

Fortinet solutions can help SLED to comply with zero-trust mandates and multifactor-authentication requirements. And they can help "provid[e] staff with tools that give them the analysis and the real-time visibility to monitor [and] detect unusual activities, whether threats come from the outside or inside," said Schneider.

For instance, Fortinet recently helped a water and wastewater district serving about 30,000 residents to strengthen its OT protections. "We deployed an easy-to-use management platform, and the improved visibility has changed the game for them," he explained.

For SLED agencies ready to tackle OT cybersecurity, "keep in mind it's a journey," he said. "Assess the assets that are on the network today, think about the long-term plan, then set realistic short-term goals. And make sure you engage top-level consultants that can help you along the way."

FORTINET



Protect Networks, Data, and Critical Infrastructure with Fortinet

With IT/OT convergence, OT systems in state and local governments present a serious cybersecurity challenge. Fortinet simplifies cybersecurity with a unified platform that secures IT and OT environments. We offer cost-effective, integrated solutions to protect your entire environment, including OT-specific solutions for critical infrastructure.

Find out more at
www.fortinet.com/solutions/industries/government/state-and-local.

FORTINET®

Cybersecurity: A Menu of State Priorities

No state or local entity should assume that it's too small or innocuous to undergo a cyberattack. Hackers will breach every government network eventually, and agencies that are underfunded and overconfident in their cyber defenses make successful attacks all-too-easy.



To manage and recover from a cyber event, organizations need updated, coherent strategies — not faded handbooks pulled off a shelf. For certain, officials must "prepare for the worst," said **Michael Gregg**, North Dakota's Chief Information Security Officer, "and be ready to deal with whatever comes [their] way."

The Journey So Far

Over the past year, Gregg and his team have focused on the increased volume and variety of cyberthreats. "The attacks that we see and the number of attacks coming in are really amplified way up from what [they were] just a few years in the past," he said. For instance, nation-state actors are targeting state entities in the U.S., denial-of-service attacks are more common, and AI is defeating traditional cyber protections. "Controls that we put in, historically, to try to prevent … problems can now very easily be bypassed with AI," Gregg said.

His office also has worked toward a whole-of-state security approach, as per a 2019 North Dakota law that gave the cyberteam command-and-control over cybersecurity in all branches of state government. Every public-sector entity — city, county, school, library, police station, etc. — gets its network services from his office, Gregg explained, and the goal is for all entities to buy and use the same tools.

A third priority has been readying the North Dakota public sector for future events "because it's not if the next bad thing will happen, but it's when," he said. That includes staff training and running through cybersecurity processes so they become second nature. Gregg calls it "sharpening the saw."

Securing Water Systems

The White House and the Environmental Protection Agency warned governors in March 2024 that municipal water systems are in the crosshairs of nation-state hackers. "Drinking water and wastewater systems are an attractive target for cyberattacks," the joint letter explained, "because they are a lifeline critical infrastructure sector but often lack the resources and technical capacity to adopt rigorous cybersecurity practices."

The letter asked governors to help ensure that their state water systems assess — comprehensively — their cybersecurity defenses and fix any vulnerabilities, e.g., changing default passwords immediately. **The letter also linked to water system-specific information regarding cybersecurity:**



Assessments



Response



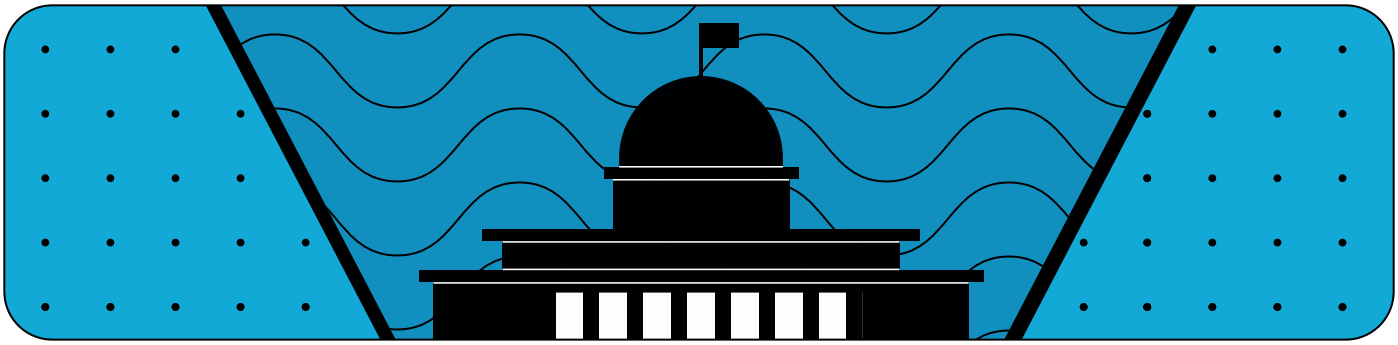
Planning



Training



Funding



On the Horizon

Through 2025, strengthening agency preparedness will be a major objective, he said. His team has begun visiting with state and local entities, spending at least half a day with each of them, to review their cybersecurity and business continuity plans. Officials discuss whether the strategies are "living," if hard-copy backups exist — because electronic documents could be inaccessible during a cyberattack — and which communication options would be available during a major event.

"In a previous job, I asked someone for a plan, and they pulled it off the shelf, blew the dust off it … and said, 'Sure, we've got a plan from [about] 30 years ago,'" Gregg remembered. That's a problem for any organization, and certainly for government.

Soon, Gregg's office will develop its approach for the North Dakota legislative session, which takes place every other year. Working with public-sector entities to discuss their priorities and the related security impacts, he and his team will consider, for instance, whether third-party risk assessments and new vendors would be appropriate.

The idea is to create a unity of effort, Gregg said, "so when we go to legislative session, we can help support our partners with what they need, and they can help support us, where we can do things to move the program forward."

Safeguarding Infrastructure

In June 2024, the Cybersecurity and Infrastructure Security Agency (CISA) issued a how-to playbook to help state, local, tribal and other entities tighten security for vital infrastructure and engage in resiliency planning. "Resilient infrastructure is critical to the safety, security, and viability of our communities," the resource said. "Additionally, a secure and resilient infrastructure can enhance the overall quality of life for community members by improving the mobility and connectivity of essential services, leading to increased economic opportunities."

The playbook supplements CISA's Infrastructure Resilience Planning Framework and explains how to:

- Begin the resiliency process.
- Prioritize infrastructure.
- Assess risk.
- Identify mitigation strategies.
- Implement solutions.



Upskilling Your Workforce for GenAI

An interview with Tony Holmes, *Practice Lead for Solutions Consultants, Public Sector in North America, Pluralsight*

In the constellation of AI technology, generative AI (GenAI) is a natural option for state and local agencies looking to innovate and improve productivity. Especially for organizations with relatively small development teams, GenAI "is where the immediate, low-hanging fruit is," said Tony Holmes with Pluralsight, which provides skills training through an online data-analytics platform.

Agencies can best prepare their workforces for GenAI by focusing on broad-based upskilling relevant to all employees, he said. "Some agencies … tend to think, 'we've got these specialists, we've hired them, they're super-smart people, and they know how to do all kinds of cool stuff,'" Holmes explained. "When in actual fact, being able to empower all of your employees to understand and effectively use generative AI is a much more powerful use case."

Expert Generalists

That's because, among other reasons, frontline workers know how AI tools could improve their daily tasks better than leadership or IT specialists probably do. Widescale GenAI literacy leads to more creativity and adaptability and better government services, said Holmes. "It's very much a grassroots approach that encourages innovation from the ground up," he said.

Unlike other fields, being a specialist isn't helpful — or even practical, given how quickly AI evolves. Because GenAI is like using Google with context added in, non-IT talent is valuable, Holmes said. "People, for example, with a liberal arts education will be much more predisposed to making abstract connections when it comes to solving problems than perhaps [IT staff who] go deep down the rabbit hole," he explained.

Agencies ultimately can foster what Holmes called "expert generalists," who adapt to new technologies as they come along.

Barriers

But there are challenges. Even when organizations recognize GenAI's potential, they often lack a specific plan, and that leads to unfocused training. Sometimes leadership roles are unclear and limited resources make it hard to implement AI broadly. Organizational silos can prevent the inter-team data sharing needed to build a holistic strategy. And then there's workforce culture.

Fear of job displacement is real, said Holmes. "But forward-looking agencies will engage with their workforce and basically use concepts like, 'hey, yes, the AI can do this part of your job, but what that does is free you up to do much more interesting stuff,'" he said.

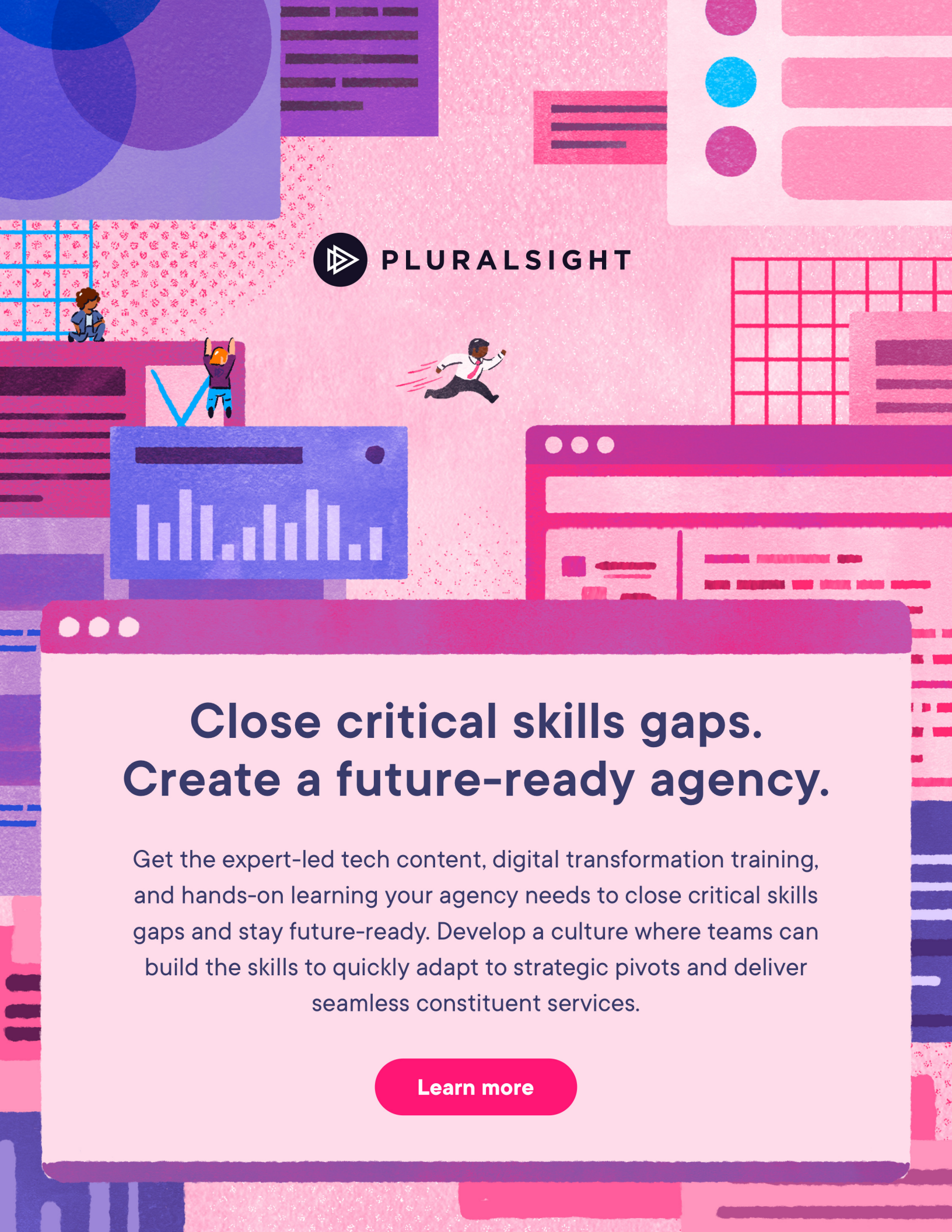
The Pluralsight Platform

When it comes to GenAI training, coursework in a variety of technologies — data, cybersecurity, cloud, etc. — can be a "force multiplier," Holmes said. The Pluralsight platform, for example, offers 7,000-plus courses that span different fields.

And while video training is important, Holmes said that people also need hands-on experience, so Pluralsight lets them play in a virtual sandbox and try GenAI prompts without releasing them on the worldwide web.

The platform's AI-driven analytics help learners track their progress and leadership gauge their employees' knowledge. That allows agencies, Holmes explained, "to avoid the pitfalls of adopting new technologies and then scrambling to hire people to execute [them]."

PLURALSIGHT



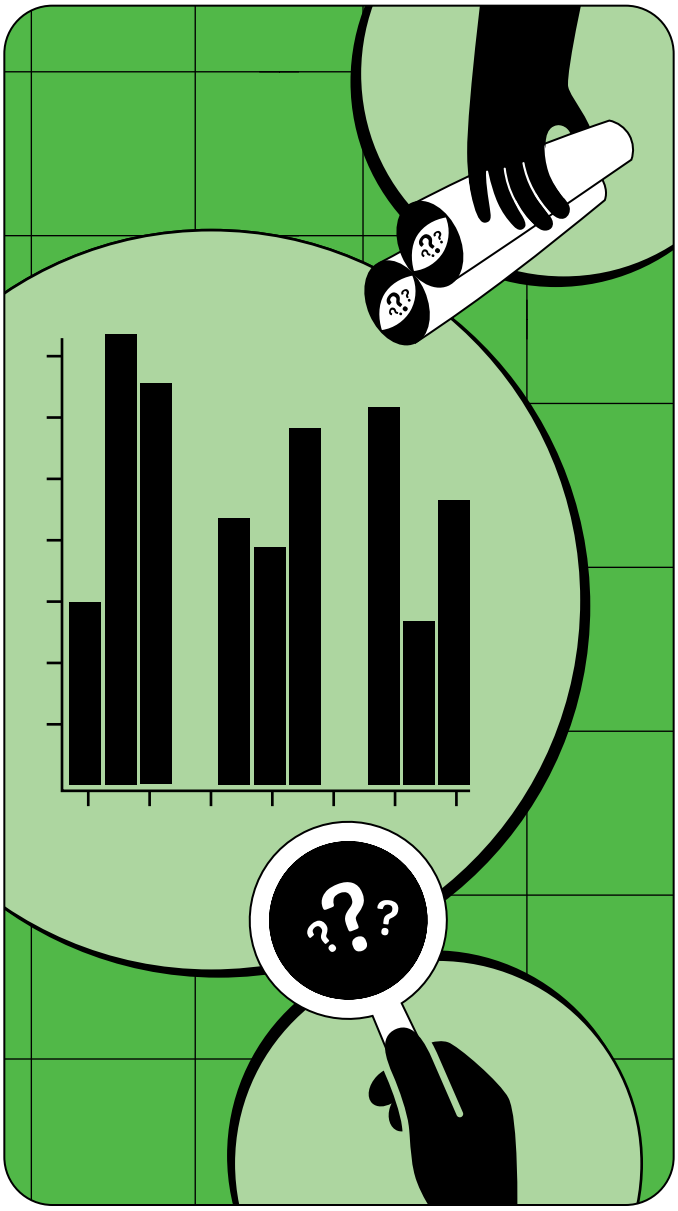
Close critical skills gaps. Create a future-ready agency.

Get the expert-led tech content, digital transformation training, and hands-on learning your agency needs to close critical skills gaps and stay future-ready. Develop a culture where teams can build the skills to quickly adapt to strategic pivots and deliver seamless constituent services.

Learn more

Better Communications Tops Data To-Do List

An interview with Mallory Bateman, Director of Demographic Research, Kem C. Gardner Policy Institute



Year in and year out, the U.S. Census Bureau offers up an abundance of data that state and local agencies can use to gain insights into the shifting demographics of their constituencies, and to shape policies and programs accordingly.

For many agencies, the challenge is learning to communicate those insights effectively. It's not enough to dig up good data. You need to craft data-driven narratives that connect with the intended audience, whether government officials, legislators or constituents.



"You can have a bar chart that is the prettiest bar chart, but if no one knows what you're trying to show or what the data is telling you, it's not helpful," said **Mallory Bateman** with the Kem C. Gardner Policy Institute.

The institute, which is based at the University of Utah, provides state and local leaders with economic, demographic and public policy research. Bateman and her team focus on demographics and work extensively with Census data, but also create their own datasets based on local input. Their research supports policy development around a wide array of issues, from transportation, energy and natural resources to education and housing.

"We take a lot of pride in really vetting our data, really putting a lot of work into understanding the different things that are going on with births, deaths, migration, the economy and so on," she said.

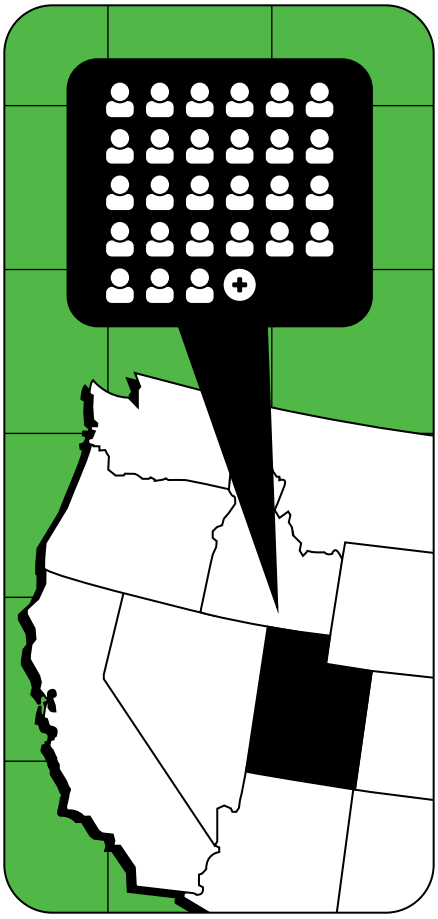
A Case Study in Data-Driven Communications

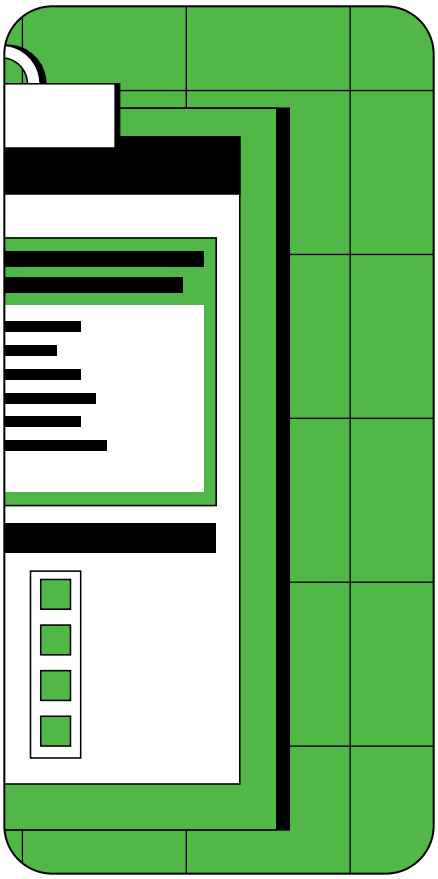
Bateman says it's important to understand the interplay between quantitative and qualitative insights — between what the data shows and what people see happening in their communities.

For example, a recent projection showed continued growth in Utah's population, while a public opinion survey showed increasing opposition to such growth. In response, the state planning coordinator worked with the Office of Planning and Budget and other groups to meet with stakeholders statewide, walking them through the data specific to their regions and offering a chance to share their concerns and stories.

Both the communities and state leaders benefited from these exchanges, Bateman said. "I think in some small ways, we brought the temperature down," she said. "And in some ways, we learned some things that maybe we wouldn't have heard because those voices aren't always in the rooms at the state level."

This initiative led to an ongoing effort to provide more guidance to communities on how to navigate population shifts, so municipalities understand their different options, whether regulatory or legislative. By working with both the quantitative and qualitative data, Bateman believes Utah can "set up a strategy for communities to feel like they can maintain the quality of life they're worried about losing."





More Data on Tap

Over the past year, Bateman's team has been digging deeper into data from the 2020 Decennial Census, with a focus on race and ethnicity. That data is readily available in a Census dataset called the Detailed Demographic and Housing Characteristics File A, or Detailed DHC-A, but it's tough for anyone who's not a data expert to understand.

"Heidi Pryor, on my team, has done a magnificent job of putting together these beautiful reports that summarize the information in a really nice way, taking a dataset that's a little bit gnarly and making it more manageable for top-level data users," Bateman said. Five such reports will be available by year's end.

She and her team also have been working on the institute's standard 10-year projection for the state's population, which is vital for policymakers developing budgets in areas such as transportation and water. In the next year, Bateman's team will begin work on 40-year projects, which assist with longer-term planning.

Those projects are "interesting to communicate to people because we base it on a set of assumptions around fertility, mortality and the economy," which might shift over time, she said. "So, we're getting more and more nuanced in our language-crafting."



How Identity Drives Security in State & Local Government

***An interview with James Imanian,** Senior Director, U.S. Federal Technology Office, CyberArk*

In today's threat environment, where ransomware and other attacks aim to steal and exploit user credentials, a focus on identity "is the first step in securing state and local systems," said James Imanian with CyberArk. Yet many state and local IT teams struggle to implement strong identity controls.

"Limited budgets mean that they've got older IT infrastructure," and IT teams may be unable to adopt modern cybersecurity strategies, he said. And they may be slow to adapt, simply because normal bureaucratic hurdles get in the way.

This means agencies often lack the tools needed to adequately address today's cyber threat — but there are steps agencies can take to strengthen their identity security.

Getting More Secure

"At the tactical level, organizations that haven't implemented multifactor authentication (MFA) need to do so," Imanian said. "That really needs to be a cornerstone of their identity security practice."

IT teams also need to regularly patch their systems. "The vulnerabilities the threat actors are using are often four or six months old," Imanian said. "If you have the ability to patch quickly, those incidents may not happen."

Security teams can implement strong password policies, using tools such as business password managers and single sign-on — which enable the use of more complex passwords without requiring people to memorize them. In addition, IT should lean more heavily into employee training and awareness.

"The human is your first line of defense: It's not your weakest link, it's your strongest," Imanian said. "[People are] going to be in the trenches, they're going to be doing the workflows. They're going to see those phishing emails, and you really need to train them well."

Making a Difference

As a global leader in identity security, CyberArk helps, offering a platform that can be the first line of defense against malicious actors and unauthorized access.

"CyberArk brings an identity security platform approach, to protect every identity with the appropriate level of privilege controls," Imanian said. "It enables secure access for any identity, human or machine, to any resource or environment, from anywhere, using any device."

The technology supports the discovery and management of user credentials and enables agencies, Imanian said, to isolate those credentials and the sessions those credentials initiate. It also enables agencies to record and audit the sessions for compliance and incident response.

The Chico Unified School District offers an example of what's possible, said Imanian. With a small IT team and a large number of users, "CyberArk helped them improve their identity security by strengthening their passwords, applying MFA and managing privileged access across their school district," he said.

Ultimately, to make best use of scarce resources, IT teams should address identity as part of a larger cyber strategy. "Understand the applications and the workflows that enable your mission, as well as your adversary's intent and capability," Imanian said. "Work with leadership to look at the big picture."

CYBERARK®

CYBERARK®
The Identity Security Company™

Identity Security and Zero Trust

Secure Government Identities and Shut Out Attackers

Learn more about CyberArk's FedRAMP High Authorized Solutions!

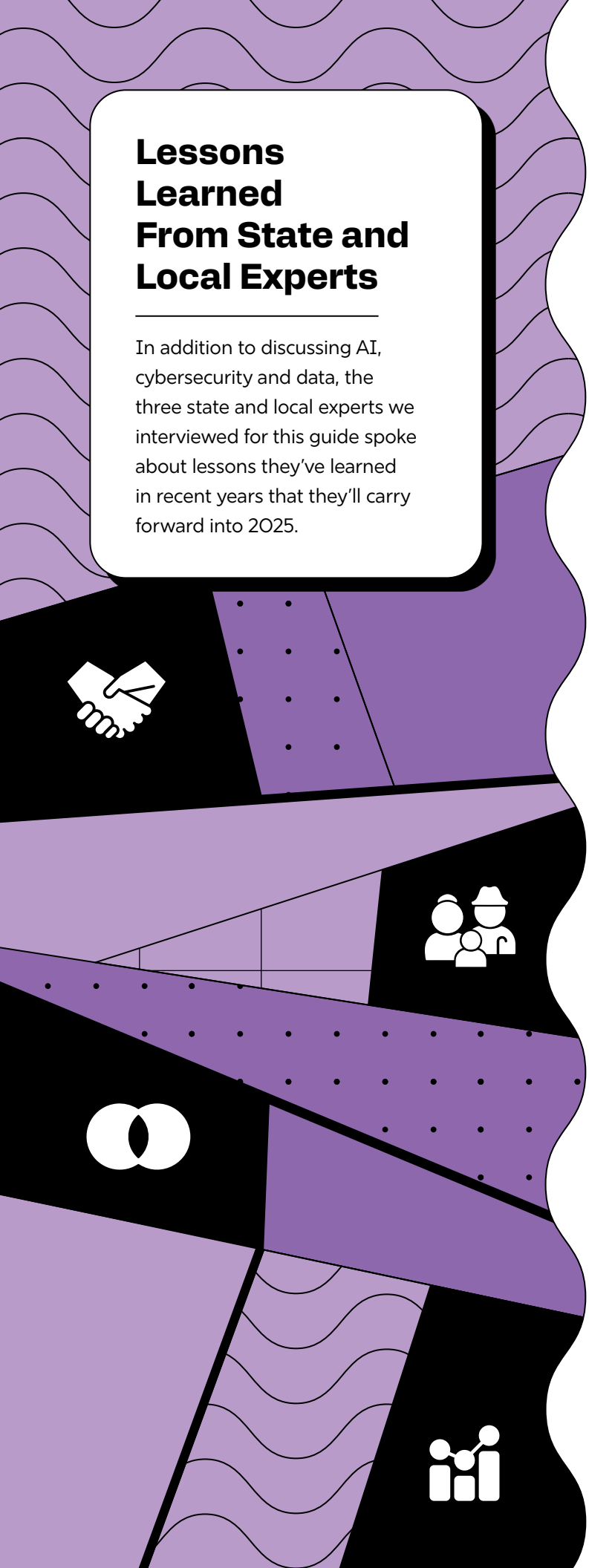
- Endpoint Privilege Manager (EPM) for Government
- Identity for Government

www.cyberark.com



Lessons Learned From State and Local Experts

In addition to discussing AI, cybersecurity and data, the three state and local experts we interviewed for this guide spoke about lessons they've learned in recent years that they'll carry forward into 2025.



Collaboration leads to more knowledge.

State and local agencies rely heavily on federal Census Bureau data to gain insights into their communities. But those insights, in fact, emerge from a collaborative process, said Mallory Bateman, Director of Demographic Research at the Kem C. Gardner Policy Institute. "The local partners do play a really important role [in data], both behind the scenes and then once it comes out," she said. Transparent data collection and dissemination through federal/local collaborations help constituents trust in — and engage with — the data.

You can't ignore generational preferences.

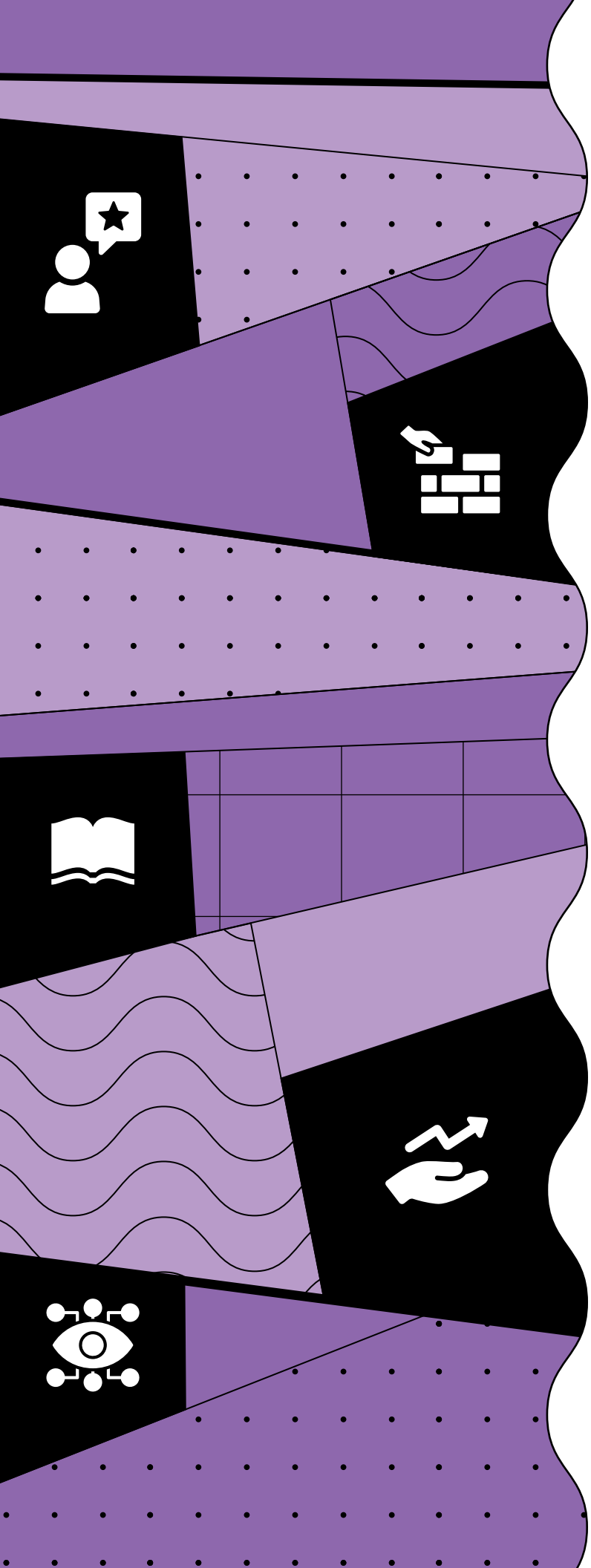
Scot Barker, Chief Innovation Officer for Burlington, Vermont, observed that most members of Gen Z aren't going to city hall to request public services. For them, a digital-first approach is needed. But what about the people who prefer an in-person experience? You must have the right tools for everyone. "You can't leave all those people behind, but you can't also ignore the next generation who wants to engage in a different way," Barker said.

Government is both similar to and different from the private sector.

"[The public sector] doesn't, obviously, move at the same pace that it does on the private side. It takes time to get things done," said Michael Gregg, Chief Information Security Officer for North Dakota. "But the key to it, in many ways, is exactly the same." He called it a "unity of effort."

Collecting data is just the beginning.

Data must be understandable and actionable, said Barker. No matter what the agency's goals are, data can't just be a confusing set of numbers on a page. Whether it's intended for the public or to be distributed among agencies, he urged data professionals to ask, "How can I clean it up and make it usable?"



Know who the experts are.

One of the challenges in working with Census data is that it takes expertise just to know what you're looking at. The good news, said Bateman, is that there are experts who take that data and turn it into great products that just might meet your needs. "There are a lot of existing resources people can turn to so that they don't have to recreate the wheel," she said. "You want to work smarter, not harder."

Buy-in comes from building relationships.

To establish larger-scale, cohesive efforts, Gregg said that officials must foster personal connections with other agencies and entities, as well as with elected officials. That's "because much of what you want to do, you don't have control to do it," he explained. Relationships with other people and agencies will help.

Storytelling is important.

Bateman emphasized moving away from a "baseball statistics" approach. She encouraged data communicators to know their audiences and what they can naturally understand and interpret. "If you're going for a public audience, keep it simple. Keep it straightforward. Don't try to mix too many things together," she said.

Make sure you're improving constituent experiences.

Sometimes, internal improvements make things easier for agency employees. But if they don't also make things better for the public, that moves away from the mission, not toward it. "We're not here for us — we're here for them," said Barker.

Have a bigger vision.

"Get a small win and then another small win and then another" to advance a larger project, said Greg. As you recognize and celebrate those small achievements, your work shows momentum, "and it's easier and easier to get people on board" for what comes next.



Conclusion

This resource is the second installment in our 2024 State and Local guide series. The first installment, Building Trust With Tech In State and Local Government, looked at how state and local agencies are leveraging technology to enhance operations and service delivery while building trust with constituents.

About GovLoop

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

Thank You

Thank you to Carahsoft, CyberArk, Fortinet, Pluralsight and Semperis for their support of this valuable resource for public-sector professionals.

Authors

Susan Kirby-Smith, Contributing Writer
John Monroe, Director of Content
Candace Thorson, Managing Editor
Lauren Walker, Senior Staff Writer

Designers

Marc Tom, Junior Graphic Designer
Julia Blurton-Jones, Motion Graphic Designer

govloop carahsoft