Preparing for Future Shocks in State Government

State CIOs play an important and expanding role in resilience.

CENTER FOR DIGITAL GOVERNMENT

NASCIO

IBM

Contents

Acknowledgements

We thank the Center for Digital Government, NASCIO and IBM professionals who helped to develop the survey, analyze the data and create this report.

NASCIO

Doug Robinson, Executive Director

Amy Hille Glasscock, Program Director, Innovation and Emerging Issues

IBM Subject Matter Expert Contributors

Dan Chenok, Executive Director, IBM Center for the Business of Government

Dave Zaharchuk, Research Director, IBM Institute for Business Value

Center for Digital Government Research and Content Team

Teri Takai, Senior Vice President

Jeana Bigham, Director of Content Studio

Steve Towns, Director of Content Strategy

Jordan Trejo, Research Analyst

Chelsea Church, Project Manager

Foreword

It's a risky world out there, and state CIOs increasingly find themselves at the forefront of managing an array of disruptive threats.

That's perhaps the ultimate takeaway from 21 state CIO interviews conducted in July and August 2023 by the Center for Digital Government in partnership with the National Association of State Chief Information Officers and IBM.

Three years ago, of course, states confronted perhaps their starkest challenge to the continuity of government. The pandemic underscored the importance of agile and adaptable technology systems, and even more so, the value of problem-solvers and innovators in government workforces. These resilience lessons shape how state CIOs approach technology modernization and workforce development.

But other powerful forces are at work, too. Climate-driven events — flooding and wind damage from increasingly violent storms, drought-fueled wildfires, massive dust storms — are prompting more states to adopt cloud and hybrid technology that reduces dependence on physical infrastructure. The difficulty of attracting a new generation of employees to public service is forcing greater focus on building new talent pipelines and unconventional career paths. Cyber threats continue to escalate, pushing state IT teams into first-responder roles to recover impacted state government systems — and often local government systems, as well. CIOs are also racing to understand emerging technologies like artificial intelligence that promise to address multiple resilience challenges, even as these tools create new forms of potential disruption.

Our interviews spanned a geographically diverse group of states ranging in size from Texas to Rhode Island. Across those jurisdictions, CIOs told us the quest for resilience is impacting everything from their technology roadmaps and workforce strategies to their management styles and inter-departmental relationships.

We encourage you to look at the strategies and tactics covered in this report for ideas that can help strengthen resilience in your state. We also point you toward important advice offered by CIOs on maintaining personal resilience in an increasingly demanding role. We hope these tips help you take better care of yourself as you address broader resilience challenges.

Finally, we want to sincerely thank the 21 state CIOs who graciously gave their time for extensive interviews on their approaches to resilience. Your thoughts and experiences will guide others as they enhance their ability to withstand disruption and prepare for future shocks.

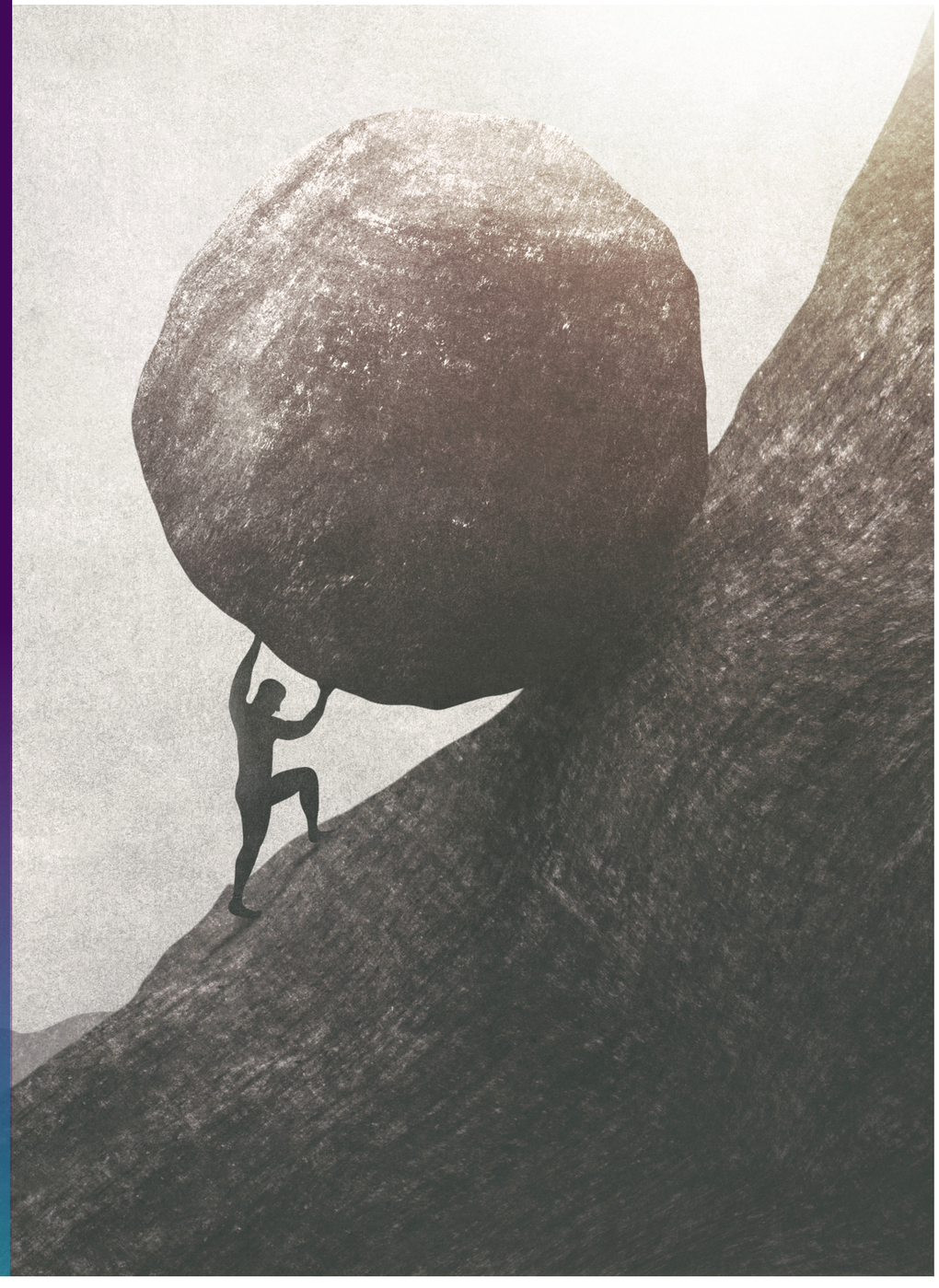
Teri Takai
Senior Vice President
Center for Digital Government

Frank Attaie
General Manager
Technology – Public Sector
IBM

Doug Robinson
Executive Director
NASCIO

Introduction

State CIOs see a growing array of threats to the continuity of government programs and services. They're working within their own teams and across the state enterprise to address these risks.



State chief information officers (CIOs) face a range of issues that could test the resilience of their states, their teams and themselves — everything from future public health crises and cyber threats to climate change, workforce shortages and disruptive new technologies. To help frame what future disruptions may look like for state CIOs — and how they can effectively tackle them — the Center for Digital Government (CDG) partnered with IBM and the National Association of State Chief Information Officers (NASCIO) to interview 21 state CIOs on the topic of resilience. The interviews uncovered key themes about the threats state governments face and the tools, processes and resources CIOs are using to build more resilient organizations.

CIOs see a direct link between IT modernization and resilience. They're working to increase investment in modern enterprise services provided by the central IT organization and evangelizing the need for modernization to business leaders in other agencies.

Our research also found state CIOs are employing other strategies to build resilience, including collaborating more effectively with internal and external partners to improve business continuity and disaster recovery (DR), embracing a hybrid cloud or multicloud approach, and upskilling and reskilling employees.

CIOs also view innovation as an enabler of resilience. They're already using artificial intelligence (AI) and automation to protect against expanding cyber threats and ensure the availability and performance of complex IT environments. In addition, they're carving out space to experiment with emerging technologies like generative AI to understand their value and potential impact.

Based on 21 interviews, here's how state CIOs are building a resilience roadmap to prepare for whatever comes next.

Top Threats for State Government Disruption

Cyber crime is more dangerous. Climate-driven risks are pervasive. Workforce shortages pose near- and long-term challenges. Emerging technologies bring unknown impacts.

CIOs view their environment as increasingly volatile. CDG research found the top threats to the continuity of government services are a mix of long-running issues that are now being magnified and newer threats driven by climate change. CIOs noted their top threats as:

☐ **Cyberattacks and fraud:** Cyber threats continue to be front and center, especially attacks launched by nation states or other sophisticated organizations targeting critical government services. CIOs expect these threats to escalate and become greater dangers as attackers employ AI and other tools.

"It would be hard to think of any threats bigger than cyber threats. You can bolster, reinforce, train and bring in technology, but it only takes that one lapse," says Chris Rein, New Jersey's chief technology officer (CTO).

☐ **Natural disasters and climate change:** Climate- and weather-driven disruptions, which may not have been on the radar for many state CIOs a decade ago, are now a key risk.

"We have a major threat of drought across the West, but it's particularly acute in Utah," says Alan Fuller, the state's CIO. "Over the last two years, our legislature has invested $500 million per year in drought remediation to address the problems we have. The Great Salt Lake is in serious jeopardy of drying up completely, and that would be an ecological disaster of epic proportions."

Fuller adds that drought also increases the risk of massive wildfires, which could pose a major threat to critical infrastructure.

> “It would be hard to think of any threats bigger than cyber threats. You can bolster, reinforce, train and bring in technology, but it only takes that one lapse.”
>
> — ***Chris Rein**, Chief Technology Officer, State of New Jersey*

“Roads could become impassable. Power, network or phone lines could be cut, so there are a number of ways these potential threats could negatively impact us,” he says.

Whether it’s droughts, earthquakes, Category 5 hurricanes or another pandemic, state governments will need to build on and advance the systems and processes they put in place during COVID — including hybrid work infrastructure, stronger identity management and portable workloads — to better prepare for inevitable future disruptions.

☐ **Technical debt and legacy systems:** Legacy systems and the niche workforces that support them were another commonly cited vulnerability. One lesson learned from the pandemic is that aging, hard-coded systems struggle to adapt to new needs. These technologies can’t change fast enough in a crisis. In addition, the institutional knowledge to run these systems is waning as long-time employees retire.

☐ **Insufficient workforce talent:** Persistent talent and skills gaps only worsen states’ legacy system challenges. The gaps are pervasive within state IT organizations and across state government. CDG research found CIOs view this as both a near-term and long-term threat.

“When you look at the percentage of employees eligible for retirement in the public sector, it really gets to be staggering,” says Amanda Crawford, CIO of Texas and executive director of the Texas Department of Information Resources. “We’re working to build up those resources in the pipeline, but at the same time we’re building the pipeline, we have increased demand for technology and the evolution of technology.”

Research from the Rockefeller Institute of Government found that state and local government employment peaked at 20 million workers before the pandemic. However, the sector lost 1.5 million jobs during the crisis. Some of those jobs have returned, but state and local governments remain about 928,000 jobs below where they were before the pandemic.[1]

With a wave of impending retirements and workers leaving for the private sector, state governments must address ongoing talent gaps as an urgent threat to resilience even as they focus on modernization.

☐ **Economic uncertainty and budget constraints:** Many CIOs said their states struggle to make sustained investments in resilience. Agencies often prioritize immediate needs over long-term resilience efforts. Current federal funding measures are also leading to one-time or short-term funding, both of which make supporting long-term, strategic modernization initiatives more challenging.

“While my grandmother used to tell me, ‘A bird in hand is worth two in the bush,’ there comes a point in time when you’re trying to do some of these critical services, like cyber, and one-time funding only gets you so far. It doesn’t get you to what you need to achieve,” says North Carolina CIO Jim Weaver.

☐ **Leadership turnover and administrative instability:** The relatively short tenure of most state CIOs also makes long-range planning and sustained resilience funding more difficult.

Many CIOs said they approach planning in two-year windows, focusing on what they can accomplish by the end of their administration’s term so that the next administration is well positioned to build on these efforts.

☐ **AI and partner resilience:** Other threats CIOs mentioned centered around rapid technological advancements such as AI and the risks and opportunities it poses, as well as private sector resilience risks.

AI — especially generative AI — poses both a disruptive threat to state governments and a valuable opportunity to automate manual tasks and increase efficiency. CIOs said effective governance and skill-building will be critical to take full advantage of this technology and minimize risks.

“We don’t fully understand yet what generative AI and some of these other newer technologies will bring forward,” says Weaver. “As we look across the threat landscape, we need to figure out how to make effective use of these tools — and we need to make sure we have people who are skilled in the right areas.”

In addition, CIOs are paying more attention to the resilience of their partners. As state governments increase their reliance on third-party service providers, the resilience of these companies impacts state resilience.

☐ **Housing and homelessness:** A few CIOs cited potential disruption from societal issues such as rising homelessness. For example, Arizona CIO J.R. Sloan says the lack of affordable housing is a concern amid rising population growth, immigration and border security issues for his state.

States are focused on maintaining and enhancing quality of life for residents, but these issues could put even more strain on government services, especially when tough economic times reduce funding or lead to program cuts.

> “When you look at the percentage of employees eligible for retirement in the public sector, it really gets to be staggering. We’re working to build up those resources in the pipeline.”
>
> — ***Amanda Crawford**, CIO, State of Texas*

Understanding the CIO's Role in Resilience

In a complex risk environment, CIOs are taking a multifaceted approach to minimize potential disruption.

Our research explored the CIO's role in resilience across three dimensions. We looked at how CIOs function as part of the state's executive leadership team to strengthen enterprise resilience. We examined their role as the state's primary provider of IT services and leader of the IT workforce. And we looked at how CIOs maintain personal resilience in a high-profile and high-pressure environment.

Enterprise Resilience

CIOs are playing a bigger and more active role in overall state government resilience. This is happening in several ways.

CIO organizations play a key role — often in partnership with traditional state emergency response agencies and law enforcement — in responding to cyberattacks on state agencies. They increasingly help local governments and schools recover from attacks, too. Louisiana and Texas are just some of the states that use this collaborative approach.

"The governor's Office of Homeland Security and Emergency Preparedness responds to requests from the executive branch and also from local government entities that have been hit with ransomware," says Dickie Howze, Louisiana's CIO. "We've responded to more than 100 incidents — but in my mind, that builds resiliency at the statewide level that we otherwise would have never had."

CIOs are also bigger participants in general disaster response due to government's growing reliance on technology and digital services. Unlike the past, they are now routinely part of teams that staff state emergency operations centers during major incidents to make sure critical systems and communications remain available.

In addition, CIOs see themselves playing an enterprise or cross-agency business continuity and resilience role. Several respondents talked about having discussions with state

agency leaders regarding business risks related to IT systems and the need for investment to improve the resilience of critical services.

This is a particularly important role for CIOs, given the lack of enterprise resilience officers and offices in state government. Among all the CIOs interviewed for this report, only Howze said his state had a chief resilience officer, a position Louisiana's state legislature just approved in July 2023.[2]

The focus on enterprise resilience is driving greater use of traditional disaster preparedness techniques. CIOs are doubling down on disaster recovery (DR) planning, drills and exercises. Multiple CIOs talked about the need to understand and establish cross-agency relationships before an incident occurs. Some state IT organizations conduct joint training with private sector organizations and other government jurisdictions.

For example, Nebraska holds annual two-week tabletop exercises with all its state agencies, the military and several private sector partners. Nebraska CIO Ed Toner says these engagements are critical for knowledge sharing.

"We share our techniques with one another, so we learn from the private sector and they learn from us," he says.

Some states have formalized their multidisciplinary approach into policy. Rhode Island CIO Brian Tardiff says his state's emergency management agency has what it calls critical infrastructure sector-specific plans (SSPs) that capture all components of incident response activities across state government. For all incident types that impact residents' safety and security, Tardiff says it's critical for state agencies to jointly develop response plans and exercises and incorporate lessons learned from previous incidents.

"Relationships are truly the key to organizational resilience," Tardiff says. "Building trust with internal and external partners is the only way a true understanding of stakeholders' concerns and gaps in capacity and competency can occur."

Our interviews indicate CIOs often serve as critical enablers of enterprise resilience in an environment where technology drives nearly every aspect of government operations. From a resilience perspective, CIOs have become chief collaborators to bring different parts of the organization together for a common purpose and to achieve shared goals.

IT Resilience

As providers of critical statewide technology services, CIOs are taking multiple steps to strengthen IT resilience, including modernizing legacy systems, moving to cloud and hybrid environments, and embracing automation. Overall, there's been a post-COVID shift in the perceived value of modernization among state governments. These investments are now seen as critical to governments' ability to withstand unexpected disruption. It's not just about the constituent experience or efficiency — it's about keeping vital operations running.

☐ **Wider acceptance of cloud as an enabler of agility and resilience:** Many CIOs are reducing their reliance on state-owned physical infrastructure by adopting hybrid and multicloud environments. Others are increasing redundancy for physical assets.

Iowa has shifted many of its assets to the cloud. It has adopted hyperconverged infrastructure to reduce its data center footprint by 80%, according to state CIO Matt Behrens. He says modernizing the state's IT infrastructure has multiple long-term benefits.

"My view is these modernization efforts are fundamentally cybersecurity and resilience efforts as much as they are business transformation efforts," Behrens says.

Moving to the cloud also increases agility. Many state CIOs said their organizations are less focused on big-bang development and more focused on modular, incremental projects to make themselves nimble and avoid vendor lock-in.

"One of the key tenets of a more modern system is that it can adapt better to change, and by being able to adapt to change, it's more resilient," says Jason Snyder, Massachusetts' CIO.

Hybrid cloud financial models offer more flexibility and are increasingly seen as a resilience advantage because they allow state governments to cost-effectively scale computing resources up or down based on demand. Agencies aren't stuck paying for capacity they don't use, and they can offload maintenance to their service provider, paying for these services using a predictable, subscription-based cost model that allows for better planning. Cloud providers are also more likely to continue investing in their services even during economic downturns, unlike state legislatures that often slash funding for IT during hard times. This means states benefit from the latest upgrades without the heavy IT lift that's typically required for in-house computing resources.

Cloud adoption has surged in the public sector over the last three years, largely out of necessity. Our interviews with CIOs suggest the hybrid cloud approach will become a central component of building states' IT resilience. Half of the CIOs interviewed for this report said cloud adoption is an important part of their resilience strategy.

☐ **A move toward recession-proof IT funding models:** CDG also asked CIOs how they protect their organizations against potential financial disruption caused by economic downturns. Respondents commonly saw fee-for-service funding models and the cloud-related shift from capital budget expenditures (CapEx) to operating expenditures (OpEx) as ways to smooth out the traditional peaks and valleys in budget allocations.

Five of the CIOs we interviewed said their IT organizations use a fee-for-service model that leaves them less vulnerable to budget cuts during economic slumps. Texas DIR, for example, relies on administrative fees from the state agencies that purchase its services.

Arizona's Sloan was among several CIOs who said the shift to cloud makes IT funding more predictable.

"We've eliminated that CapEx rollercoaster and kind of leveled things out. Now we know what it takes to run the business," he says. "It also avoids situations where an economic downturn hits at the wrong time in the replacement cycle for your data center and you end up taking equipment that was already five or six years old and making it last seven or eight years."

Along with shifting to an OpEx model, Kansas smartly used COVID relief funding to make capital improvements and reduce its capital expenses. Jeff Maxon, the state's chief information security officer and interim chief technology officer, says these improvements have included both physical infrastructure and new technologies that couldn't be categorized as CapEx expenditures in the state's budget. This move has helped the state build a significant rainy day fund that will increase its financial resilience in the event of an economic downturn, potentially helping it minimize or avoid budget-cutting measures that could impact future IT modernization or ongoing investment in current modernization initiatives.

Other organizations, like the Georgia Technology Authority (GTA), negotiate group contracts. Dmitry Kagansky, Georgia's CTO, says aggregating costs and services is a key part of GTA's operational model.

Strategies for Reducing the Impact of Economic Downturns

- ✓ Use fee-for-service funding models for IT organizations
- ✓ Shift from CapEx to OpEx
- ✓ Adopt standard technology platforms
- ✓ Emphasize long-term planning

"Once you get to a certain size, that gives you much more financial stability because you're buying things in quantity. If an agency doesn't need something, there may be another one that does," he says. "Being able to negotiate contracts across a large number of services and products gives access to those products to even the smallest agencies at a reduced rate."

☐ **Standardizing wherever possible:** Adopting standard technology platforms is another way state CIOs are improving resilience. This approach helps fill workforce gaps, since employees across the organization often use the same tools. It also supports faster development or modification of needed services.

Bill Kehoe, CIO of Washington state, says he is focused on expanding enterprise services and IT governance to promote standardization. Like many state governments, Washington operates under a federated IT model, which often creates technology silos.

"We're trying to mature our enterprise services and ensure as many agencies as possible are utilizing those services," Kehoe says.

Standardized tools and processes, including centralization of core functions, can support coordination that strengthens resilience. It also makes digitizing and scaling government services easier and streamlines maintenance, all of which is critical to help states better navigate future disruptions.

☐ **Increased reliance on automation and AI:** CIOs said automation and AI are important to resilience. Use of intelligent management and performance monitoring tools has grown as state computing environments have become more complex. Many service providers are embedding AI into their products, and as a result, states are quickly becoming more AI-enabled. They're using AI to increase operational efficiency, automate their security apparatus and to some degree, address ongoing talent gaps.

"Part of our strategy is determining how we use AI and RPA [robotic process automation] to help fill some gaps in skill sets," says Michigan CIO Laura Clark. "Can we automate some tasks and shift them off our plate, so that we can use the existing staff we have to build out our practices or to focus on the more complex issues we need to solve?"

Overall, a quarter of the CIOs we interviewed said leveraging AI-driven automation is one of the main ways they foster resilience today. CIOs are also exploring the ramifications of newer forms of AI, such as generative AI.

Ohio formed an AI working group composed of technical team members and policy-focused employees to advance responsible AI practices. Katrina Flory, the state's CIO, says this type of cross-functional collaboration is critical as the use of generative AI grows.

"We had a number of bots and RPA deployments. Like other states, we're trying to figure out what's that right balance," she says.

Robert Osmond, Virginia's CIO, says his state is establishing systems and rules to ensure it acts as a responsible operator and doesn't abdicate its decision-making authority to AI.

"Many agencies are using different aspects of generative AI and different types of artificial intelligence," Osmond says. "What we're trying to do is make sure the rigor in training and education is going hand in hand with the capability, so that one doesn't outpace the other."

☐ **Growing attention on contractor relationships:** The importance of strong relationships with internal and external partners was a major theme throughout our interviews with CIOs. All of them viewed these relationships as vital to building resilience.

"Private sector partners have expertise and they have investments in technology. They're going to stay ahead of us state governments," says Sloan. "It's important they provide us with the future technologies that we need — and those we don't even know we need yet. Then, we can more quickly assimilate those solutions than if we were all running on our own."

Respondents said trust, transparent communication, and being able to rely on internal and external partners in times of crisis are essential to state resilience. However, greater reliance on service providers also increases the need for stronger partner management practices.

Katie Savage, Maryland's secretary of information technology, says her organization works hard to make sure it understands the business problem it is trying to solve before pursuing a technology solution. Sometimes the department goes as far as prototyping a solution in house before it seeks an external vendor. Conducting robust due diligence during the discovery phase helps Maryland's Department of Information Technology more clearly define its relationships with partners and get more value from the state's IT investments.

CIOs say they need to work collaboratively with external partners, but they're also putting guardrails around these relationships. These include developing vendor scorecards and significant penalty frameworks if SLAs aren't met (Iowa); prioritizing integration capabilities rather than purchasing one partner's full technology stack (Washington); using global and local partners to increase flexibility and reduce supply chain risks (Rhode Island); and focusing on modular, incremental projects that don't require huge multiyear contracts (New Jersey).

All these approaches, in isolation or in combination, can build partner resilience. This, in turn, will contribute to greater overall resilience for state governments.

Overall, a quarter of the CIOs we interviewed said leveraging AI-driven automation is one of the main ways they foster resilience today. CIOs are also exploring the ramifications of newer forms of AI, such as generative AI.

Workforce and Employee Resilience

CIOs increasingly seek employees with qualities like adaptability and problem-solving. They're willing to train them for traditional technology skills.

CIOs are evolving their management styles to improve employee and workforce resilience. They are focusing on approaches that build employee qualities like adaptability, problem-solving, open-mindedness and career growth. Developing a resilient government workforce requires a multi-faceted strategy, but for some state governments, certain tactics are already driving more success than others.

☐ **Growing talent:** Training and upskilling employees is common across the board. Many CIOs said their organizations focus on building talent internally, since it's often difficult to compete with the private sector's high salaries. In Georgia, GTA partners with local technical and community colleges to take advantage of already developed IT training courses. Weaver, North Carolina's CIO, says his state has "a very healthy training budget" it can deploy to help employees meet a new annual requirement for 36 hours of training and development.

☐ **Creating pipelines:** Other states, like Nebraska, partner with local schools to build their talent pipeline. Toner, Nebraska's CIO, says the state has effectively recruited students for entry-level positions, so much so that 47% of Nebraska's application development workforce and 20% of its infrastructure workforce has come from one local community college.

How State CIOs are Building Resilient IT Workforces

- ✓ Training employees
- ✓ Offering remote work
- ✓ Recruiting students and entry-level employees
- ✓ Establishing a culture of engagement
- ✓ Standardizing titles and career paths
- ✓ Providing career advancement opportunities/raising pay

“We don’t hire for positions, we hire people. We put them in positions they are interested in, then we allow them — and I think this is where we get a lot of resiliency — to switch roles. If a job opens, they can apply for it and do something totally different,” Toner says, adding that several state employees have switched from application development to infrastructure roles.

Similarly, Nevada is reducing technical skill requirements for many new hires, focusing instead on qualities such as their desire to serve and ability to work as part of a team. Nevada recently created IT professional trainee-level positions that give the state greater hiring flexibility and provide new employees with a long-term growth path in the central IT organization.

“The millennial generation of employees is willing to stay in an organization as long as they have a growth path — that’s huge for them,” says Nevada CIO Timothy Galluzi. “We also have a compelling story for IT professionals in Nevada. Nowhere else in the state are they going to deal with this level of technology and this level of impact.”

☐ **Cultivating the future workforce:** CIOs said building and strengthening talent pipelines is a necessity as current employees age out of the workforce.

“The age of our workforce is a threat from a resiliency standpoint. We do have single points of failure out there. We will be losing a lot of intellectual capital over the next five years,” says Jonathan Askins, CTO for the state of Arkansas.

Some states are offering remote work to increase retention and expand access to talent outside their traditional geographic boundaries. However, this practice varies across jurisdictions. Other states are standardizing IT job titles and cross-training employees so they learn different areas of the business.

Kansas, for example, is rationalizing and standardizing some 90 different IT position titles used across state agencies. Maxon, the Kansas CTO, says the approach builds resilience because the state can easily identify employees with cross-functional skills during times of crisis.

“If we have an incident at an agency and we have to draw from other agencies to help, it gives us a quick way of doing that,” he says.

☐ **Fostering workplace transparency:** Several CIOs we interviewed said part of their job is to create safe spaces for their employees to experiment with new technologies to better understand how to use them and not be penalized for trying things that ultimately aren’t successful. They want to foster an environment of transparency, where staff can report bad news or openly discuss internal problems without fear of reprisal.

Snyder, Massachusetts’ CIO, holds monthly “Ask Me Anything” meetings that encourage open discussion. He also does “active walkarounds,” where he visits different offices and asks for feedback.

“We’re trying to reduce the hierarchy, flatten the organization and give everyone a voice,” he says. “Open discussion of problems encourages our teams to participate creatively in solutions.”

Jennifer Lorenz, acting CIO for the state of New York, says it’s crucial for CIOs to empower their teams and nurture buy-in and participation from everyone.

“CIOs need to work on creating more than one person who knows how to solve the problem. We need to get away from that hero mentality and really create a safe space for individuals to learn,” Lorenz says.

Tennessee CIO Stephanie Dedmon says evangelizing lessons learned should be a key component of any CIO’s job, especially during times of crisis. Dedmon did this after several massive disruptions, including Nashville’s Christmas Day bombing in 2020. However, she says there’s always an opportunity to do more.

“That’s one key thing, I think, about fostering resilience in my role, is just sharing the lessons learned and what we can do differently,” she says.

Several CIOs we interviewed said part of their job is to create safe spaces for their employees to experiment with new technologies to better understand how to use them and not be penalized for trying things that ultimately aren’t successful.

Personal Resilience for CIOs

Maintaining health and perspective is essential in a job that comes with 24/7 responsibilities.

Whether it's providing technical and operational support during a mass casualty situation, handling incident response and recovery, or accelerating digital transformation, CIOs have a tougher job than ever before. Therefore, while they focus on advancing enterprise, IT and workforce resilience, they'll need to build their own personal resilience.

CIOs identified multiple ways to maintain personal resilience. First, many said it was important to maintain perspective. CIOs said tapping into their passion for the work and their organization's mission kept them resilient despite day-to-day challenges. Taking time to disconnect is also critical for CIOs, given the rigors of the job. Many respondents talked about how spending time with family, taking vacations and engaging in hobbies strengthened their on-the-job resilience. Others prioritize health and wellness, exercising regularly and practicing healthy eating habits to help them withstand the demands of the position.

Leaning on their team and peers is another way CIOs make their jobs more sustainable. Many of them discussed the importance of not feeling alone or isolated. They cited the need to build strong and trusted management teams in their organizations. They also pointed to the value of engaging with the community of state CIOs to commiserate, understand shared issues and find effective solutions.

Dedmon says it's important for CIOs to interact with their counterparts across the country. With only about 54 CIOs at the state level (including U.S. territories), the community is small, so it's vital for CIOs to support and learn from each other.

"My best piece of advice is call somebody who can be helpful. Someone to listen to you and say, 'It's okay, it's normal. You'll be okay and here's some advice,'" Dedmon says.

Before they can take care of anything or anyone else, CIOs need to take care of themselves. By doing so, CIOs will be better positioned to support their states through the next inevitable transformation or crisis and build long-term resilience across the enterprise, IT and workforce levels.

The Path to Resilience

CIOs play a dynamic role in strengthening state government's ability to withstand disruption and prepare for future shocks.

Whether it's cyber threats, climate change, public health crises or an evolving funding landscape, threats to state government operations are multiplying. It's never been more urgent for state governments to strengthen capabilities that allow them to withstand disruption today and prepare for future shocks.

CIOs play a dynamic and expanding role in this process. Our research shows that state CIOs are engaged in a range of often overlapping activities and strategies, including IT modernization, workforce training and development, managing partner relationships and fostering stronger internal collaboration.

CIO organizations are now tightly aligned with state emergency management agencies to respond to cyber incidents that threaten government operations and recover vital IT systems during traditional disaster events. State CIOs are also leading enterprise-wide conversations around IT investment and business risk. And they're at the forefront of remaking workforce and workplace culture to strengthen state government resilience at the employee level.

Just as important, CIOs are looking toward the future, working to understand how emerging technologies such as generative AI will impact state government and enable new levels of smart automation to strengthen resilience.

"We want to foster a culture of innovation where we try new things, because that's part of being resilient, too," says Crawford, the Texas CIO. "What worked in the past isn't necessarily going to work in the future. The one constant is things are going to change."

Finally, CIOs are building their own personal resilience to fully give back to their organizations and communities. As they navigate a more volatile operating environment, focusing on the true intention behind their work and who they serve can empower them to keep going even on the most challenging days. After all, the CIO role ultimately is less about technology and more about people.

"At the end of the day, it comes back to mission," Crawford says. "Part of the reason my family lives in Texas is because the opportunities here have allowed us to carve out a great life. As CIO, I can help others do the same."

About

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories, and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information, and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research, publications, briefings, and government affairs, NASCIO is the premier network and resource for state CIOs.
www.nascio.org

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

Sponsored by

Restlessly reinventing since 1911, International Business Machines Corporation (IBM) has decades of experience strategically partnering with leading government organizations all over the globe, to help them build innovative technology solutions that accelerate the digital transformation of government.

IBM provides hybrid cloud and AI solutions with a platform-centric approach, focused on providing two primary sources of client value — technology and business expertise. These solutions draw from an industry-leading portfolio of capabilities in software, consulting services, and a deep incumbency in mission-critical systems, all bolstered by one of the world's leading research organizations. IBM is committed to unleashing the transformative potential of foundation models and generative AI. We provide open, trusted, and targeted value-creating AI solutions for government and businesses. Watsonx, our integrated AI and data platform, embodies these principles, offering a seamless, efficient, and responsible approach to AI deployment across a variety of environments.

The essentials of transforming government are rooted in hybrid cloud, data and AI, automation, and cybersecurity. Each are foundational for government to continue to take bold steps forward — let's embrace the age of AI value creation together.
www.ibm.com

Contacts

CDG

Teri Takai, Vice President
teri.takai@erepublic.com

Steve Towns, Director of Content Strategy
916-932-1300
stowns@erepublic.com

Jeana Bigham, Director, Content Studio
916-932-1300
jbigham@erepublic.com

IBM

Frank Attaie, General Manager, Technology - Public Sector, IBM
1-416-949-4569
Frank.Attaie@ibm.com

Myra Dudley, State and Local Technology Sales Director, IBM
1-240-988-7154
dudleym@us.ibm.com

Chris Shriver, Vice President, Senior Partner,
State and Local Government Leader, IBM Consulting
1-919-345-7121
cshriver@us.ibm.com

NASCIO

Doug Robinson, Executive Director
drobinson@nascio.org

Amy Hille Glasscock, Program Director,
Innovation and Emerging Issues
aglasscock@nascio.org

Endnotes:
1. https://rockinst.org/blog/the-great-resignations-impact-on-local-government/
2. https://gov.louisiana.gov/index.cfm/newsroom/detail/4189

ADOBESTOCK SHUTTERSTOCK