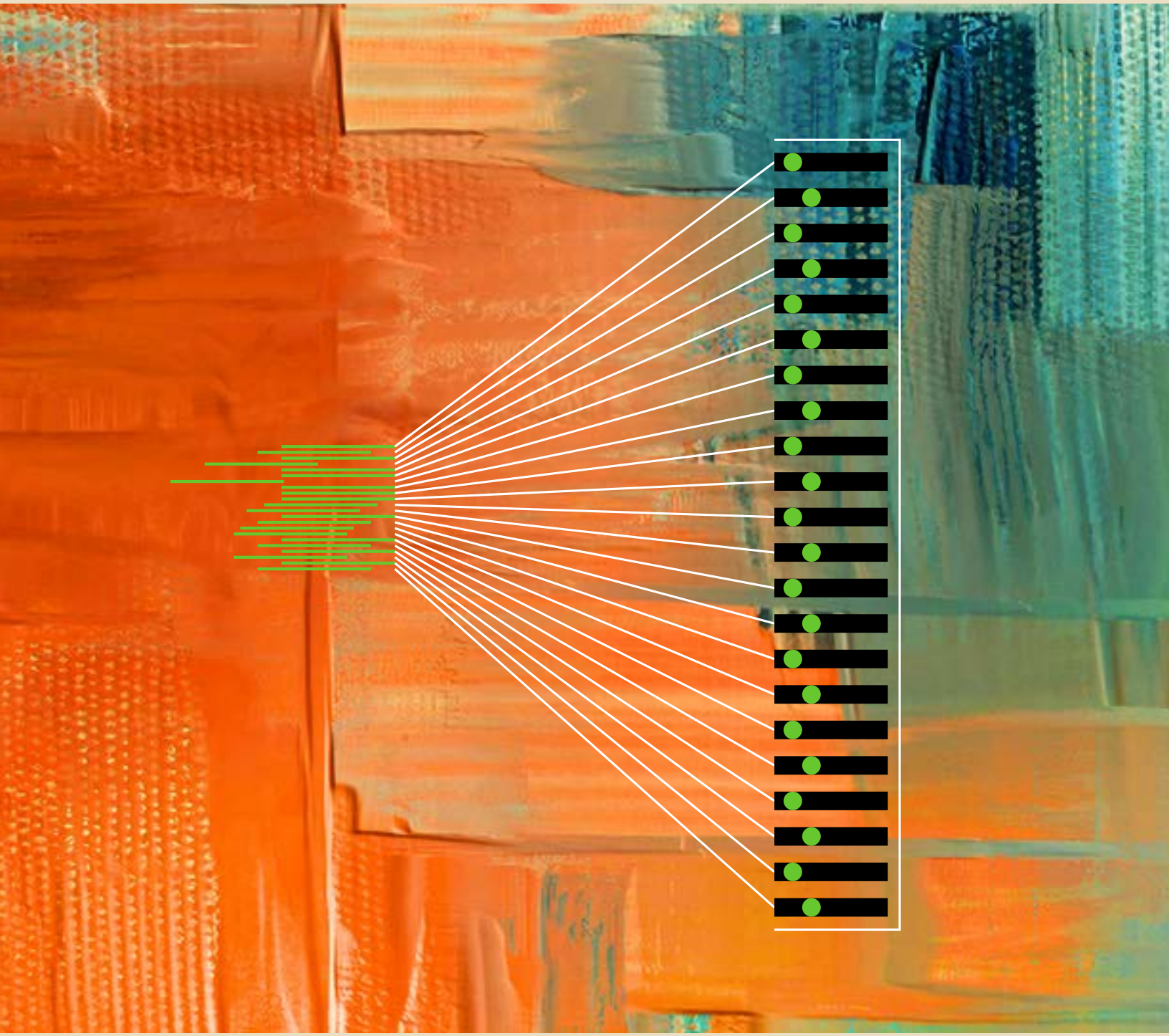
# 2026 NASCIO-Deloitte Cybersecurity Study

**A joint biennial report (9th edition) from the National Association of State Chief Information Officers (NASCIO) and Deloitte**

*State CISOs are navigating more intense threats and the proliferation of AI in the face of tightening budgets*



NASCIO

Deloitte.

Since 2010, the National Association of State Chief Information Officers (NASCIO) and Deloitte & Touche LLP[1] have conducted a biennial survey of state chief information security officers (CISOs) to better understand the cybersecurity landscape across state government.

The 2026 NASCIO-Deloitte Cybersecurity Study reveals a challenging picture. State chief information security officers are protecting public data systems at a time when cyber threats are growing in sophistication, as foreign adversaries, sophisticated hackers and cybercriminals are increasingly using new artificial intelligence–based tools to probe for weaknesses.

Against this backdrop, the responsibilities of CISOs continue to expand. CISOs are being asked to help states adopt AI guidelines that maintain cybersecurity integrity, while introducing new defenses against a host of novel AI-based threat vectors. Moreover, some states are taking a more active role in supporting local government and critical infrastructure—both highly attractive targets for cyber criminals—embracing a "whole-of-state" cybersecurity approach.

At the same time, CISOs tell us that budgets—which had been relatively strong in the post-pandemic years—aren't keeping pace.

This year's study includes insights from the CISOs of all 50 states, the District of Columbia and the US Virgin Islands (learn more about the study methodology in "About the study").

Responses from this year's survey uncovered five themes:

- **Facing an evolving threat landscape:** Rapid advances in attack sophistication are challenging state CISOs, with AI viewed as both an emerging threat vector and a powerful tool for cyber defense.
- **Getting future-ready:** CISOs are adopting new tools and regulatory frameworks to meet the evolving technology landscape.
- **Looking at whole-of-state cybersecurity:** The survey points to a growing interest in centralized state support for the cybersecurity efforts of local governments, public education and critical infrastructure.
- **The expanding CISO role:** The proliferation of AI and generative AI (GenAI), as well as a growing appreciation of the need to safeguard public data, is bringing new responsibilities to the CISO role.
- **Dealing with a resource crunch:** Compared with recent survey cycles, CISOs tell us that their funding shortfalls are growing more dire, while continuing to face challenges around maintaining a cyber workforce with the needed skills.

We appreciate the CISOs who participated in this year's survey. Both NASCIO and Deloitte are pleased to share these insights to help state CISOs fulfill the critical mission of safeguarding the public's data.

*—Meredith Ward, NASCIO and Mike Wyatt, Deloitte*

# Key takeaways

- As threats become more sophisticated, far fewer CISOs expressed confidence in their ability to secure public data. The percentage of CISOs who characterized themselves as "extremely" or "very confident" has dropped dramatically, **from 48% in 2022 to 22% in 2026** (figure 1).
- CISOs are significantly less confident in the ability of local government and public higher education to secure public data. The percentage of CISOs who described themselves as "not very confident" in these entities rose significantly, **from 35% in 2022 to 63% in 2026** (figure 2). This lack of confidence may explain why **roughly one-fifth of CISOs indicated that their states were moving forward with a whole-of-state approach to cybersecurity**.
- Generative AI also represents an area of increased responsibility, with **94% of CISOs indicating that they are actively involved with the development of GenAI security policies** (figure 8).
- CISOs overall reported a rapidly deteriorating budget picture. In the 2026 survey, only 22% of CISOs reported a budget increase of 6% or more, down from 40% in 2024. Perhaps more concerning, **16% of CISOs reported *reductions* to their budgets** in this survey, compared with *none* in 2024 (figure 21).
- Looking into the future, CISOs indicated their top three barriers to meeting cybersecurity challenges were: **legacy infrastructure, increasing sophistication of threats and insufficient funding for cybersecurity** (figure 7).

# The threat landscape: Rapid gains in attack sophistication shake state CISOs' confidence

State CISOs reported that cyber threats are more numerous, more varied and more sophisticated than ever before. As one CISO notes, "With the rising adoption of AI and agentic AI, the speed at which attacks are occurring is accelerating at a blistering pace." As a result, state CISOs are less confident about their ability to safeguard data assets. Many expressed concerns about the preparedness of local governments and educational institutions, as well as others who interact with state systems and data.

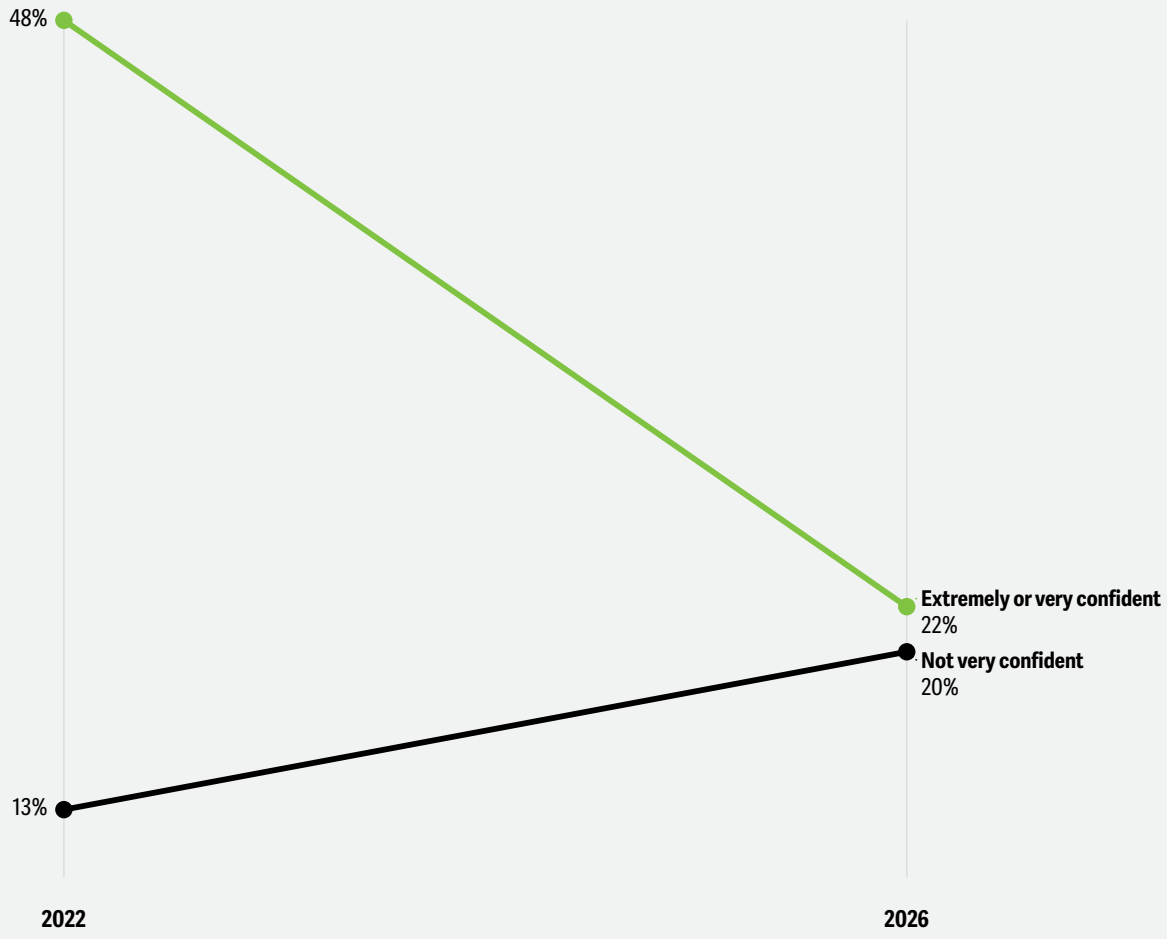
## CISOs are far less confident they can protect state and local systems

Perhaps the most notable finding of this year's survey: the significant drop in state CISOs' perceived security of their state's information assets (figure 1).

*Figure 1*

## State CISOs report a sharp decline in confidence that state assets are protected from external cyberthreats

*Question: "How confident are you that your state's information assets are protected from cyberthreats?"*




Note: Percentages may not total 100% because "Somewhat confident" and "Not applicable or do not know" responses are not shown in the figure.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

CISOs' confidence in local governments and public higher education cyber capabilities has also dropped significantly (figure 2). Cybercriminals are targeting an ever-widening range of local entities, compromising health care information, police databases and more, aiming for ransom payments or—in some cases—merely to disrupt public sector operations.[2]

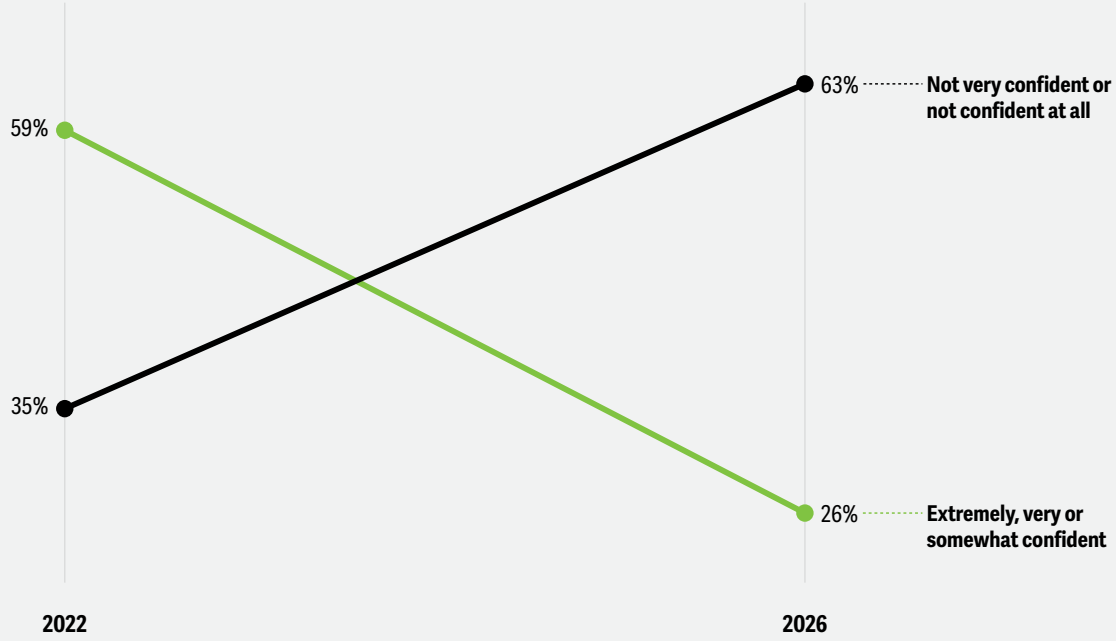
This is important because government systems are often interconnected—think of a state benefit system administered at the county level—meaning that local breaches or ransomware attacks could pose a threat to the broader state information ecosystem. Despite the efforts of local governments and public colleges,[3] CISOs report significantly lower confidence in these institutions' ability to stop increasingly sophisticated adversaries, some of whom are using smart technologies to cast a wide net to probe for weaknesses.[4]

The decline in CISOs' confidence may be a factor in the growing interest in adopting a whole-of-state cybersecurity strategy[5] (see the section on "**Whole-of-state cybersecurity gains interest, but adoption remains uneven**").

*Figure 2*

## State CISOs are significantly less confident in the cyber capabilities of local government and public higher education

*Question: "How confident are you that your state's information assets are protected from cyberthreats within local government and public higher education?"*




Note: Percentages may not total 100% because the response "Not applicable or do not know" is not shown in the figure.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

### How attack vectors are changing

Over the past year, states have fended off a range of attacks, with CISOs most often citing malicious code, web applications, financial fraud and zero-day attacks (figure 3). Bad actors also exploit compromised credentials and former employee accounts to execute attacks.

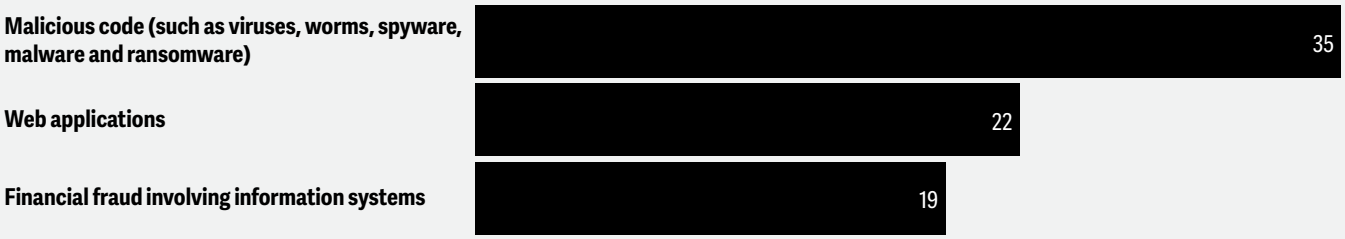
State CISOs have a slightly different set of future concerns than in previous years. Concerns over malware threats have declined since 2022, as have concerns regarding foreign state-sponsored espionage. This may suggest that defenses are stronger—or that other threats have become more prominent. Concerns about third-party security breaches have increased, and phishing attacks—which target the imperfect behaviors of humans, a weak-link point of vulnerability—remain a concerning attack vector.

Interestingly, CISOs view both AI-enabled attacks and foreign espionage as somewhat less of a worry looking ahead (figure 4).[6]

*Figure 3*

## Malicious code remains the most common cybersecurity incident reported by state CISOs

*Number of states (Question: "Select the top 3 causes of cybersecurity incidents in your state in the last 12 months.")*

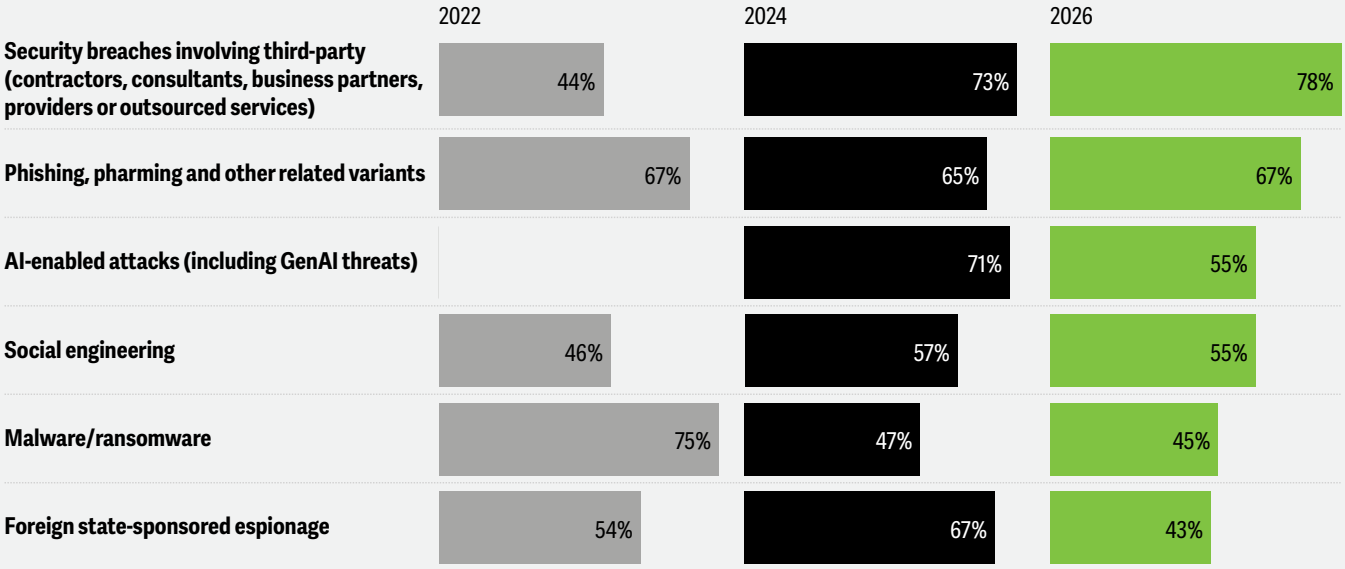



Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 4*

## CISOs expect malware, ransomware and foreign state-sponsored espionage to remain major threats, though somewhat reduced since prior surveys

*Question: "How much of a threat do each of the following cyberthreats pose to your state in the coming year?"*



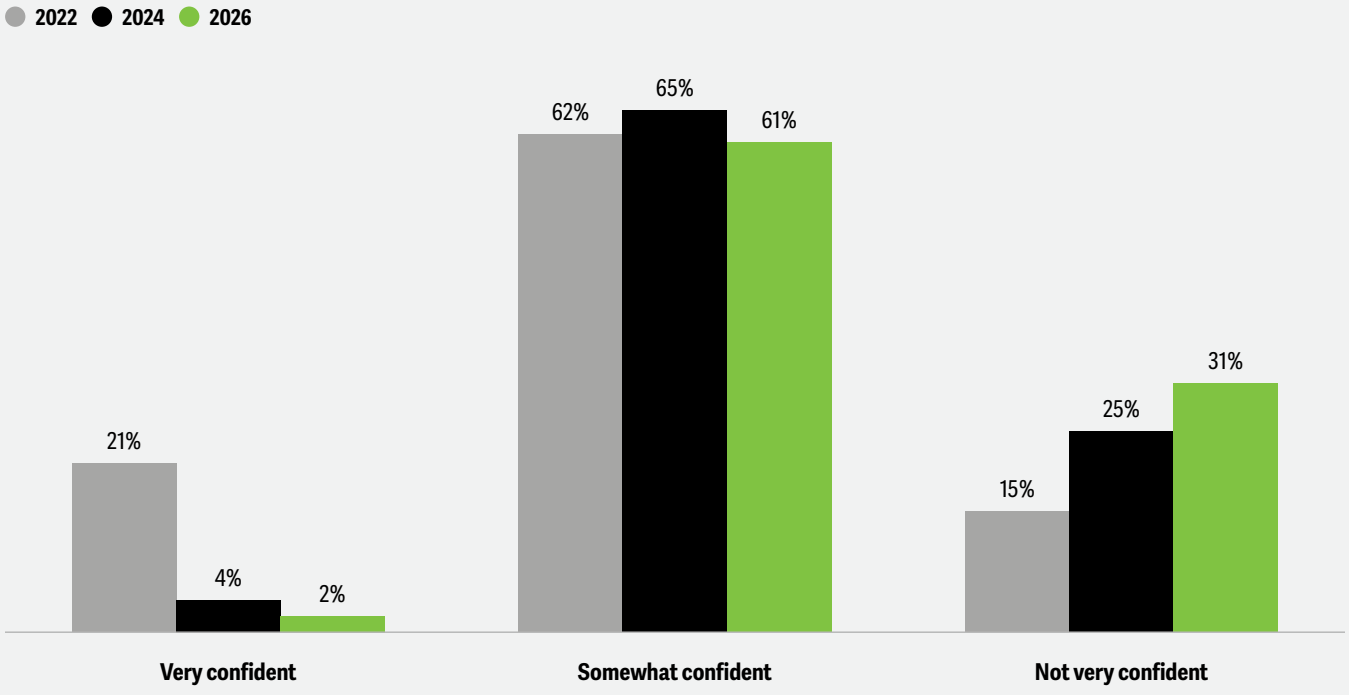

Note: AI-enabled attacks (including GenAI threats) was not asked in the 2022 survey.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 5*

## CISOs continue to be concerned about the cybersecurity practices of third-party partners

*Question: "How confident are you in the cybersecurity practices of your contractors, service providers and business partners?"*




Note: Percentages may not total 100% because the response "Not applicable or do not know" is not shown in the figure.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

CISOs expressed growing concerns regarding other parties that interact with their data, possibly based on the growing complexity of information networks, as third-party interactions may introduce risks to transparency, access and credentials, and other vulnerabilities (figure 5).

### The growing threat of AI-based technologies is accelerating both the scale and speed of cyber threats

AI-based attacks are becoming more sophisticated, stretching state resources. These technologies have the capability to generate vast numbers of attacks at minimal cost, and a single successful breach can have significant operational and reputational consequences.

The AI threat isn't limited to automated system attacks. Some newer, widely available AI tools can generate sophisticated deepfakes that can fool humans and evade detection systems. In addition, AI ransomware-as-a-service marketplaces run on cryptocurrency, and AI agents can probe systems for weaknesses and launch adaptive attacks. In short, AI is expanding the capabilities of malicious actors.[7]

There is another AI vulnerability—the use of AI by state employees and the tools they use. Multiple CISOs told us about the hazards of a practice that many software users have noticed: product vendors incorporating GenAI features into existing programs and platforms. While these smart technologies often improve functionality, they can also create new attack surfaces as features may lead to employees entering personally identifiable information or other sensitive data. "The state has published a statewide acceptable use policy to help steer our customer agencies in AI usage," one CISO remarks, "but vendors auto-enabling AI features in products already leveraged by our customers causes major concern for data protection, privacy and risk."

Another CISO tells us: "GenAI is advancing faster than existing governance structures can adapt, creating growing uncertainty around security, privacy and ethical use. Vendors are increasingly embedding AI capabilities into products and services without

sufficient transparency or state-level control, effectively inflicting AI on operational environments before comprehensive risk assessments or policy frameworks can be applied. This uncoordinated adoption has outpaced the development of formal security guidelines, governance models and ethical standards, leaving the state in a reactive position."

Indeed, one of the biggest developments for state CISOs is GenAI's ubiquity and rapidly growing capabilities, presenting both new threats and new ways of countering those threats.[8] The challenge can feel overwhelming, especially for under-resourced IT teams. One CISO sums up the pros and cons: "GenAI is accelerating both the sophistication and volume of cyber threats, enabling adversaries to craft highly-targeted phishing, automate exploitation and rapidly detect and exploit known vulnerabilities. At the same time, it offers state IT security teams powerful capabilities for real-time threat analysis, automation of routine tasks and faster incident response—provided it's implemented with strong governance and risk controls."

Asked to describe GenAI's impact on security in their states—including implications for security guidelines, governance and the ethical use of AI—CISOs voiced both concern and optimism. "The push to implement GenAI has highlighted the lack of maturity in some of our agencies around data classification and unintended access/sharing," one CISO tells us. "Many are unprepared for the challenges GenAI will present." Others saw it as a useful tool. "We are leveraging GenAI to accelerate the development of our core cybersecurity documentation, including AI policies, incident response run-books, risk assessments and plans of action and milestones for mitigation," another state CISO says.

Data privacy and protection is a rising concern, with GenAI using and repurposing data in ways not always fully understood. But some information security offices are using the technology to rethink and codify state AI policy. We heard from CISOs regarding the need for better data classification and data loss prevention strategies, as well as greater focus on promoting cybersecurity education on data privacy and ethics.

The survey revealed that states are at various stages of establishing structures to ensure safe use of AI and GenAI. As one CISO notes: "We have published artificial intelligence guidelines that emphasize secure and ethical use of AI, warn of privacy and data exposure risks when using AI/machine learning systems, and encourage agencies to prevent misuse and minimize risk when handling sensitive or regulated data." Publishing guidelines is only part of the

journey, however. Some states are looking at mechanisms to limit risk, including blocking some high-risk GenAI tools and leveraging existing risk management services to ensure that AI and GenAI guidelines are being followed. Other steps may include performing risk assessments.

Other CISOs noted additional concerns:

- "We are mainly concerned about overexposure of data and lack of transparency on how AI could be used to make decisions."
- "Strong guardrails ensure GenAI systems do not inadvertently disadvantage vulnerable groups—especially our large elderly population, who face heightened risks of exploitation and digital fraud. Above all, all states should prioritize robust data-protection policies that safeguard personal information and reinforce public trust as AI capabilities continue to evolve."

# Future ready: How CISO priorities are shifting in the AI age

In their survey responses, CISOs shared how they are preparing for a rapidly changing future of intense threats, constrained resources and unforeseeable AI impacts.

## Where CISOs are focusing their efforts now

Top priorities for CISOs have shifted markedly since the 2024 survey. When asked to identify their states' top cybersecurity initiatives for 2025 and 2026, half of CISOs named implementing effectiveness metrics. Capturing the effectiveness of spending on cyber can be difficult, but without metrics it is hard to show the benefits from investments. Tracking operational, compliance and risk-based key performance indicators—for example, incident response time and phishing click rate—can help show the return on cyber investment.[9]

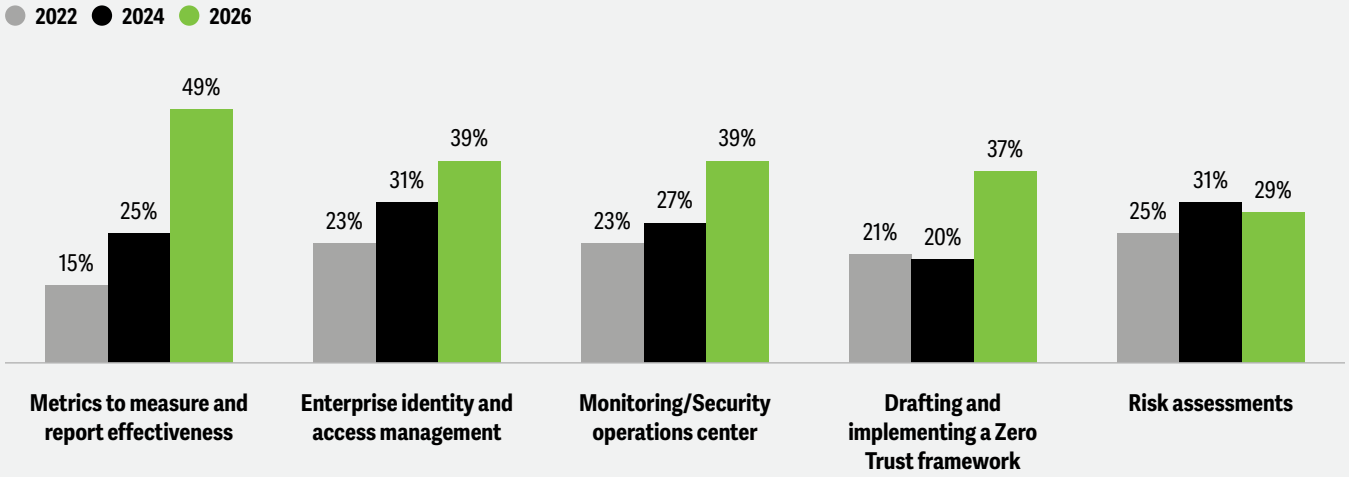
Other top planned initiatives, such as enterprise identity and access management (IAM) and implementing a Zero Trust framework, are also significantly more prominent than in past years (figure 6).

When we asked CISOs about the challenges they face in addressing their cybersecurity challenges, a clear picture emerged: Confronting ever more sophisticated threats, CISOs are often constrained by a reliance on legacy infrastructure—which is often more difficult to safeguard from cyberattack—as well as outdated solutions. Fighting back may require new software, which can be expensive, as well as other up-to-date high-tech countermeasures—along with staff capable of wielding these tools. Without adequate funding, CISOs can't properly protect states' information and systems. Our survey shows striking increases in the number of respondents citing budget shortages and legacy infrastructure—another consequence of limited funding—as barriers to addressing cybersecurity challenges (figure 7).

*Figure 6*

**Measuring cybersecurity effectiveness emerges as a top initiative for CISOs**

*Question: "Identify your state's top 5 cybersecurity initiatives for 2025 and 2026."*

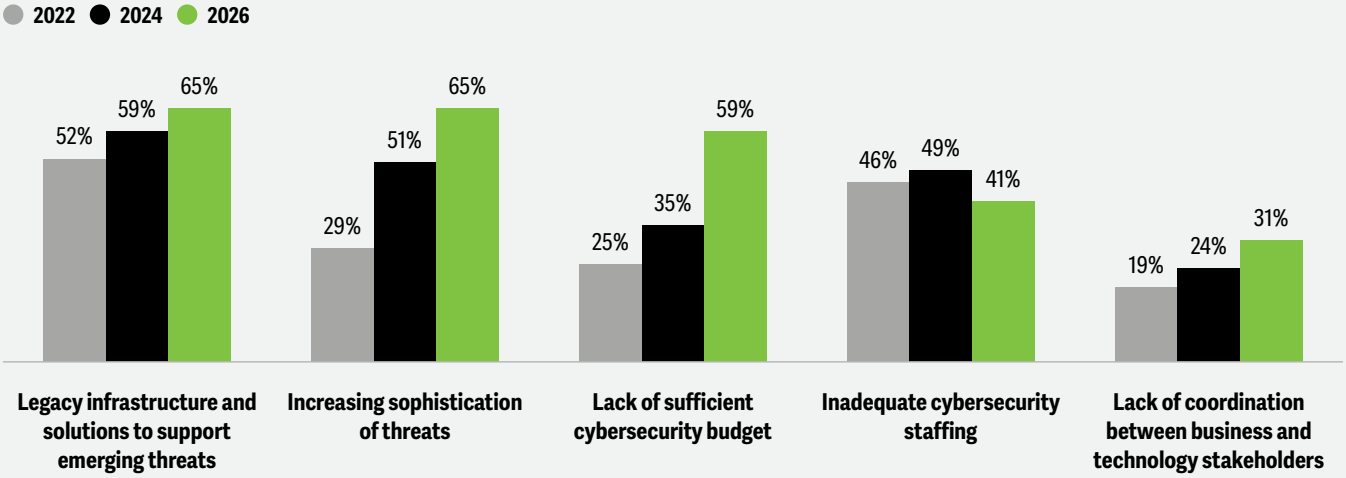



Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 7*

## CISOs cite sophisticated threats, aging infrastructure and budget as their top challenges

*Question: "Identify the top 5 barriers that you believe your state faces to address cybersecurity challenges."*




Source: 2026 NASCIO-Deloitte Cybersecurity Study.

### AI: An accelerant for both attack and defense

For CISOs, being ready for the future means being ready for AI, GenAI and whatever else comes next. This means defending against AI-based attacks, as well as using AI effectively within state government. Thoughtful use of AI may entail employing it to defend against cyberattacks, automate monitoring of threats and augment the capabilities of the cybersecurity workforce.[10]

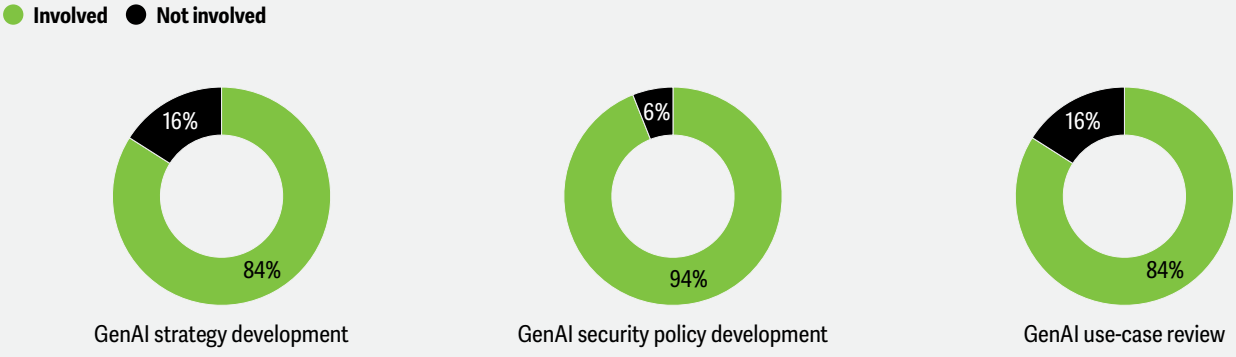
When state agencies introduce new AI-based tools to workers, whether for cyber defense or for other purposes, CISOs need to ensure that they don't inadvertently introduce additional vulnerabilities.

The good news is that many states are putting CISOs at the center of their overall GenAI planning: developing strategy and security policy as well as reviewing cases (figure 8). As one respondent puts it: "[The] CISO is fully involved in the development and review process of new AI use cases and is part of the development of policy."

*Figure 8*

## CISOs are heavily involved in establishing state-level GenAI strategies and best practice

*Question: "What is the current level of CISO involvement in GenAI–related developments in your state?"*




Source: 2026 NASCIO-Deloitte Cybersecurity Study.

One CISO reported using AI technology in "automatic triaging of security alerts, and summarization of events" and is "exploring its use in report creation, threat identification and training." Several are using GenAI in their states' SIEM (security information and event management) and SOAR (security orchestration, automation and response) programs. "AI is being embedded in many of our security tools," one CISO says. "We are using it to write policy, and we have plans to embed additional AI capabilities into our data analysis in the SIEM."

All but one CISO reported either already using GenAI or planning to incorporate the technology (figure 9). Looking ahead, CISOs shared ambitious plans to expand GenAI-related cyber defense capabilities:

- "There is an opportunity to deepen integration of cybersecurity threat modeling."
- "Involving security at the evaluation stage of tools instead of the last stop before procurement."
- "CISO involvement should focus on AI-enabling the security operations center (SOC) to enhance threat detection, triage and response automation. This includes integrating GenAI for advanced analytics, contextual alert enrichment and streamlined incident reporting."

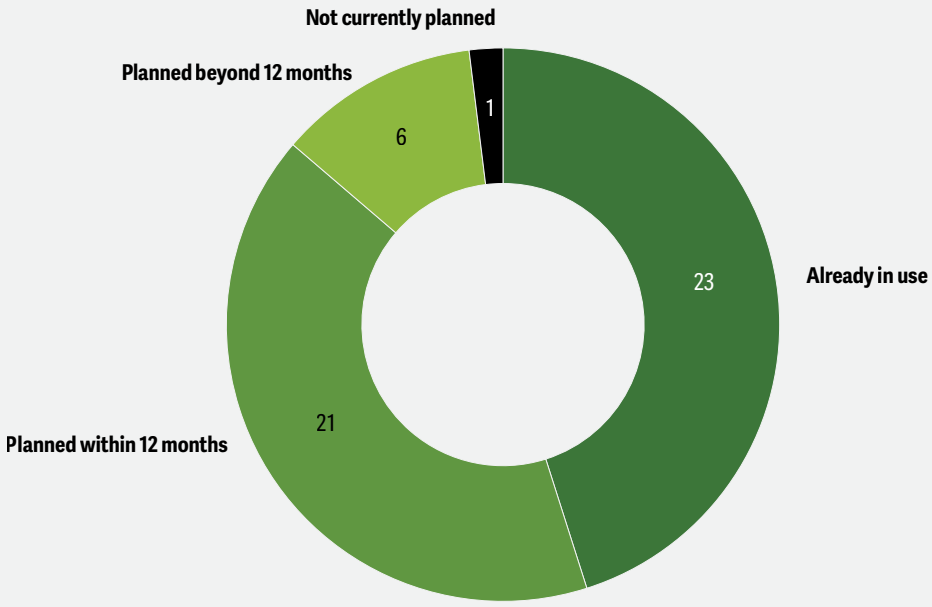
## Threat response and frameworks

Structurally, states respond to cyber incidents in a variety of ways. Much of this response has remained stable—about the same number of states look to dedicated response teams, central IT security groups and individual agencies—but after funding and staffing reductions at the federal level,[11] fewer states are responding to incidents with outreach to federal support organizations and agencies (figure 10). The Multi-State Information Sharing and Analysis Center, for example, shifted to a fee-based membership system after the cessation of federal funding, which may have contributed to the observed decline.[12]

*Figure 9*

### Nearly all CISOs are already using or plan to use GenAI to enhance cybersecurity operations

*Number of states (Question: "Do you plan to use GenAI to improve your cybersecurity operations?")*

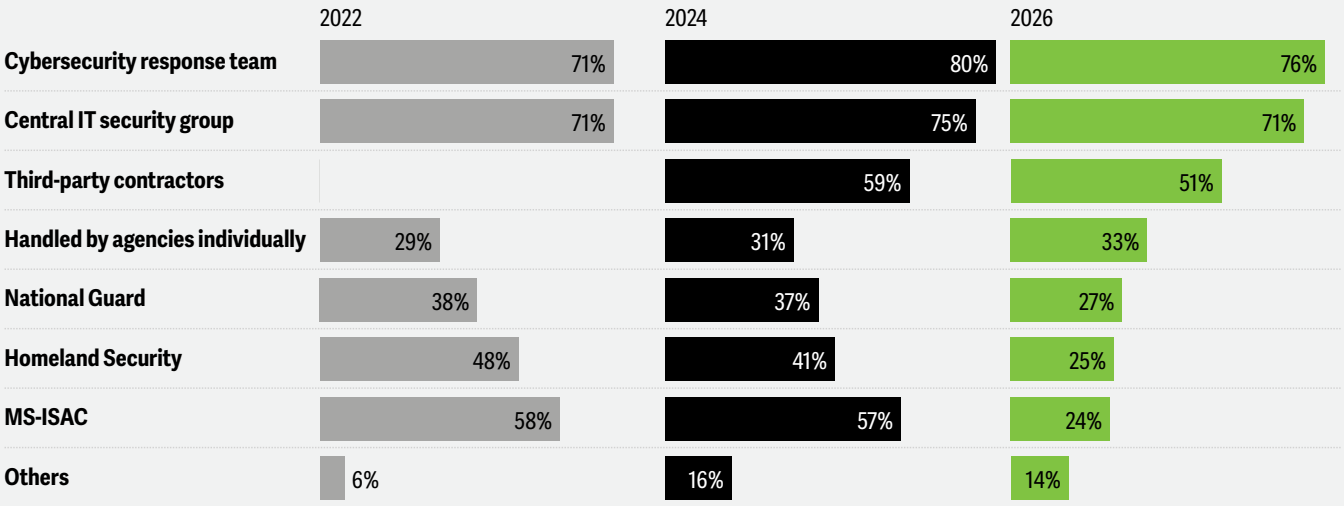



Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 10*

## State cyber response strategies are stable—with a shift away from reliance on and partnership with federal agencies

*Question: "How does your state respond to a cyber incident?"*




Note: "Third-party contractors" was not provided as an option to respondents in the 2022 survey.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

As the cyber landscape shifts, so do the available compliance frameworks.[13] The overwhelming majority of states rely on the National Institute of Standards and Technology's regularly updated Security and Privacy Controls for Systems and Organizations (NIST SP 800-53),[14] with most also using Center for Internet Security standards (figure 11).[15]

*Figure 11*

## NIST and CIS compliance frameworks remain the dominant standards guiding state cybersecurity programs

*Question: "What are the external cybersecurity standards, regulations, frameworks or guidance your state chooses to adhere to, comply with, or rely on, in carrying out its information security program?"*


Note: The latest CIS standard has reduced the number of controls from 20 to 18.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

# Whole-of-state cybersecurity gains interest, but adoption remains uneven

This year's survey provided a strong signal that while far from universal, a significant number of states and state CISOs are moving toward taking a whole-of-state approach to cybersecurity.

Whole-of-state cybersecurity, at its core, involves state governments and state CISOs providing support to entities outside of state government itself.[16] These entities might include local governments; various types of critical infrastructure; educational entities (K-12 as well as public higher education); and private entities that are critical to public health and safety, such as hospitals.

The survey findings indicate that states are in different places on this issue: Some are moving aggressively toward greater state support, while others are still focusing on state information assets and exploring possibilities. As one CISO says, "This is a public policy discussion which we are preparing for, meaning what position will the state take long-term in supporting local units of government with cybersecurity services."

Asked whether their states are considering options for whole-of-state coverage, CISOs offered a wide variance of responses, with roughly one-fifth indicating that they were fully or partially moving forward with a whole-of-state approach. One CISO reported that "We already operate a whole-of-state model by providing no-cost cybersecurity shared services" to certain municipalities and county governments—while other CISOs indicated initial steps or plans to do so. Yet others indicated they had no plans to adopt such an approach.

A number of states pointed to the federal State and Local Cybersecurity Grant Program (SLCGP) as a primary driver of their whole-of-state program. One CISO says that the program "helped drive collaboration and buy-in from the local government entities," while another tells us, "SLCGP funds have laid the groundwork for baseline cyber capabilities in local governments." The uncertainty regarding the program's renewal at the time the survey was conducted may have contributed to some states' hesitancy to move forward with whole-of-state expansion.[17]

Among those respondents most positive about the whole-of-state approach, we heard the following:

- "We currently have adopted a whole-of-state cybersecurity program. We have an enterprise SOC that provides cybersecurity operations support to all executive branch, higher education, cities, counties and school districts."
- "We do today and will be growing field and regional support going forward."
- "This is being implemented as an opt-in approach."
- "We provide a centralized cybersecurity operations center for some local governments and K-12. Given necessary resources, we hope to expand on that."

The respondents considering a whole-of-state program "in the next few years" are taking different routes. One tells us that they "would like to" implement whole-of-state planning, "as this is the most beneficial model." Another suggests, "Thinking about it but still need to work out approach and funding model." Another CISO notes, "We are exploring ideas based on other states' models."

Several respondents mentioned collaborations with various vendors and service providers as well as with public higher education. One notes: "We have a partnership with higher ed to deliver

cybersecurity assessments for local governments and schools using student resources." Another explains, "A task force of multiple state agencies has been established to review opportunities on how the state can assist local governments and K-12 schools with cybersecurity efforts."

Whole-of-state planning and activity is directly linked to how states structure their cybersecurity strategy: either centralized, with the CISO's office responsible for the enterprise policy and services; or federated, with the CISO responsible for enterprise policy with a mix of centralized shared services and agency-led services specific to each. Our survey results suggest that CISOs are increasingly favoring a centralized model (figure 12).

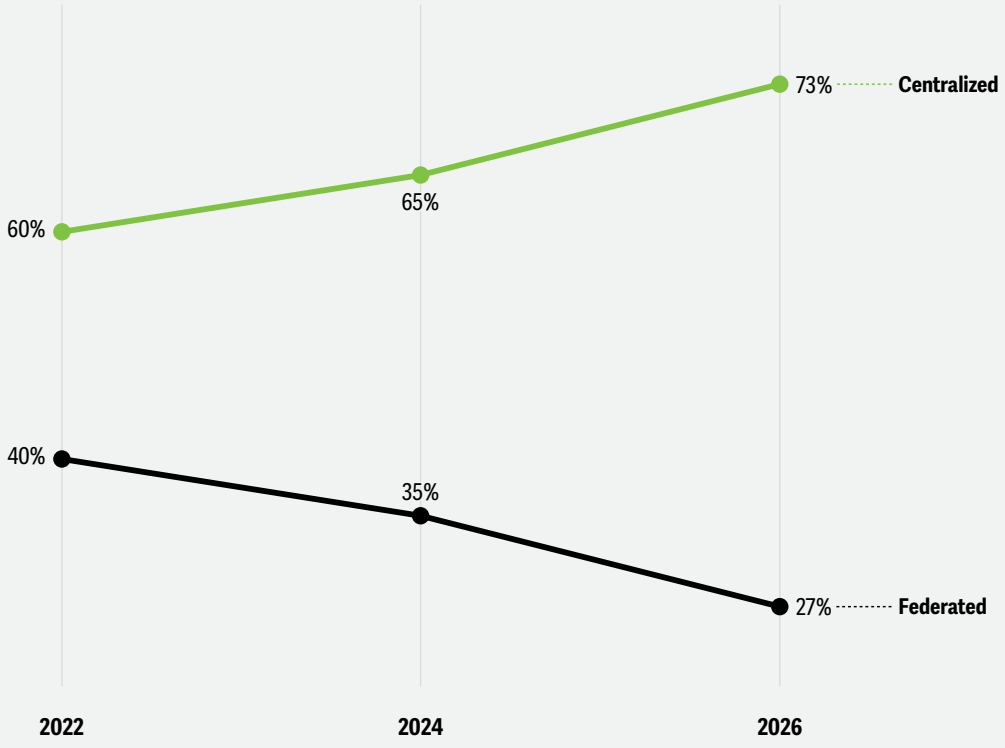
But just because a centralized model might be viewed as more effective doesn't mean that's how the system is currently structured. CISOs report that their offices' various functions—risk, privacy and cybersecurity—are organized differently (figure 13), balanced between centralized and more decentralized, federated models.

There is a clear challenge presented by threats to local entities. Not only are they an enticing target—states are taking unclear and mixed approaches, often due to lingering questions: *What is the state's role in protecting these local entities? Where does the funding come from? What is the relationship between these local entities and the state CIO's office?* In many states, local communities welcome assistance from the state—especially if it is funded—while in other states local officials may wish to maintain greater independence. And of course, states have different legislative rules about the relationship between local government jurisdictions and state government.

*Figure 12*

## CISOs increasingly favor a centralized operating model, with the office responsible for enterprise policy and services

*Question: "Which operating model do you think will be most beneficial to your state?"*

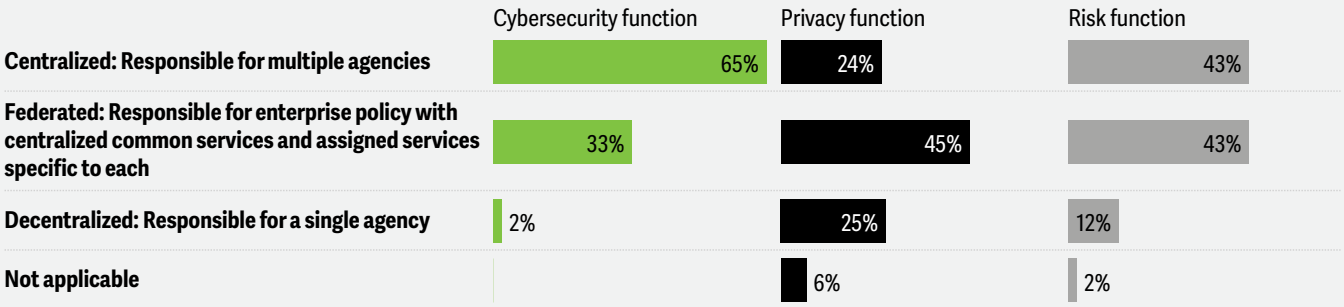



Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 13*

## Cybersecurity functions are more centralized than other functions across states

*Question: "How are your state's cybersecurity, privacy and risk functions structured?"*




Source: 2026 NASCIO-Deloitte Cybersecurity Study.

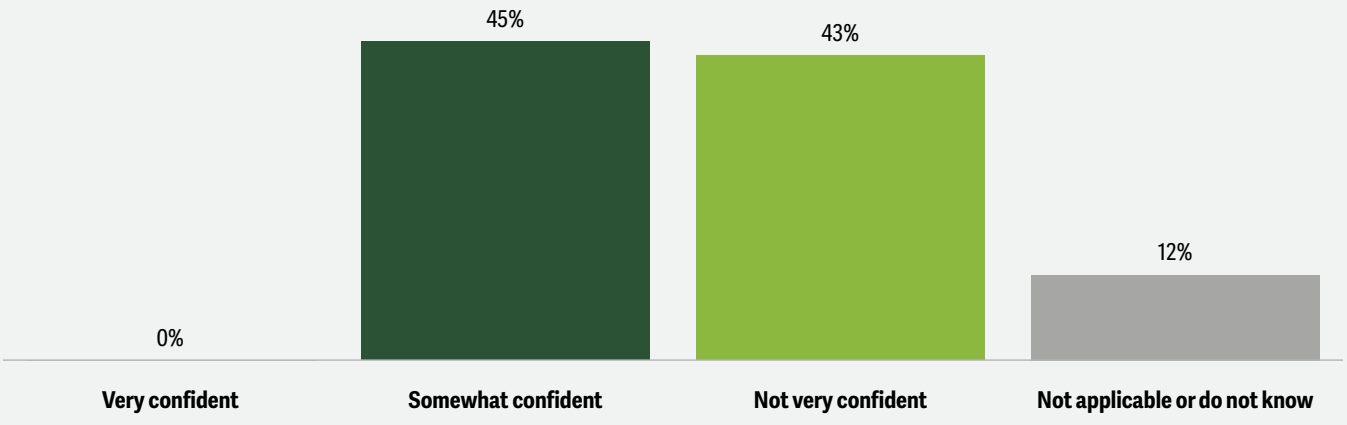
One major question is how CISOs expect their SOCs to evolve over the next two to four years to better support local government entities and public higher education. Survey respondents offered a range of answers, from "We expect to offer county, municipal and K-12 SOC services within the next four years;" to "Growing to provide fusion center-type intelligence sharing with municipalities, with a potential to offer SOC services in the future;" to "We don't even have a SOC at the state level. We pay [vendors] to do that kind of work."

In a hyper-connected world, it is often the more vulnerable public systems that can provide an entry point for malicious actors. Smaller county and municipal governments, as well as public education systems and infrastructure, can be vulnerable; and a number of states are starting to look toward providing more support to these entities. CISOs are particularly concerned about local governments' vulnerability (figure 14). A stronger whole-of-state orientation could help municipalities defend against cyber threats that could also affect state systems.

*Figure 14*

## No state CISO is "very confident" in local governments' cyber practices; 43% of state CISOs say they are "not very confident"

*Question: "How confident are you in the cybersecurity practices of local governments?"*

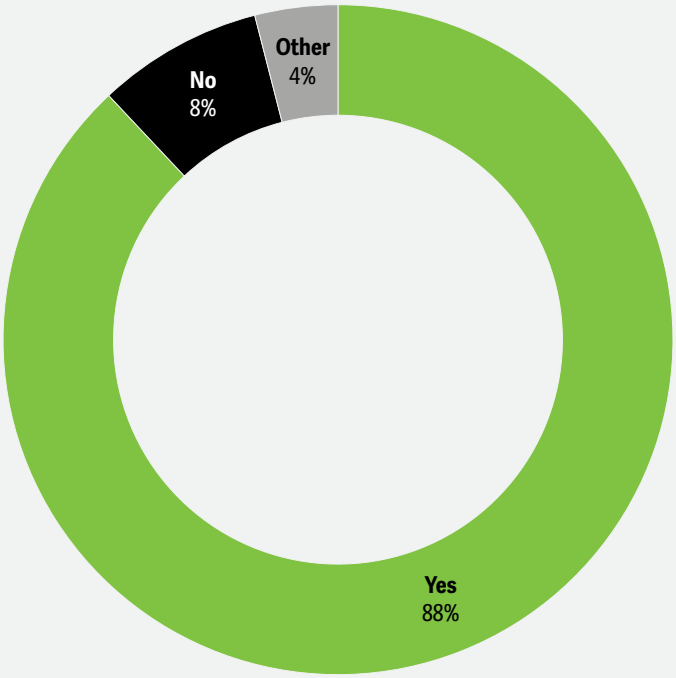



Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 15*

## A wide majority of states now have an enterprisewide security operations center

*Question: "Do you have an enterprisewide security operations center (SOC)?"*




Source: 2026 NASCIO-Deloitte Cybersecurity Study.

The institution of enterprisewide SOCs has been a major development for CISOs. All but a few CISOs now oversee enterprisewide SOCs—hubs that help provide real-time monitoring, threat detection, incident response and related services (figure 15).[18]

Some CISOs expect to expand the scope and capabilities of their SOCs in the coming years; as one respondent puts it, this includes "expanding local government participation, growing to regional support." Several CISOs expressed that they were "looking to expand services to more local governments in the future," but noted that such expansion was dependent on available budget:

- "Just received authority to implement statewide SOC. Now planning on expanding efforts to non-executive branch entities."
- "Subject to appropriations, the SOC will continue to grow and offer services to both local partners and higher education entities. We may develop a sub-SOC focused solely on serving municipalities."
- "I would expect our SOC to evolve to have more operational authority over the assets of our local government and public higher education entities."

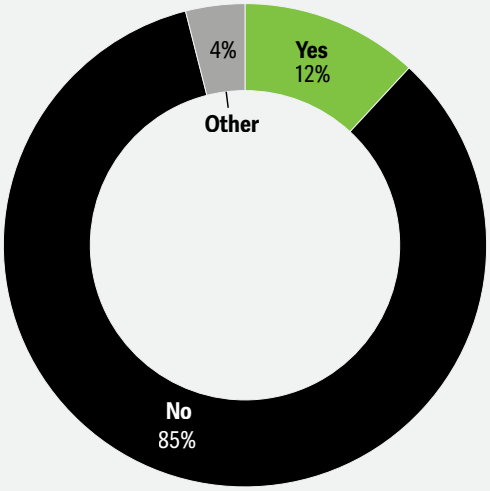
With cyber bad actors increasingly targeting schools,[19] K-12 is a focus for state SOCs:

- "We are currently onboarding all of K-12 into our SOC; will continue to onboard cities, counties and other public agencies in 2026 and beyond."
- "A task force of multiple state agencies has been established to review opportunities on how the state can assist local governments and K-12 schools with cybersecurity efforts. The implementation and expansion of existing SOCs are options that are being considered."
- "We currently provide services to local governments; working to add K-12 in the next fiscal year."

*Figure 16*

## Only a few CISOs reported having regional SOCs

*Question: "Do you have a regional security operations center?"*




Note: Percentages may not add to 100% due to rounding.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

With regard to regional SOCs (RSOCs)—operational entities pooling cybersecurity data and resources across agencies and other organizations in a geographical region—only six CISOs currently participate in such an arrangement (figure 16).[20] One CISO said their state was "looking to expand into RSOCs since we just got the enterprise SOC going." Another foresaw "more RSOCs to be deployed to provide services to local government entities."

# The CISO role expands beyond security into strategy and governance

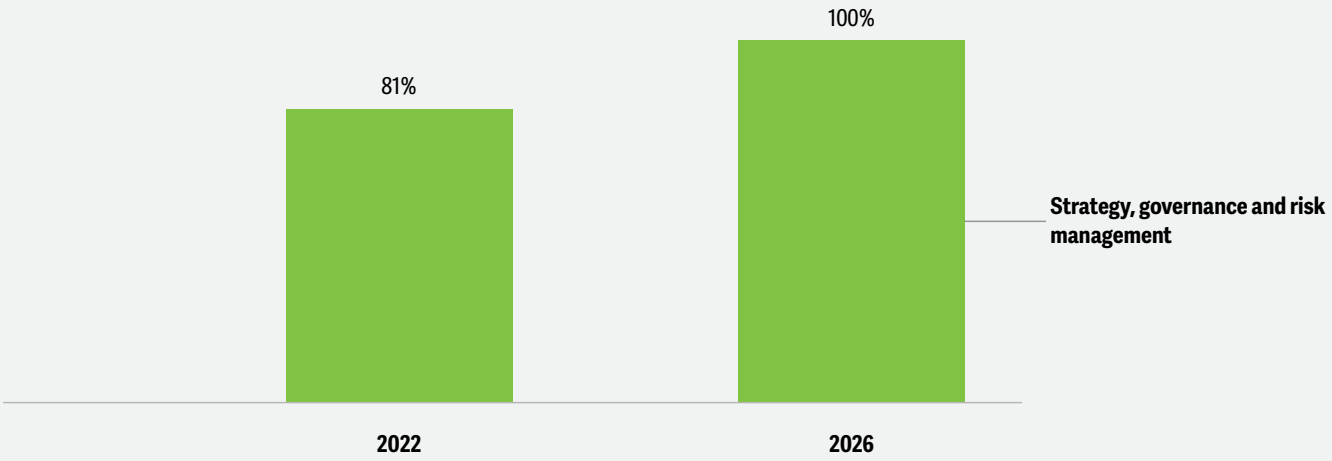
It wasn't always a given that the CISO would be central to a state's information technology organizations. In 2010, when Deloitte and NASCIO began this biennial survey, states handled cybersecurity in a far less systematic and robust way. Few states defined roles and responsibilities in statutes and not every state even had a top executive overseeing information security, much less someone with an official CISO title.[21]

What we've seen over the years is a steady expansion of state CISOs' portfolio of responsibilities.

*Figure 17*

**It's unanimous: Every CISO told us they now offer strategy, governance and risk management services to state agencies**

*Question: "What services do you offer to your state agencies?"*




Note: The following services have been considered as part of strategy, governance and risk management: governance (architecture, policies, standards), regulatory compliance, risk assessment and management, security compliance of vendors and contractors, strategy and planning, budgeting, adoption of emerging technologies (cloud, blockchain, artificial intelligence, robotic process automation, low-code and no-code), Internet of Things, election security, cyber insurance and asset inventory.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

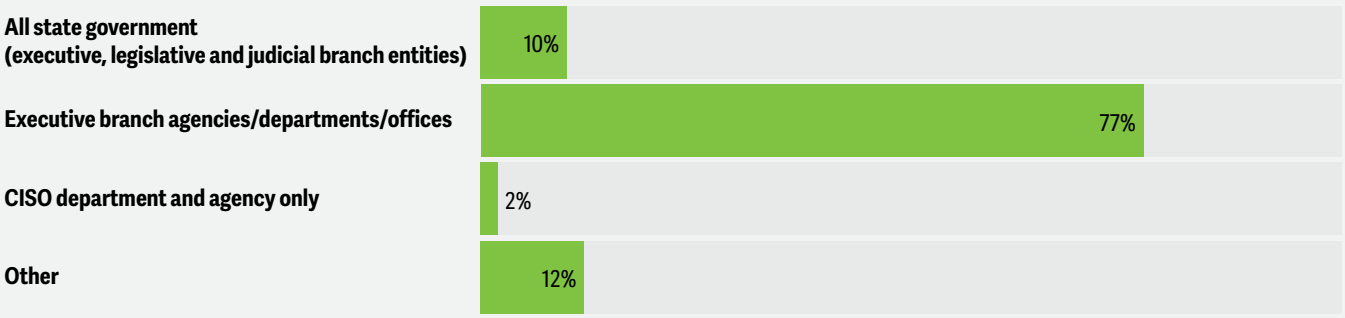
For example, between the 2022 survey and this year's survey, the fraction of state CISOs offering strategy, governance and risk management services to state agencies rose from 81% to 100% (figure 17). CISOs have become a primary resource for cybersecurity throughout state government.

Responses from the three most recent NASCIO-Deloitte surveys show a consistent baseline: Just over three-quarters of state CISOs oversee cybersecurity for executive branch agencies and departments. In 2026, about 77% respondents said they oversee cybersecurity for executive branch agencies, departments and offices and an additional 10% indicated that their scope extended beyond the executive branch (figure 18). Nearly all state CISO offices offer a critical set of core services to state agencies, including security management and operations; incident response; and network and infrastructure (figure 19). And CISOs are increasingly shouldering the responsibility of overseeing cybersecurity for state agencies.

*Figure 18*

## CISOs' portfolios of responsibilities is well established, with just over three-quarters overseeing cybersecurity for the executive branch

*Question: "Scope of authority: For which of the following organizational entities does your state's CISO have responsibility?"*



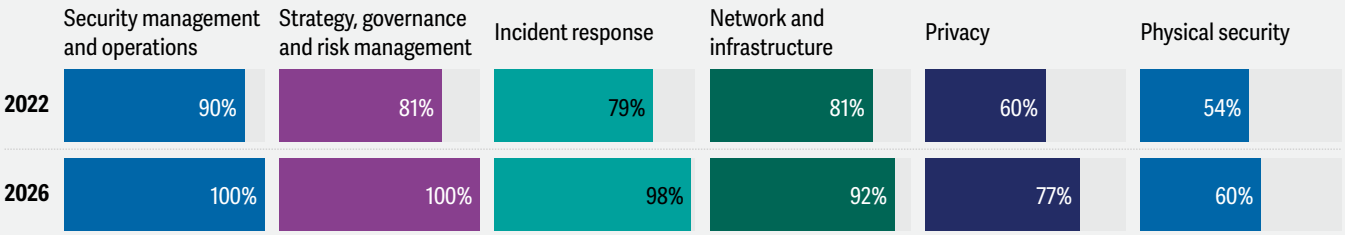

Note: Percentages may not add to 100% due to rounding.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 19*

## CISOs offer a broad array of cybersecurity services to state agencies

*Question: "What services do you offer to your state agencies?"*




Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 20*

## A majority of CISOs report having responsibilities around AI in terms of both external threats and internal use

*Question: "What is included within the mandate and scope of your responsibility as the state CISO to protect?"*


Source: 2026 NASCIO-Deloitte Cybersecurity Study.

While AI has been around for a while, its use in state government has only recently begun to change operational models and alter the threat landscape. With the use of smart technologies growing, state CISOs are increasingly responsible for not only keeping up with AI-based external threats but monitoring whether public employees are using AI responsibly (figure 20).[22] The percentage of CISOs who oversee state agencies' adoption of emerging technologies has risen from 38% in 2022 to 43% in 2024 and now 69% in 2026.

CISOs told us about the steps they are taking to more effectively use AI in threat detection and response, including the automated integration with cyber threat intelligence services and the incorporation of real-time data from local governments and public education. The goal is to proactively automate alerts and initial responses. A few of the things we heard about ongoing efforts and plans included:

- "We are looking to better automate notification processes (we have a CRM) to more rapidly notify local units of government of security issues that they need to investigate."
- "Today, we monitor and alert on malicious activity and also proactively block anything identified by our endpoint detection and response solution. However, there are still many situations where there is manual intervention by our analysts, and they work with coordinators within local government and higher education to gain approval to take any additional action. In order for us to keep pace with the attackers, we are going to have to learn to trust automation so that we can automatically take remediation actions first and then involve people to review what actions took place. We can no longer wait for approval from an entity to take action."
- "We are expanding our internal SOC capabilities to include additional source data, use cases, automation and AI integration."

# Resource crunch: Funding slows as talent demand grows

The cyber threat landscape is becoming only more treacherous, and the scope of CISOs' responsibilities continues to grow—yet resources aren't keeping up with the demand. Unlike most IT projects, cybersecurity is never finished. Cybersecurity is an ongoing struggle against increasingly sophisticated adversaries.

This year's survey revealed that after several years of relatively strong budget support, there has been a serious turning of the tide: The budget picture in many states is bleak. At the same time, CISOs continue to struggle in the area of talent, reporting a serious gap between the capabilities of their staff and the demands they are facing.

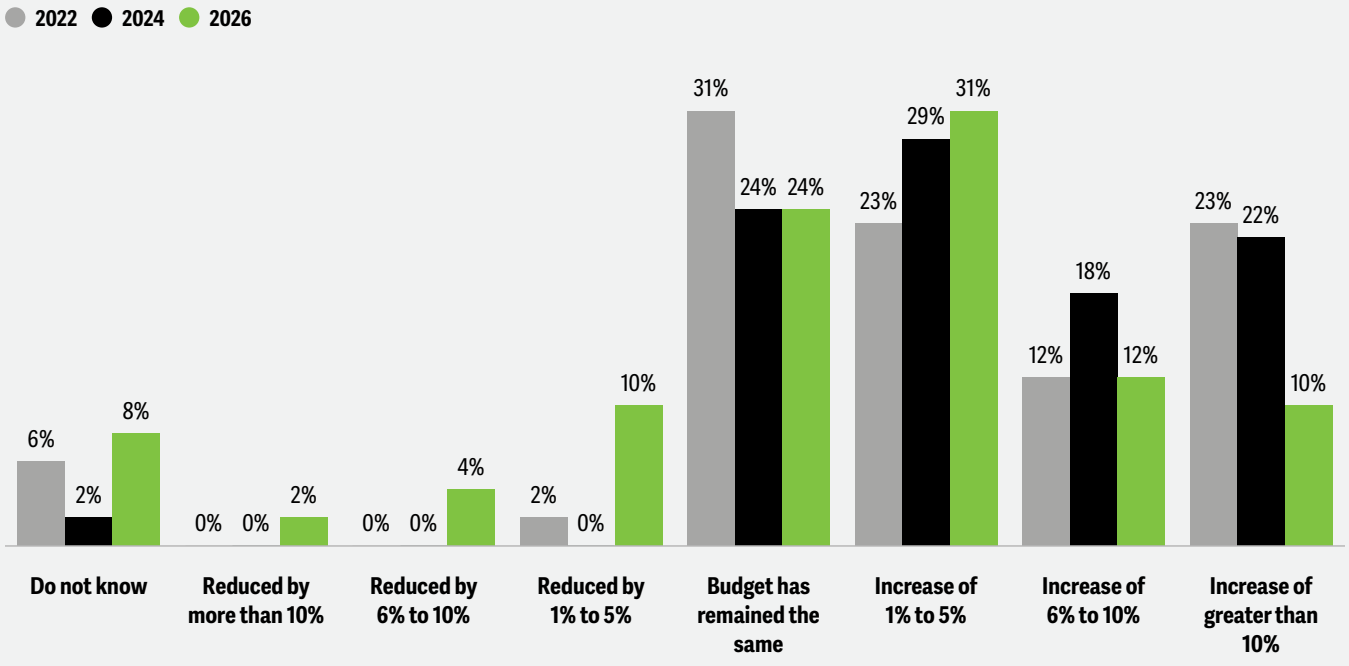
## Funding is falling short

Eight states reported year-over-year cybersecurity budget reductions, with three noting annual reductions of more than 5%. More than half saw either a modest increase or a flat budget (figure 21).

*Figure 21*

### CISOs reported a decline in year-over-year budget increases, and 16% reported that budgets were actually reduced

*Question: "Please select the option which best describes the year-over-year trending in your state's cybersecurity budget for years 2023 and 2024."*




Note: Percentages may not total 100% because the response "Other" is not shown in the figure.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

These responses paint a grim picture. Only 22% of CISOs reported increases of 6% or more in their budgets, down from 40% in the 2024 survey. On the other end of the spectrum, a concerning 16% of CISOs reported an outright reduction in budget; contrast this to the 2024 survey, in which no state reported a decline.

It should be noted that state cybersecurity funding is often challenging to precisely quantify, as spending is typically embedded in broader IT, agency, or program budgets. Even in states that have statewide cybersecurity line items, these may not be comprehensive. This lack of visibility in operations may help explain why metrics and reporting capabilities were a priority for CISOs this year, as such metrics can help demonstrate the benefits of cybersecurity expenditures. Nonetheless, these survey results signal that CISOs are reporting a decline in funding increases, especially when compared with their growing responsibilities. Moreover, rising costs—in terms of both talent and technology—means that flat or slightly increased budgets may feel like budget reductions.

Several factors could be behind the funding challenge, including:

- Growing pressure on state general funds
- The expiration of one-time federal support from programs such as the American Rescue Plan Act of 2021
- Reduced federal support of programs such as the Cybersecurity and Infrastructure Security Agency and the Multi-State Information Sharing and Analysis Center, shifting some costs to states

These shortfalls are particularly concerning, since cybersecurity budgets now cover a broader range of responsibilities than ever before. Nearly every CISO reported that they're responsible for security operations and monitoring; workforce and outsourcing issues; and governance, strategy and compliance. Most also handle identity and access management (figure 22).

### The role of SLCGP funding helps—but uncertainty limits adoption

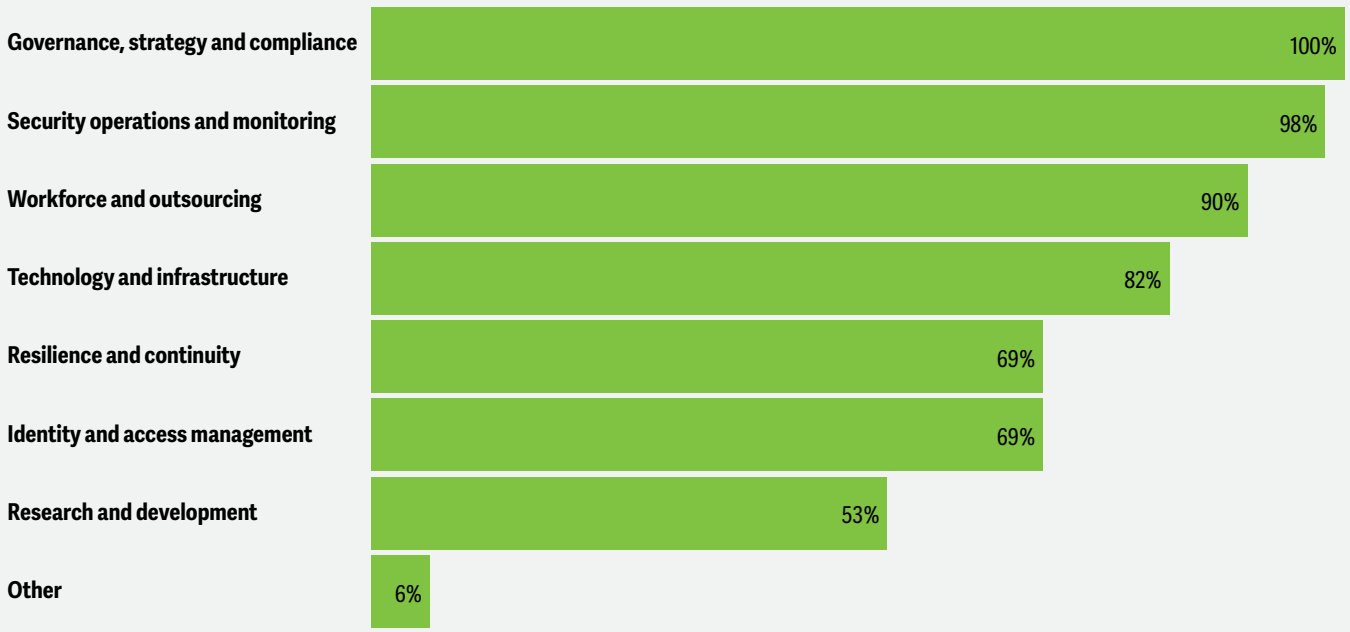
Many states have relied on the federal SLCGP to bolster operational funding as well as for additional programs targeted to help local government.

Several CISOs told us how they were using SLCGP funding to extend cyber protection:

*Figure 22*

**CISO funding covers governance, compliance, security operations and more**

*Question: "Which of the following are covered under your state's cybersecurity budget?"*




Source: 2026 NASCIO-Deloitte Cybersecurity Study.

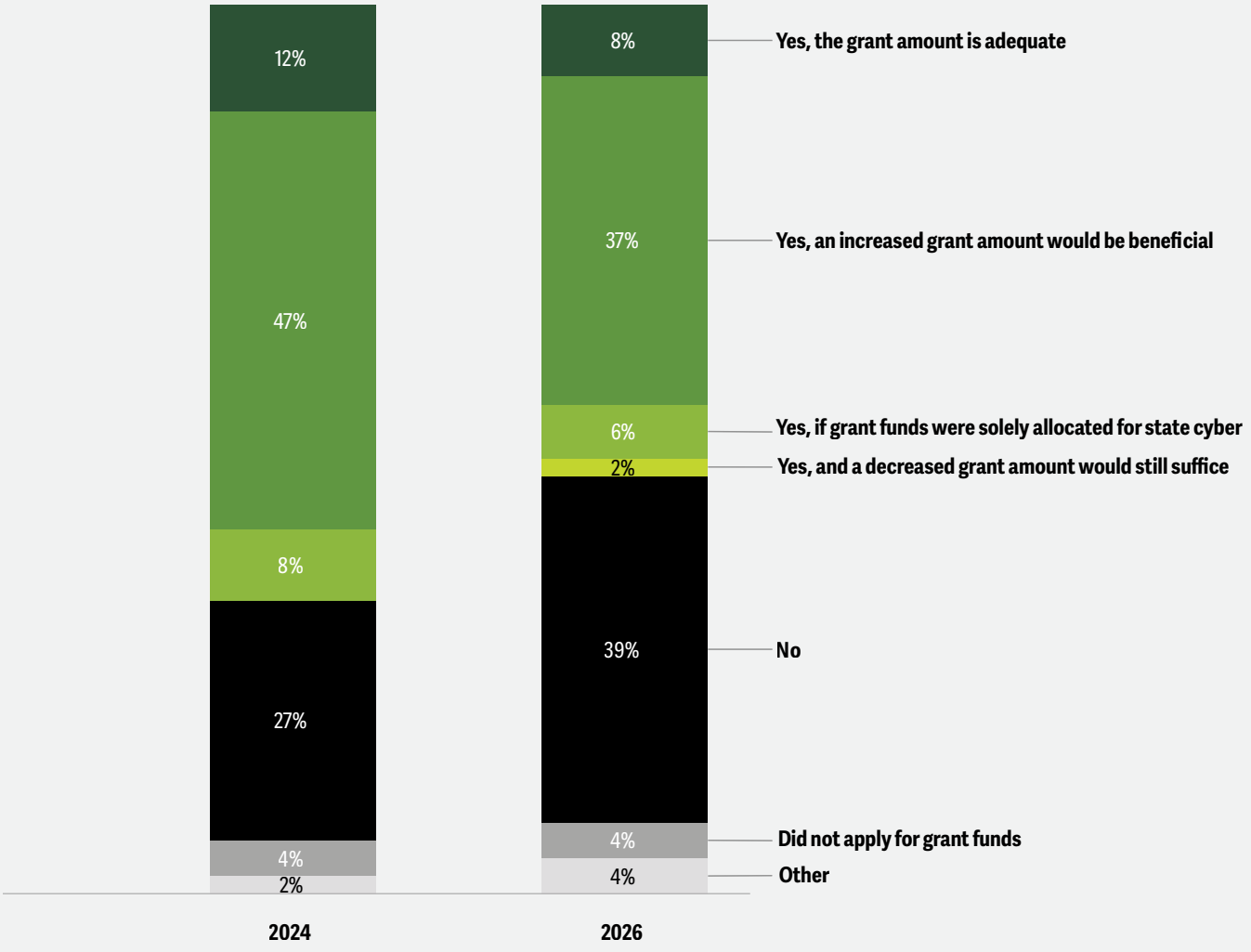
- "We are utilizing funds to deploy multi-factor authentication (MFA) hardware tokens to state accounts and providing MFA tokens to local governments."
- "We have extended services (endpoint protection and response, security awareness training and vulnerability management) to 85% of local government, with a goal of reaching 100% by next year."
- "We have awarded critical service improvement projects to many local government agencies. Cyber assessments are also being done through the SLCGP funding for small local government entities, helping to inform other cybersecurity projects to be collectively funded."
- "We have seen an increase in adoption of foundational controls like the use of .gov, MFA and cyber training with some submissions to replace end-of-life and end-of-support hardware or software."

But CISOs also told us that more funding would be helpful. Nearly 40% of CISOs stated that SLCGP grants were inadequate, with another 37% saying that an increased amount would be beneficial (figure 23).

*Figure 23*

## CISOs have generally appreciated local grant funding and would like to see more of it

*Question: "In your opinion, were the grant funds available through the State and Local Cybersecurity Grant Program sufficient?"*




Source: 2026 Deloitte-NASCIO Cybersecurity Study.

CISOs are also finding it challenging to plan ahead with the SLCGP facing an uncertain future in Congress, with months of lingering questions throughout 2025 clearly influencing survey answers.[23] One CISO noted that "SLCGP adoption is slow due to concerns around the sustainability of federal grant funding."

And the program's complexity drives some of CISOs' discontent, with several citing "implementation challenges" and others noting related impacts:

- "We have trouble getting qualified entities to apply."
- "Unfortunately, due to the complex application process, limited funding and short four-year time frame of the program, the SLCGP has not achieved the desired impact. Too many cities and towns need easier access to more resources in order to fully advance their cyber posture."
- "The SLCGP has advanced our state's cybersecurity posture or operations. However, the match requirement has been challenging. Also, decreasing budgets at the state level make it very difficult to make use of the federal funds without growing our ongoing operational costs."

## The talent gap persists, despite more success attracting skilled talent

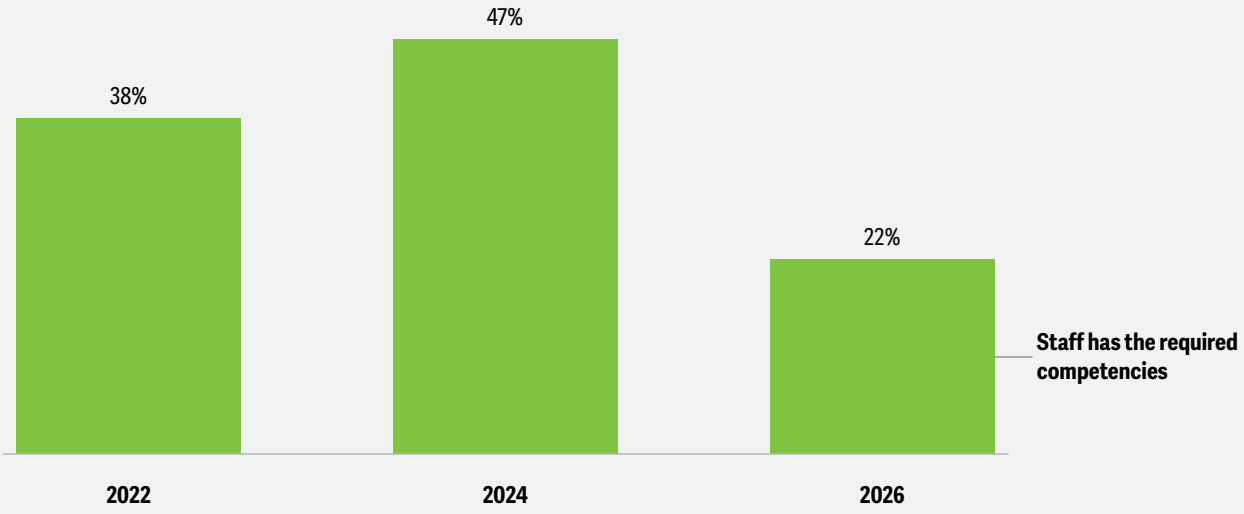
There is one possible bright spot in the survey: Fewer CISOs cited the availability of cyber professionals as a top concern: The percentage of CISOs that identified inadequate availability of cybersecurity professionals as a top five barrier declined from 50% in 2022 to 22% in 2026. Nonetheless, CISOs still reported that "inadequate staffing" remains a leading concern. One possible conclusion is that while hiring challenges have lessened, states are struggling to fully staff up due to headcount and budget constraints, leading to a familiar challenge: A gap exists between the capabilities available on staff and the skills needed to face current cyber challenges.

Headcount is only part of the issue, of course: Staff need to be able to actually do the work at a time when rapidly improving technologies are driving new threats and dramatically fewer CISOs report that their states' cybersecurity professionals possess the knowledge and skills necessary to keep up with the cyber issues of today and tomorrow. Only 22% of CISOs—down from 47% in 2024—say their staff has the required competencies (figure 24), with eight of 51 CISOs reporting that staff "has significant gaps in competencies." This doesn't necessarily indicate that people across the board need more training—rather, it may be that offices are under-staffed, or employees lack certain specific skills.

*Figure 24*

### Significantly fewer CISOs see their cybersecurity professionals having the knowledge and skills needed to keep up with incoming threats

*Percentage of respondents selecting "Yes" to the question: "Do your state's internal cybersecurity professionals have the required competencies (such as knowledge, skills and behaviors) to handle existing and foreseeable cybersecurity requirements?"*



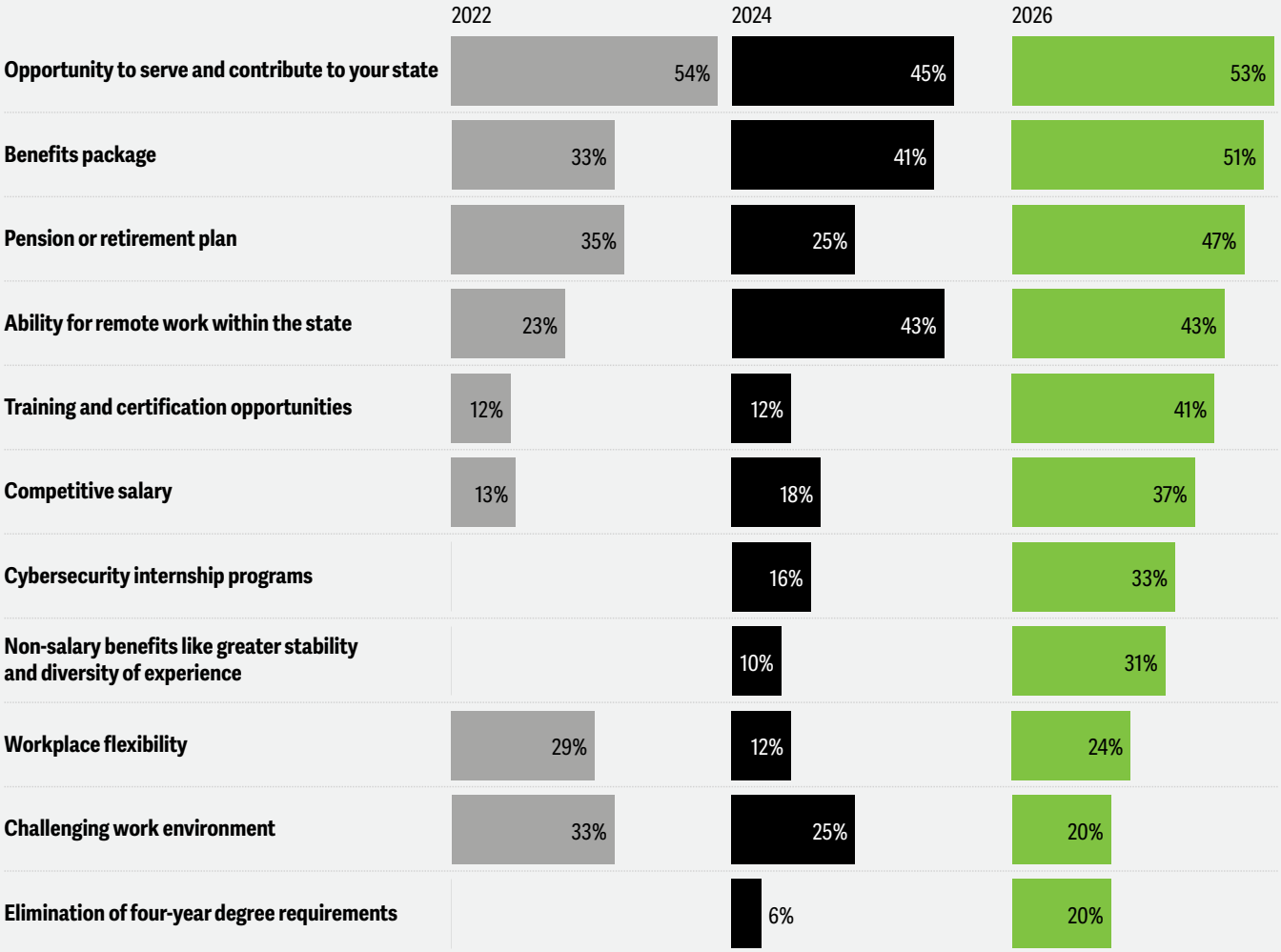

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

Despite these findings, trends suggest that CISOs are in a more competitive position to hire cybersecurity experts. Substantial growth in interest in training and certification (from 12% in 2024 to 41% in 2026) and eliminating four-year degree requirements (from 6% in 2024 to 20% in 2026) indicates increasing prioritization of practical skills over formal credentials (figure 25).

*Figure 25*

## State CISOs increasingly see salary, benefits and training opportunities as key factors in attracting and retaining talent

*Question: "What are the top 3 factors to attract and retain cybersecurity talent to work for your state?"*




Note: Cybersecurity internships programs, non-salary benefits and elimination of four-year degree requirements were not included as response options in the 2022 survey.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

## NASCIO-Deloitte Cybersecurity Study: Key topics through the years

*Tracking the themes that have emerged since 2010 shows an interesting evolution in the role of the state CISO*

| Year | Budget | Workforce | Threats | Strategy and issues |
|---|---|---|---|---|
| **2026** | Cyber budgets fail to keep pace with rising demands | CISOs still struggle to fill the gaps in workforce capabilities | Rapidly evolving threats—including AI-based threats—lower CISO's confidence in their ability to safeguard data | CISOs' responsibilities are expanding; new roles involve AI, GenAI and, in some cases, whole-of-state cyber support |
| **2024** | Budget concerns return | Turnover at the top—average CISO tenure less than two years; Continued struggles to retain top cyber talent | AI/GenAI: new threats and potential new tools; Identity and access management | Protecting critical infrastructure and operational technology |
| **2022** | Federal relief funds continue | Expanded use of third parties | Threats from criminal networks and malevolent state actors | Cyber vulnerability of infrastructure |
| **2020 (COVID-19)** | Federal funds provide temporary budget relief in light of massive demand | Employee fatigue, remote work; Expanded diversity initiatives | Remote workforce security; Financial fraud and cyberthreats | Whole of state approach, advent of federal local grant program |
| **2018** | Few states with dedicated budget line item | Use of contractors, vendors and third parties to augment state cyber staff | Greater importance to cybersecurity within government operations | CISO roles continue to become embedded in statute; CISO function grows in stature as awareness of threats grow |
| **2016** | Dedicated cybersecurity strategies to command greater budgets | Dedicated cybersecurity strategies to build staff with necessary competencies | States take a more proactive approach to manage risks; "Growing sophistication of threats" as a challenge reduces | For the first time, all states report having a CISO |
| **2014** | Budget strategy disconnect—money misdirected by funding restrictions | Renewed efforts toward recruitment and training; Enhanced flexibility to deal with enduring skills gap | Growing sophistication of cyberthreats | CISO responsibilities become more standardized |
| **2012** | Insufficient funding | Emerging cyber skills gap | Ensuring compliance with good cyber practices within state government | Preparedness for evolving threats |
| **2010** | Inadequate budgets and unreliable funding sources | Staff shortage due to insufficient budgets | Evolving cybersecurity roles and relationships | Basic security hygiene; Emerging cybercrime |

Source: Deloitte analysis.

# Appendix 1: About the study

The 2026 NASCIO-Deloitte Cybersecurity Study uses survey responses from state CISOs who answered 54 questions—many of them multipart—crafted to capture the enterprise-level strategy, governance and operation of security programs. Our survey, launched in late October 2025, received responses from all 50 states, the US Virgin Islands and the District of Columbia. One respondent submitted a partially completed survey, resulting in some questions having 51 responses. Figure 26 illustrates the demographic profile of CISO participants' states.

Several questions were open-ended, inviting respondents to describe their states' various initiatives. For readability, we have eliminated some extraneous or less relevant responses in the charts, meaning that totals may not equal 100%.

*Figure 26*

## Budget and workforce of responding states and territories

| | 2022 | 2024 | 2026 |
|---|---|---|---|
| **Indicate the approximate annual state budget for the current budget year (US$)** | | | |
| 1 billion to 10 billion | 27% | 20% | 19% |
| 11 billion to 25 billion | 21% | 18% | 27% |
| 26 billion to 50 billion | 19% | 24% | 8% |
| More than 50 billion | 23% | 27% | 35% |
| Do not know | 10% | 12% | 12% |
| **Number of state government employees in your state (excluding higher education employees)** | | | |
| 5,000 to 15,000 | 13% | 18% | 13% |
| 15,001 to 25,000 | 13% | 18% | 21% |
| 25,001 to 75,000 | 52% | 47% | 44% |
| More than 75,000 | 17% | 18% | 21% |
| Do not know | 4% | 0% | 0% |

Note: Percentages may not total 100% due to rounding.

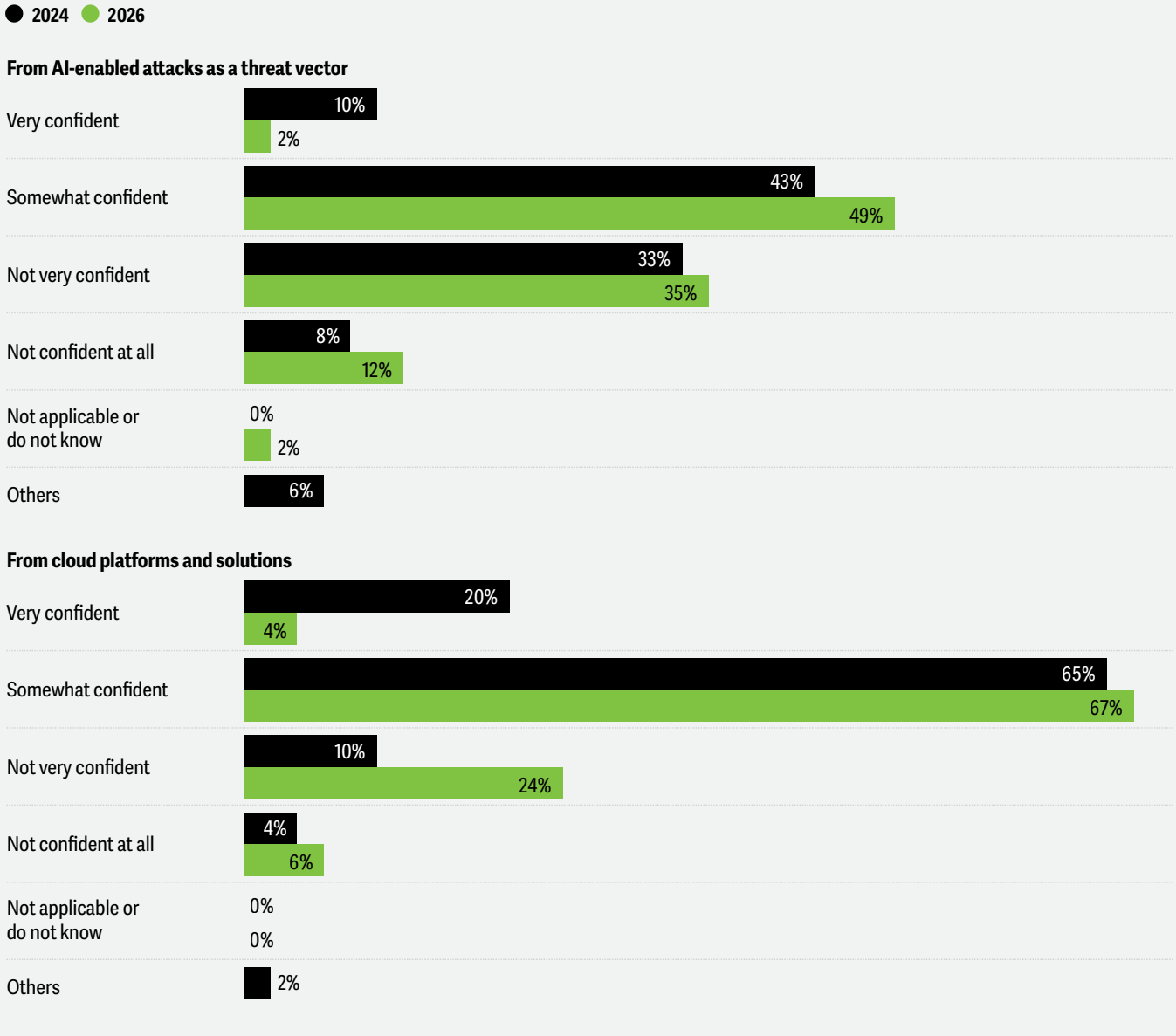
Source: 2026 NASCIO-Deloitte Cybersecurity Study.

# Appendix 2: Additional survey analysis deep dives

*Figure 27*

## State CISOs reported shifting confidence in dealing with AI and cloud-based threat vectors

*Question: "How confident are you that your state's information assets are protected from the following types of cyberthreats and their origination?"*



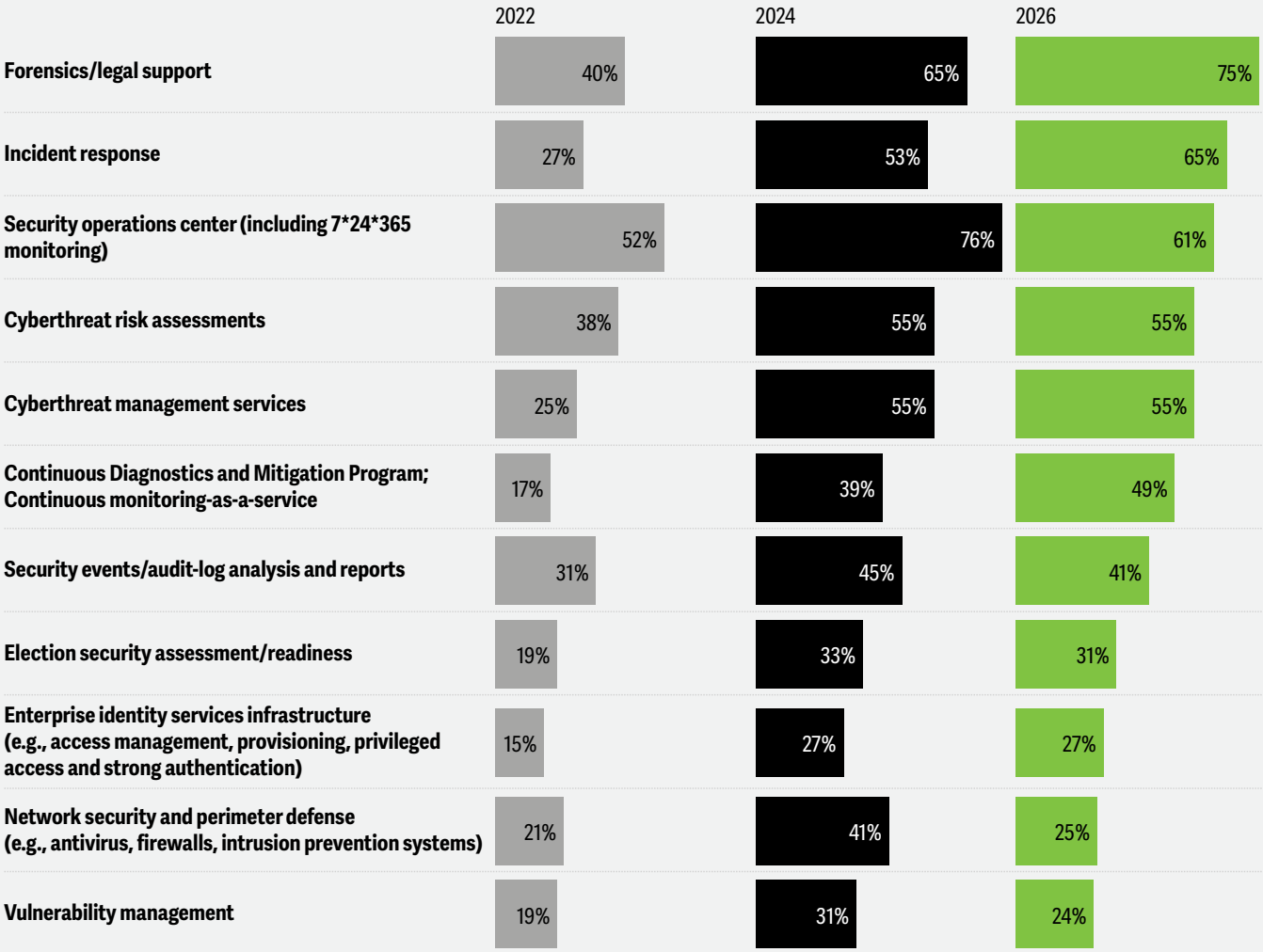

Note: Percentages may not total 100% due to rounding.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 28*

## More states are outsourcing—partially or completely—some cybersecurity functions, from administrative work to incident response

*Question: "What cybersecurity functions does your state outsource (partially or completely)?"*

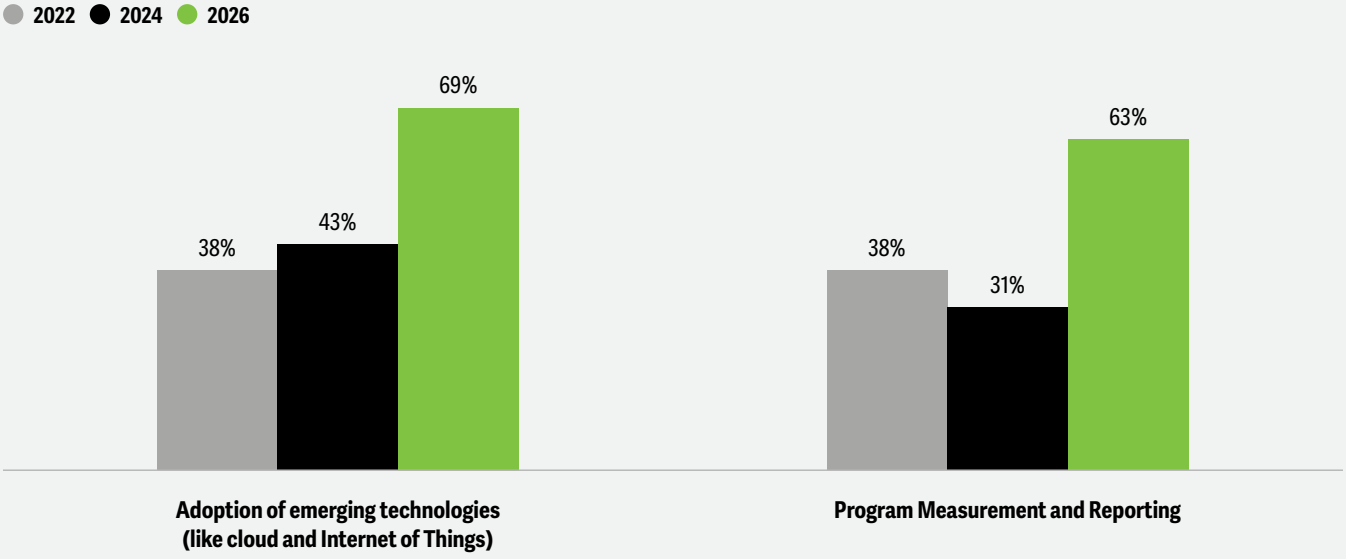



Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 29*

## More CISOs reported offering state agencies help with cybersecurity metrics as well as guidance for incorporating cloud and IoT technologies

*Question: "What services do you offer to your state agencies?"*

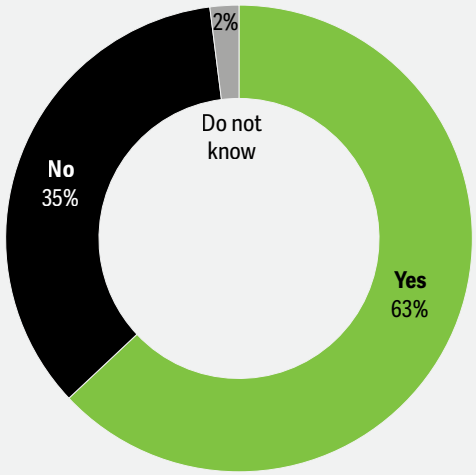



Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 30*

## Nearly two-thirds of states have advisory councils to help guide cybersecurity strategy and coordinate stakeholders

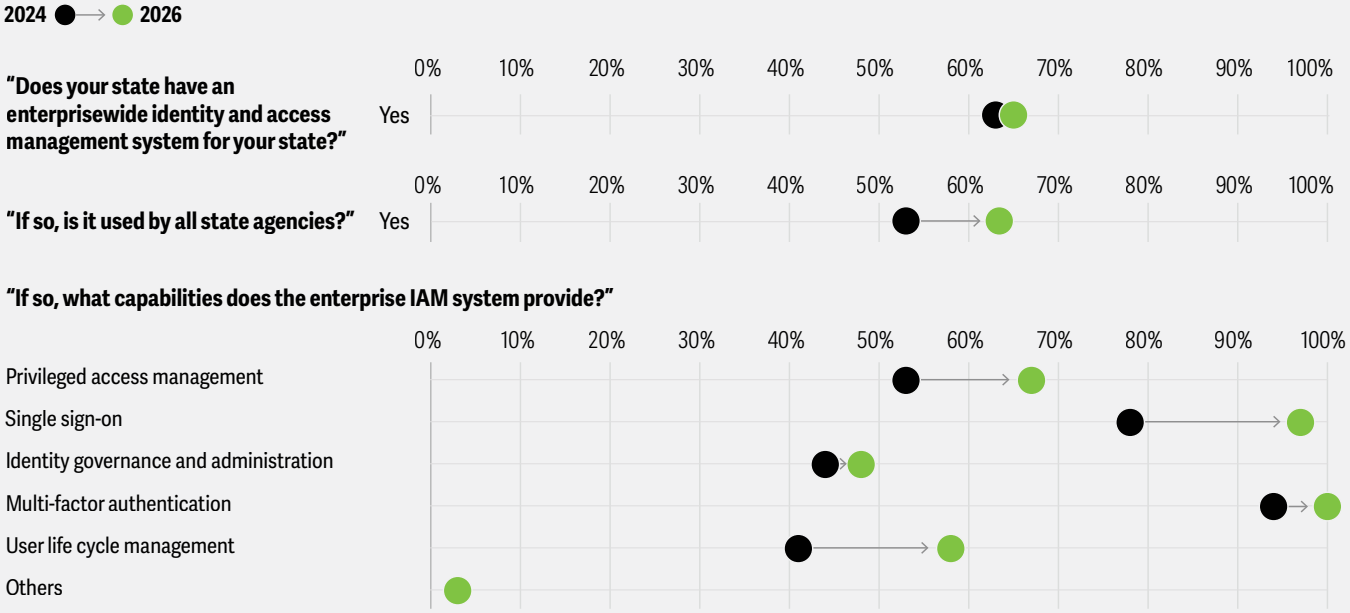
*Question: "Does your state have a cyber advisory council that works with the CISO to identify requirements for the cybersecurity strategy?"*




Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 31*

## Nearly two-thirds of states have enterprisewide IAM systems with statewide usage and capabilities increasing

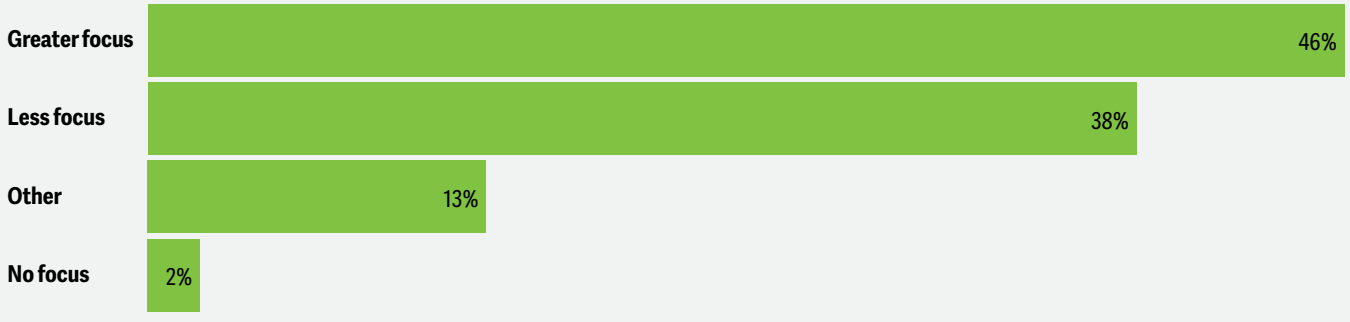



Source: 2026 NASCIO-Deloitte Cybersecurity Study.

*Figure 32*

## When it comes to local governments and higher education, states are divided in their cybersecurity approach

*Question: "What is your state's approach to cybersecurity for local government entities and public higher education?"*




Note: Percentages may not add to 100% due to rounding.

Source: 2026 NASCIO-Deloitte Cybersecurity Study.

# Endnotes


1. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.
2. Liora Ziv, "Digital frontlines: The escalating cyber war on municipalities worldwide," CyberProof, July 1, 2025.
3. Sk Tahsin Hossain et al., "Cybersecurity in local governments: A systematic review and framework of key challenges," *Urban Governance* 5, no. 1 (2025): pp. 1-19; Multi State Information Sharing and Analysis Center, "Strengthening critical infrastructure: State, local, tribal, & territorial progress & priorities, Volume 2," Aug. 11, 2025.
4. Mohammed Khalil, "Data breaches in education 2025: Why schools are the #1 cyber target," DeepStrike, Aug. 18, 2025.
5. Sam Park et al., "Whole-of-state cybersecurity: Protecting the public information ecosystem," *Deloitte Insights*, Jan. 30, 2026.
6. Clare Mohr et al., *Global Cyber Threat Intelligence (CTI): Annual Cyberthreats Trends Report 2024*, Deloitte, March 2025.
7. Lily Morris, "Security vs. sophistication: How cybercrime is evolving faster than defenses," *The National CIO Review*, Oct. 16, 2025.
8. Kieran Norton et al., "How can tech leaders manage emerging generative AI risks today while keeping the future in mind?" *Deloitte Insights*, Feb. 20, 2025.
9. Ben Nettleton, "Common cybersecurity metrics: Key KPIs to measure," Kiuwan, Nov. 20, 2025.
10. Syracuse University School of Information Studies, "AI in cybersecurity: How AI is changing threat defense," July 20, 2025.
11. Christina A. Cassidy, "Trump administration halts funding for two cybersecurity efforts, including one for elections," *The Associated Press*, March 10, 2025.
12. *Government Technology*, "MS-ISAC cybersecurity network moves to paid membership model," Sept. 24, 2025.
13. Barry McIntyre, "NIST ranked 2025's most valuable cybersecurity framework," Cyber Security Tribe, April 22, 2025; Anna Fitzgerald, "NIST vs CIS: How to decide which cybersecurity framework is right for you," Secureframe, Aug. 28, 2025.
14. NIST Computer Security Resource Center, "Security and privacy controls for information systems and organizations, 5.2.0," Aug. 27, 2025.
15. Center for Internet Security, "The 18 CIS critical security controls," version 8.1, accessed Jan. 3, 2026.
16. John Wilson, "Whole-of-state cybersecurity as a smarter way to scale," *StateTech*, Dec. 16, 2025; Sophia Fox-Sowell, "Critical infrastructure relies on 'whole-of-state' information sharing, says report," *StateScoop*, Feb. 28, 2025.
17. Eric Geller, "Senators push to renew cyber grant program for state, local governments," *Cybersecurity Dive*, Dec. 2, 2025.
18. Mary Scott Nabers, "Cybersecurity is no longer local—America is moving toward a centralized defense model," Strategic Partnerships, Sept. 10, 2025.
19. Anna Merod, "82% of K-12 schools recently experienced a cyber incident," *K-12 Dive*, March 10, 2025; Jon Munshaw, "K-12 schools face cybersecurity risks inside and outside of the classroom," Sophos, Sept. 18, 2025; Alyson Klein, "Cyberattacks are a big problem. Can schools manage without federal help?" *Education Week,* Sept. 9, 2025.
20. Adam Stone, "Regional security operations centers strengthen cybersecurity for local governments," *StateTech*, Sept. 22, 2025.
21. In the 2010 survey, four states reported having no enterprise CISO role. Deloitte and NASCIO, "State governments at risk: A call to secure citizen data and inspire public trust," 2010.
22. Naman Chaurasia et al., "Scaling gen AI in US state and local governments: Opportunities, challenges, and the path to achieving large-scale value," *Deloitte Insights*, May 16, 2025.
23. Colin Wood, "Cyber grant uncertainty puts state programs in limbo, GAO report finds," *StateScoop*, April 29, 2025; Chris Teale, "'Uncertainty' swirls around federal funding cuts' state and local impact," *Route Fifty*, July 18, 2025.

# Acknowledgments

We thank the National Association of State Chief Information Officers (NASCIO) and Deloitte professionals who helped to develop the survey and execute, analyze and create the report.

At NASCIO, we thank executive director **Doug Robinson** and all CISOs who participated in the 2026 survey.

At Deloitte, we thank subject matter specialists **Srini Subramanian**, **Bharane Balasubramanian**, **Kiran Mantha**, **Lori James**, **Lauren Gabriel** and **Bharath Chari** of Deloitte & Touche LLP for their leadership on the survey effort, data analysis and benchmarking. We express our gratitude to **John O'Leary** and **Sushumna Agarwal** of Deloitte Services LP for their data analysis, writing and operational support. Additional thanks go to the broader Deloitte survey, data analysis and benchmarking team: **Glynis Rodrigues**, **Apurba Ghosal**, **Thirumalai Kannan**, **Rohith Reddy**, **Srinivasarao Oguri** and **Sanjay Vadrevu** of Deloitte Services LP.

We would also like to thank the writing and marketing team, including **Matthew Budman** and **Allison Del Re** of Deloitte Services LP.

# About the authors

**Meredith Ward**
mward@nascio.org

Meredith Ward is the deputy executive director for the National Association of State Chief Information Officers (NASCIO) and has served at the association since 2013. She has over 20 years of experience in state, local, federal and international professional associations and is a 2024 Women in Cyber honoree. Prior to her current position, Ward worked in government and media affairs in Washington, D.C., and acquired over 10 years of experience building relationships with members of Congress, their staff and members of the media. She has worked extensively on issues related to cybersecurity, public sector workforce, technology acquisition, criminal justice and state technology. Ward holds a Bachelor of Arts degree, with an emphasis on Government, from Centre College.

**Michael Wyatt**
miwyatt@deloitte.com

Michael Wyatt is a cyber principal at Deloitte. He has over 30 years of professional experience and serves as the cyber leader for Deloitte's state local and higher education practice as well as for the state of Texas. Previously, Wyatt led Deloitte's global identity management practice and Deloitte's US identity practice. In addition, he leads statewide breach remediation and information security program development and implementation for the states of Utah and South Carolina. He has led the design and delivery of numerous complex identity management and cybersecurity projects across multiple industries including state government, higher education, financial services, media, energy, aerospace and defense and health care.

# About the National Association of State Chief Information Officers (NASCIO)

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and technology executives and managers from the states, territories and District of Columbia. NASCIO's mission is to advance government excellence through trusted collaboration, partnerships and technology leadership. 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 and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs.

# About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation. We produce cutting-edge research that guides public officials, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide fresh insights that advance an understanding of what is possible in government transformation.

# Continue the conversation

**Meredith Ward**
Deputy executive director | NASCIO
+1 859 514 9209 | mward@nascio.org

Meredith Ward is the deputy executive director at the National Association of State Chief Information Officers. She has more than 20 years of experience in state, local, federal and international professional associations.

**Mike Wyatt**
GPS SLHE cyber leader, government and public services | Deloitte & Touche LLP
+1 512 226 4171 | miwyatt@deloitte.com

Michael Wyatt is a cyber principal at Deloitte, serving as the cyber leader for Deloitte's state local and higher education practice and for the state of Texas. He leads statewide breach remediation and information security program development and implementation for Utah and South Carolina.

**William D. Eggers**
Executive director | Deloitte Center for Government Insights
+1 571 882 6585 | weggers@deloitte.com

William D. Eggers is the executive director of Deloitte's Center for Government Insights where he is responsible for the firm's public sector thought leadership.

# Contributors

**Editorial:** Rupesh Bhat, Preetha Devan, Aparna Prusty, and Cintia Cheong

**Creative:** Jim Slatton, Harry Wedel, Molly Piersol, and Govindh Raj
**Cover artwork:** Jim Slatton

Deloitte.

Published in collaboration with Deloitte Insights.

**About this publication**

This document contains general information only and NASCIO and Deloitte are not, by means of this document, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this document contains the results of a survey conducted by NASCIO and Deloitte. The information obtained during the survey was taken "as is" and was not validated or confirmed by NASCIO or Deloitte.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.