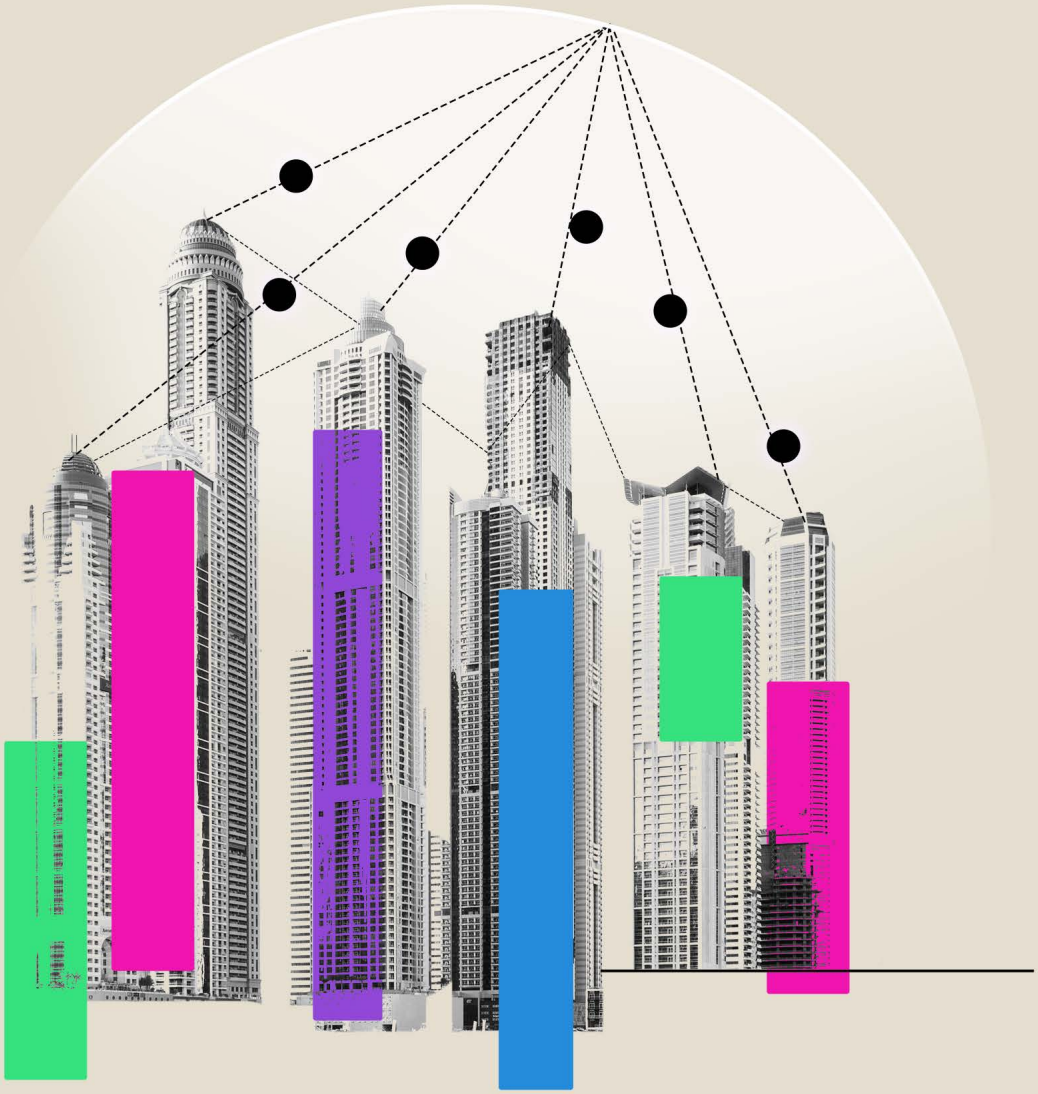
Deloitte. Insights

NASCIO



2022 Deloitte-NASCIO Cybersecurity Study

State cybersecurity in a heightened risk environment

A joint biennial report (7th edition) from Deloitte and the National Association of State Chief Information Officers (NASCIO)

About the authors

Srini Subramanian | ssubramanian@deloitte.com

Srini Subramanian is a principal in Deloitte & Touche LLP's Cyber practice and is the Global Industry leader for Risk Advisory in the government and public services industry. He has 35 years of IT experience and 25 years of cyber risk services experience in the areas of information security strategy, innovation, governance, identity, access management, and shared services. Subramanian actively participates in National Governors Association Cyber Policy Council, NASCIO, and various state committees to help elevate cyber risk in government. He has coauthored the biennial *Deloitte-NASCIO Cybersecurity Study* since its first publication in 2010.

Meredith Ward | mward@nascio.org

Meredith Ward is director of policy and research at NASCIO and has served at the association since 2013. She has more than 20 years of experience in state, local, federal, and international professional associations. Prior to her current position, Ward worked in government and media affairs in Washington, D.C., and acquired over a decade of experience building relationships with members of Congress, their staff, and members of the media. She has worked extensively on issues related to cybersecurity, IT acquisition, criminal justice, workforce, and state technology.

Contents

Foreword

Paving the path for cybersecurity in the postpandemic age

THE SEVENTH BIENNIAL Deloitte-NASCIO Cybersecurity Study arrives at a unique juncture for state chief information security officers (CISOs) and chief information officers (CIOs). Emerging from nearly three years of the COVID-19 pandemic, the landscape in which state CISOs operate has changed. While it may take years to know which transformations wrought by the pandemic will endure, we know that digitization has accelerated. The social distancing required by the health crisis made digital and mobile platforms the crux of work and daily life. This means that the future role of the state CISO is more important than ever, as new vulnerabilities and opportunities arise from greater use of these networks.

The 2022 survey was the result of robust participation by 50 states and three territories. At this pivotal moment, we find that the state CISO position has continued to gain strength and authority. As noted in the last biennial study, during the early days of the pandemic, CISOs performed the herculean task of migrating state government operations, services, and employees to a virtual environment nearly overnight. They enhanced safeguards such as multifactor identification, risk monitoring, and incident readiness to secure a remote workforce. As a result of these measures and the dedication of state employees, state agencies continued operating and providing services in the face of immense challenges.

Now, CISOs have a chance to build on that momentum to chart strategies for the post-pandemic era. To meet the needs of an even more hyperconnected age, they must tackle some longstanding challenges, while laying the groundwork for the adoption of newer technologies on the horizon. From this year's survey results, we identified three key takeaways critical to enhancing the CISO's role in the future.

Dealing with the talent gap. Attracting, retaining, and continually training a cybersecurity workforce primed for the future has become more difficult. It is encouraging to see an increasing trend to effectively embrace the delivery of cyber services, but states must reposition state employment to compete effectively with private sector and federal employers for millennial and Generation Z workers whose workplace ideals differ from those of previous generations. For example, the ability to work remotely, in part or in full, is now a basic expectation.

Embracing the entire state. In the ongoing effort to fortify resilience across their states, CISOs must extend their leadership to all levels of government, including the local level. Due to the many interactions that take place between local and state agencies, local government presents a threat vector. CISOs should increase their cooperation with higher education institutions to act as a bridge between state and local government and to also create a pipeline of cybersecurity professionals to address the talent gap.

Setting a new course. The postpandemic world brings new challenges and opportunities. CISOs need to have the foresight both in terms of budgets and new technologies to keep pace with the expectations of the increasingly digitized environment.

We thank the 53 states and territories that participated in our detailed survey. We salute your dedication to safeguarding citizen data and to securing the business of your state.

–Srini Subramanian and Meredith Ward

Key takeaway 1

Dealing with the talent gap

Fighting cyberthreats requires ready forces

In 2022, the demand for high-skilled workers has grown even more acute for both public and private sector employers. Reassessing their life choices during the COVID-19 pandemic, many employees joined the Great Resignation, and millennial and Gen Z workers are more carefully choosing workplaces that reflect their preferences. In this environment, the lack of cybersecurity professionals and staff remains among the top five barriers that CISOs cite (figure 1). Despite CISOs' growing responsibilities and the increasing sophistication of technology and threats, head counts for state cybersecurity professionals remain about the same as in 2020 (figure 2). In addition, over 60% of CISOs report gaps in competencies among their staff (figure 31).

States face heavy competition in hiring from the private sector and federal government. The private sector is combating the talent shortage by increasing pay, flexibility, and rapid career advancement to appeal to younger workers. Having lived through the experience of the pandemic, many no longer put work at the center of their lives. Though younger workers value the sense of purpose that government jobs offer, they are also demanding greater work/life balance, remote work and flexibility, and opportunities to maintain wellness.[1]

Many millennial and Gen Z workers are also looking to be part of a diverse workforce with an inclusive culture. Indeed, research shows that diverse teams, with their varying perspectives, are more effective and productive.

FIGURE 1

Inadequate availability of cybersecurity professionals is among the top five barriers that CISOs cite

Identify the top five barriers that you believe your state faces to address cybersecurity challenges.

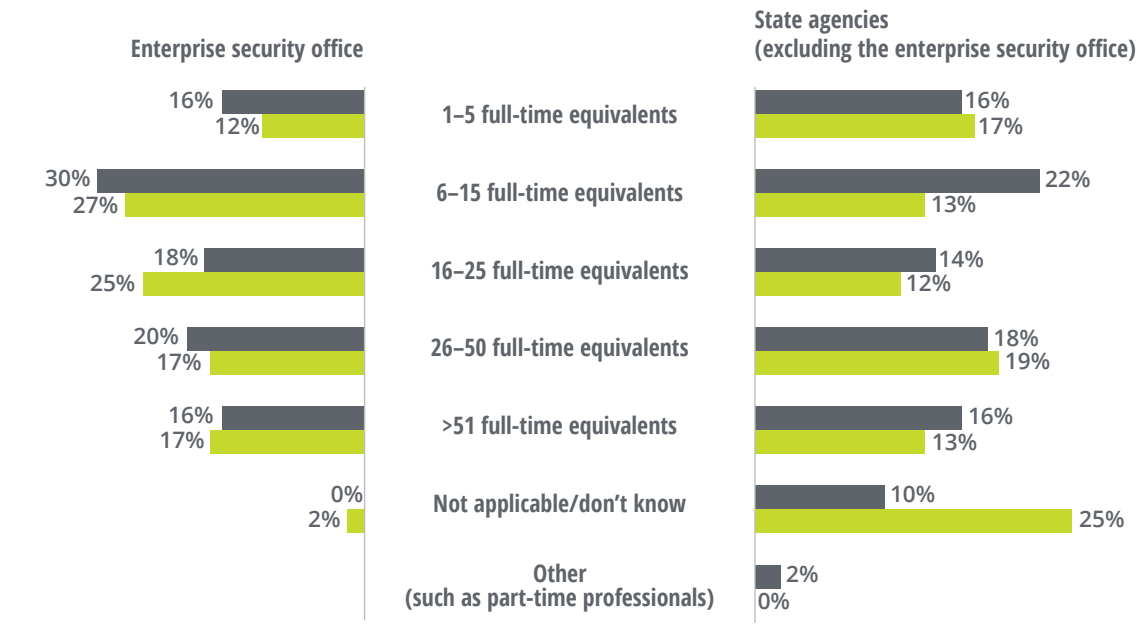
2020	2022
01 Lack of sufficient cybersecurity budget (46%)	**01** Legacy infrastructure and solutions to support emerging threats (52%)
02 Inadequate cybersecurity staffing (42%)	**02** Inadequate availability of cybersecurity professionals (50%)
03 Legacy infrastructure and solutions to support emerging threats (34%)	**03** Inadequate cybersecurity staffing (46%)
04 Inadequate availability of cybersecurity professionals (28%)	**04** Decentralized IT and security infrastructure and operations (38%)
04 Lack of dedicated cybersecurity budget (28%)	**05** Increasing sophistication of threats (29%)

Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study*.

FIGURE 2

Head counts for state cybersecurity professionals haven't changed much since 2020

How many dedicated cybersecurity professionals does your state employ? (Do not include contractors in this count.)



Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study*.

States are not meeting many of the demands of this new generation of tech workers. The top factors with which CISOs attract and retain talent remain largely the same as in years past. They include the opportunity to serve the public, job stability, and a retirement plan (figure 3).

Only 25% of states reported using remote work as a talent attraction tool (figure 4). This is somewhat surprisingly low, as CISOs have worked hard to ensure the security of work-from-home arrangements, with more than half expressing confidence in these efforts (figure 5). Moreover, the labor market is increasingly offering workers the option to work from home.

In addition, state CISOs are working to incorporate diversity, equity, and inclusion (DEI) practices, such as designating a DEI leadership position or teams to foster a culture of inclusion. In some cases, there was incomplete awareness of the DEI practices in place (figure 6).

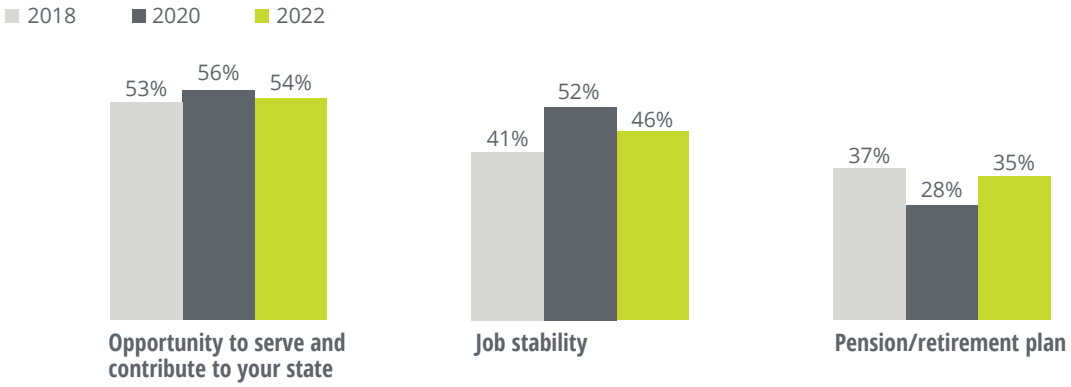
The long process that state CISOs must complete to hire staff at every level is giving competitors a better shot at hiring the best talent. About half of respondents say it takes three to six months to hire mid-level personnel and more than six months to hire director-level personnel (figure 7).

To close the gap, CISOs continue to rely on staff augmentation (figure 8). States are demonstrating more interest in outsourcing specific function areas and contracting with managed service providers (figure 9). For example, more than half of respondents report outsourcing security operations center functions, which require 24x7 monitoring (figure 10).

FIGURE 3

The top factors to attract and retain talent include the opportunity to serve the public, job stability, and a retirement plan

What are the top three factors to attract and retain cybersecurity talent to work for your state?

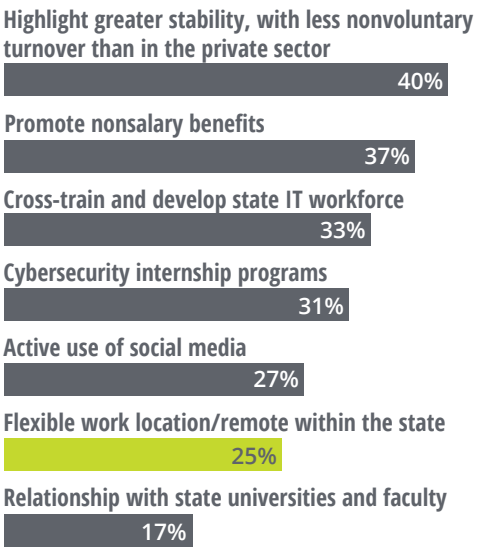


Sources: *2022 Deloitte-NASCIO Cybersecurity Study*; *2020 Deloitte-NASCIO Cybersecurity Study*; *2018 Deloitte-NASCIO Cybersecurity Study*.

FIGURE 4

Only 25% of states reported offering remote work as a way to attract cybersecurity talent

Identify the top three talent management practices followed by your state to attract and retain state cybersecurity workforce.



Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 5

Most CISOs have high confidence in the security of their work-from-home arrangements

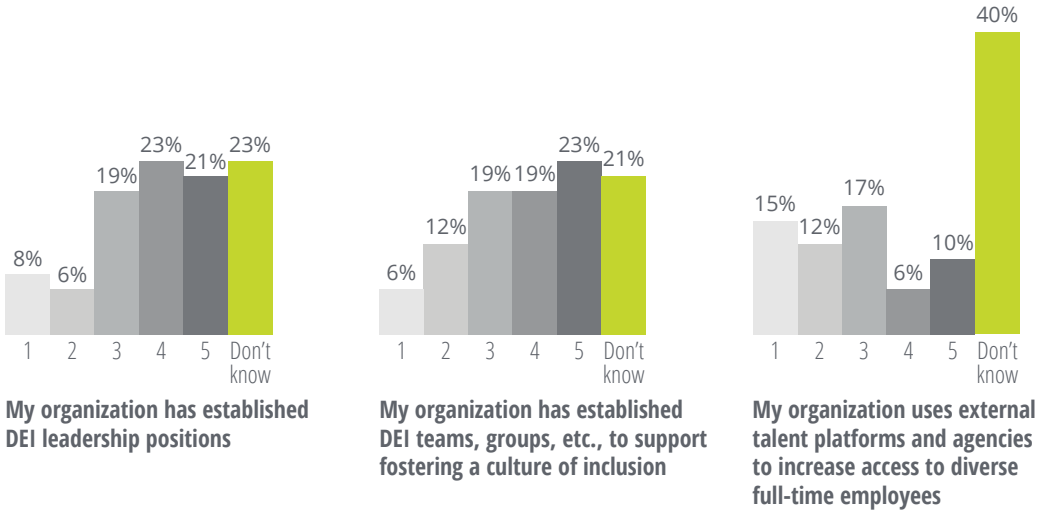
How confident are you that your state's information assets are protected from the following types of cyberthreats?

Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 6

Many CISOs reported incomplete awareness of the DEI practices in their organizations

The following are practices to improve DEI within an organization. Please select the degree to which you agree with each statement as it applies to your organization. (1 = Strongly disagree, 5 = Strongly agree)

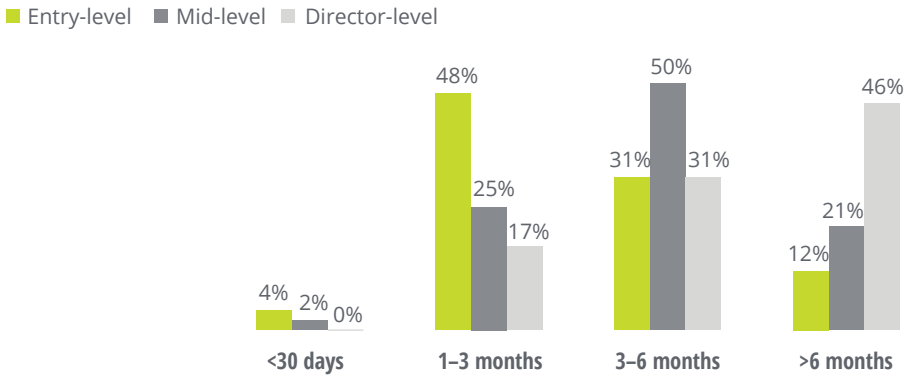


Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 7

The time taken to hire talent is delaying the process and putting states at a disadvantage

What is the average time to initiate and complete the hiring process for a cybersecurity position in the enterprise security office?

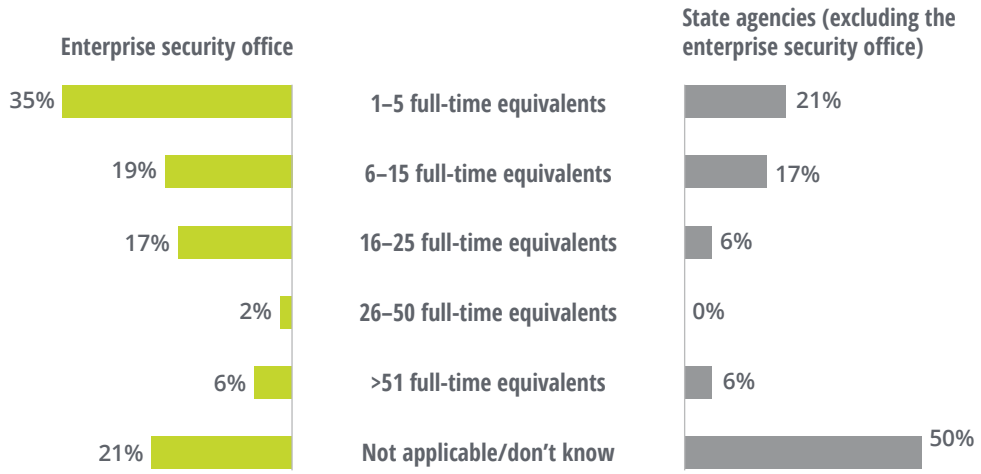


Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 8

CISOs regularly contract for cybersecurity professionals

If your state has staff/specialist augmentation, indicate the number of cybersecurity professional contractors employed.

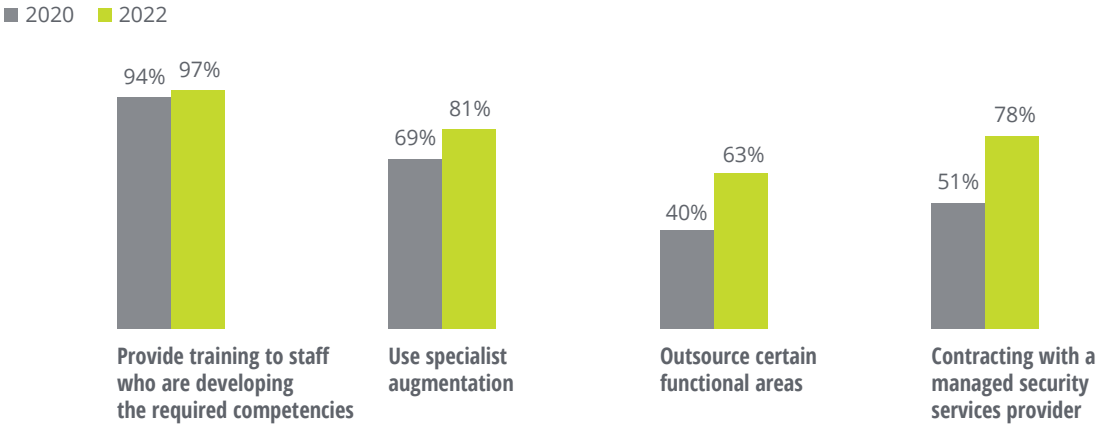


Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 9

Many states want to outsource specific function areas and contract with managed service providers

If you selected "Staff has gaps in competencies," how does your state plan to close the competency gap?



Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

Call to action

As they continue to compete with the private sector and federal government for talent, CISOs have an opportunity to reboot efforts to attract and retain up-and-coming cyber professionals by providing more of the workplace attributes they seek and to develop a more effective pipeline for fresh talent.

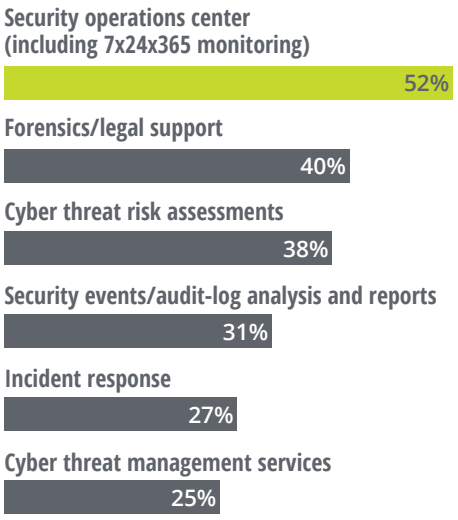
- **Transform state employment practices to attract next-generation workers.** The technology talent shortfall has reached a critical juncture. Although CISOs do not control state hiring practices, they need to make a case for a transformation of public talent management or face increasingly untenable talent shortages. To attract the best talent, states can take steps such as offering remote work options, providing an opportunity to work with up-to-date tech tools, shortening the hiring cycle, modernizing job titles and classifications using the National Initiative for Cybersecurity Education (NICE) framework, and other measures.

- **Turn to external resources to fill the gap.** As CISOs continue to build a robust in-house staff, they can turn to private-public partnerships to close the gap. Management of third-party vendors is maturing, as CISOs rely on them more to provide not only securities operations center functions, but also forensic and legal support and cyberthreat risk assessments (figure 10). CISOs have more confidence in the cybersecurity practices of contractors than other third parties such as local governments and higher education (figure 11).

FIGURE 10

CISOs rely on outsourcing for security operations center functions

What cybersecurity functions does your state outsource (partially/completely)? (Please select all that apply.)

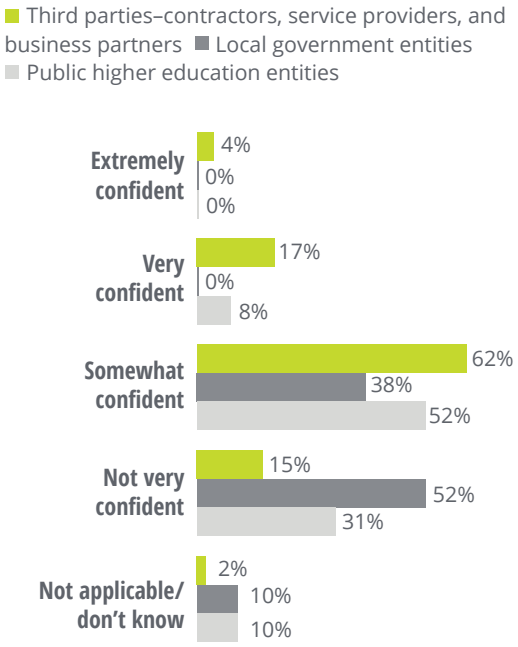


Sources: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 11

CISOs have more confidence in the cybersecurity practices of contractors than other third parties

How confident are you in the cybersecurity practices of your third parties?



Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

Key takeaway 2

Embracing the entire state

Tighter collaboration with local governments and state higher education institutions provides greater security across the state

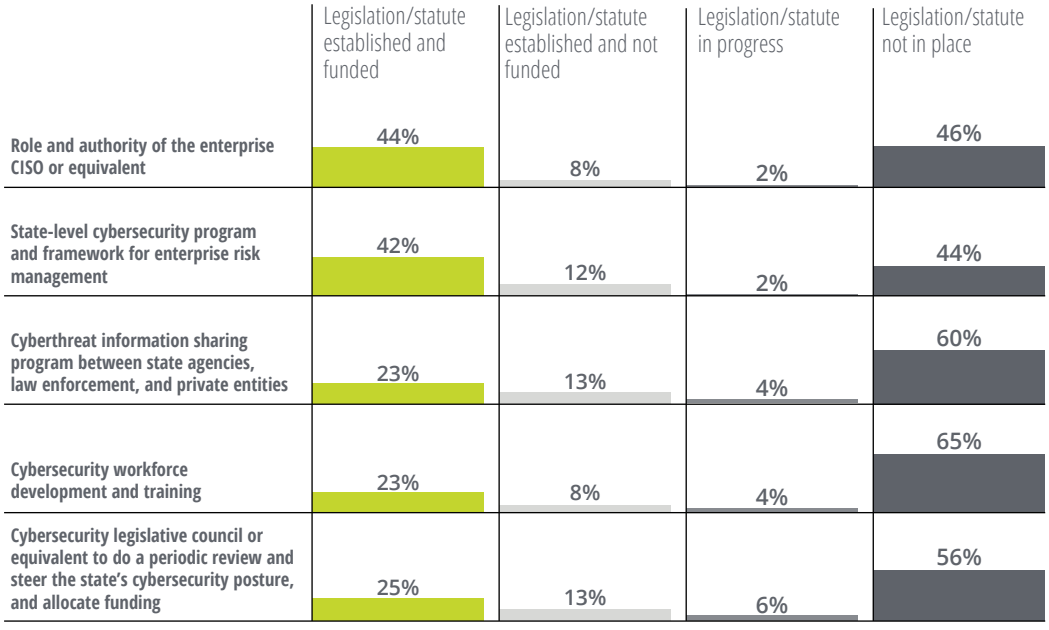
CISOs have made significant progress not only within the executive branch but also with state legislatures, and they are beginning to get the institutional support they need. Notably, state legislators are codifying into law various roles of the CISO and providing funding for initiatives such as enterprise risk management frameworks, cybersecurity legislative councils, and cybersecurity training (figure 12). Many states now also require CISOs to provide periodic reports to senior state levels, such as the governor, legislature, and secretaries of state (figure 13).

Yet, CISOs' relationships with other important entities—such as local, city, and county governments; public higher education institutions; health care systems; and the private sector—are lagging. To build more resilient cyber safeguards, CISOs need to collaborate and share information on cyberthreats with all levels and branches of government and the private sector within state

FIGURE 12

State legislators are codifying and funding CISO roles

What is the current status of your state's cyber legislation/statutes for each of the following cybersecurity provisions?



Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

borders. A whole-of-state approach—encompassing this full array of stakeholders—is key to fortifying protections wherever vulnerabilities may occur.

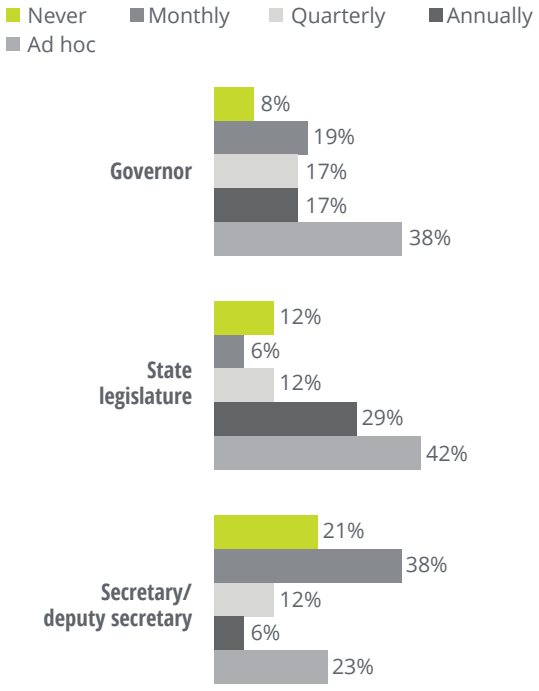
A centralized model of state cybersecurity governance, where the CISO's office leads the cybersecurity efforts of state agencies and collaborates with local governments and public higher education, helps strengthen state cybersecurity overall. A more centralized state budgeting process also enables CISOs to know where and how funds are allocated and helps reduce duplicative expenditures. Even at the state level, however, it is interesting to note that nearly one-third (29%) of respondents leave cyber incidents to agencies themselves to manage, rather than to a central IT security group.

Overall, CISOs' relationships with local governments and public higher education institutions trails that with state-level agencies. Currently, most CISOs actively engage with technology decision-makers and state business decision-makers in formulating state cybersecurity strategies, but few engage local governments and state public education institutions (figure 14). Few local government and public higher education institutions have adopted core CISO enterprise cybersecurity services, including security awareness, incident response, risk and vulnerability

FIGURE 13

Many states now also require CISOs to provide periodic reports to executive leadership

On what schedule are you required to provide reports on cybersecurity status or posture of the enterprise cybersecurity office to the following authorities and stakeholders?

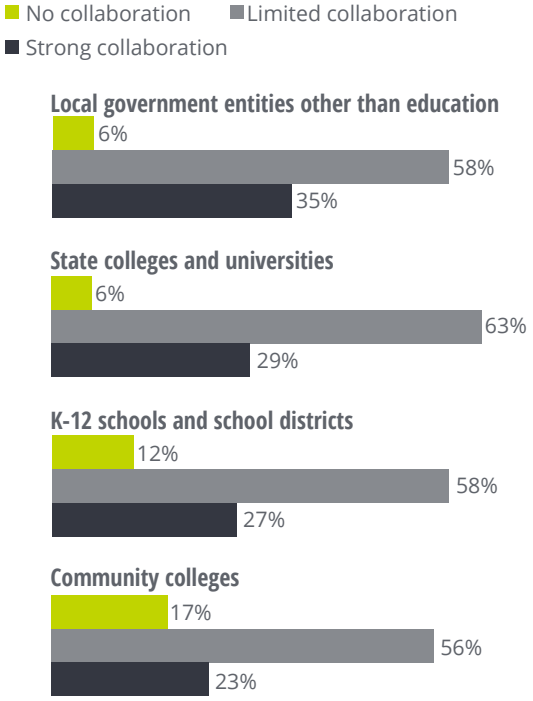


Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 14

Not many CISOs engage with local governments and state public education institutions for cybersecurity strategies

Have you collaborated with any of the following entities as part of your state's security program during the past year?



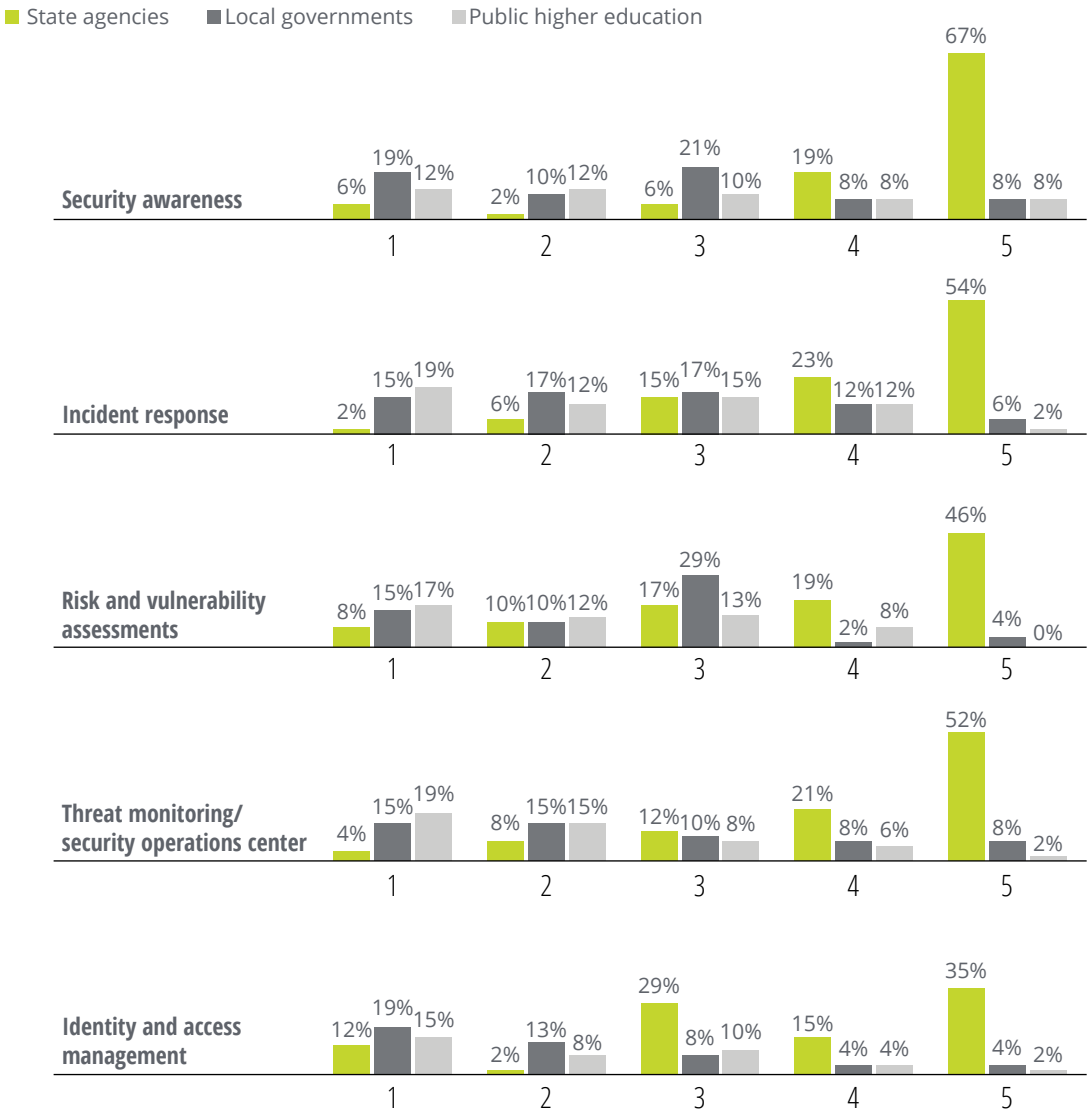
Source: *2022 Deloitte-NASCIO Cybersecurity Study*.

assessments, threat monitoring and security operations centers, and identity and access management to the same extent as state agencies (figure 15). While the level of adoption by local governments and public higher education may also depend on the availability of services offered by the state to them, the contrast in the level adoption indicates the need for attention. As an example, less than half of CISOs provide cybersecurity training to local government and public higher education staff, while the extent of adoption of such training to state agencies and contractors is more mature (figure 16).

FIGURE 15

State agencies are increasingly adopting enterprise security services; however, local governments and public higher education are in early stages of adoption

What is the degree of adoption of your enterprise security services among your agencies? (1 = Least adopted, 5 = Most adopted)



Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 16

CISOs are training state staff and contractors much more than their local and higher education counterparts

Does your state provide cybersecurity training (at least annually) to:

Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

CISOs report having more confidence in the cybersecurity practices of third-party vendors than those of local government and public higher education (figure 11). Indeed, CISOs often have little visibility into these entities. Many report that they don't know how local governments and public higher education institutions are managing their third-party contractors, for instance.

As new federal grants for cybersecurity become available, CISOs have an opportunity to build closer collaboration with local government entities. The Infrastructure and Investment Jobs Act (IIJA) of 2021 provides the first federal grant program earmarked specifically for cybersecurity. The IIJA's State & Local Cybersecurity Grant Program, administered by the Department of Homeland Security, provides federal funds to strengthen the cyber resilience of state and local grant recipients. State & Local Cybersecurity Grant requires that state recipients allocate 80 percent of grant funds to local government entities.

Our survey shows 46 states and territories plan to apply for grants from this program. The grants can enable the delivery of shared services to local governments. With the funds, states anticipate requiring local governments to implement measures including cybersecurity training, risk assessments, security monitoring, incident response, endpoint detection, and vulnerability management (figure 17). In addition, the American Rescue Plan Act of 2021 provides stimulus funding for a variety of activities including cybersecurity. Respondents indicated they had leveraged ARPA for a variety of cybersecurity needs, the most common being defense technology including endpoint protection, identity and access management, and security operations center (figure 18).

The availability of these funds is not enough to guarantee progress at the local government level, however. Indeed, CISOs see challenges ahead in implementing these federal grant programs. More than 60% of respondents report that the biggest barrier to successfully meeting the requirements of federal grant programs is resistance by local government to state oversight (figure 19). States should consider using local institutions of higher education to serve as regional hubs that connect local governments to the whole-of-state approach to cybersecurity, perhaps through a shared SOC model.

Call to action

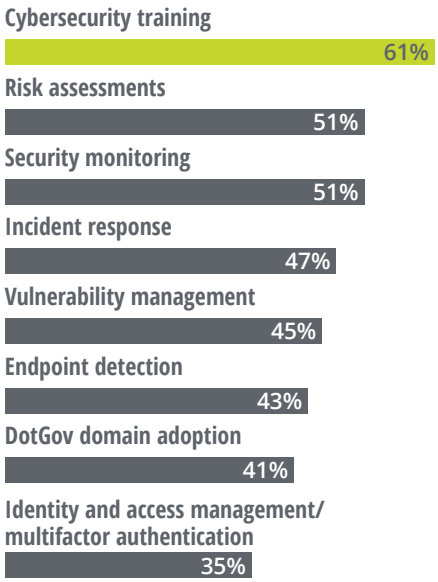
Closer working relationships between state CISOs and local governments and public education entities could go a long way in reducing the state's cyber risk exposure. CISOs have an opportunity to improve state cybersecurity with these measures.

- **Advocate for a whole-of-state approach.** For CISOs to be more effective in taking a whole-of-state approach, they first need mechanisms to promote collaboration within the executive branch. They should explore executive or legislative establishment of appropriate tools to foster whole-of-state coordination authority. States also have an opportunity to bolster their security by ensuring that state laws recognize and fund cybersecurity for local, city, and county governments and higher education institutions. State CISOs can highlight the importance of such legislation before state legislators. Only 10% of respondents report having such legislation, and more than half report no such legislation. In addition, many states are exploring creative governance by establishing a joint cyber task force or shared services initiatives to establish a whole-of-state approach. CISOs can use these councils and task forces to build closer collaboration with local governments and public higher education entities (figure 20).

FIGURE 17

States anticipate requiring local governments to implement measures including cybersecurity training, risk assessments, and security monitoring

In order for local governments to receive funds under the State and Local Cybersecurity Grant Program, what cyber components will your state require local governments to implement?

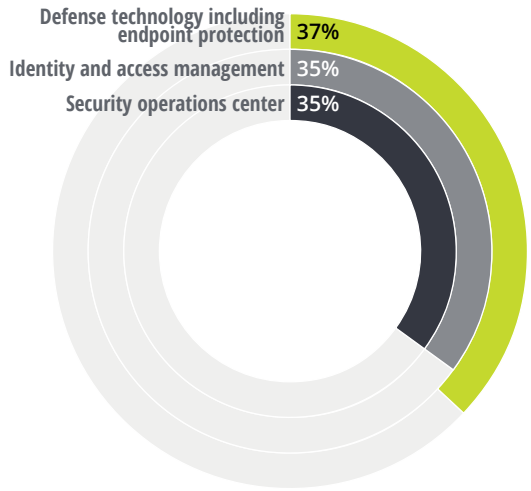


Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 18

Top three areas where ARPA was used for cybersecurity

Please select the areas where you have consumed or plan to consume funding from the American Rescue Plan Act (ARPA) of 2021. (Please select all that apply.)



Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

- **Use federal grants to promote collaboration with local governments.** CISOs can use the opportunity provided by the State & Local Cybersecurity Grant Program to build closer collaboration with local governments on cyber protections, including cybersecurity training at local government levels. The experience could pave the way for future collaboration.

FIGURE 19

Most respondents cite resistance from local government to state oversight as the biggest barrier to meeting the requirements of federal grant programs

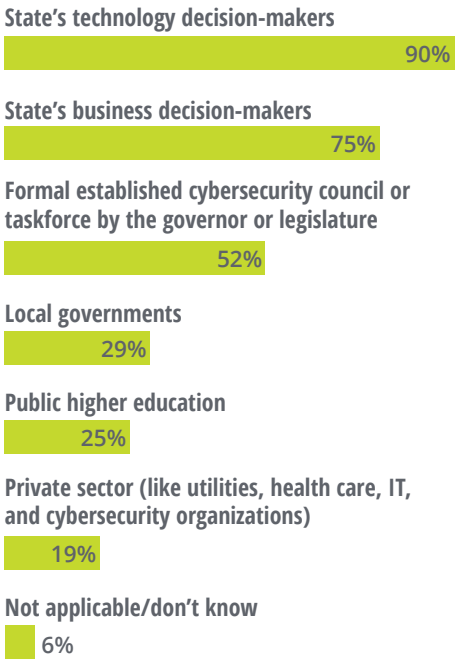
What have been, or do you anticipate will be, the most significant barriers to successfully meeting the requirements of the State and Local Cybersecurity Grant Program and reducing cyber risk to your state and local governments? (Please select all that apply.)

Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 20

CISOs indicated limited collaboration was occurring with local governments and public higher education entities

Does your state actively engage with the following stakeholders in identifying requirements for the state's cybersecurity strategy? (Please select all that apply.)



Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

Key takeaway 3

Setting a new course

Emerging from the pandemic, CISOs can position themselves for the future

Nearly three years since the pandemic began, the world in which CISOs operate has changed. In the realm of technology, many applications have migrated to the cloud. And with remote work, digital and mobile platforms have become part of the fabric of daily life by which people work, communicate, and transact. Remote or hybrid work may become a permanent fixture, posing new management challenges. Citizens, now used to the convenience of remote access, are likely to demand more and improved digital experiences from government—for everything from renewing licenses to paying taxes to receiving state benefits—all the while expecting security and privacy safeguards of their information.

The role of the state CISO only grows in importance in this environment. Bad actors exploited the dispersed work-from-home arrangements during the pandemic, increasingly indulging in activities such as ransomware attacks and financial fraud. Geopolitical developments also added to the complications with foreign state-sponsored espionage and threats to election security. All the while, new technologies from cloud computing to artificial intelligence offer both new capabilities and vulnerabilities to consider.

To forge ahead, CISOs need to secure the basics—a sound budgetary foundation—while they consider new technological capabilities to modernize operations and constituent services.

Firm financial footing sets a lasting foundation

For the first time since this survey began in 2010, CISOs are reporting that budgetary concerns are no longer a top barrier to cybersecurity initiatives. The lack of a sufficient cybersecurity budget didn't even rank in the top five concerns landing behind legacy infrastructure, talent shortage, and other issues (figure 1).

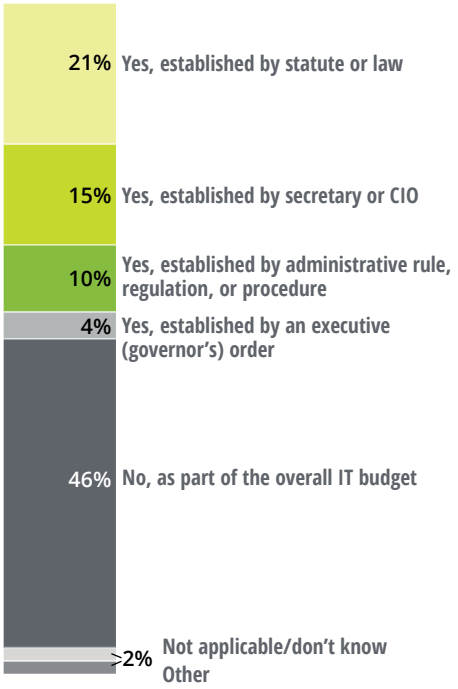
Over the last year, state receipts were greater than expected due to pandemic relief funds and other factors. In fiscal year 2022, state budget spending grew at 13.6%, the highest increase in more than 40 years, and in fiscal year 2023, state budget spending is expected to grow by 4.2% over prior year levels.[2] Meanwhile, state and local governments are poised to receive new cybersecurity grants over the next four years under the State & Local Cybersecurity Grant Program. It is unclear how long this positive budgetary scenario will last. But at this unique moment, CISOs have a chance to make greater progress on their priorities.

To assume a leadership role appropriate to oncoming challenges in the postpandemic era, states must establish a sound financial foundation for the long run for cybersecurity. As digitization increasingly becomes widespread, state cybersecurity funding cannot be left to chance year after year. CISOs need to be able to draw upon a constant, dependable source of funding throughout different economic and political cycles. Most states do have a dedicated budget line item for cybersecurity, whether established by law, executive order, or other mechanisms (figure 21).

FIGURE 21

Most states have a dedicated budget line item for cybersecurity

Does your state have a cybersecurity budget line item?



Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

In those states that have not, CISOs and CIOs must continue to push for it.

Establishing cybersecurity as a governmental priority with a budget line item can help state CISOs and CIOs raise funding levels before state legislature and executive branch leaders. Certainly, CISOs concur that regulations backed by a commitment for funding are more effective than those without one (figure 22).

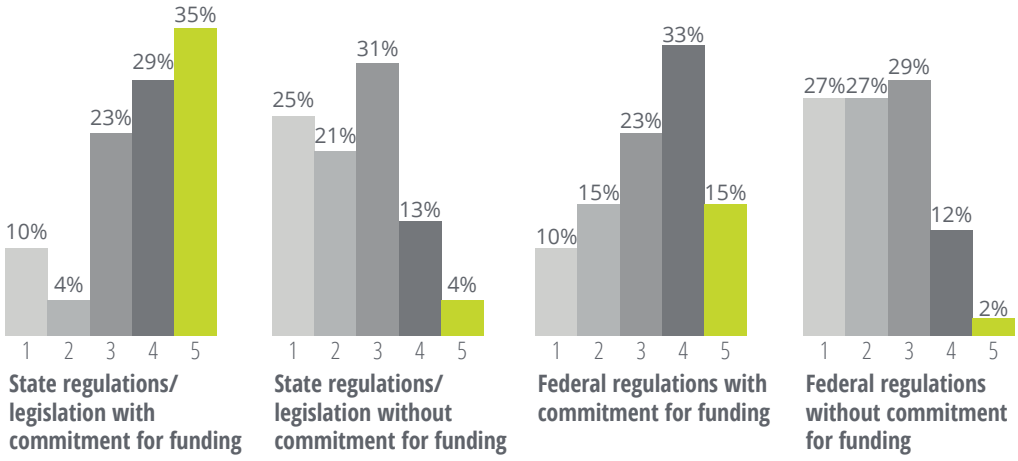
States are beginning to make some progress on cybersecurity budgets. For the first time, a handful are allocating more than 10% of their budget to cybersecurity, in alignment with federal government levels,[3] but most still allocated between 2–10% (figure 23).

CISOs need to continue to establish more secure and adequate funding, as only with such funding can they formulate longer-term strategies to incorporate pressing priorities, such as emerging technologies.

FIGURE 22

CISOs concur that regulations backed by a commitment for funding are more effective than those without one

How effective are applicable federal and state cybersecurity regulations at improving your state's cybersecurity posture and reducing risk? (1 = Least effective, 5 = Most effective)

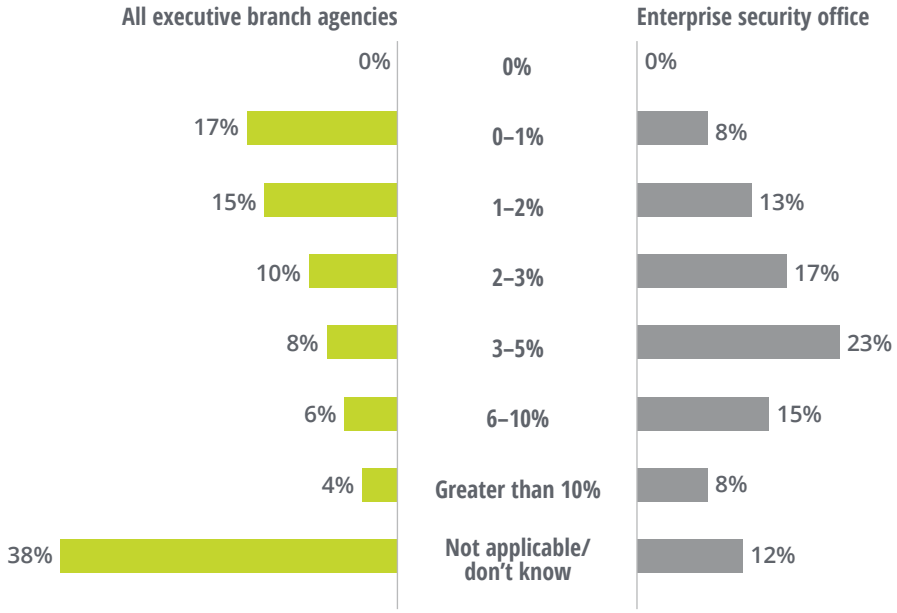


Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 23

A handful of states are allocating more than 10% of their IT budget to cybersecurity

What percentage of your state's IT budget is allocated to cybersecurity?



Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

Emerging technologies present new opportunities

In the postpandemic digital landscape, CISOs have a critical role to play in actively guiding the evaluation and implementation of useful new technologies. Citizens accustomed to positive digital experiences in other realms have come to expect that from state government. Many states have taken a big step forward in this regard by providing digital identities for citizen services. Capabilities, such as cloud computing, artificial intelligence, and Robotic Process Automation (RPA), allow states an opportunity to further enhance digital modernization in service of their missions and constituents.

Active participation in the state innovation agenda also provides CISOs benefits such as greater visibility with other state leaders. To serve as a partner in innovation, the key is to be a leader to advocate for and enable new technologies in a secure fashion. By establishing involvement from the onset in the evaluation of emerging technologies, CISOs can best help ensure that cybersecurity is baked into new applications before procurement and during implementation.

In the last few years, CIOs have worked with many innovations, such as RPA, chatbots, and other AI tools to streamline and improve citizens' digital experience. Meanwhile, they have also had to contend with many issues involving legacy infrastructure, cited as first among CISOs' top barriers (figure 1). Overall, cyber strategy ranked as the top priority for CISOs while emerging technologies such as artificial intelligence ranked low (figure 24).

FIGURE 24

Majority of states focused on cyber strategy, multifactor authentication, and risk assessments as upcoming initiatives

Identify your state's top five cybersecurity initiatives for 2022–23.

Source: *2022 Deloitte-NASCIO Cybersecurity Study.*

Call to action

To meet the challenges of a postpandemic world, CISOs have an opportunity to lay solid groundwork to fund states' growing cybersecurity needs, while investing in technologies for the future.

- **Lay a sound financial foundation.** To ensure ongoing funding support through various economic and political cycles, CISOs and CIOs should continue to push for cybersecurity as a distinct line budget item in states where this has not occurred. In their regular reports to state leadership, they should continue to underscore the importance of cybersecurity as a priority and the need for consistent and adequate funding. State CISOs with a multiyear strategic plan secure funds more successfully than those that don't. Annual updates on progress over the last year and overviews of plans for the next year make a big difference in positioning cybersecurity as a business enabler.

- **Build the cornerstones of the future—cloud and emerging technology.** With solid funding, CISOs can embrace underpinnings of the future, including the continued adoption of cloud and other new technologies to enable the smarter government services. A key challenge is to maintain the security of existing capabilities even as more functions migrate to the cloud. In one example, many states have made good progress providing strong authentication while eliminating passwords, boosting both security and convenience.

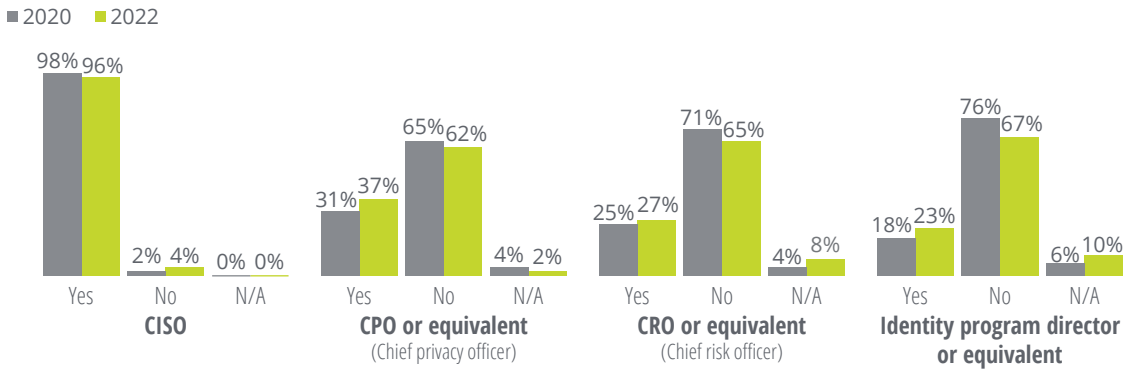
Survey analysis deep dives

Strategy and governance

FIGURE 25

All states now have a CISO, although not all territories do, and many are establishing positions for CPOs, CROs, and identity program directors

Does your state have the following enterprise-level positions?

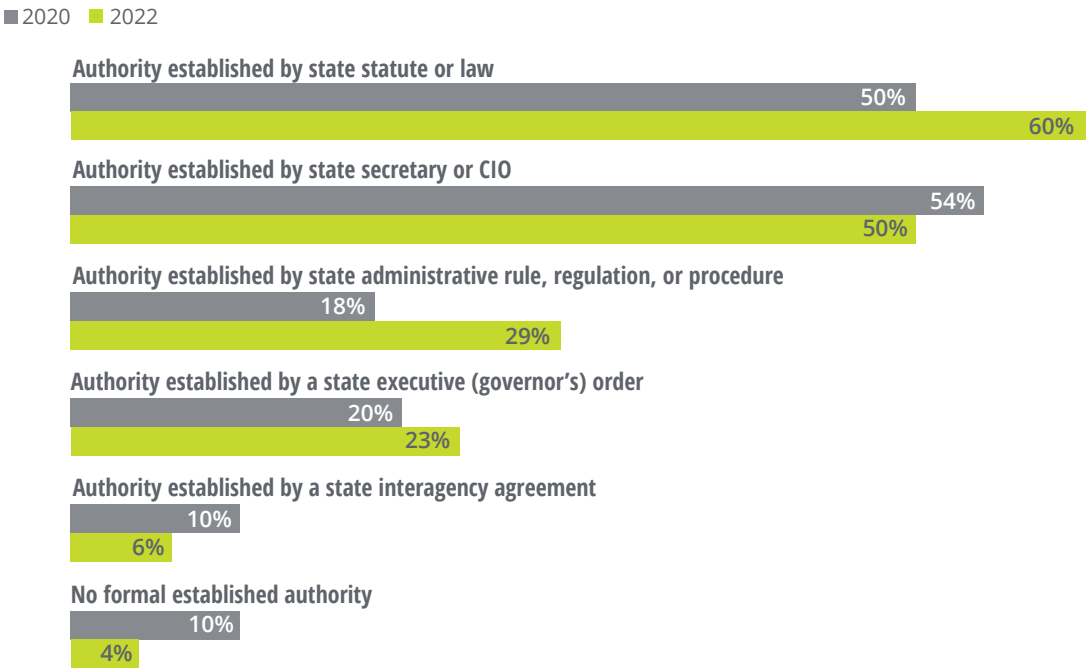


Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 26

More CISO positions are now established by state law

What mechanism establishes your state's CISO or equivalent position's authority over the other organizational entities for which it has responsibility?

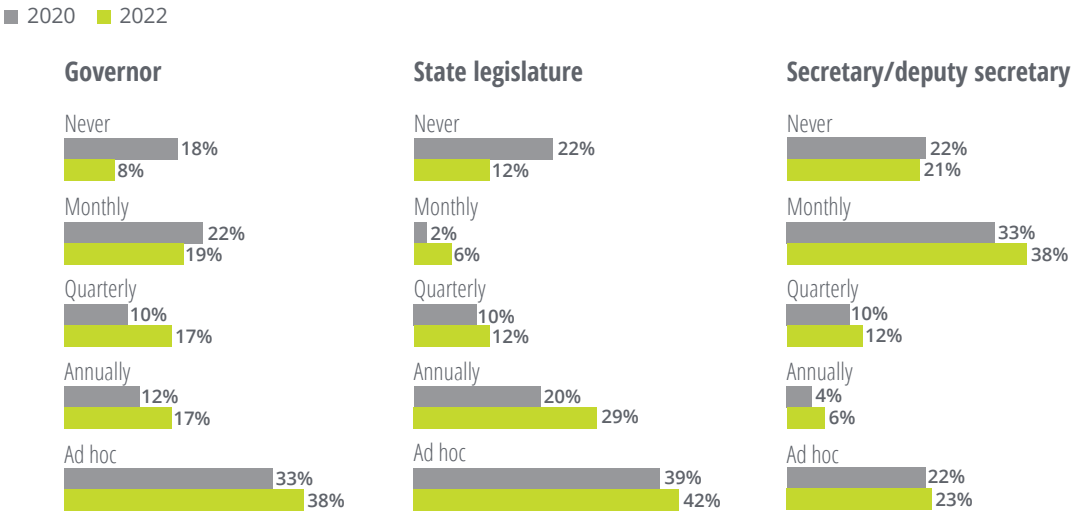


Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 27

CISOs are required to provide more regular reports on the state's cybersecurity status to state leaders, including the governor, legislature, and agency secretary

On what schedule are you required to provide reports on cybersecurity status or posture of the enterprise cybersecurity office to the following authorities and stakeholders?

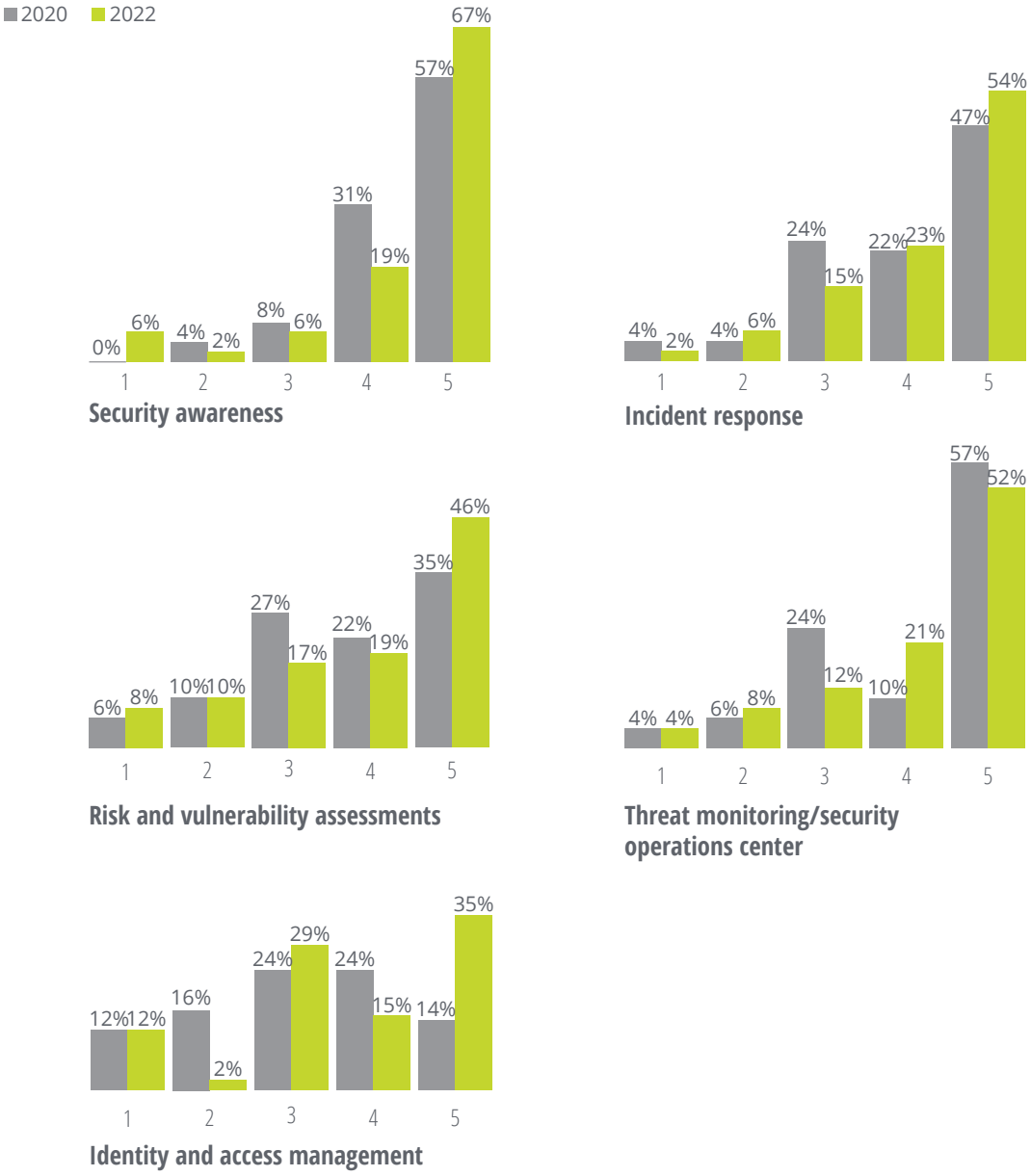


Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study*.

FIGURE 28

State agency adoption of CISO services, such as identity and access management, security awareness, incident response, and risk and vulnerability assessments is generally increasing

What is the degree of adoption of your enterprise security services among state agencies (1 = Least adopted, 5 = Most adopted)?



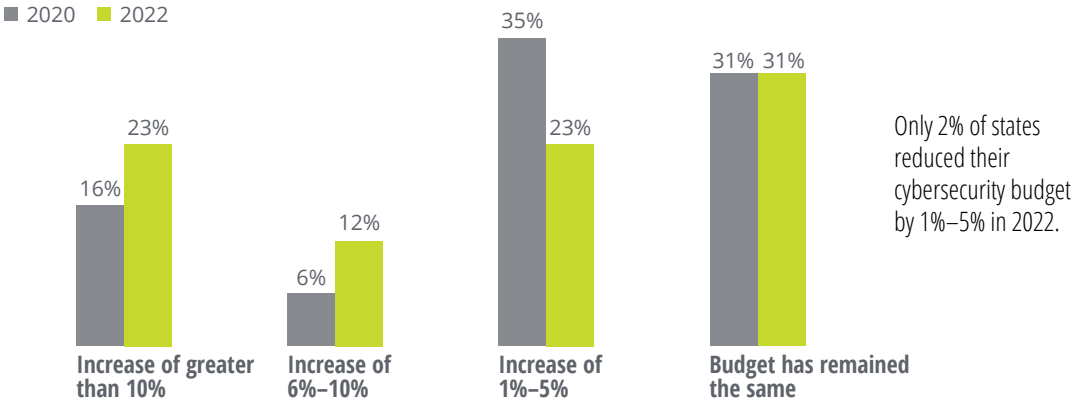
Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study*.

Budget

FIGURE 29

Thirty states reported increases to their cybersecurity budget over the past year

Please select the option which best describes the year-over-year trending in your state's cybersecurity budget for years 2020 and 2021.

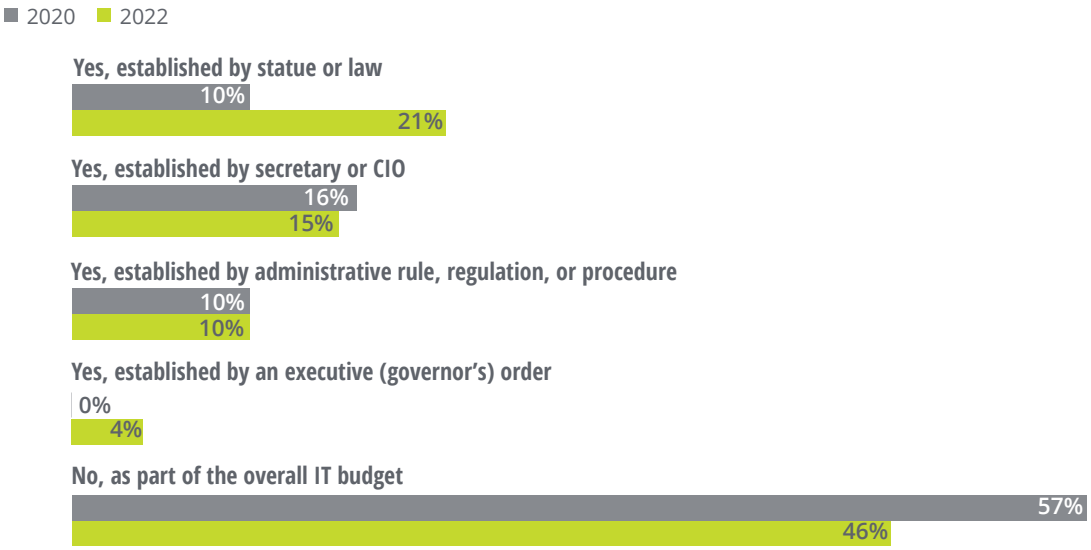


Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study*.

FIGURE 30

States reported making progress in establishing a cybersecurity budget line item by law or executive order

Does your state have a cybersecurity budget line item?



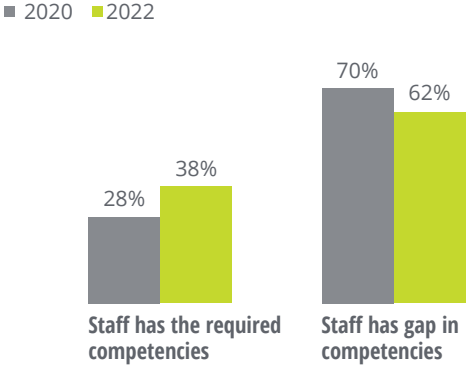
Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

Cyber workforce

FIGURE 31

Most CISOs report that staff has a gap in competencies

Do your internal cybersecurity professionals have the required competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements?



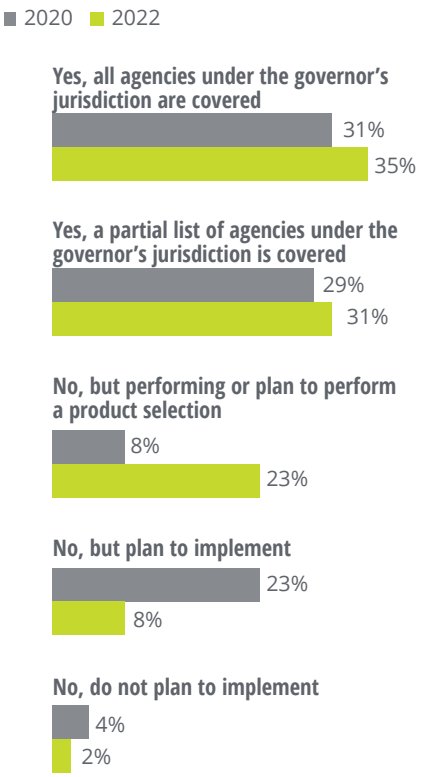
Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

Identity and access management

FIGURE 32

Most states are offering enterprisewide identity and access management (IAM)

Does your state provide an enterprisewide IAM solution?

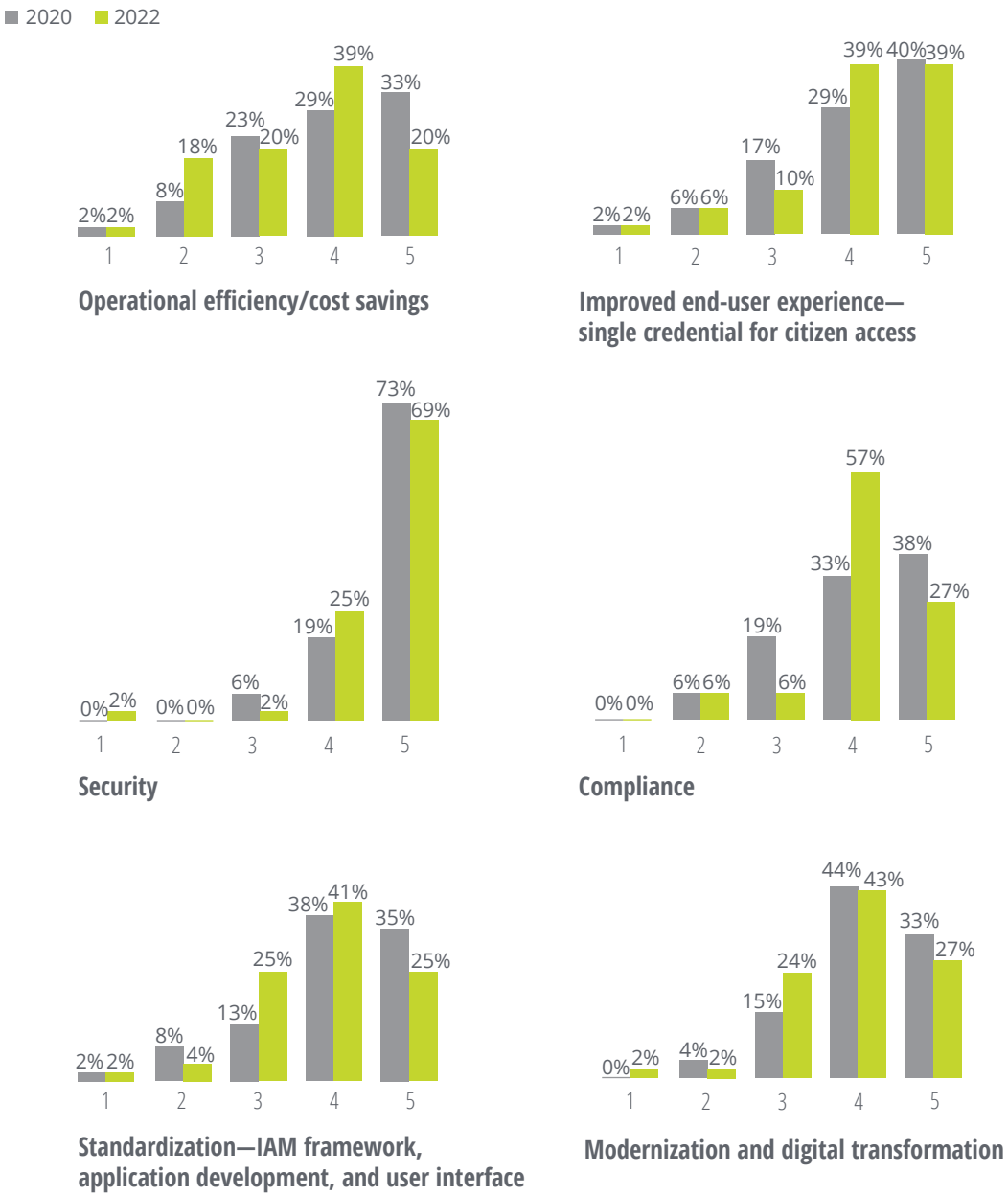


Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study*.

FIGURE 33

Security, end-user experience, and compliance are the top drivers for enterprise IAM program

On a scale of 1 to 5, how important are the following reasons to your IAM investment decisions? (1 = Least important, 5 = Most important)



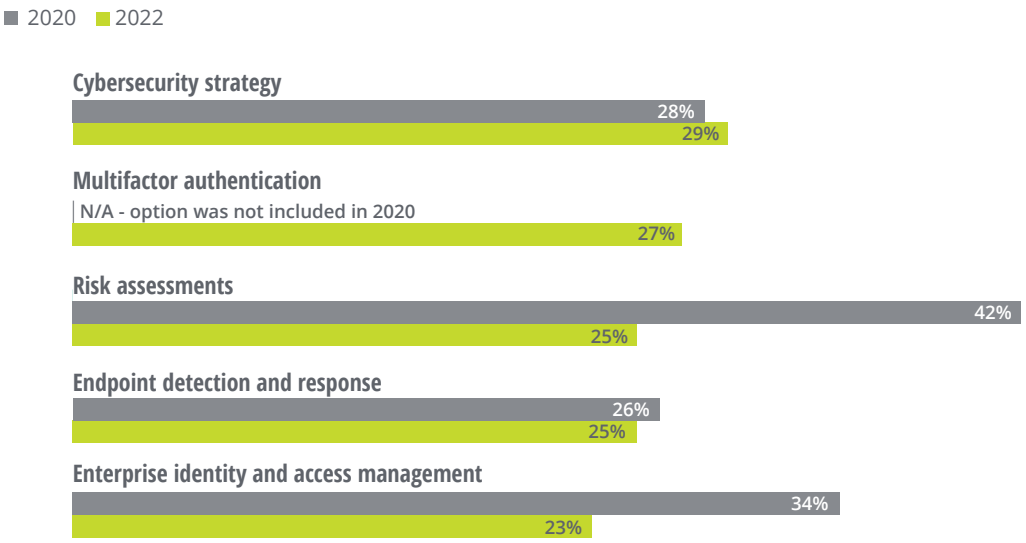
Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study*.

Cyber operations

FIGURE 34

CISOs' top cybersecurity initiatives for 2022–23 show decline in both risk assessments and enterprise identity and access management

Identify your state's top five cybersecurity initiatives for 2022–23.

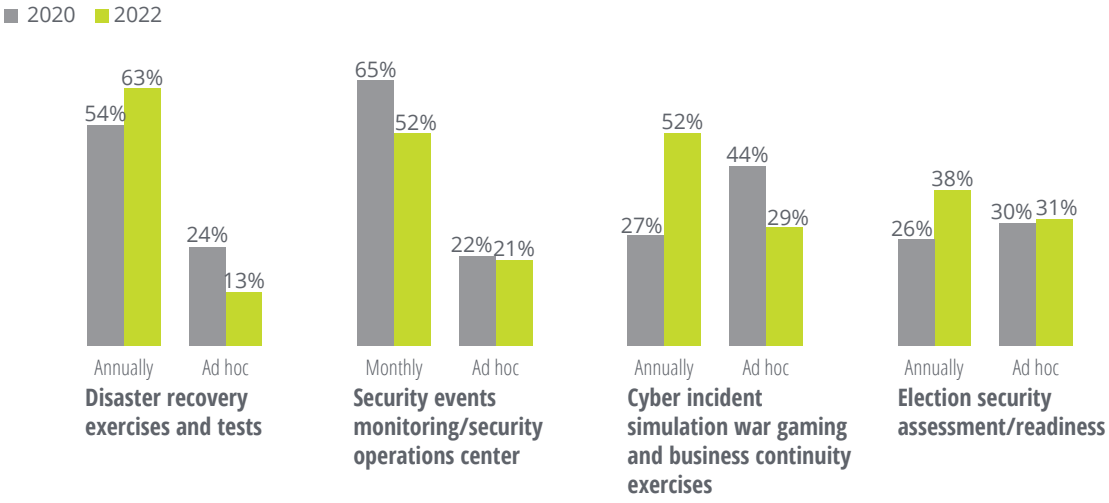


Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 35

Most states are performing periodic assessments of their cyber incident war gaming, business continuity, and election security exercises

How often does your state perform the following cybersecurity assessments?

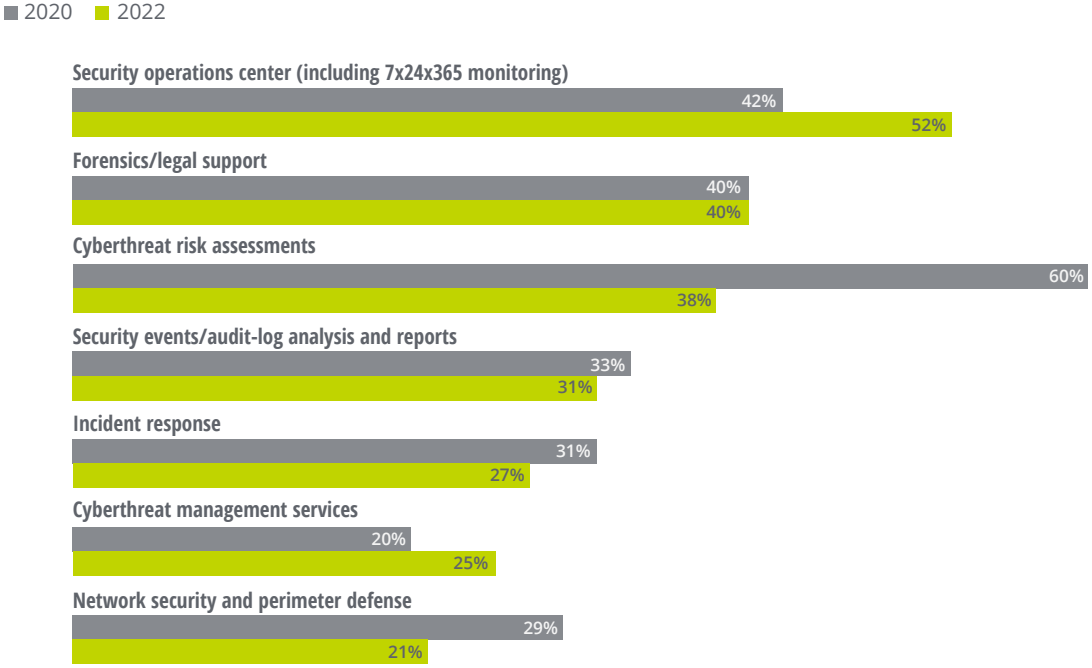


Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study*.

FIGURE 36

Many states are outsourcing cybersecurity functions, including security operations center and forensic/legal support

What cybersecurity functions does your state outsource (partially/completely)? (Please select all that apply.)



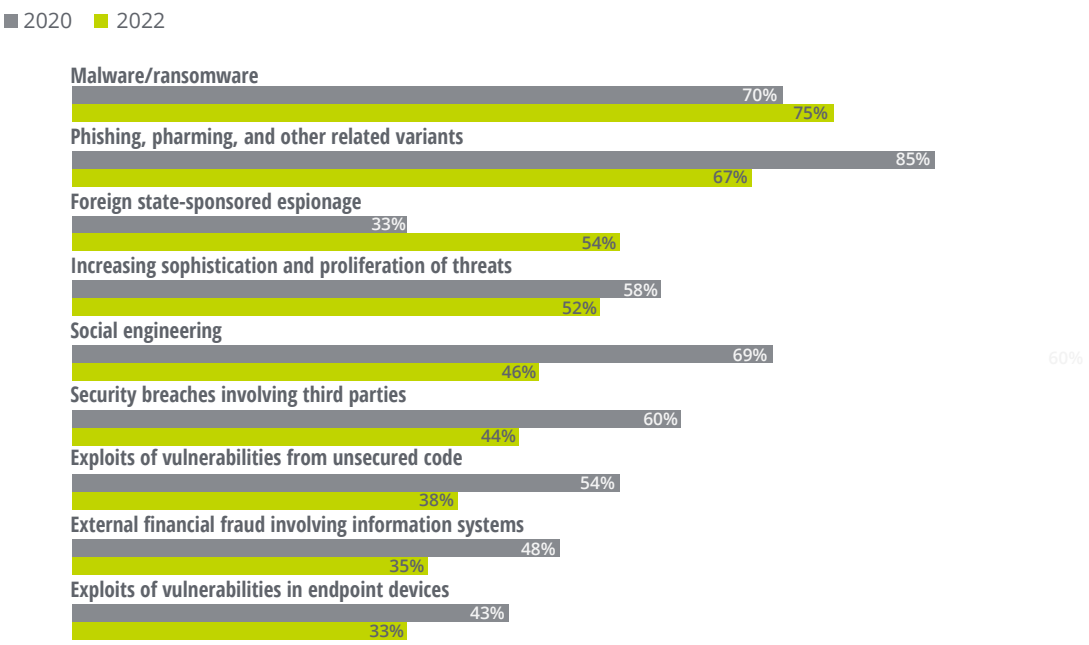
Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

Cyberthreats

FIGURE 37

Malware/ransomware and phishing continue to be top threats, with foreign state-sponsored espionage rising significantly

How much of a threat do each of the following cyberthreats in the coming fiscal year pose to your state? Very high and somewhat higher threat (combined).

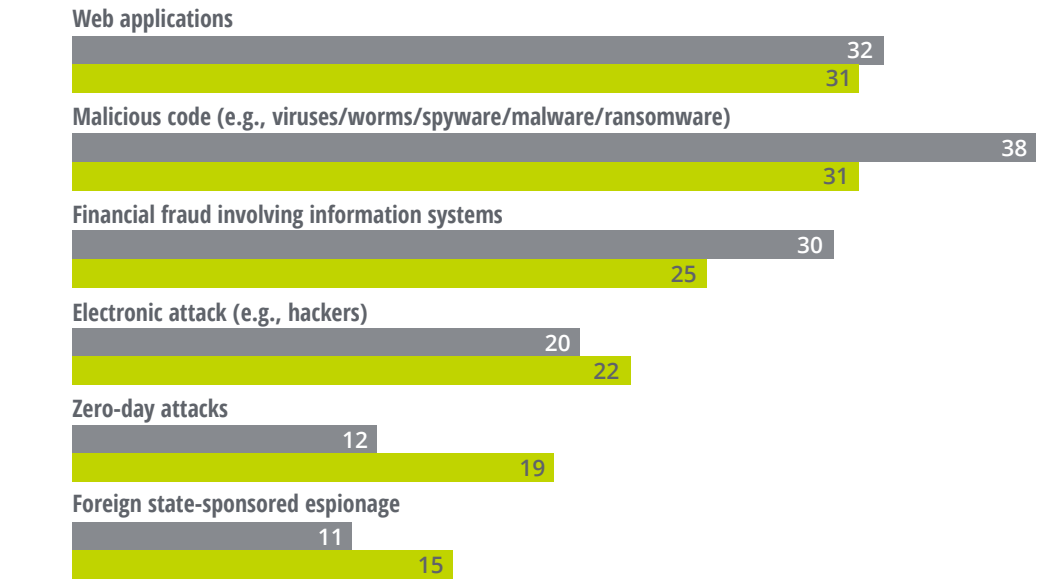


Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

FIGURE 38

CISOs reported a variety of causes behind data breaches and cybersecurity incidents

Which of the following are the leading causes for data breach/incidents in your state over the past 12 months?



Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

Appendix

Survey methodology

THE 2022 *Deloitte-NASCIO Cybersecurity Study* uses survey responses from:

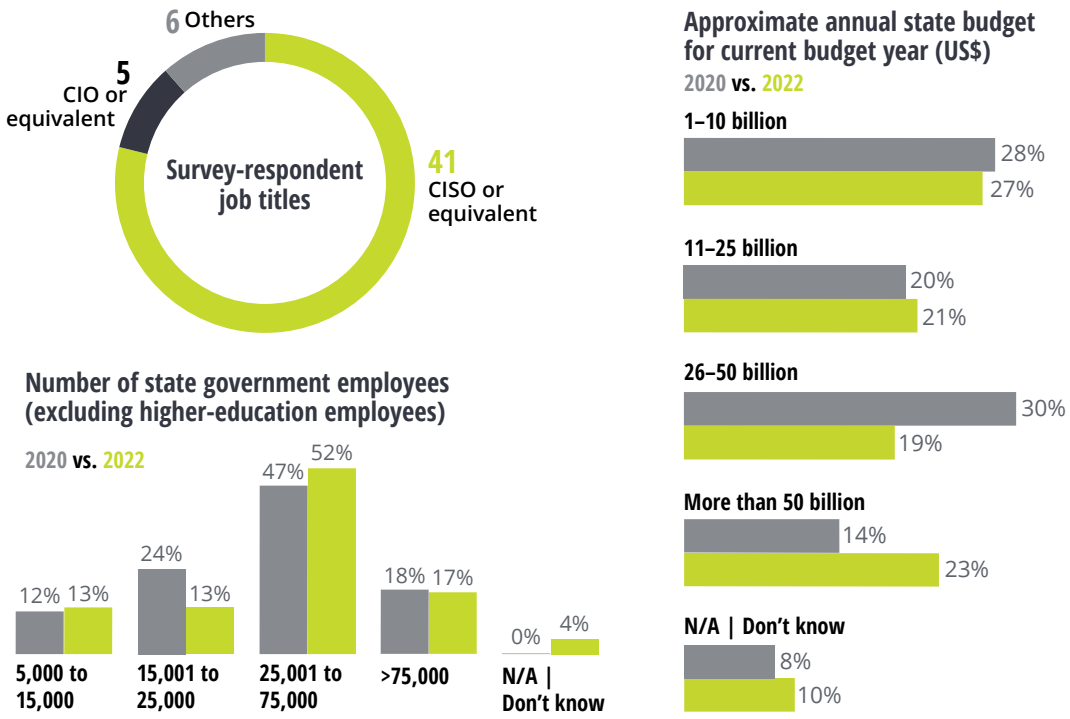
- US state enterprise-level CISOs, who answered 66 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Participation was high: 53 states and territories responded. Figures 39 illustrates the CISO participants' demographic profile and that of their states.

For better readability, we have included relevant and select responses in the charts. Hence, the percentage totals may not equal to 100%.

- The survey gave respondents the opportunity to add additional comments when they wanted to further explain an "N/A" or "other" response. A number of participants provided such comments, offering further insight into the analysis.

FIGURE 39

Survey methodology



Sources: *2022 Deloitte-NASCIO Cybersecurity Study* and *2020 Deloitte-NASCIO Cybersecurity Study.*

Endnotes

1. Amrita Datar et al., *Government can win the talent race—Here's how*, Deloitte Insights, May 23, 2022.
2. National Association of State Budget Officers, "The fiscal survey of states," accessed September 6, 2022.
3. White House, *Internet technology and cybersecurity funding*, accessed September 6, 2022.

Acknowledgments

The authors would like to thank the NASCIO and Deloitte professionals who helped to develop the survey and execute, analyze, and create the report.

On the behalf of NASCIO, they would like to thank executive director **Doug Robinson**, program director of innovation and emerging issues, **Amy Glasscock**, CIPM, and all CISOs who participated in the 2022 survey.

From Deloitte, the authors would like to thank subject-matter specialists **Mike Wyatt** and **Clayton Frick** of Deloitte & Touche LLP; and **John O'Leary** of Deloitte Services LP. In addition, they would also like to thank the Deloitte survey team for data analysis, and benchmarks, including: **Bharane Balasubramanian, Bharath Chari**, and **Julia Slattery** of Deloitte & Touche LLP; and **Sushumna Agarwal, Thirumalai Kannan**, and **Apurba Ghoshal** of Deloitte Services LP.

Lastly, the authors would also like to thank the marketing and writing team including **Allison Malewig** from Deloitte Services LP and writer **Catherine Yang**.

About Deloitte Cyber

Deloitte Cyber helps organizations manage cyber risk and create value through enhanced security, visibility, and privacy. Our program design, implementation, operation, and response services, coupled with our deep industry and mission knowledge, help our clients protect and defend their most valuable assets, facilitate secure digital transformation efforts, and adapt rapidly to emerging threats.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystallizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

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 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 and publications, briefings, and government affairs, NASCIO is the premier network and resource for state CIOs. For more information, visit www.nascio.org.

Contact us

Meredith Ward
Director of Policy and Research | NASCIO
+ 1 859 514 9209 | mward@nascio.org

Srini Subramanian
Principal | Global Industry leader | Risk Advisory | Government and Public Services
Deloitte & Touche LLP
+ 1 717 651 6277 | ssubramanian@deloitte.com

Mike Wyatt
Principal | Cyber Identity | Risk Advisory | Government and Public Services
Deloitte & Touche LLP
+1 512 226 4171 | miwyatt@deloitte.com

Julia Slattery
Specialist leader | Cyber & Strategic Risk | Risk Advisory | Government and Public Services
Deloitte & Touche LLP
+1 804 343 8549 | jslattery@deloitte.com

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

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Abrar Khan, Emma Downey, Arpan Kumar Saha, and Aishwarya Iyer

Creative: Sofia Sergi, Swagata Samanta, and Molly Woodworth

Audience development: Maria Martin Cirujano, Kelly Cherry, and Nikita Garia

Cover artwork: Sofia Sergi