# 2020 Deloitte–NASCIO Cybersecurity Study

States at risk: The cybersecurity imperative in uncertain times

A JOINT BIENNIAL REPORT (6TH EDITION) FROM DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

# Message from NASCIO's president

2020 has been a year such as few of us have ever seen in our lifetimes and, hopefully, never will see again. The impacts that COVID-19 has had on our world cannot be overstated, and state governments have certainly felt its effects. While state chief information officers (CIOs) and chief information security officers (CISOs) have always made cybersecurity a high priority, this year they faced new challenges. CIOs and CISOs dealt with both internal and external issues as they worked to expand and secure employee remote work and citizen services.

COVID-19 also presented new opportunities for criminals to try and exploit both the public and private sectors, and, as the news media has widely reported, individual citizens have also been increasingly targeted. You will notice in the report that CISOs identified financial fraud as three times as great of a data breach/incident threat as they did in 2018. To put it mildly, CIOs and CISOs had to stay more vigilant this year than ever.

In addition to the data on which we have reported since the first Deloitte–NASCIO Cybersecurity Study in 2010 on budget, workforce, and other issues, this year our themes are focusing on COVID-19, cybersecurity governance, and state and local collaboration. We also added some new questions and topics, and state CISOs offered insightful open-ended feedback.

Finally, this is the 10th year of this study and the sixth iteration, and we had 51 state and territory CISOs participate this year—a new record. I cannot express my gratitude enough to these women and men who work every day to keep our states secure and are true public servants.

**Denis Goulet**
*NASCIO President, Commissioner, and CIO*

# Foreword

## The cybersecurity imperative in uncertain times

The sixth biennial Deloitte–NASCIO Cybersecurity Study reflects insights from 51 state and territory respondents on the CISO's role and budget, governance, reporting, workforce, and operations. The CISOs filled out this year's survey in May/June 2020—an unprecedented time as the world adjusted to the impact of the COVID-19 pandemic. State governments responded by moving their enterprise operations, services, and employees to a virtual environment, and the study captures COVID-19's impact on state cyber posture to the extent visible during the early response to the pandemic.

We commend the efforts of CISOs across the country who demonstrated their agility by quickly putting measures into place to guard against increased vulnerabilities while supporting state agencies' ability to conduct business. CISOs rose to the challenge, working closely with their state IT departments to balance cybersecurity risks and business continuity. They secured networks for remote work by enabling or expanding multifactor authentication, enhancing system monitoring to receive early detection and alerts, and reviewing readiness plans to address the possibility of unexpected cybersecurity incidents. They also responded to support an unexpectedly mostly virtual workforce, enabling a quick shift to online video meetings and teleconferencing with appropriate security measures. As a result, most states maintained essential business functions and service to citizens in exemplary fashion, particularly in light of tightly constrained cyber budgets.

While the pandemic has highlighted the resilience of CISOs, it has also brought to light some long-standing challenges facing state IT and cybersecurity. State governments' need for digital modernization is evident, along with the essential role that cybersecurity needs to play in the discussion. CISOs struggle with the challenges of securing adequate budgets and talent, as well as coordinating a consistent security implementation across agencies.

The CISO position has evolved into a mature and respected role, and the pandemic has further highlighted its critical nature. This survey identified several key takeaways critical to further enhancing the CISO's status:

- Recognize that cyber is at the forefront of the postpandemic workforce of the future, and CISOs will play a key role in states' digital adoption and technology modernization initiatives.

- Extend the influence of the CISO through collaboration and partnerships with local governments and public higher education entities, providing both cybersecurity services as well as guidance to these often-overwhelmed partners.

- Transition to a centralized form of governance for the cybersecurity function across the state and agencies, while maintaining proximity to business initiatives at the agency/program level.

The 2020 study also revisits the three "bold plays" of the 2018 Deloitte–NASCIO Cybersecurity Study, covering funding, innovation, and collaboration, to assess progress on these strategic shifts for state CISOs.

We appreciate the participation of the 51 states and territories that responded to our detailed survey. We applaud your ongoing commitment to safeguarding citizen data and securing the business of your state.

## AUTHORS OF THE STUDY

**Meredith Ward**
*Director, Policy & Research, NASCIO*

Meredith Ward is director of policy and research at NASCIO. She has more than 18 years of experience in state, local, federal, and international professional associations.

**Srini Subramanian**
*Principal, Deloitte & Touche LLP*

Srini Subramanian leads Deloitte's Risk & Financial Advisory practice for the State, Local, and Higher Education (SLHE) sector. He has extensive experience in information security strategy, innovation, governance, identity, access management, and shared services, and has coauthored the Deloitte-NASCIO Cybersecurity study since its inception in 2010.

# Key takeaway

# 1

# COVID-19 has challenged continuity and amplified gaps

**The pandemic widened cyber challenges: budget, talent, threats, and the need for partnerships**

COVID-19 dominated every state leader's agenda in 2020, and that's true for the CISO as well. But even before the pandemic, CISOs were dealing with a fast-changing landscape. The ongoing struggle for adequate funding, the challenges in cyber staffing, and ever-evolving cyberthreats were already a reality. The coronavirus acted as a major accelerant, increasing the urgency of initiatives that were already of critical importance.

Consider what the pandemic has meant for the workforce's ability to work remotely. Telework was already happening but on a smaller scale.

## Before the pandemic, 52% of respondents said *less than 5% of staff worked remotely*.

But once COVID-19 hit, remote work suddenly became the dominant operating principle of state government. Based on responses from this year's survey, during the pandemic 35 states have had more than half of employees working remotely; nine states have had more than 90% remote workers. In response, CISOs established safeguards for teleconferencing and collaboration solutions and enabled secure system access with multifactor authentication. Most states also provided guidance on new phishing attacks and offered video/teleconferencing policy education to end users.

**COVID-19 amplified everything.**

In a flash, there was more data to protect due to unprecedented surge in demand for government services such as unemployment compensation and other digital services, more channels over which that data was traveling, more threats to deal with, more everything— except funding. Cyberthreats also increased in identity and financial fraud.

The pandemic forced state governments to act quickly in response to public health and safety concerns, in many cases taking the lead to protect their citizens from the spread of the virus. CISOs and their staff rose to the occasion to support the increased demands for technology, enabling remote work despite being severely constrained by the lack of resources for cybersecurity. They worked closely with IT departments to secure the government enterprise, the virtual work environment, technology infrastructure, and the supply chain.

FIGURE 1

## Top safeguards reinforced or established by CISOs as part of the COVID-19 response

**01** Safeguard teleconferencing and video solutions and update policy and procedures

**02** Establish secure work connections with multifactor authentication

**03** Provide guidance on phishing and disinformation campaigns

**04** Ensure continuity of operations plans/business continuity plans are up-to-date

**05** Provide continuous guidance on COVID-19–related scams and precautions
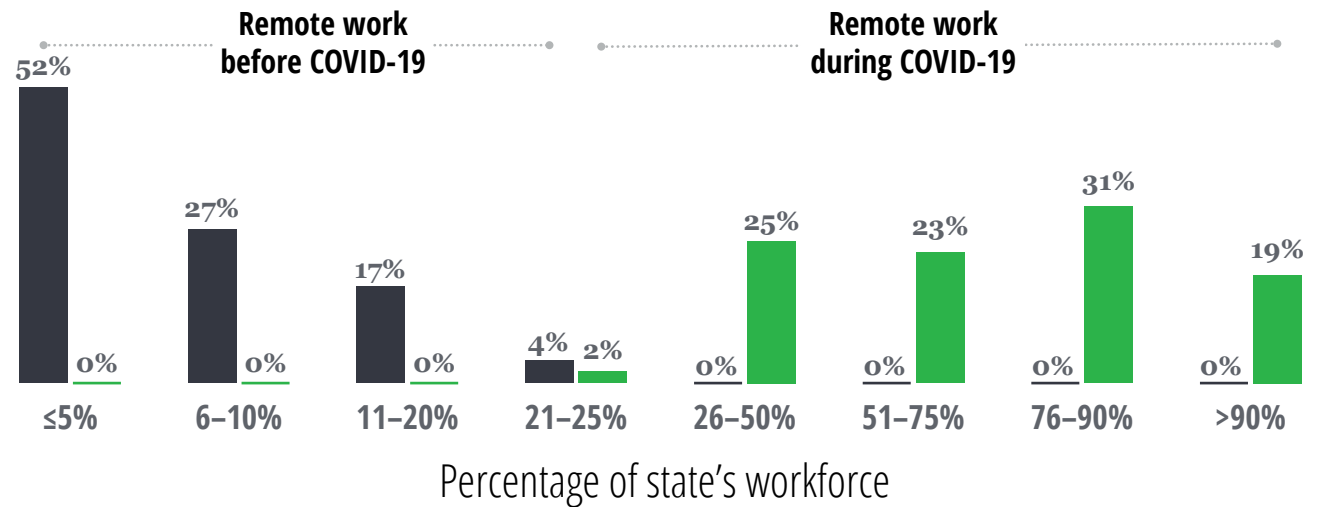
Source: 2020 Deloitte-NASCIO Cybersecurity Study.

**COVID-19 dramatically increased the remote workforce, presenting a challenge to CIOs and CISOs and requiring teamwork to implement effective solutions and safeguards.**

While states responded effectively to enable the move to a virtual working environment, the exercise exposed some kinks in the cybersecurity armor. Increasing incidents of financial fraud involving information systems have already taken place, and more are expected in the year ahead, likely due to the increase in health care spending and unemployment payments. Phishing, pharming, and other threats may also increase.

FIGURE 2

## States' remote workforce before and during COVID-19

*What percentage of your workforce worked remotely before COVID-19? And during?*
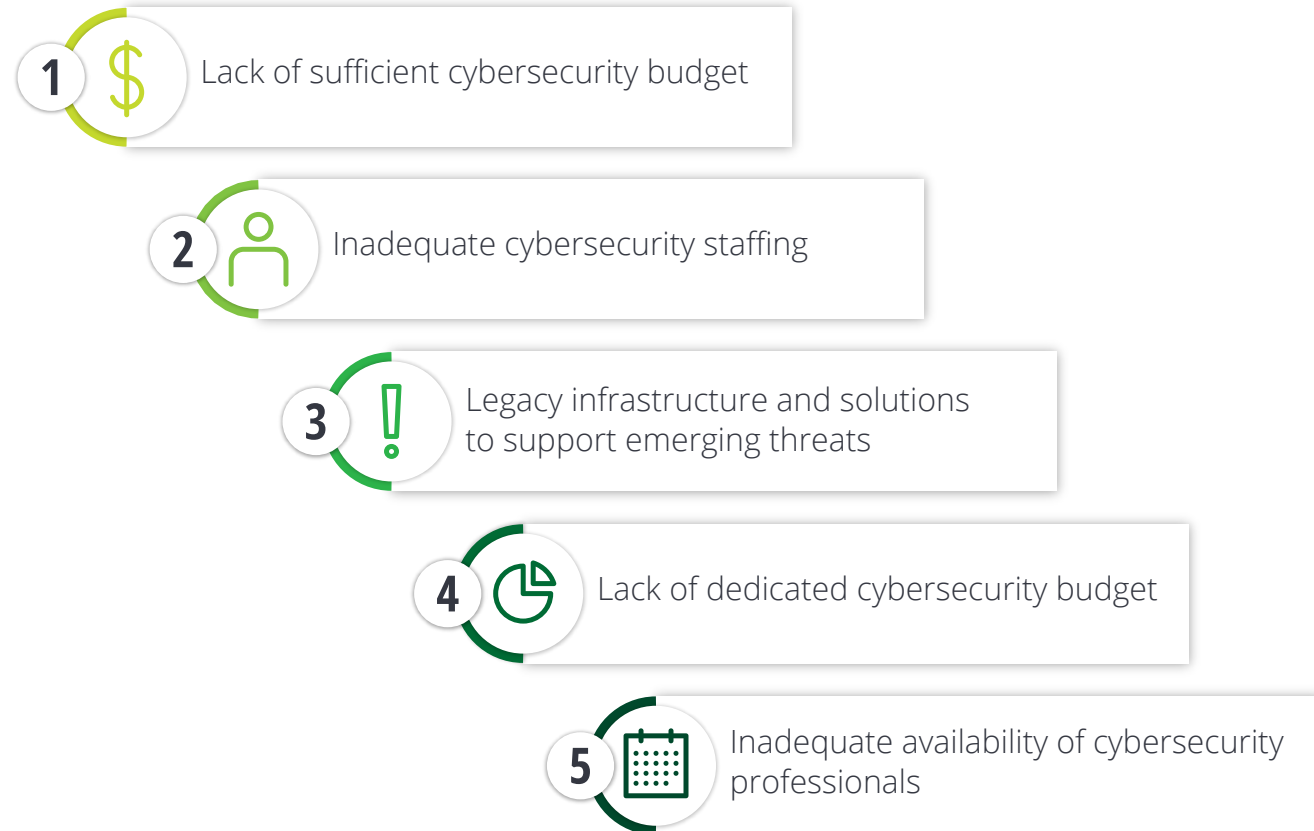


Source: 2020 Deloitte-NASCIO Cybersecurity Study.

Reinventing statewide operations overnight—moving quickly at scale, relying on available resources—amplified the importance of cybersecurity and highlighted shortcomings in the cybersecurity ecosystem. The strain on budgets, talent, partnerships with other agencies, and the significance of cyberthreats became increasingly visible as CISOs made do with what they had. These needs are consistent with the top barriers CISOs say they face in addressing cybersecurity challenges.

Further, some of the COVID-19 responses are likely to become permanent changes—for instance, we may see a sizable portion of the state workforce continue to function remotely even after offices reopen. Similarly, delivering citizen services without the need to visit government offices in person may become the norm as well; digital enablement of citizen services is a key component of making that a reality. States will need to adjust to this new reality, and CISOs will need to orient their strategies to meet the security needs of this next normal.

FIGURE 3

**Top barriers to overcome cybersecurity challenges**

1. $ Lack of sufficient cybersecurity budget

2. Inadequate cybersecurity staffing

3. ! Legacy infrastructure and solutions to support emerging threats

4. Lack of dedicated cybersecurity budget

5. Inadequate availability of cybersecurity professionals

Source: 2020 Deloitte-NASCIO Cybersecurity Study.

# Call to action

*CISOs should build upon the success of their pandemic response to elevate their position in strategic discussions and adjust their strategies to the new reality. Two areas stand out:*

- **Cosponsor the tech modernization agenda.** In most states, increasing reliance on digital government and the virtual workplace have underscored the need for IT modernization. In fact, surveyed CISOs named legacy infrastructure and solutions as one of the top barriers to addressing emerging threats (figure 3). Cybersecurity must be a central focus as modern technology environments are designed, especially with cyberthreats' increasing risk and sophistication. During the pandemic, CISOs have been able to demonstrate the value and essential nature of a robust cybersecurity effort; they should keep this forward momentum going strong by insisting on a seat at the table as states plan, prepare, and invest for the future. The timing is right: In the 2020 NASCIO State CIO Top 10 priorities,[1] cybersecurity remains the top priority for the seventh year running, while

innovation and transformation made the list for the first time. CISOs should be involved in every step of the technology modernization effort and champion the technology modernization efforts with the CIOs, given the significant role cybersecurity plays as the driver.

- **Secure the future of work.** Dramatic changes in the workplace highlight the need to balance agility and security when it comes to implementing cyber safeguards. As a result of the pandemic, a majority of states have reinforced or established safeguards at the enterprise and agency levels. They have also taken action to safeguard their workforce and consumers and to protect infrastructure.

States are also looking at the new realities of training, monitoring, and securing the workplace of the future: Some new state

workers may never step into a state facility at all. The future of work for states may entail remote workers that could include part-time special-skills or gig workers. One CISO noted that during the early response to the pandemic, their agency was challenged in "providing onboarding and secure access for hundreds of new temporary employees hired to provide assistance with unemployment claims processing and contact tracing." State CISOs not only need to reimagine cyber awareness training and culture—they have to create mechanisms to better secure citizen data and manage digital identities in highly distributed computing and digital environments. This also means CISOs should continue to be proactive in staying on top of these rapidly emerging trends and implement solutions that protect state assets and confidential citizen data.

# Key takeaway 2

## Connecting the cyber dots across state, local, and higher education

**Collaboration with local governments and public higher education is critical to managing increasingly complex cyber risk within state borders**

State and local governments are top targets for ransomware and other cyberattacks, and they can benefit by working together to protect against the risk of cyberattacks. While recognizing the autonomy of local governments, there is a value to having states build a collaborative relationship with local governments and institutions of public higher education. Especially when undertaking modernization initiatives, all parties can benefit from sharing knowledge and resources, and coordinating approaches. Such a collaborative approach may offer considerable advantages in terms of cost efficiencies, better cyber hygiene and culture, and improved security of citizens' data.

CISOs should also take note that the US Congress is evaluating bills such as the State and Local IT Modernization and Cybersecurity Act[2] to allocate several billion in funding to cybersecurity for state and local governments, including significant support to be directed toward counties and municipalities. Some of these proposals recognize that state and local governments can achieve better cyber protection by modernizing the underlying technology infrastructure. This legislative focus is partly in response to the targeted ransomware attacks in 2019 that caused significant disruptions for local governments.[3]

*56% of CISOs are not very confident* and *35% of CISOs are only somewhat confident* in the cybersecurity practices of their local governments.

*Only 28% of states reported* that they had collaborated extensively with local governments as part of their state's security program during the past year, *with 65% reporting* limited collaboration.

Extensive Limited
**COLLABORATION**

**There is little doubt that cyberthreats are growing.**

Survey results showed that the probability of a security breach is higher over the next 12 months than in 2018. The survey found a high likelihood of threats coming from social engineering, the increasing sophistication and proliferation of cybercriminals, as well as phishing and pharming schemes.

Smaller public entities—such as counties, cities, towns, and educational institutions—may be particularly vulnerable, a sentiment reflected in our survey. In fact, 40% of CISOs said they feel only somewhat confident that their state information assets are adequately protected from cyberattacks targeting local government and public higher education entities. Low confidence may stem from limited collaboration and a lack of information about their cybersecurity practices and controls.

Similar findings emerged regarding collaboration with state colleges and universities: Twenty-four percent reported extensive collaboration, with 63% reporting limited collaboration. Community colleges follow this pattern, with 27% reporting no collaboration. Almost 60% of CISOs say the cybersecurity capabilities and controls of local government and public higher education entities are unknown.

By strengthening connections with their county, municipal, and higher education counterparts, CISOs have an opportunity to improve cybersecurity within state borders. Such a collaboration and proactive measures can help reduce the possibility of operational downtime, financial impact, and disruption of services to citizens.

# Call to action

*Building bridges to local governments and public education entities could help close the cybersecurity confidence gap, reduce the state's exposure to risk, and increase opportunities for funding. CISOs have clear actions to pursue:*

- **Advocate for enhancing local government cybersecurity.** Many state CISOs see increased engagement with local governments as strengthening the state's overall cyber posture, and they have made it a top cybersecurity priority.[4] States are also recognizing that cybersecurity threats extend far beyond IT as a matter of importance: It is a critical threat to business, homeland security, and public safety as well as a voter confidence issue and economic development opportunity. A whole-of-state approach—one that engages local, city and county governments, legislative and judicial branches of government, and public higher education—could potentially strengthen cybersecurity at all levels of government and bolster protection.

- **Encourage the adoption of services provided by the state.** Federal bills for tech modernization—including the State and Local Cybersecurity Improvement Act and the State Homeland Security Grant Program (SHSGP)[5] to make grants for emergency IT expenses—expect states to play an influencing and leadership role in elevating tech and cyber in local government. Many states offer a variety of services that are available to local governments and public education entities, including incident response, security management operations, network and infrastructure, strategy, governance, and risk management. Yet only 27% of states provided cybersecurity training to these entities last year—a relatively mature cyber offering in states that can be extended to other entities. Promoting awareness of these services could improve adoption through a formal awareness campaign, hosting cyber summits, and sponsoring workshops and other learning opportunities.[6]

# Key takeaway 3
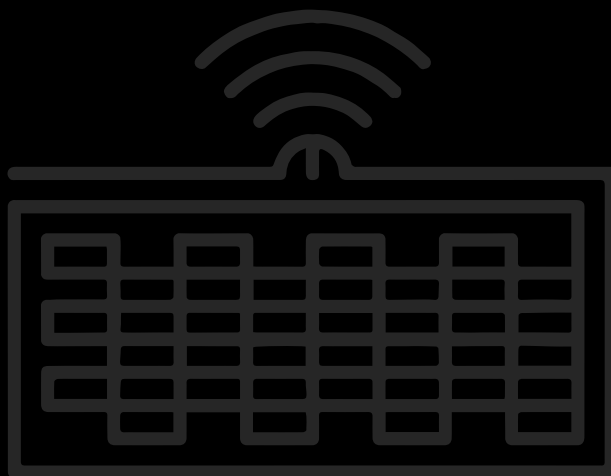
## Strength, consistency, and enforcement in numbers

**A centralized structure helps CISOs position cyber in a way that improves agility, effectiveness, and efficiencies**

The study shows that 40% of the states continue to operate in a federated model, in which CISOs are responsible for enterprise policy with a mix of centralized shared services and agency-led services specific to each, and 10% operate in a decentralized model of cybersecurity governance under which individual state agencies are on their own for cyber services and execution with only policy guidance from the CIO. As CISOs look to take on a more visible role in technology modernization and securing the workforce of the future, a centralized cybersecurity governance structure (centralized model under which the enterprise CISO is responsible for cybersecurity for all agencies) will position them for enhanced effectiveness. Fully three-quarters of state CISOs believe that a centralized model can most effectively improve the cybersecurity function.

By moving to a centralized model, states may be able to consolidate resources and break down the silos of efforts across enterprise-level and agency-specific programs.

## For example, if all states were to follow a *centralized model*:

*44% of states* would have more than 51 full-time employees
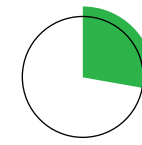
*28% of states* would have 26–50 full-time employees

This concentration of resources in a centralized model could help enhance competencies and improve both opportunities for training and career opportunities for cyber staff. A centralized function could be more agile and efficient at deploying scarce cyber resources for the agencies and programs with the most need.

**We believe the advantages of a centralized structure are increasingly evident:**

- As states pursue tech modernization initiatives, CISOs need to be at the forefront of conversations to elevate cybersecurity initiatives. Among state agencies, there is a high degree of adoption in the areas of security awareness and threat monitoring; however, the adoption of critical services—such as risk assessments, threat monitoring, and identity and access management adoption—trails. A centralized model should help to increase adoption of essential enterprise security services.

- States have an opportunity to leverage federal funding, with program-specific and state-level grants for implementing and delivering cybersecurity services in a shared model to benefit all agencies.

- While IT budgets allocated for cybersecurity are limited (only 1–2% of the total budget in 22% of states and 3–5% of the total budget in 20% of states), some agencies have their own cybersecurity budgets that is not reflected in the numbers. The ability to manage a centralized cybersecurity budget is likely to help elevate the overall cyber posture.

- Cross-training and upskilling can also be simplified and more easily scaled, providing more career growth opportunities for the cyber staff.

FIGURE 4

**Most states indicate that a centralized operating model can best reduce cybersecurity risk**



OUT OF
*50 states*

0 Decentralized
12 Federated
38 Centralized
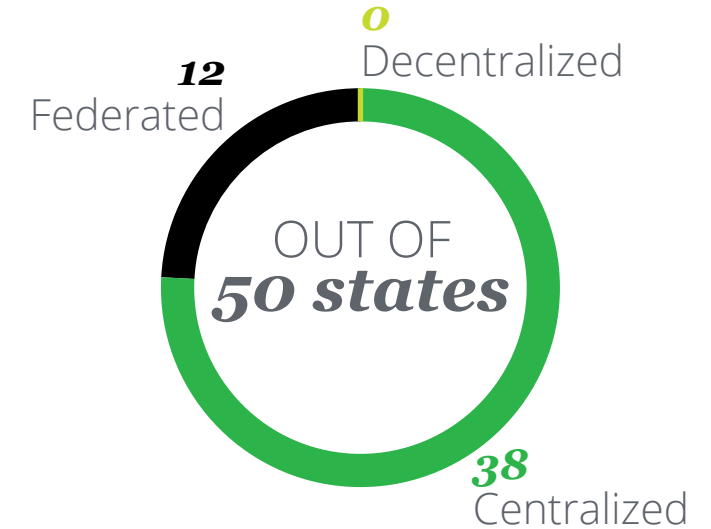
Decentralized:
Responsible for a single agency

Centralized:
Responsible for multiple agencies

Federated:
Responsible for centralized common services with assigned services specific to each agency

Source: 2020 Deloitte-NASCIO Cybersecurity Study.

# Call to action

*A centralized organization is often in a better position to manage operations, resources, and talent (full-time employees and outsourced resources).*

In a centralized model, leaders have the responsibility to deliver cybersecurity services at the enterprise level and monitor compliance against a harmonized set of federal and state cyber regulations. This centralized organization could report on workforce metrics and measure a state cyber program's effectiveness. This centralized model better positions the state to succeed in extending critical cyber services to local governments and public higher education.

In a centralized model, leaders have the responsibility to deliver cybersecurity services at the enterprise level and monitor compliance against a harmonized set of federal and state cyber regulations. This centralized organization could report on workforce metrics and measure a state cyber program's effectiveness. This centralized model better positions the state to succeed

in extending critical cyber services to local governments and public higher education.

## One additional consideration on the move to a centralized model

One objection to adopting a centralized model is the possibility of cyber resources not being close enough to the business and program initiatives taking place at the agency level. Even today, the study reports that only 20% of state leaders see business operations and cybersecurity initiatives as appropriately aligned.

With a centralized model of governance, there is a potential to further distance cybersecurity initiatives from the business priorities and initiatives. To avoid such an outcome, states could consider specific roles

such as a *business information security officer*, specifically tasked with being close to the agency/business/ programs and empowered to help create the necessary linkage with the business.

# Progress on the 2018 Deloitte–NASCIO Cybersecurity Study bold plays

## STATE CISOs MADE SOME PROGRESS, BUT MORE IS NEEDED

**In 2018, we challenged CISOs to take on three strategic "bold plays" to break through long-standing challenges and accelerate positive change.**
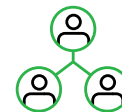
The bold plays are strategic shifts that may take years for results to be visible, and our 2020 survey results show that while progress is being made, now is not a time to declare victory. In fact, it is critical to continue pressing forward on these bold plays.

Advocate for dedicated cyber program funding

CISOs as an enabler of innovation, not a barrier

Team with the private sector and higher education

# Bold play

# 1

## Advocate for dedicated cyber program funding

In terms of a dedicated cybersecurity budget line item, there is no real progress, with only 36% of states reporting that they have a cybersecurity budget established by the agency secretary, CIO, or administrative rule, regulation, or procedure.

2018
2020

*The number of states that receive funding through the overall IT budget increased from 48% in 2018 to 57% in 2020.*
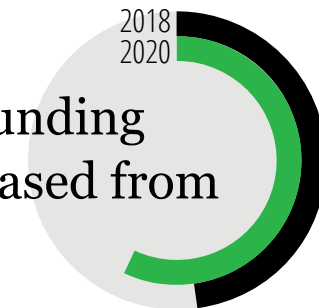
We believe that a dedicated cyber program funding—even when assigned as part of the overall IT budget—can help state CISOs and CIOs give the state legislature and executive branch leaders the right level of visibility into state cybersecurity spend in an effort to raise funding levels.

The 2020 study shows that most states still allocate less than 3% of their total IT budget on cybersecurity. In contrast, the 2020 Deloitte–FS-ISAC Cybersecurity Study[7] indicates that financial services companies allocate 10.9% of the IT budget spend to cybersecurity. Federal government agencies also continue to spend a greater percentage of their IT budgets on cybersecurity than many states (figure 5).

FIGURE 5

## Federal agencies spend a greater percentage of their IT budgets on cybersecurity than many states

Federal agencies' cybersecurity budgets as a percentage of total IT budget and year-over-year growth

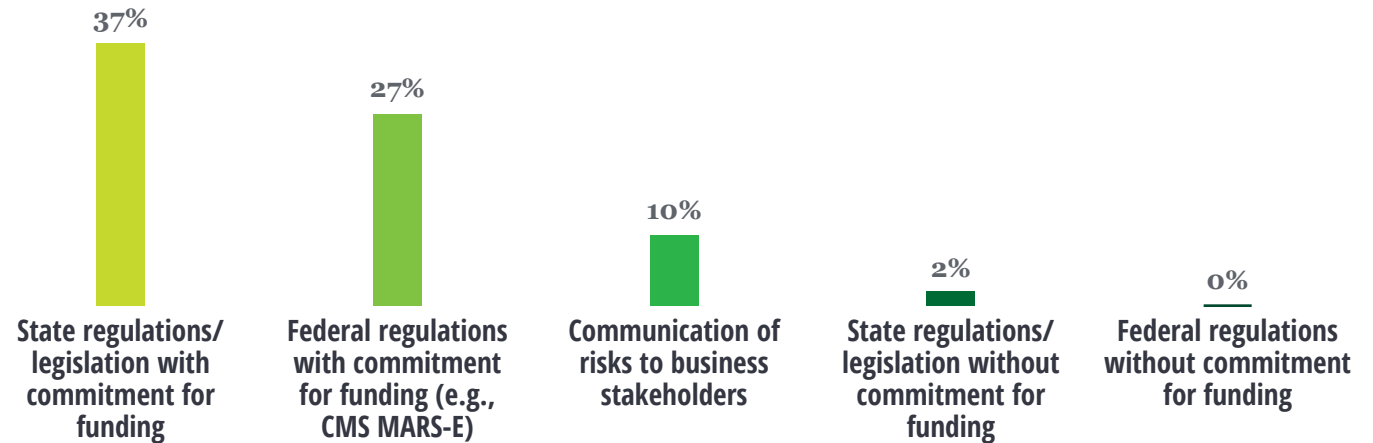|  |  | 2019 | 2020 | 2021 |
|---|---|---|---|---|
| Department of Transportation | Percentage of IT budget | 5.63% | 7.09% | 7.33% |
|  | Year-over-year increase | 10.54% | 21.12% | −4.92% |
| Health and Human Services | Percentage of IT budget | 6.44% | 8.43% | 8.12% |
|  | Year-over-year increase | 18.50% | −7.18% | 9.19% |
| Social Security Administration | Percentage of IT budget | 11.40% | 10.54% | 10.79% |
|  | Year-over-year increase | 4.21% | 1.76% | −1.25% |
| Treasury | Percentage of IT budget | 10.82% | 11.77% | 14.06% |
|  | Year-over-year increase | −7.23% | 15.19% | 17.06% |
| Justice | Percentage of IT budget | 25.07% | 30.07% | 28.16% |
|  | Year-over-year increase | −0.67% | 7.56% | 3.19% |

Source: Deloitte analysis.

Financial services companies also report spending US$2,691 per full-time employee on cybersecurity, and that budgets have seen an increase from US$2,337 in 2019—a 15% boost in cyber spending.[8] If states were to mirror the financial services model and report on cyber spend per employee, a typical state with 40,000 employees would translate to a US$108 million in cyber spending—a considerable difference with the current state cyber budget levels.

**CISOs continue to report that regulations backed by a commitment for funding are most effective at improving states' cybersecurity posture and reducing risk.**

FIGURE 6

## Which regulations are most effective at improving cybersecurity posture and reducing risk?



| | |
|---|---|
| 37% | State regulations/legislation with commitment for funding |
| 27% | Federal regulations with commitment for funding (e.g., CMS MARS-E) |
| 10% | Communication of risks to business stakeholders |
| 2% | State regulations/legislation without commitment for funding |
| 0% | Federal regulations without commitment for funding |

Source: 2020 Deloitte-NASCIO Cybersecurity Study.

The prevalence of multiple versions of federal agency cybersecurity regulations, with inconsistent federal funding, exacerbates CISOs' challenges. One survey respondent said, "Federal regulations and the audit process need to be harmonized. It is not contributing to improving the state's cybersecurity posture." Imagine a single set of harmonized cyber regulatory requirements that satisfy all of the federal agency cyber requirements, and how it could help the state CISOs in demonstrating compliance. And when gaps are identified, justifying the need for federal cyber funding to mitigate such gaps would become that much simpler. This is also consistent with a May 2020 GAO report.[9]

**In summary, dedicated cyber program funding and a harmonized set of cyber regulations from the federal agencies could enable better management of federal regulations and help states to obtain the much-needed federal funding.**

# Bold play
# 2

## CISOs as an enabler of innovation, not a barrier

In our 2018 study, we challenged state CISOs to elevate the role of cybersecurity by taking a leadership position in digital modernization, embracing emerging technologies such as artificial intelligence, the Internet of Things, and smart government. Two years later, emerging technologies are still not yet a high priority among state CISOs when compared to operational cybersecurity initiatives.

In contrast, CISOs in the financial services industry are using emerging technologies and innovation to their advantage. Respondents in the 2020 Deloitte–FS-ISAC Cybersecurity Study[10] cited emerging technologies such as cloud, data analytics, and robotic process automation as top cybersecurity investment priorities, emphasizing access control, protective technology, and data security as key rationales. These new technologies present a new set of solutions that can help financial institutions transform operations and achieve cost reductions.

Perhaps as a result of their pursuit of innovation and presenting solutions to business problems, the financial services industry could *continue to see an increase in cybersecurity spending*.

CISOs in state government should look to their colleagues in financial services and glean inspiration from their success. By emphasizing emerging technologies, advocating for their adoption, and presenting appropriate solutions, CISOs can become well-positioned to collaborate with CIOs and lead their states' charge toward innovation. The CISO role in the adoption and collaboration is even more relevant given that the technology modernization initiatives will likely accelerate the adoption of cloud, robotic process automation, and mobile technologies for the next few years.

# Bold play
# 3

# Team with the private sector and higher education

As noted in the 2018 study, CISOs should consider leveraging public-private partnerships and collaborations with local colleges and universities to provide a pipeline of new talent, as well as consider outsourcing to private sector firms. Our 2020 study found that the cybersecurity functions being outsourced are beginning to see an increase—a step toward helping states grapple with cyber talent challenges: Sixty percent of states outsource cyberthreat assessments compared with 43% in 2018; 42% outsource a security operations center versus 38% in 2018; 40% outsource forensic legal support versus 32% in 2018.

It is concerning that *confidence in third parties has decreased*. Standardizing governance and adherence to leading practices and policies can help increase confidence in these third-party partnerships.
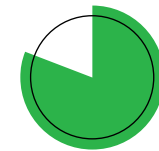
*81% of states* say they are only somewhat or not very confident in third parties' cybersecurity practices.

Significant opportunities exist for states to collaborate with local governments and public higher education entities. Our study indicates there is much work to be done to improve these collaborations and partnerships, as confidence in the security practices of third parties within local and higher education entities is only moderate. CISOs should consider partnering with local colleges and universities to pursue a pipeline of new talent through internships, co-ops, and apprentice programs, while working together to develop common strategies to improve statewide services.

# Survey data
# analysis deep dives

In the following section, we take a detailed look at the survey findings.
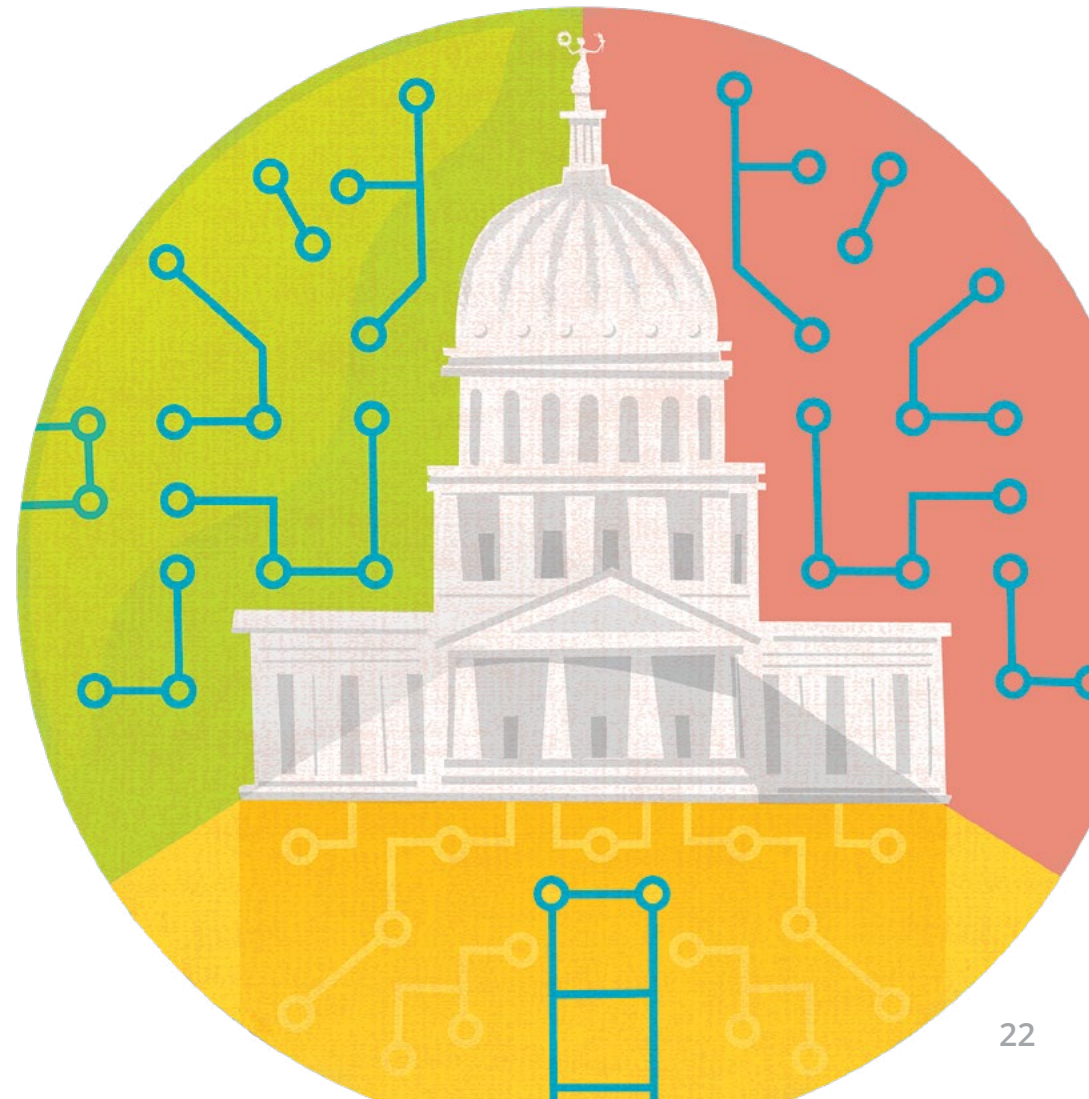
# Strategy and governance

## *Only 10 states:*

→ Have appropriately aligned on cybersecurity initiatives with the goals and initiatives of business/program stakeholders.

→ Have legislation in place that provides funding to support the role and authority of the enterprise CISO or equivalent.

## CISOs receive input on cyber strategy from:

**01** State technology decision-makers | **47 states**

**02** State business decision-makers | **39 states**

**03** Private sector | **23 states**

**04** Higher education | **16 states**

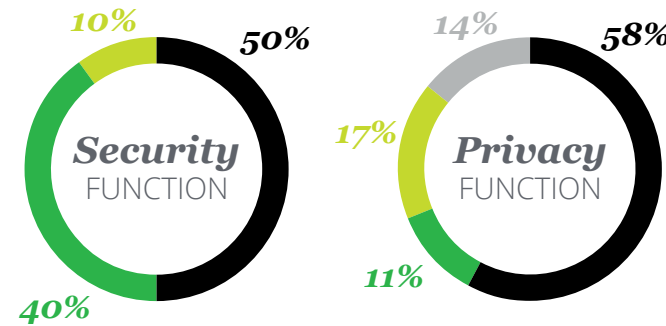## Declining trend on periodic executive cybersecurity report

**2018–2020**

To governor:
**24 to 22 states**

To legislature:
**27 to 16 states**

## Cybersecurity and privacy functions: Operational model

■ Federated  ■ Centralized  ■ Decentralized
■ N/A, don't know



**Security** FUNCTION — 50%, 10%, 40%

**Privacy** FUNCTION — 58%, 14%, 17%, 11%

## Top cyber services provided to the state, local, and public higher education entities

**01** Incident management

**02** Awareness and training

**03** Investigation and forensics

**04** Security operations center

**05** Vulnerability management

## Enterprise security services adopted by state agencies

**57%** Security awareness

**57%** Security operations center

**47%** Incident response

**35%** Risk and vulnerability assessments

**14%** Identity and access management

## Risk and privacy leadership in states

**16** States with chief **privacy** officer

**13** States with chief **risk** officer

## CISO's role in procurement of hardware, software, and service providers

**01** Establish security policies and guidelines (**90%**)

**02** Evaluate a security questionnaire that vendors need to complete for procurement opportunity (**67%**)

**03** Prohibit procurement of specific manufacturers/vendors/products (**38%**)

# Budget

## Budget continues to be the top barrier

**01** Lack of sufficient cybersecurity budget (**46%**)

**02** Inadequate cybersecurity staffing (**42%**)

**03** Legacy infrastructure and solutions to support emerging threats (**34%**)

## Top five areas covered in the cybersecurity budget

2020 vs. 2018

**86%** Audit logging and security information and event monitoring — +16%

**84%** Security operations center — +18%

**76%** Cybersecurity strategy and road map — +4%

**76%** Threat intelligence and analytics — +6%

**76%** Compliance and risk management — +10%

## *Only 18 states* have a cybersecurity budget line item.

## Average cybersecurity spend in 2020 (percentage of IT budget)

**1−3%** Most state governments

**16.3%** Federal agencies*

**10.9%** Financial institutions

*Federal civilian agencies under the CFO Act of 1990.*

## Only a few states reported a budget increase since 2018

**2018** vs. **2020**

Increase of 1–5%: 24% / 35%

Increase of 6–10%: 10% / 6%

Increase of >10%: 14% / 16%
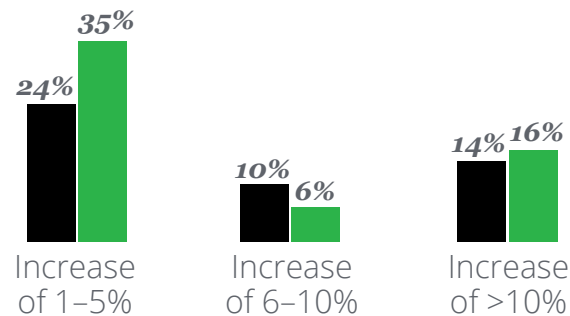
## Additional cyber funding sources

2020 vs. 2018

**46%** US Department of Homeland Security — +13%

**40%** Interagency collaboration — +2%

**23%** Other state funding from legislature — +15%

**19%** Business or program stakeholders — -16%

## Cyber funding charge back versus appropriations

Appropriations 20%

Chargeback 25%

Hybrid of chargeback/appropriations 39%

Don't know, N/A 8%

Other 8%
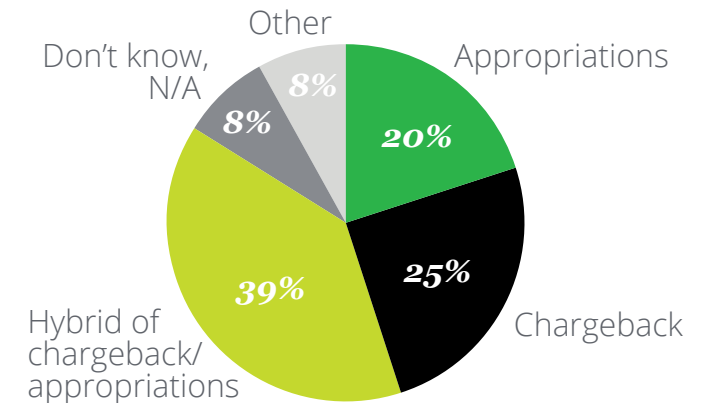
# Cybersecurity workforce

## Top benefits to attract/retain cybersecurity talent

**01** Opportunity to serve and contribute

**02** Job stability

**03** Workplace flexibility and predictable work hours

## Top talent management practices to attract and retain cyber workforce

**01** Promote nonsalary benefits

**02** Highlight greater stability

**03** Internship programs

## Barriers impacting the development and support of cyber workforce

**01** State salary rates and pay grades

**02** Lack of qualified candidates

**03** Workforce leaving for private sector

## Leading outsourced cyber functions

**2020 vs. 2018**

**60%** Cyberthreat risk assessments — +17%

**42%** Security operations center — +4%

**40%** Forensics/legal support — +8%

## States' plan to close the cybersecurity competency gap

**2020 vs. 2018**

**94%** Provide training to staff who are developing the required competencies — +31%

**69%** Use specialist augmentation (e.g., consultants and contractors) — +66%

**51%** Contracting with a managed security services provider — +44%

**40%** Outsource certain functional areas — +27%

*Only eight states* are very confident on cybersecurity practices of third parties. *Twenty-six states* were somewhat confident, down from 31 states in 2018.

## Dedicated cybersecurity professionals at the enterprise security office

| Full-time equivalents | 2010 | 2018 | 2020 |
|---|---|---|---|
| 1 to 5 | 47% | 18% | 16% |
| 6 to 15 | 39% | 49% | 30% |
| 16 to 25 | 4% | 14% | 18% |
| 26 to 50 | 4% | 14% | 20% |
| >51 | 2% | 4% | 16% |
| Other | 4% | 0% | 0% |

*No state* has fully adopted and established the National Initiative for Cybersecurity Education (NICE) workforce framework and *only eight states* are implementing portions of the NICE framework.

# Identity and access management (IAM)

## IAM moves up in enterprise priority

| | Ranking | |
|---|---|---|
| | **2018** | **2020** |
| Risk assessments | *1* | *1* |
| **Enterprise identity and access management** | *11* | *2* |
| Cybersecurity strategy | *4* | *3* |
| Operationalizing cybersecurity | *13* | *3* |
| Metrics to measure and report effectiveness | *1* | *3* |

***Only 15 states*** have an enterprisewide IAM solution that covers all agencies under the governor's jurisdiction.

## IAM is critical to tech modernization and digital transformation

**2020 vs. 2018**

| | | |
|---|---|---|
| **92%** | Security | +3% |
| **77%** | Modernization and digital transformation | +7% |
| **73%** | Standardization: IAM framework, application development, and user interface | -3% |
| **71%** | Compliance | +5% |
| **69%** | Improved end-user experience: single credential for citizen access | -8% |
| **63%** | Operational efficiency/cost savings | -2% |

## Top IAM initiatives

**01** Multifactor authentication (**90%**)

**02** Privileged identity management (**52%**)

**03** Cloud-based IAM (**48%**)

## Top barriers to adopt enterprise IAM

**01** Complexity of integrating with legacy systems (**65%**)

**02** Competing or higher-priority initiatives (**46%**)

**02** Decentralized environment of the state (**46%**)

# Cyber operations

## Financial fraud ranked higher as an external threat

**01** Malicious code | **26 states**

**01** Web applications | **26 states**

**03** Financial fraud involving information systems | **22 states (only 5 states in 2018)**

*Only 22 states* use DMARC* for their state's enterprise email systems.

*Domain-based Message Authentication, Reporting, and Conformance*

## States improving on performing regular cyber assessments

2020 vs. 2018

**67%** Security events monitoring/security operations center  +2%

**63%** Annual disaster recovery exercises and tests  +3%
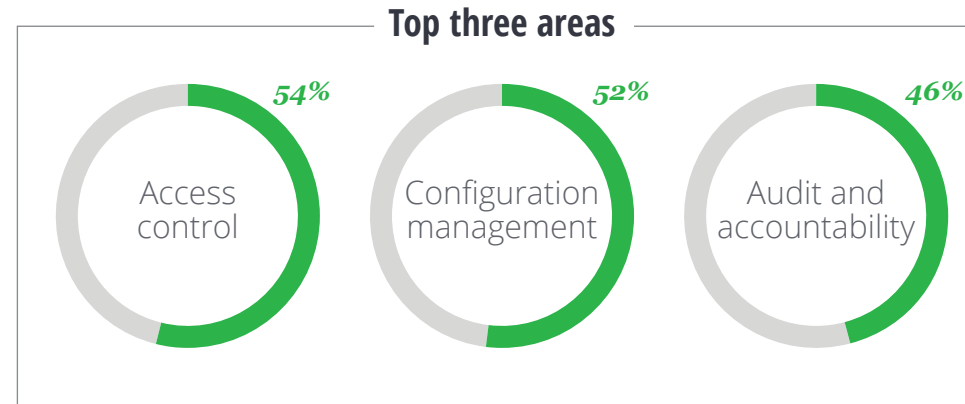
**60%** Application security testing and code review  +6%

## Areas where external audit findings have identified gaps in the past year

### Top three areas

54% Access control

52% Configuration management

46% Audit and accountability

**44%** Identification and authentication

**42%** Risk assessment

**40%** System and services acquisition

**40%** Contingency planning

**38%** System and communications protections

**31%** Security assessment and authorizations

**29%** Incident response

**27%** System and information integrity

**25%** Planning

**23%** Physical and environmental protection

**23%** Media protetion

**21%** Personnel security

**21%** Maintenance

**19%** Awarness and training

**17%** N/A, don't know

**15%** Privacy

**4%** No internal/external audit findings

27

# Cyberthreats

*54% of the states* are not confident in their ability to address threats from emerging technology.

*30 states* said financial fraud was a leading cause of breaches in the past year compared to *10 states in 2018*.

Leading causes of breaches continue to be from external sources: *malicious code* (68%), *web applications from external sources* (81%), and *"hacktivism"* (86%), which is on the rise.

*Twenty-two states* perform a periodic election security assessment.

*In 29 states*, the enterprise CISO and agency CISO are the officials responsible for coordinating and responding to cyber incidents.

## CISO confidence in tackling types of threats ("very confident" and "extremely confident" combined answers)

**2020 vs. 2018**

**6%** Threats originating from use of emerging technologies (e.g., Internet of Things) — +2%

**10%** Threats originating from business partners/vendors — +4%

**15%** Threats originating from local government and public higher education entities — New in 2020

**19%** Threats originating from cloud platforms and solutions — +9%

**19%** Threats originating internally — -4%

**23%** Threats originating from applications — +11%

**42%** Threats originating externally — +5%

## CISOs' top concerns for potential breaches have seen increases since 2018. Other notable changes:

**74 to 85%** Phishing/farming
**59 to 70%** Ransomware/malware
**47 to 54%** Exploits of unsecured code

## Leading cybersecurity standards that states use:

**01** National Institute of Standards and Technology (NIST) Special Publications (**88%**)

**02** Center for Internet Security (**73%**)

**03** NIST Cybersecurity Framework (**63%**)
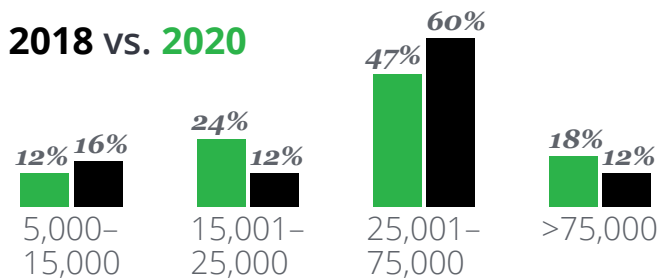
# Appendix: Survey methodology

**The 2020 Deloitte–NASCIO Cybersecurity Study uses survey responses from:**

- US state enterprise-level CISOs answered 61 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Participation was high: Responses were received from 51 states and territory respondents. These figures illustrate the CISO participants' demographic profile and that of their states.

- 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.
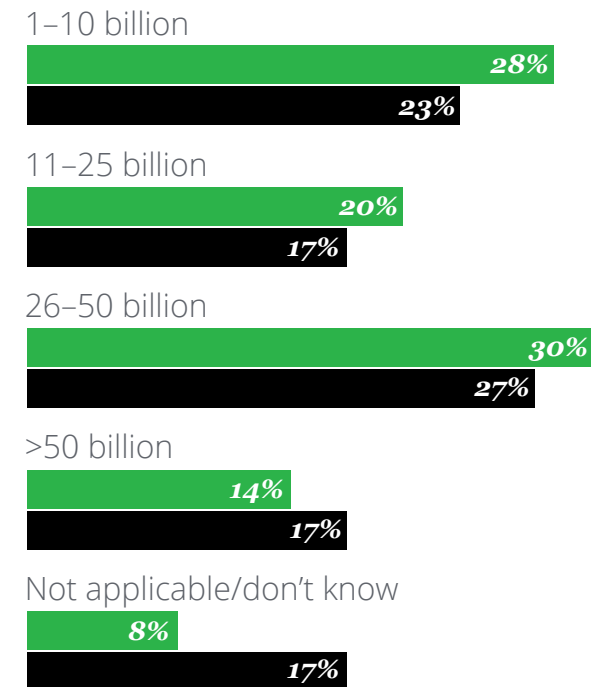
**SURVEY RESPONDENT _job titles_**

- *5* Other
- *3* Chief risk officers
- *43* CISO or equivalent
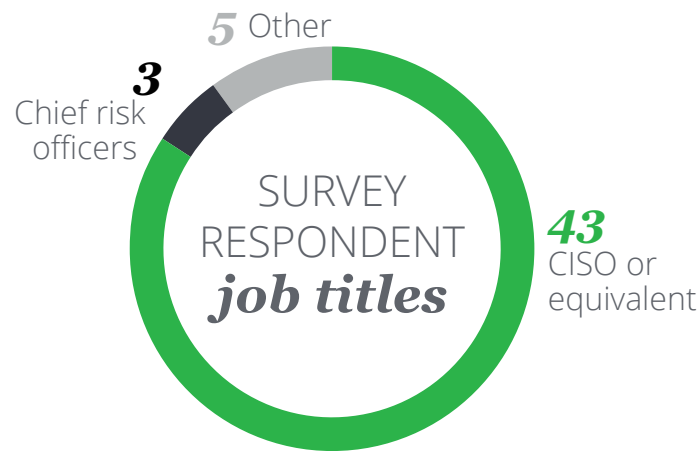
## Number of state government employees (excluding higher education employees)

**2018** vs. **2020**

| | 5,000–15,000 | 15,001–25,000 | 25,001–75,000 | >75,000 |
|---|---|---|---|---|
| 2018 | 12% | 24% | 47% | 18% |
| 2020 | 16% | 12% | 60% | 12% |

## Approximate annual state budget for current budget year (US$)
**2018** vs. **2020**

**1–10 billion**
- 28%
- 23%

**11–25 billion**
- 20%
- 17%

**26–50 billion**
- 30%
- 27%

**>50 billion**
- 14%
- 17%

**Not applicable/don't know**
- 8%
- 17%

Source: 2020 Deloitte-NASCIO Cybersecurity Study.

# Endnotes

1. NASCIO, "State CIO top ten policy and technology priorities for 2020," December 2019.

2. *Government Technology*, "House bill could mean billions for state, local IT," August 17, 2020.

3. Dan Lohrmann, "2019: The year ransomware targeted state & local governments," *Government Technology*, December 23, 2019.

4. NASCIO, "Stronger together: State and local cybersecurity collaboration," January 15, 2020.

5. US Department of Homeland Security, "Homeland Security Grant Program (HSGP)," accessed September 11, 2020.

6. NASCIO, "Stronger together."

7. Julie Bernard, Deborah Golden, and Mark Nicholson, *Reshaping the cybersecurity landscape: How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions*, Deloitte Insights, July 24, 2020.

8. Ibid.

9. U.S. Government Accountability Office, "Cybersecurity: Selected federal agencies need to coordinate on requirements and assessments of states," May 27, 2020.

10. Bernard, Golden, and Nicholson, *Reshaping the cybersecurity landscape*.

# About the authors

**Srini Subramanian   |   ssubramanian@deloitte.com**

Srini Subramanian is a principal in Deloitte & Touche LLP's Cyber practice and leads the Risk & Financial Advisory practice for the State, Local, and Higher Education sector in the government and public services industry. He has nearly 35 years of IT experience and nearly 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 18 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.

# Contacts

**Srini Subramanian**
Principal | State, Local & Higher Education Risk & Financial Advisory leader | Government and Public Services | Deloitte & Touche LLP
+1 717 651 6277 | ssubramanian@deloitte.com

Srini Subramanian is a principal in Deloitte & Touche LLP's Cyber practice.

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

Meredith Ward is director of policy and research for the National Association of State Chief Information Officers.

# Acknowledgments

We thank the 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 the state CISO survey review team: **Adam Ford**, Illinois; **Bill Nash**, Wisconsin; **Nancy Rainosek**, Texas; **Tim Roemer**, Arizona; and **Maria Thompson**, North Carolina.

At Deloitte, we thank subject-matter specialists **Bharane Balasubramanian**, **Mike Wyatt**, **Timothy Li**, **Clayton Frick**, and **Jesse Goldhammer** of Deloitte & Touche LLP; **John O'Leary** of Deloitte Services LP; and **Ron Baldwin** and **Art Stephens** of Deloitte Consulting LLP.

Thank you to the **Deloitte survey team, data analysis, and benchmarks**: **Bharath Chari**, Deloitte & Touche LLP; **Sushumna Agarwal**, Deloitte Services LP; **Glynis Rodrigues**, Deloitte Services LP; **Thirumalai Kannan**, Deloitte Services LP.

Thanks also to the marketing and writing team, including **Annette Evans**, Deloitte Services LP; **Anudeep Gurram**, Deloitte Services LP; and **Marie Willsey**, writer.

# About Deloitte

**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.

**The Deloitte Center for Government Insights** produces groundbreaking research to help government address its most complex problems. Through publications, forums, and immersive workshops, we engage with public officials on a journey of positive transformation, crystallizing insights to help them understand trends, overcome constraints, and expand the limits of what is possible.

For more information, visit www.deloitte.com or read about the Deloitte Center for Government Insights at www.deloitte.com/us/center-for-government-insights.

# About 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.

**Deloitte.**
Insights

**NASCIO®**
Representing Chief Information
Officers of the States
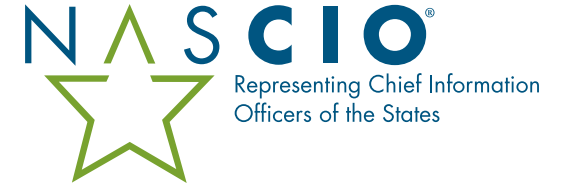
Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

**About Deloitte Insights**

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

**About this publication**

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication 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 finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respec-tive affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.