

Deloitte.
Insights



2018 Deloitte-NASCIO Cybersecurity Study

States at risk: Bold plays for change

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

Contents

Message from NASCIO's president		2
Foreword		3
Overview: States need bold actions to make progress		5
Survey data analysis		14
Appendix: Acknowledgments and survey methodology		35
Endnotes		36

Message from NASCIO's president

ONE OF THE most important priorities of a state chief information officer (CIO) is to reduce risk to their state. Cybersecurity and reducing cyber risk, specifically, is top of mind for every state CIO and many factors contribute to this. For example, it is unknown how many cyberattacks have been attempted on state government collectively, but one state estimates that two years ago there were 150 million attacks a day, while today there is an average of 300 million attacks per day. The same state has seen as many as 800 to 900 million in one day.

However, the magnitude of this threat is rarely matched in attention and funding in state government. That is why, in 2010, NASCIO collaborated with Deloitte to survey state chief information security officers (CISOs) about the status of cybersecurity in their states. As we have done biennially since, we again asked about perspectives and insights and we have compiled and highlighted those findings here.

You'll notice a few things in this year's study. First, there are three bold plays which are recommendations for state CISOs to disrupt the status quo. Simply put, the time is now to be bold in state cybersecurity. You also may notice that, for the first time, all 50 state CISOs participated. These are the men and women who are committed to being bold around cybersecurity in the states.

Finally, you may have also seen that this study was cited in the White House FY19 Budget Request as the most "comprehensive study of state-level cybersecurity spending." We hope that remains true, but we can commit that NASCIO will continue to use the findings of this study and other work to advocate for increased funding and all resources necessary for states to remain bold in their cybersecurity efforts.

Bo Reese

NASCIO President and CIO, State of Oklahoma

Foreword

THE FIFTH BIENNIAL Deloitte-NASCIO Cybersecurity Study reflects insights from all 50 states on the CISO's role and budget, governance, reporting, workforce, and operations.

Since our first study in 2010, we have seen the CISO's job evolve into a mature, well-defined role. Today, CISOs have achieved solid standing in their states' executive management ranks alongside other senior government leaders, expanding their focus from operational to broader strategic concerns accordingly. CISOs have grown stronger both through greater official recognition of cyber risks and their own efforts to build competencies and reach. Most states have a formally approved governance process delineating both a central vision and guidelines for cybersecurity across the state enterprise.

CISOs have also increased their frequency of reporting to governors and other senior state officials and furthered their collaboration with federal and state governments. As they continue to build a cybersecurity practice, CISOs report gaining more confidence in their abilities to combat cyber threats.

Yet these strides in governance and in establishing the CISO role's legitimacy have not resulted in significant progress in overcoming the top challenges US states face in implementing effective cybersecurity programs. CISOs continue to face perennial challenges in acquiring an adequate budget and workforce to carry out their responsibilities. While CIOs, CISOs, and business leaders may never be able to fully address these hurdles, they and other state leaders should make a concerted effort to close the gap lest it widen even further. The magnitude of the resource gap in the states is particularly telling when compared with federal agencies that are more successful in securing more funding.

With state CISOs enjoying a solid platform in an era of escalating cyber threats and the inevitable need to embrace technologies that introduce new cyber risks, it is now time to take bold action. We encourage state CIOs and CISOs to consider bold initiatives that include a combination of key



legislative and advocacy measures to gain significant additional resources to scale cybersecurity programs:

- Cyber legislation equipped with funding to advance state cyber risk programs
- Federal funding to meet mandated federal cyber requirements
- Public-private-academia partnerships to overcome persistent talent gap issues and improve service levels in security functions delivered

When governors, legislators, and business and technology leaders collaborate, these bold initiatives are possible. Indeed, CISOs need to continue to elevate themselves as business leaders and to embrace innovation to influence greater change. These bold plays become even more urgent as enterprises adopt greater connectivity, advanced technologies, and data-sharing.

We sincerely thank the participants in this year's survey and appreciate every one of the 50 state CISOs who responded. Your time and commitment can help states in their efforts to effectively manage cyber risk and protect citizen data.

AUTHORS OF THE STUDY

Doug Robinson
Executive Director, NASCIO

Srini Subramanian
Principal, Deloitte & Touche LLP

Overview: States need bold actions to make progress

THE 2018 DELOITTE-NASCIO Cybersecurity Study, based on survey responses from all 50 US state CISOs or CISO equivalents, finds that CISOs have made progress in solidifying their role as their state's enterprise cybersecurity leader. Every state has an enterprise-level CISO role, many recognized by legislative mandate, working closely with state CIOs to lead the charge against internal and external cyber threats. As part of the state executive team, CISOs are now engaging in more regular communications with state leaders, with about a quarter reporting to their governors once a month on cyber risk status.

Every state has an enterprise-level CISO role, many recognized by legislative mandate, working closely with state CIOs to lead the charge against internal and external cyber threats.

The primary barriers faced by state CISOs continue to be shortfalls in resources—inadequate budget and lack of available cybersecurity talent. However, with the solid platform and mandate for leadership they have built, CISOs have an opportunity to take bold measures to overcome these challenges. Through concerted

effort with their CIOs and business leaders, legislatures, and federal agency partners, they can equip their states with the right level of capabilities and resources to tackle tomorrow's cyber threats.

CISOs have built an executive leadership platform

Our 2018 survey shows that CISOs have established a platform for leadership, achieving recognition as their state's key cyber risk management executive. All 50 states have established the CISO's authority via the legislature, secretary, or CIO. In addition, most states

now have a formally approved cybersecurity strategy and governance process that articulates and oversees the state's cybersecurity vision and guidelines and provides consistency across the enterprise.

While CISOs continue to report to the CIO, they have improved their access to other state leaders, communicating regularly about cyber risk issues with the governor and the legislature. Likewise, increased engagement with the technology industry and the business community on strategic decisions is also helping to strengthen the CISO's leadership platform.

But even though CISOs have established a solid foundation and gained in visibility and support from state leaders, a number of chal-

lenges persist—many from the time of our 2010 survey. States should change course to address these persistent challenges, particularly in an era of exponential cyber threat growth and increasing executive awareness of the importance of addressing the barriers.

In the following section, we highlight CISOs' key challenges and suggest three bold plays that could help them make significant strides, bringing states in closer alignment with what the more progressive federal agencies and

other commercial industries, such as financial services, have achieved.

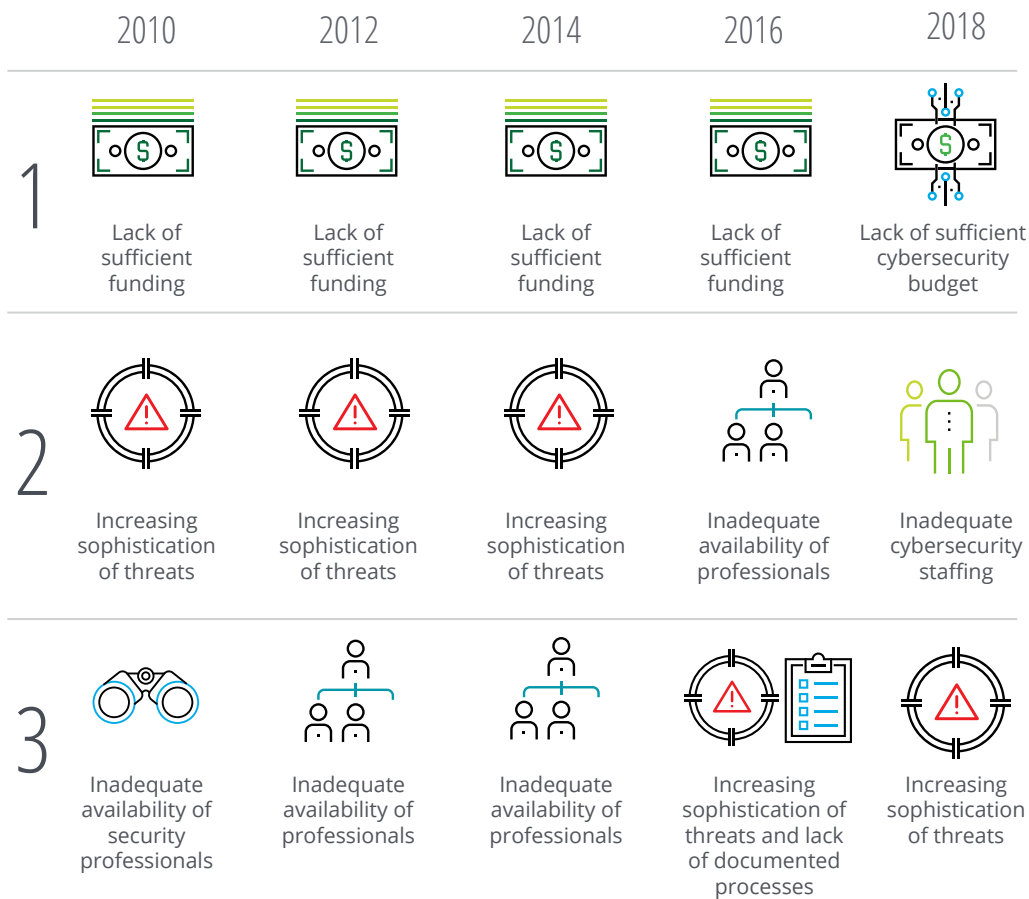
Persistent challenges continue in the status quo

While a majority of CISOs have made advancements in establishing their cybersecurity programs, shortages in both funding and cyber talent continue to exist. Based on our 2018 study responses, CISOs overwhelmingly agree

FIGURE 1

Since 2010, CISOs have been challenged by insufficient funding and cyber talent availability

Identify the top barriers that your state faces in addressing cybersecurity challenges (top three per study).



Source: 2010 through 2018 Deloitte-NASCIO Cybersecurity Studies.

that, while they have obtained senior executive support, they continue to be challenged by inadequate funding, struggling to secure a sufficient, reliable budget to develop their statewide security program. In most states, the CISO's only source of cybersecurity funding is derived from the state's IT budget, and is not designated as a separate line item. And the percentage of state enterprise IT budgets allocated to enterprise cybersecurity is still 1–2 percent, and annual budget increases have not kept pace with the needs of today's security landscape and tomorrow's evolving challenges.

On the talent front, our survey finds that cybersecurity staffing has once again emerged as a top barrier that states face in addressing cybersecurity challenges. In particular, hiring, retention, and the competency gap continue to be concerns. Though the states' professional cybersecurity workforce has experienced slow growth since 2010, salary and paygrade structures, as well as competition from the private sector and the federal government, continue to hinder hiring and retention. State CISOs

are taking action to improve the situation, documenting job descriptions and classifications and providing training, certification, and leadership programs to help attract and retain talent and close the competency gap. But these measures are not enough. Consider how the states stack up against typical financial services institutions (figure 2) from as far back as 2010.

CISOs need bold plays to accelerate change

To break through these long-standing resource and funding roadblocks, CISOs should look to disrupt the status quo by pursuing three bold plays that could help states make progress and close the widening gap with many federal agencies and commercial industries.

BOLD PLAY NO. 1: ADVOCATE FOR DEDICATED CYBER PROGRAM FUNDING

Nearly half of all US states do not have a cybersecurity budget line item. On the other hand, federal government agencies report cybersecurity funding in the president's budget

FIGURE 2

Current cyber FTE averages for states still fall below the average number of cyber FTEs employed by financial services institutions in 2010

How many dedicated cybersecurity professionals does your enterprise security office employ?



* Financial services institutions similar in size to an average state.

Source: 2010 Deloitte-NASCIO Cybersecurity Study; 2010 Deloitte Global Financial Services Industry (GFSI) Study; 2018 Deloitte-NASCIO Cybersecurity Study.

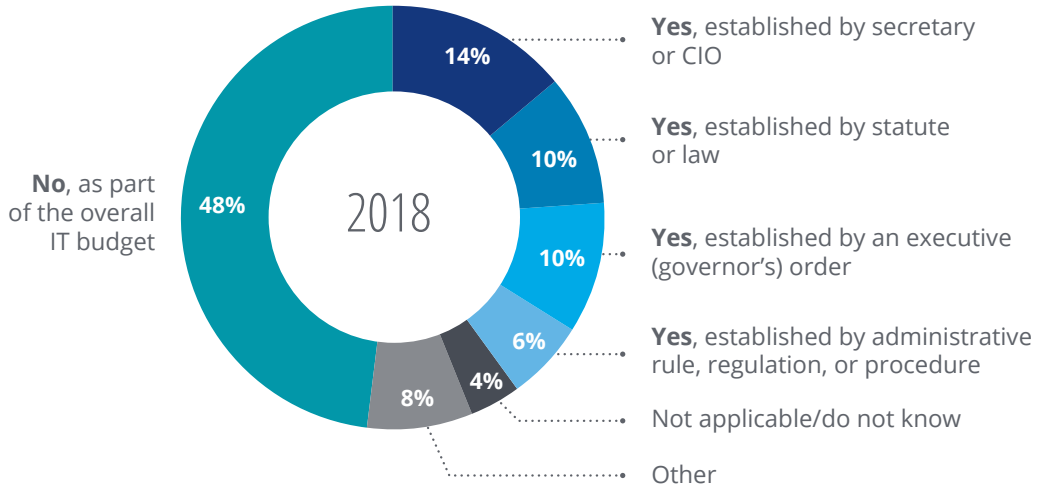
as a portion of their overall IT spending. In fiscal year 2019, the cybersecurity budget for all federal agencies, excluding the Department of Defense, totals about US\$8 billion

(we excluded military agency budgets from this figure because the defensive and offensive spend for national security is likely not as relevant to state governments' mission).¹ Federal

FIGURE 3

Almost half of states do not have a separate budget line item for cybersecurity

Does your state have a cybersecurity budget line item? (50 respondents)

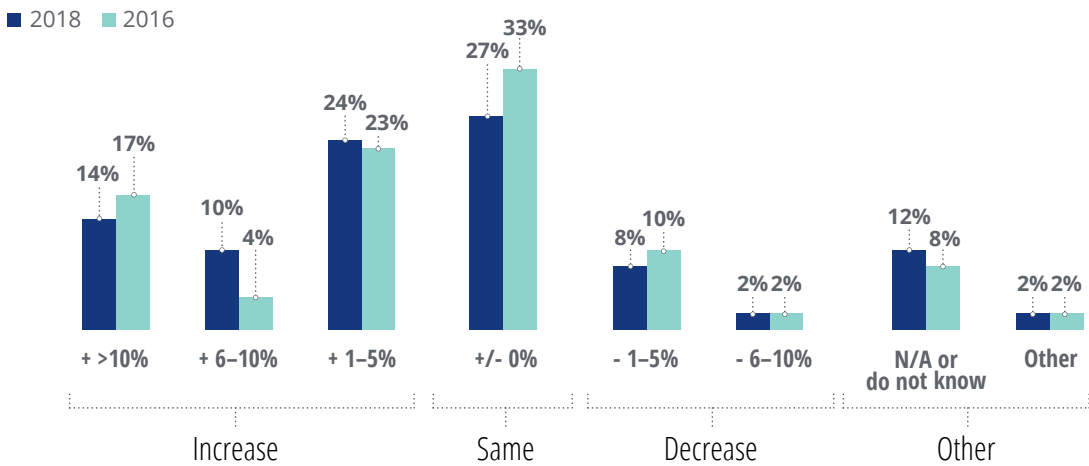


Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 4

CISO budgets are growing slowly; compared to 2016, only an additional two states have reported a budget increase

Characterize the year-over-year trending in your state's cybersecurity budget for years 2016 and 2017. (49 respondents)



Source: 2018 Deloitte-NASCIO Cybersecurity Study.

civilian cybersecurity budgets have increased more year over year than state cybersecurity budget allocations. According to Forrester's directional data from its 2017 benchmark, private US industries spent an average of 28 percent of their IT budget on security technologies.²

The figure below shows actual spending by large federal agencies that perform similar functions and their year-over-year differences

in cybersecurity spending. These figures contrast with those of many states, which typically spend between 1 percent and 2 percent of their IT budget on cybersecurity.






These comparisons reinforce the need for urgent action by states. Two goals CISOs can pursue are:

- **Make cybersecurity a budget line item.** CISOs should strive to establish a dedicated budget line item for cybersecurity

FIGURE 5

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

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

			2017	2018	2019
	Department of Transportation	Percentage of IT budget	4.48%	5.10%	5.63%
		Year-over-year increase	N/A	13.76%	10.54%
	Health and Human Services	Percentage of IT budget	5.45%	5.44%	6.44%
		Year-over-year increase	N/A	-0.15%	18.50%
	Social Security	Percentage of IT budget	8.59%	10.94%	11.40%
		Year-over-year increase	N/A	27.34%	4.21%
	Treasury	Percentage of IT budget	10.78%	11.67%	10.82%
		Year-over-year increase	N/A	8.17%	-7.23%
	Justice	Percentage of IT budget	27.08%	25.24%	25.07%
		Year-over-year increase	N/A	-6.79%	-0.67%

Source: US Government Publishing Office, "Cybersecurity funding," *An American budget: Analytical perspectives, Budget of the US government*, 2018, pp. 273–288.

as a subset of the overall technology budget. While the percentage of state IT spending on cybersecurity may be much lower than that of private sector industry and federal agency enterprises of similar size, the line item can help state CISOs and CIOs give the state legislature and executive branch leaders the right level of visibility into state cybersecurity expenses in an effort to raise funding levels. State legislation could demand visibility into cyber budgets at both the state and individual agency levels. In addition, our 2018 survey results indicate that federal and state cybersecurity mandates, legislation, and standards with funding assistance result in more dramatic progress than those that are unfunded.

- **Advocate for and demand funding from large federal agencies to implement their security requirements and controls.** This approach has been successful in areas other than cybersecurity, such as for programs for health, human services, and law enforcement and justice.

Funding mechanisms for these programs can provide a model for CISOs to emulate in acquiring new funding streams outside their traditional allocation in shrinking state-level technology budgets. For example, state Health and Human Services (HHS) agencies were able to secure funding from the federal Centers for Medicare and Medicaid Services (CMS) to establish CMS’s suggested Minimum Acceptable Risk Safeguards (MARS) for systems that consume Medicare and Medicaid data. This allowed state HHS agencies to leverage an additional source of external funding separate from the state IT budget.³ Our survey data demonstrates that regulations and requirements with funding are more effective (figure 6).

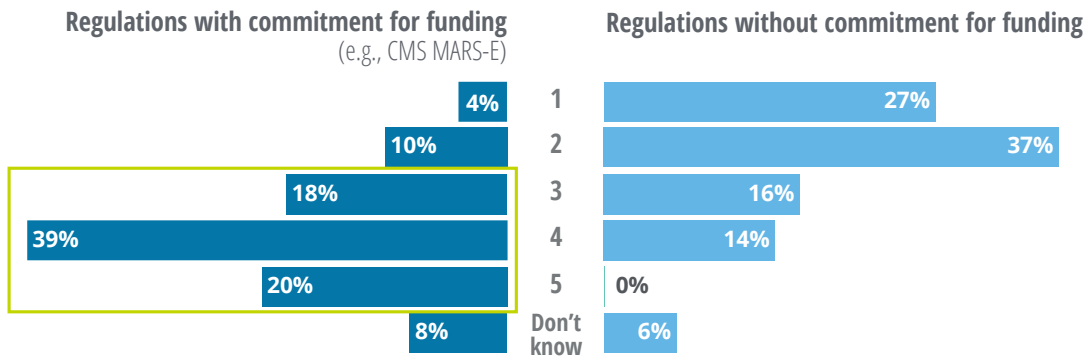
BOLD PLAY NO. 2: CISOs AS AN ENabler OF INNOVATION, NOT A BARRIER

An integral part of being a cyber leader is the imperative to guide states in embracing technology innovations securely. CISOs should be at the forefront of the

FIGURE 6

Cybersecurity initiatives can be more effective with committed funding

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) (49 respondents)



Source: 2018 Deloitte-NASCIO Cybersecurity Study.

“**Fourth Industrial Revolution**”—digital disruption through emerging technologies such as artificial intelligence, the Internet of Things (IoT), and smart government. The 2014 Deloitte-NASCIO Cybersecurity Study encouraged CIOs to engage CISOs in identifying creative ways to include cybersecurity as a critical part of modernization efforts such as cloud computing and mobile technologies. Yet in this year’s survey, emerging technology initiatives in areas such as IoT, artificial intelligence, smart enterprises (smart cities), and blockchain technology rank at the bottom of the CISO initiative list, indicating that they may not yet be a priority for CISOs. To take on emerging technologies, CISOs should actively participate with state CIOs in shaping the innovation agenda, collaborate with state digital and innovation officers, and lead the charge to help program leaders embrace and securely adopt new technologies.

Being at the forefront of program and business innovation may afford the CISOs more

opportunities to collaborate with other leaders to gain their support to advance cyber risk programs. Such early involvement can also help identify whether cybersecurity is baked into new applications of emerging technologies, technology evaluations, and procurements.

BOLD PLAY NO. 3: TEAM WITH THE PRIVATE SECTOR AND HIGHER EDUCATION

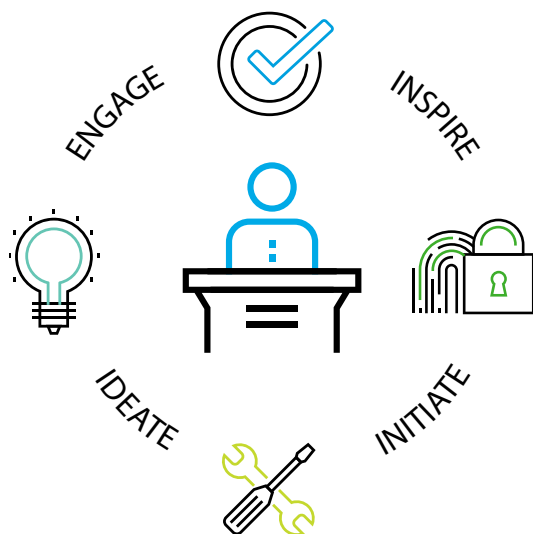
The enduring cybersecurity talent shortage and a persistent competency gap in the available talent require CISOs to cast a wider net for the right people to staff their teams. To address the talent shortage, CISOs can make use of public-private partnerships, developing contracting models with assured service levels for certain cybersecurity functions and competencies.

According to the Deloitte-NASCIO Cybersecurity Study data from 2010 through 2018, CISOs have increased their use of outsourcing by two- to three-fold for certain functions, including cybersecurity risk assessments, audit log analysis, and threat management and monitoring. However, more than half of US states still do not outsource these functions. Doing so can be a significant opportunity as states continue to struggle with hiring and retaining qualified security staff.

State CISOs should work to understand and define the cybersecurity functions that can be delivered by their state workforce, and then forge long-term partnerships with the private sector for their remaining cybersecurity functions and competencies, with continual improvement and service level expectations. Many state CIOs had to follow a similar strategy when it came to data centers, networking, and telecommunications services—managing con-

FIGURE 7

CISOs as innovators



tracts as service owners rather than delivering the capabilities with only the state technology workforce.

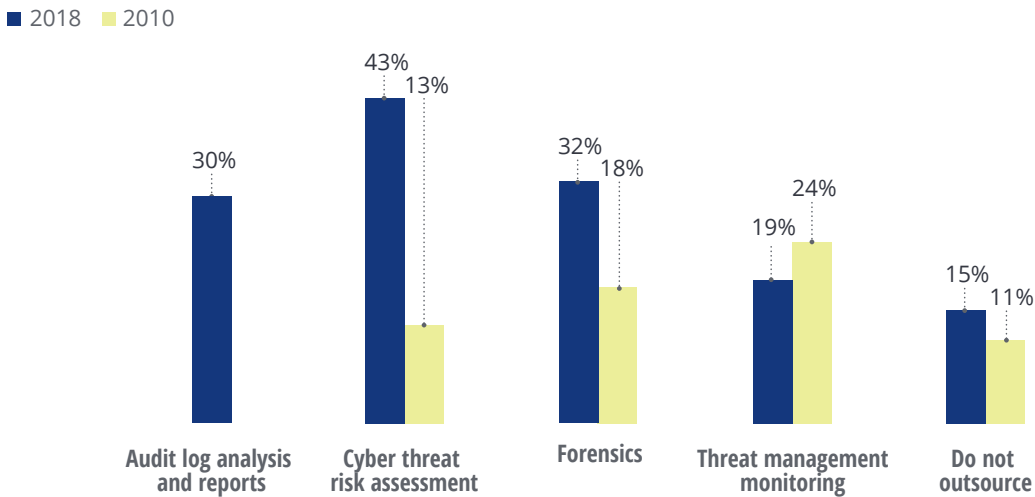
CISOs can also leverage partnerships with local colleges and universities to provide a pipeline of new talent through internships,

co-ops, and apprenticeship programs. To help combat the competency gap, CISOs can establish a network among state and local agencies, academia, and corporations to share threat information, capabilities, and contracts to strengthen state cyber defenses.

FIGURE 8

While outsourcing has increased for certain functions, more than half of US states have yet to outsource many of them

Select the cybersecurity functions that your state outsources. (47 respondents)



Source: 2010 and 2018 Deloitte-NASCIO Cybersecurity Studies.

BOLD PLAYS FOR CHANGE



ADVOCATE FOR DEDICATED CYBER PROGRAM FUNDING

CISOs should raise cybersecurity's visibility with the state legislature and executive branch by making it a line item in the IT budget. They can also seek funding from federal agencies to support compliance with those agencies' security mandates.



CISOs AS AN ENABLER OF INNOVATION, NOT A BARRIER



CISOs should actively participate in shaping the state's innovation agenda, collaborate with state digital and innovation officers, and lead the charge to help program leaders securely adopt new technologies.



TEAM WITH THE PRIVATE SECTOR AND HIGHER EDUCATION

CISOs should leverage 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.



Survey data analysis

In the following section, we take a detailed look at the survey findings.

Cyber risk strategy and governance

CISOs have made progress in establishing a solid position among the state executive leadership team. In more than 31 states, the CISOs' authority is now set by legislation, the state secretary, or CIO, rather than by administrative rule, executive order, or interagency agreement. The vast majority of CISOs (90 percent) have extended their scope of authority beyond their own agency to align with all executive agencies in their state government.

CISOs have improved the frequency of communications with the governor and legislature and also increased their frequency of engagement with business and technology

Despite the progress they have made, CISOs still face many barriers to fulfilling their cybersecurity responsibilities.

leaders. A fifth of state respondents say they report monthly to the governor, and a third report monthly to the state secretary or deputy

secretary. Monthly reporting to business stakeholders has also increased to 25 percent in 2018 from 10 percent in 2016.

In another sign of the maturation of the CISOs' role, most states now have documented and approved governance plans—40 states in 2018, compared to 29 states in 2016. However, they still lag in the documentation and approval of cybersecurity strategies. Though 44 states engaged both business and technology stakeholders to provide inputs to their state cybersecurity strategy, 33 state CISOs continue to indicate that state executives' commitment to improve the state's cybersecurity posture does not translate into improved cybersecurity funding.

Despite the progress they have made, CISOs still face many barriers to fulfilling their cybersecurity responsibilities. The biggest barrier reported in 2018 is lack of sufficient cybersecurity budget. Second among this year's top barriers is inadequate cybersecurity staffing. As in 2016, the growing sophistication of threats was the third top barrier.

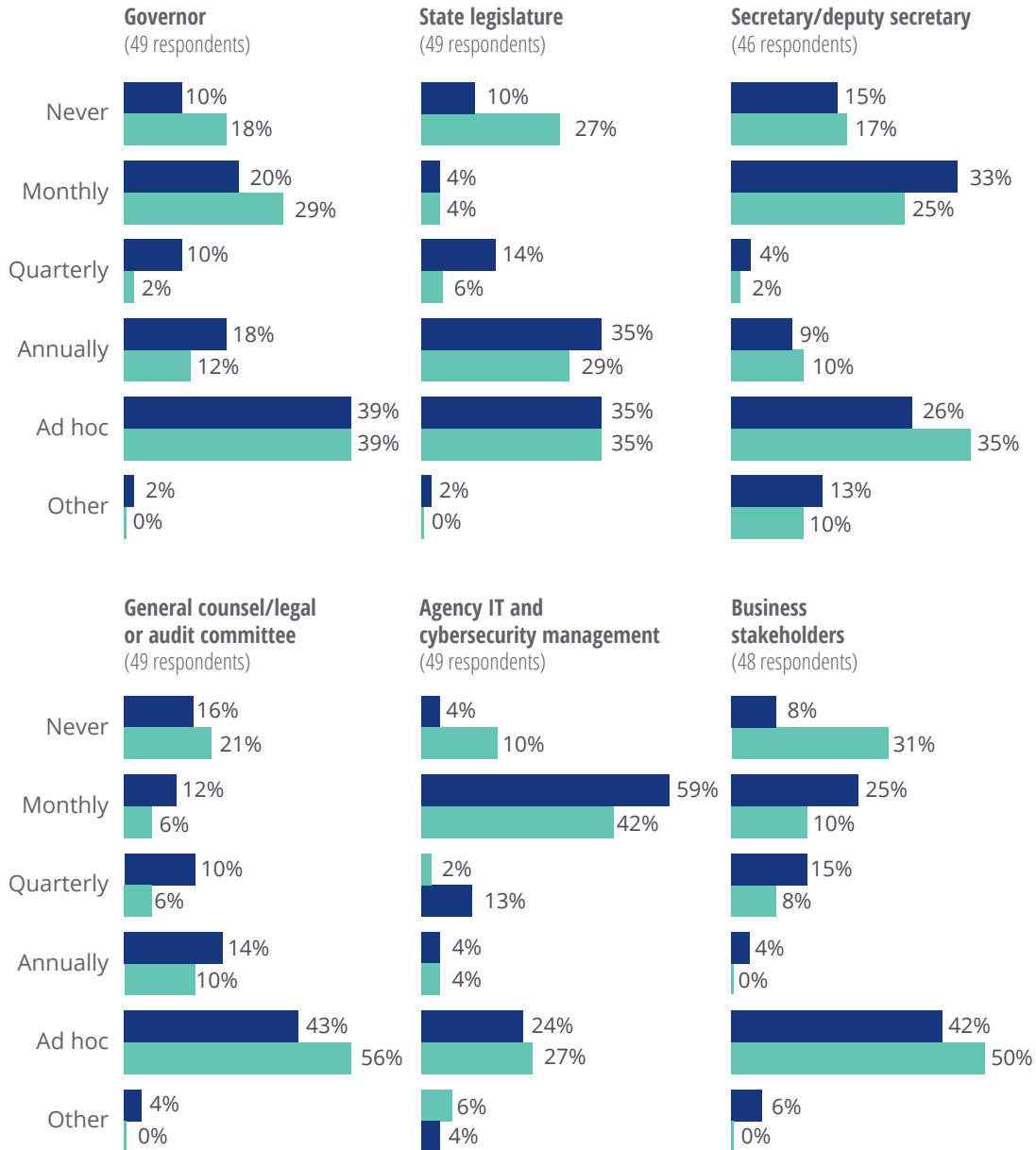
In the area of privacy, more states than in previous surveys report having a chief privacy officer (CPO). In 2018, more than a quarter of states have one, compared to less than a fifth in 2016.

FIGURE 9

CISOs have established a frequent reporting cadence to state leadership

To what extent are you required to provide reports on cybersecurity status or posture of the enterprise to the following positions?

■ 2018 ■ 2016



Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 10

Nine out of 10 states now have a documented cybersecurity strategy and governance plan

Does your state maintain the following strategy artifacts? (50 respondents)

		Documented/ approved	Documented but not approved	Within the next 12 months
Cybersecurity strategy	2018	68%	22%	10%
	2016	67%	14%	18%
Governance for cybersecurity <small>(i.e., defined responsibilities, policies, standards, and procedures)</small>	2018	80%	10%	10%
	2016	58%	21%	21%

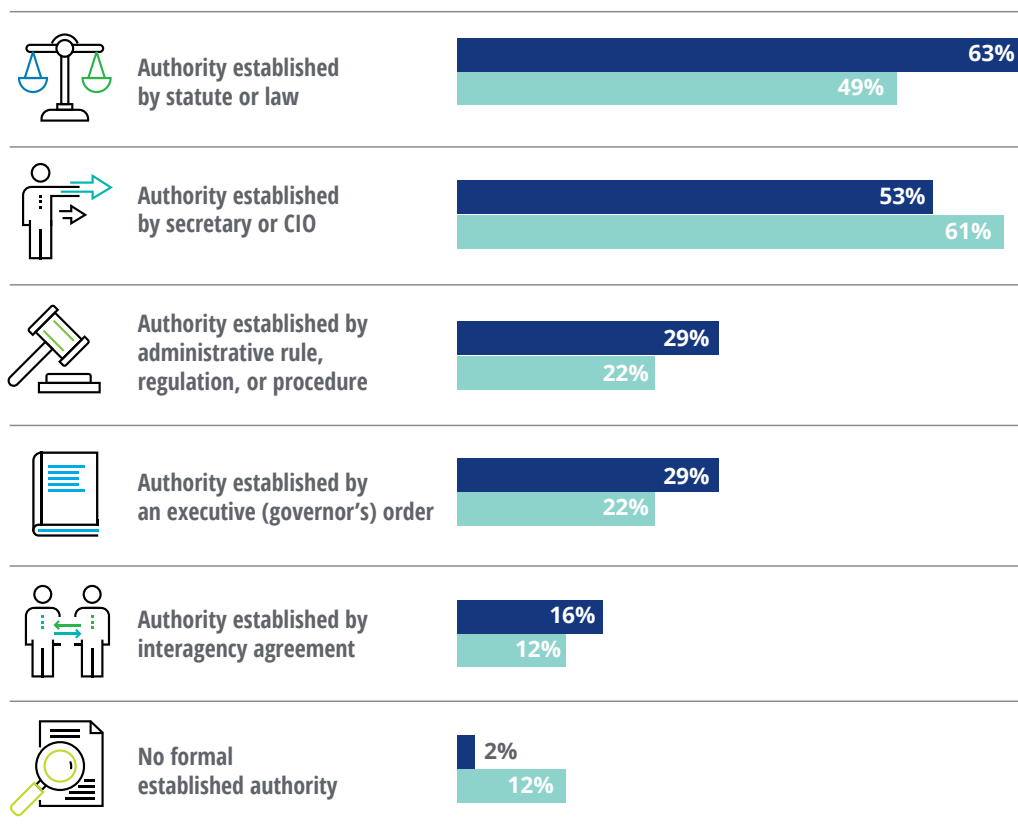
Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 11

The CISO's role is firmly established, increasingly through legislation

What mechanism establishes your state's CISO or equivalent position's authority over the other organizational entities for which it has responsibility? (49 respondents)

■ 2018 ■ 2016

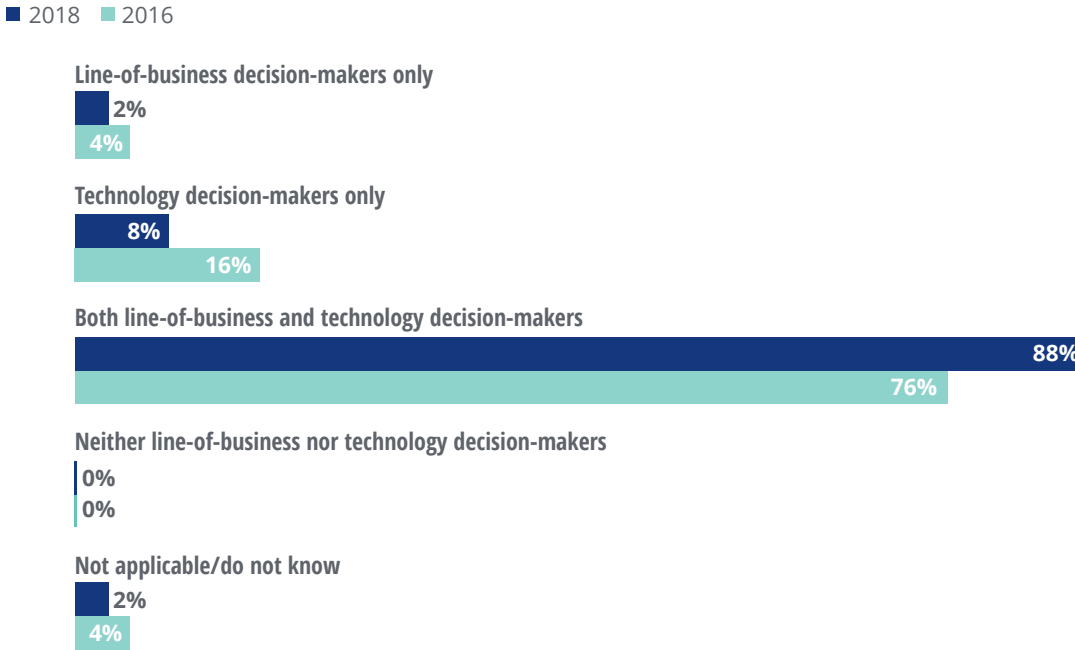


Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 12

Both business stakeholders and technology decision-makers are more actively engaged in defining their state cybersecurity strategy

Does your state actively engage both business stakeholders (agency directors/commissioners/secretaries) and technology decision-makers in identifying requirements for the state's cybersecurity strategy? (50 respondents)

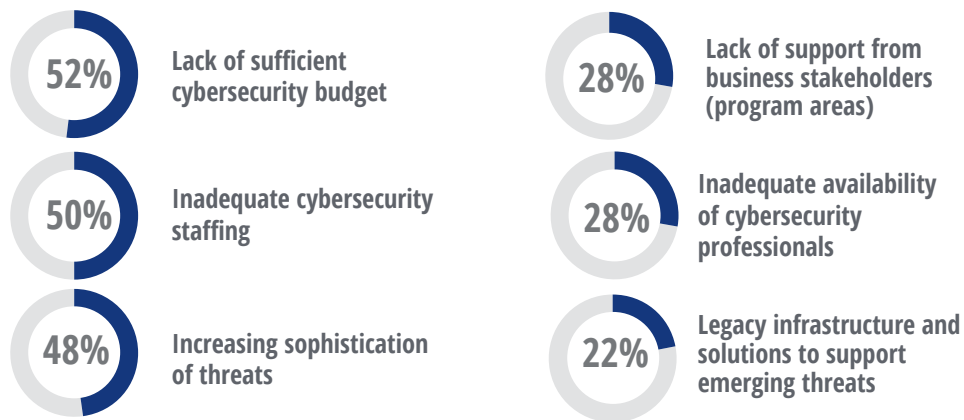


Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 13

Budget and staffing remain top barriers to an effective cyber program

Identify the top five barriers that your state faces in addressing cybersecurity challenges. (50 respondents)



Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 14

The majority of states do not have an enterprise chief privacy officer (CPO)

Does your state have an enterprise-level chief privacy officer? (50 respondents)

■ 2018 ■ 2016



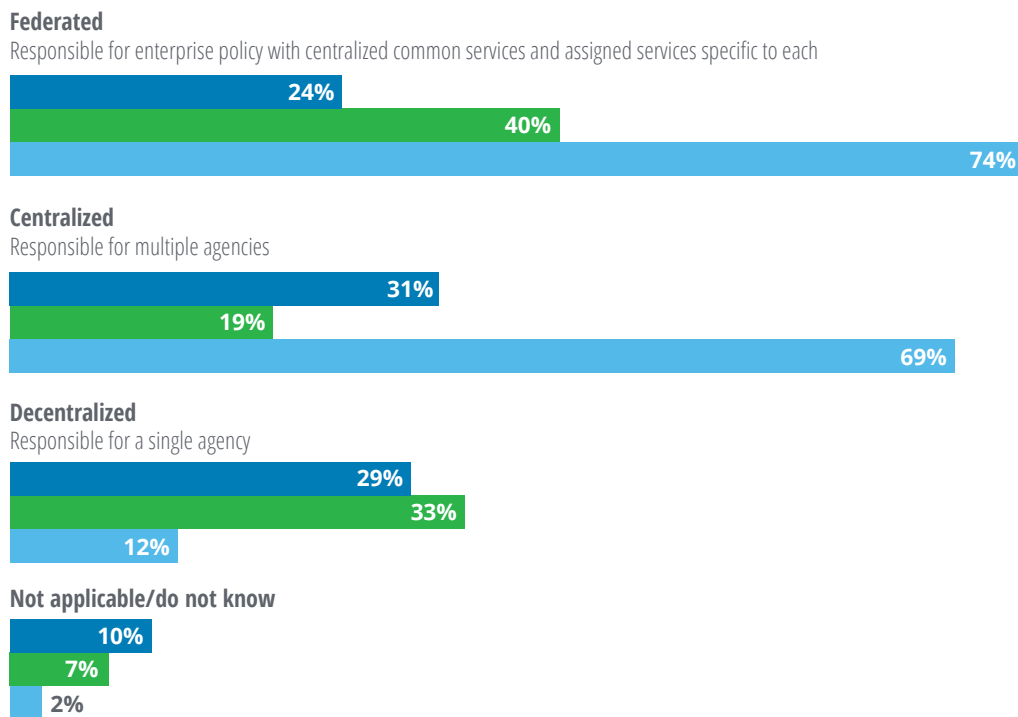
Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 15

Privacy and risk functions should look to CISOs' security models to establish their enterprise authority

How are your state's cybersecurity and privacy functions structured? (42 respondents)

■ Risk function ■ Privacy function ■ Security function



Source: 2018 Deloitte-NASCIO Cybersecurity Study.

Budget

State CISOs rely primarily on the state's IT budget to provide them with the required funding. However, 20 states have established a separate cybersecurity budget line item. Only 10 states have a separate source of funding for cybersecurity.

Some CISO budgets are growing, albeit slowly. Compared to 2016, an additional two states have reported an increase in the budget. Yet 19 states continue to see no growth or a reduction in their cybersecurity budget. In stark contrast to the federal agencies and US industries noted earlier in the report, many states

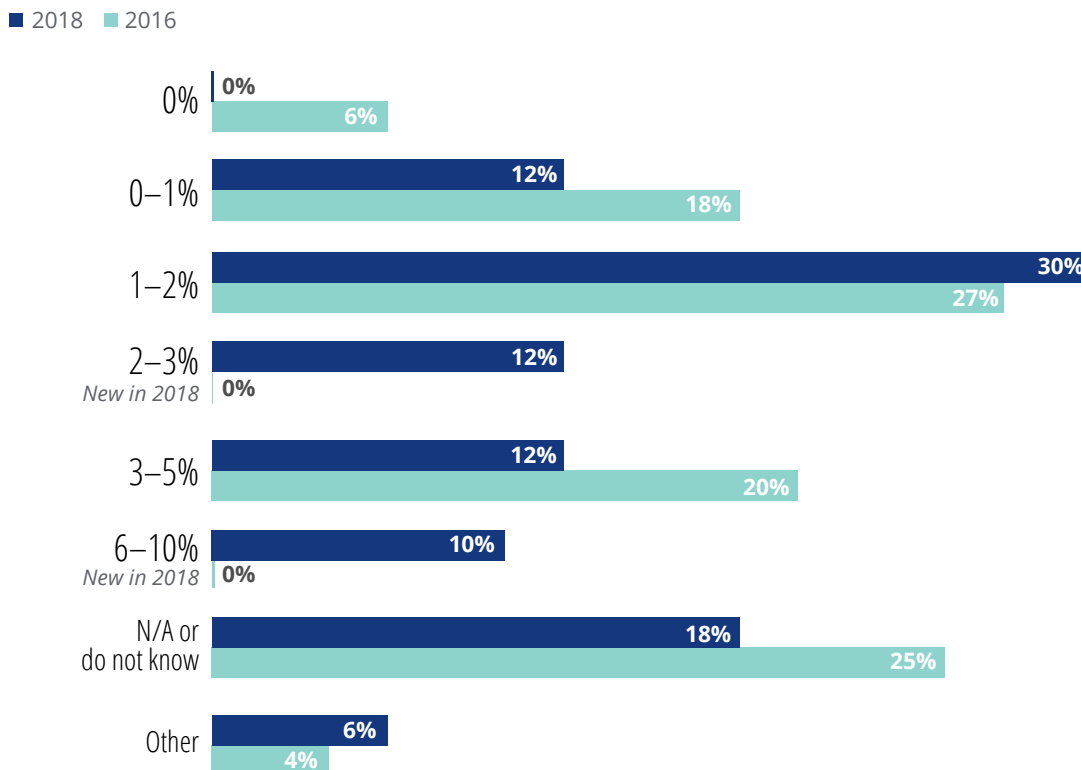
(27) receive less than 3 percent of their state's IT budget for cybersecurity.

More than two-thirds of the CISOs in our survey indicate that threat monitoring—audit logging, threat intelligence, and security operations centers—are leading functions covered by the cybersecurity budget, followed by cybersecurity strategy and risk management. Compared to 2016, an additional 15 states indicated that their cybersecurity budget included a security operations center (SOC). Only seven CISOs indicated that physical security, election security, and critical infrastructure protection are part of their cybersecurity budget.

FIGURE 16

Most states indicate that their cybersecurity budget is now 1 to 3 percent of their total IT budget

What percent of your state's enterprise IT budget is allocated to enterprise cybersecurity (all executive branch agencies)? (50 respondents)

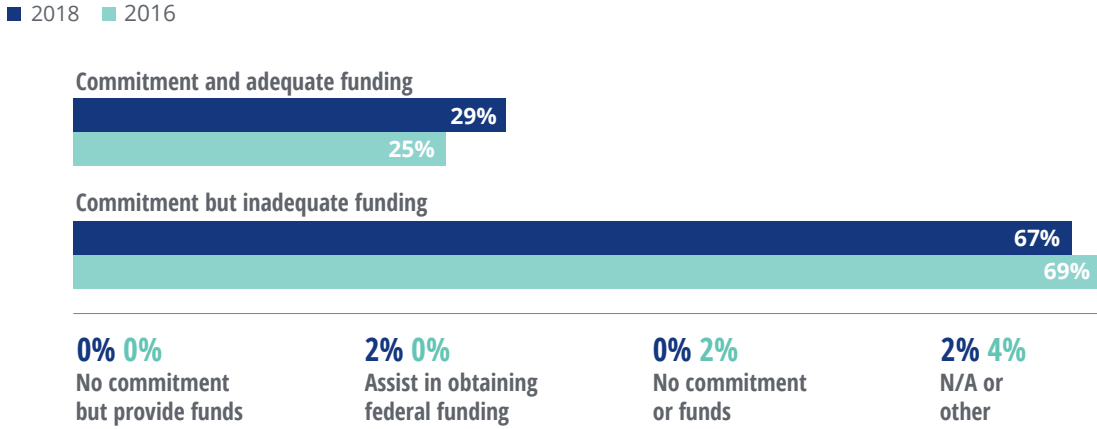


Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 17

CISOs have executive commitment, but funding challenges persist

Which of the following best describes the state of senior executive support (governor's office, agency secretary, or CIO)? (49 respondents)



Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 18

CISOs overwhelmingly indicate that threat monitoring (audit logging, threat intelligence, and security operations center) is the top function covered by the cybersecurity budget

Which of the following are covered under your state's cybersecurity budget? (50 respondents)



* Security information and event management

Source: 2018 Deloitte-NASCIO Cybersecurity Study.

Cybersecurity workforce

States have made little progress in increasing their cybersecurity workforce. Compared to 2016, only four states have added staffing. Some 30 state CISOs continue to acknowledge that they face a cyber competency gap. To address the talent shortage, some—less than half—of surveyed CISOs turn to outsourcing, while 20 state CISOs also attempt to impart specialized cybersecurity training to their workforce. Cyber threat risk assessments, 24 x 7 SOCs, and forensics are the top functions that states outsource.

Salary structure, competing private sector jobs, and a lack of qualified candidates influence the long hiring process. In addition, our survey finds that many states do not have properly documented cybersecurity competencies, which can make it harder to establish appropriate cyber career paths.

State salaries, paygrades, and pay structures still fall behind those of private-sector counterparts, leading to the attrition of experienced state employees to the private sector. To counter this, states must proactively work to retain and develop employees and offer them competitive salaries and benefits to achieve success in the long term.

FIGURE 19

Most enterprise CISOs still have a small cybersecurity team

How many dedicated cybersecurity professionals does your enterprise security office employ? (49 respondents)

- 1–5 full-time equivalents
- 6–15 full-time equivalents
- 16–25 full-time equivalents
- 26–50 full-time equivalents
- > 51 full-time equivalents



Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 20

Even with the addition of staff augmentation, overall enterprise cybersecurity team size is small

If your state has staff/specialist augmentation, indicate the number of cybersecurity professional contractors employed. (48 respondents)



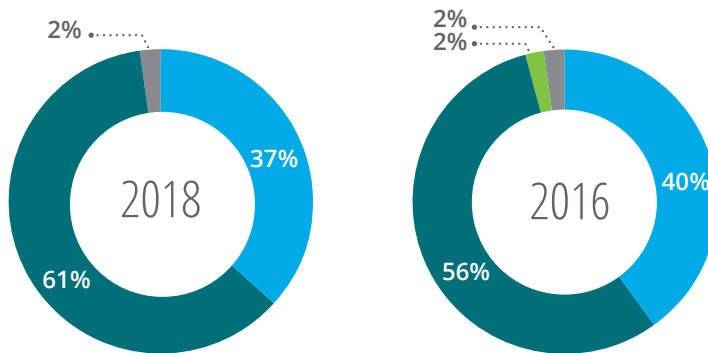
Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 21

Thirty state CISOs acknowledge that they face a cyber competency gap—an increase from 2016

Do your internal cybersecurity professionals have the required competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements? (49 respondents)

- Staff has the required competencies
- Staff has gap in competencies
- Not applicable/do not know
- Other



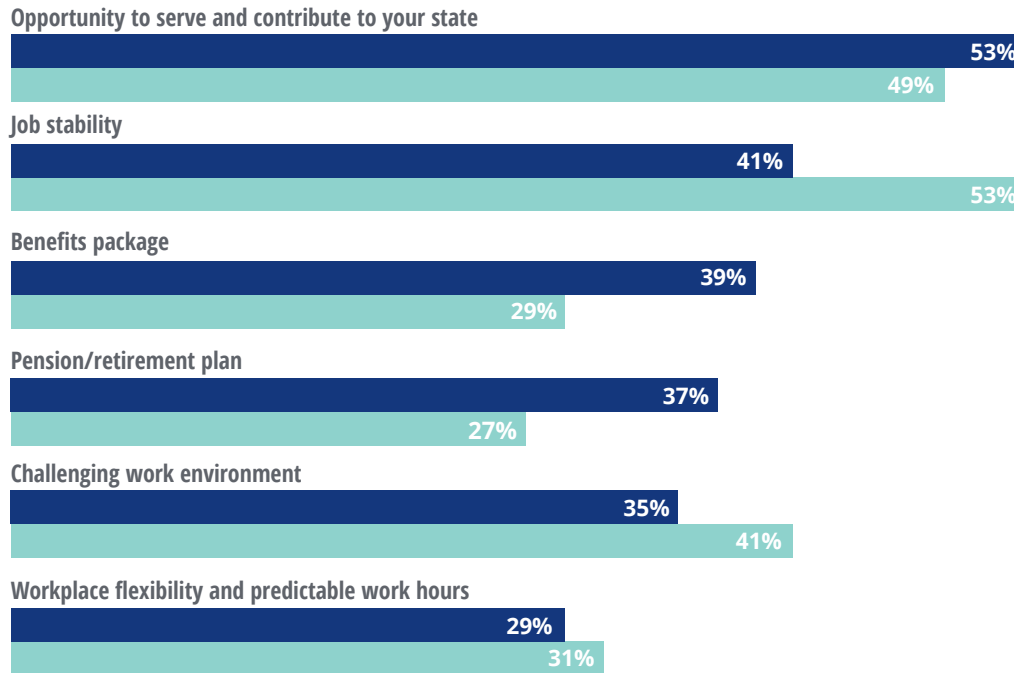
Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 22

Most states promote the opportunity to serve along with benefit and retirement packages to attract and retain cybersecurity talent

What are the top three factors in attracting and retaining cybersecurity talent to work for your state? (49 respondents)

■ 2018 ■ 2016



Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 23

State salaries, paygrades, and structure still fall behind what the private sector offers

What are the top three human resource factors that negatively impact your ability to develop, support, and maintain the cybersecurity workforce within your state? (49 respondents)

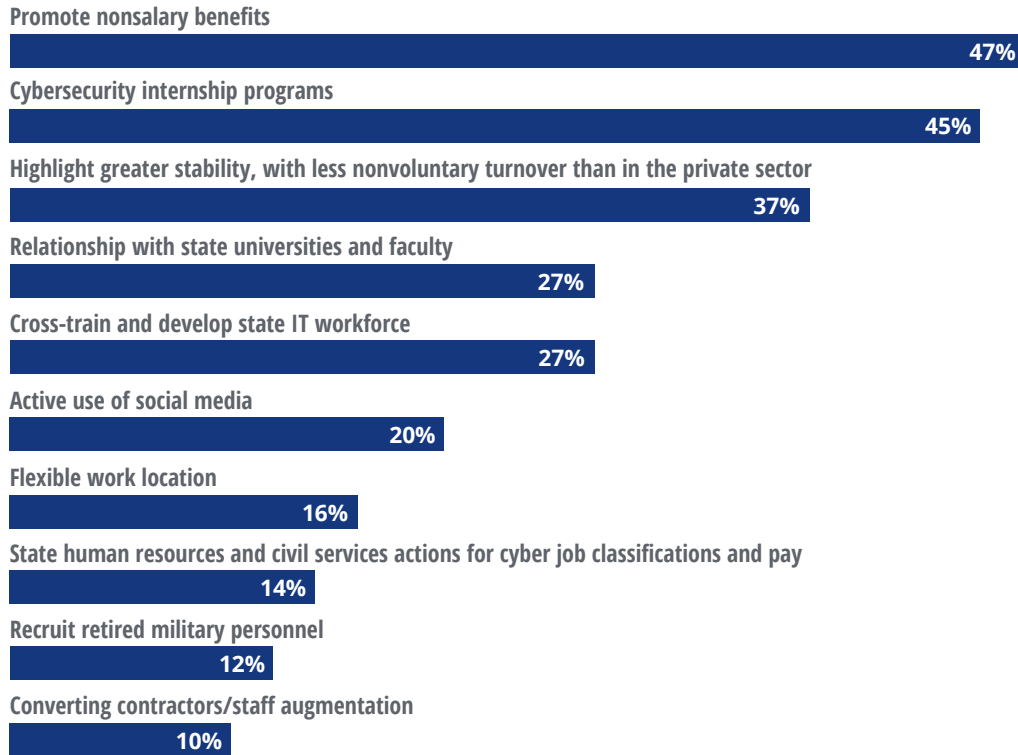
- 94%** State's salary rates and paygrade structures
- 51%** Workforce leaving for private sector careers
- 47%** Lack of qualified candidates due to demand from federal agencies and private sector
- 24%** Work location—lack of qualified cyber workforce in the state capital
- 18%** Outdated classifications and job descriptions for cybersecurity positions
- 12%** Lack of a defined career path and opportunities in cybersecurity
- 12%** Lengthy hiring process

Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 24

States continue to promote nonsalary benefits and greater stability as factors to attract and retain cybersecurity talent

Identify the top three talent management practices followed by your state to attract and retain the state cybersecurity workforce. (49 respondents)

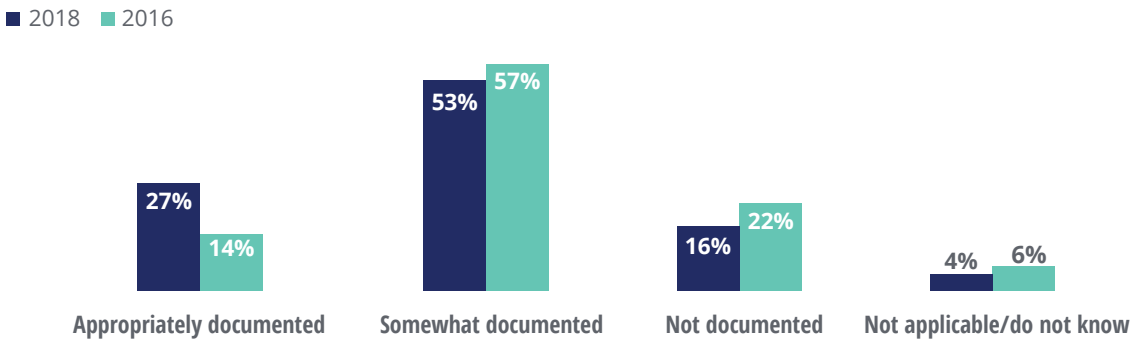


Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 25

Only a quarter of states have appropriately documented cybersecurity competencies

To what extent has your state's human resources function documented the required cybersecurity competencies as part of the job description/classification? (49 respondents)



Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

Cybersecurity operations

When asked about the effectiveness of federal and state cybersecurity regulations, more than half of surveyed CISOs responded that regulations that come with funding are more effective than regulations without a funding commitment (figure 6). Indeed, 29 state CISOs agreed that regulations are most effective when provided with appropriate funding (CMS Minimum Acceptable Risk Safeguards for Exchanges (MARS-E), for instance). Some 30 state CISOs also indicated that their states lack a cybersecurity legislative council to periodically review and steer their state's cybersecurity posture and allocate appropriate funding.

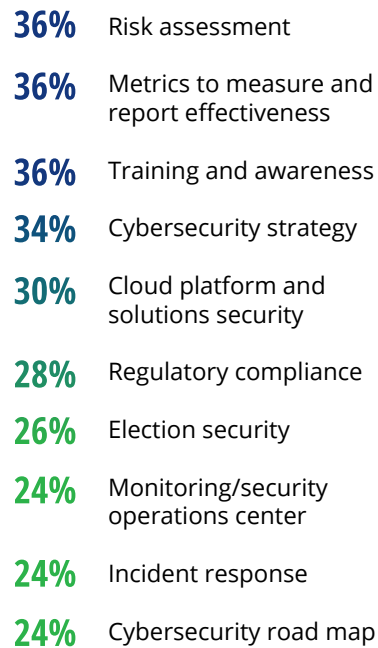
Despite funding issues, the vast majority of CISOs do comply with important federal and state regulations. The five regulations or regulatory bodies that all states have to comply with remain unchanged since 2016: the Internal Revenue Service (IRS), the Criminal Justice Information Service (CJIS), the Health Insurance Portability and Accountability Act (HIPAA), the Centers for Medicaid and Medicare Services (CMS), and the Social Security Administration.

Strategic and emerging cybersecurity issues are rising as CISO priorities while operational issues are declining, presumably as CISOs have gained greater control over them. CISOs report that their top cybersecurity initiatives for 2018–2019 include training and awareness, metrics to measure and report the status of cybersecurity, risk assessment, and strategy. The study also shows growing attention to strategic emerging issues—including election and cloud platform security—which are ranked high among CISOs' priorities. Meanwhile, initia-

FIGURE 26

Risk assessment, metrics, training, strategy, and cloud security top the list of 2018/2019 cybersecurity initiatives

Identify your state's top five cybersecurity initiatives for 2018/2019. (50 respondents)



Source: 2018 Deloitte-NASCIO Cybersecurity Study.

tives declining in priority include monitoring and SOCs, operationalization of cybersecurity, governance, disaster recovery, and data protection. CIOs and CISOs should deliberately align operational technical cyber responsibilities—for monitoring, SOC, disaster recovery, and data protection—if CISOs wish to succeed in elevating their role to that of a state cyber risk managerial function.

Further evidence of CISOs' growing proficiency includes an increase in delivering cybersecurity awareness training and regular assessments of top security threats. Awareness training for state employees and contractors, at least annually, is now the established model in

the vast majority of states—94 percent in 2018 compared to 84 percent in 2016. In addition, CISOs are conducting more regular assessments of key threats, reporting a dramatic rise since 2016 in monthly assessments for Web applications, the top threat experienced by CISOs this year. CISOs still have room to improve for threat assessments that are being performed on an ad hoc or yearly basis. Among threats that were experienced over the last 12 months, CISOs report that Web applications were the top target, yet only 19 states perform application security testing on a quarterly or monthly basis.

Security threats and confidence in third parties

Despite budgetary challenges, CISOs have gained confidence since 2016 in their ability to

protect against threats and to monitor third-party cybersecurity practices. However, more than 25 percent of surveyed CISOs are not confident in protecting against Web applications and emerging technologies such as cloud solutions and IoT.

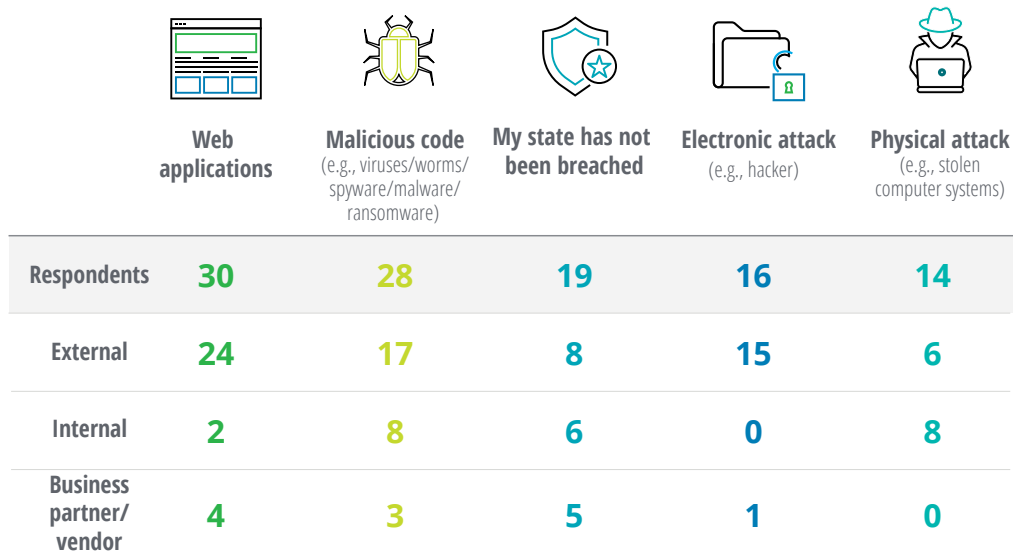
Many CISOs indicated that they plan to focus cybersecurity awareness training on helping to address the top three threats they identified: phishing, social engineering, and ransomware. Meanwhile, CISOs’ confidence that state assets are protected against threats, including those generated internally and externally, has shifted from “not very” confident in 2016 to “somewhat” and “very confident” in 2018.

More states have increased security over third parties, improving their oversight of cybersecurity capabilities, controls, and agency

FIGURE 27

Web applications and malicious code are the leading sources of security breaches

In terms of security breaches over the past 12 months, which of the following applies to your state?



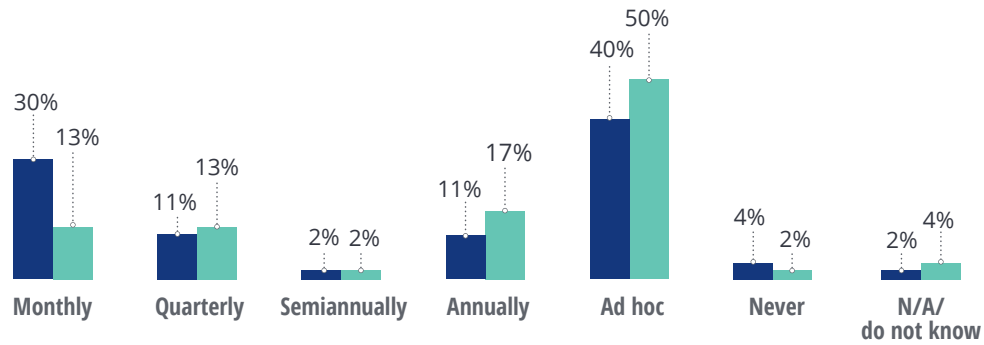
Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 28

States have improved the frequency of application security testing

How often does your state perform application security vulnerability testing and code review?
(47 respondents)

■ 2018 ■ 2016



Source: 2016 and 2018 Deloitte-NASCI0 Cybersecurity Studies.

dependencies. The percentage of state respondents that have identified and assessed these third parties—including contractors, service providers, and business partners—rose to 31 percent in 2018 from 18 percent in 2016. But still, only 23 percent of the respondents review these third-party services regularly.

Our 2018 survey results show a small increase since 2016 in the two top methods of

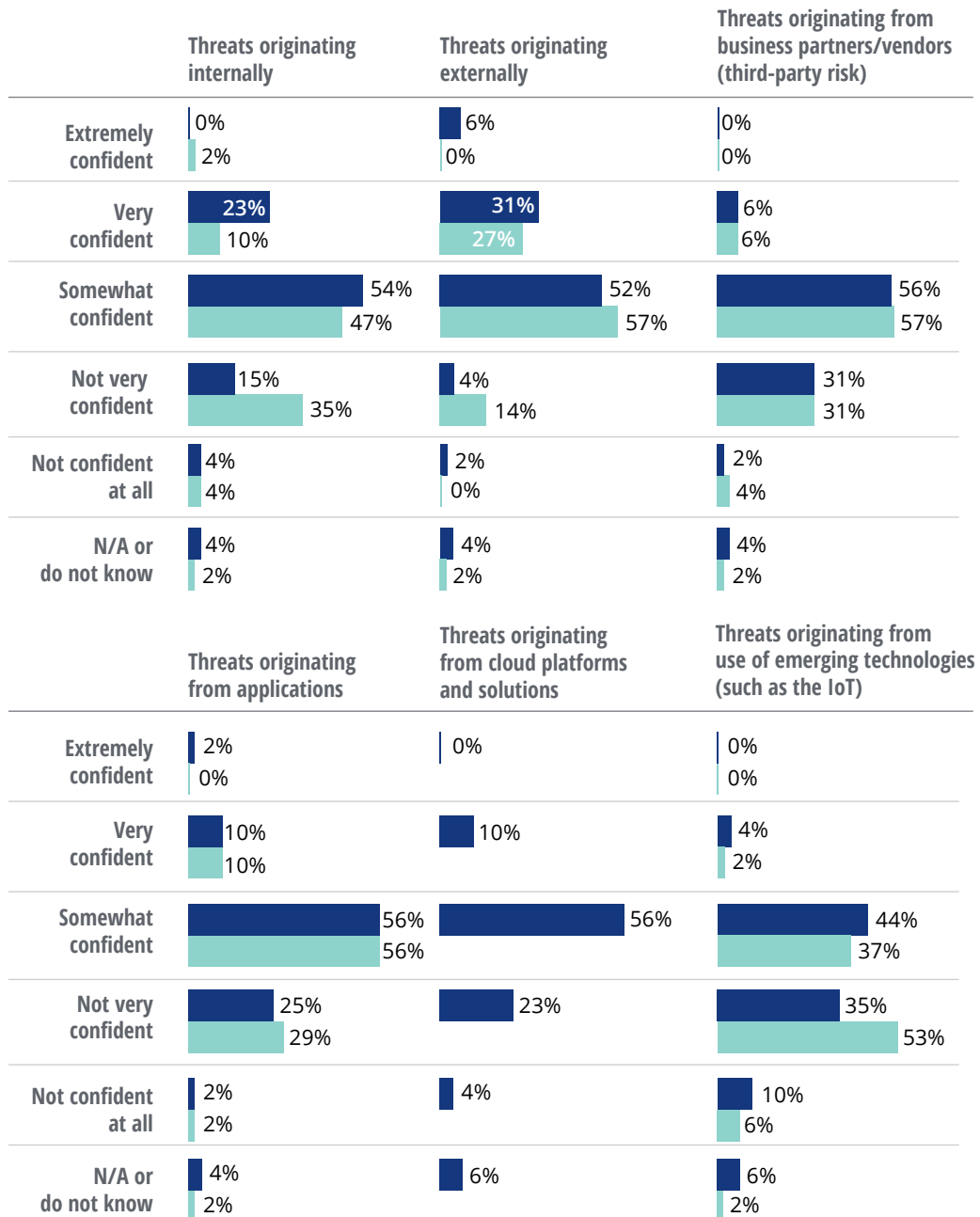
managing the adequacy of third-party cybersecurity practices. More states now monitor and control third-party access to their systems and data and require some form of independent attestation, which can include a Statement on Standards for Attestation Engagements (SSAE) 18, Payment Card Industry Data Security Standard (PCI DSS), and the like.

FIGURE 29

CISOs' confidence level has improved in protecting against external threats

Please indicate your level of confidence that your state's information assets are protected from cyber threats. (48 respondents)

■ 2018 ■ 2016



Note: Cloud platforms and solutions were not broken out separately in the 2016 survey.

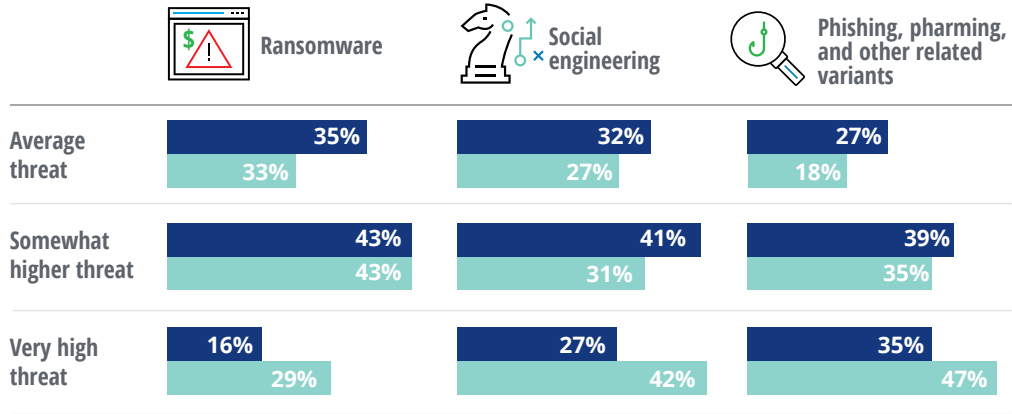
Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 30

Ransomware, social engineering, and phishing are the top cyber threats for states

Please choose the prevalence of the following cyber threats in your state for the next year. (49 respondents)

■ 2018 ■ 2016



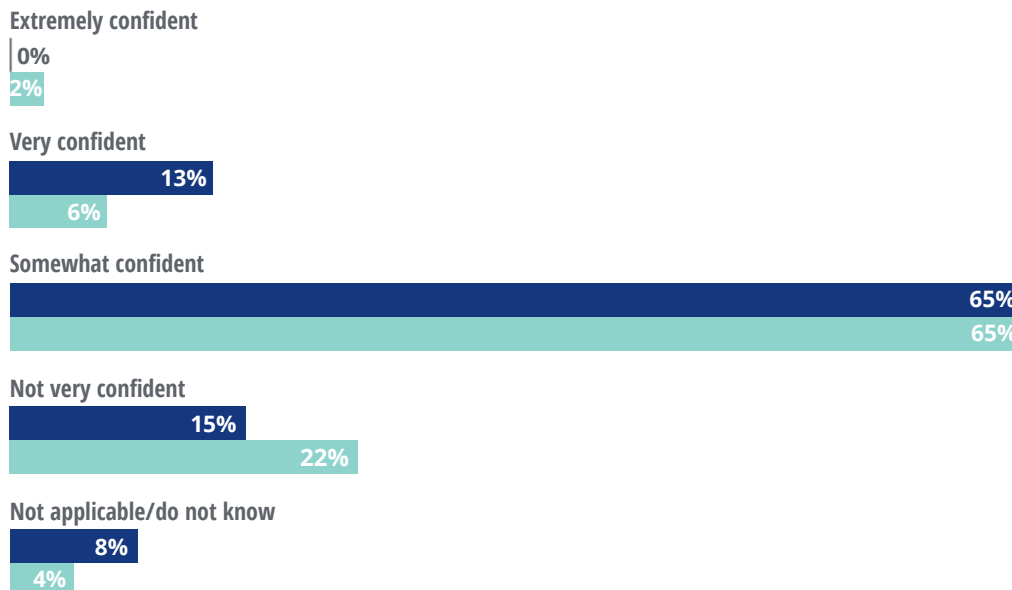
Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 31

The majority of CISOs say that they are “somewhat confident” in their third parties’ cybersecurity practices

How confident are you in the cybersecurity practices of your third parties (contractors, service providers, business partners)? (48 respondents)

■ 2018 ■ 2016

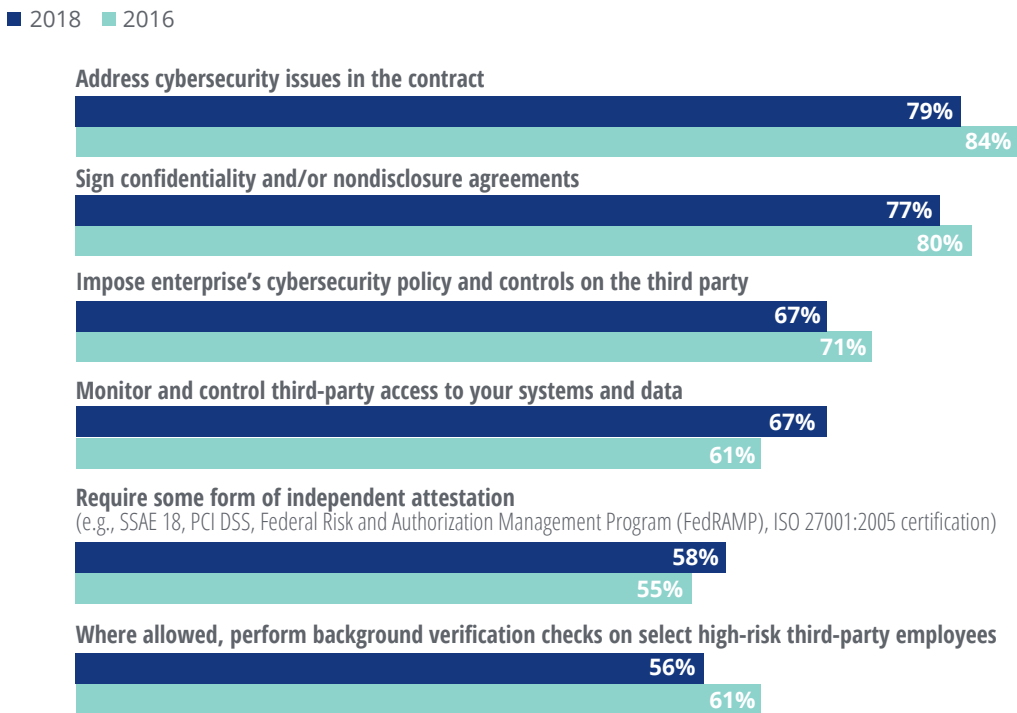


Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 32

CISOs’ top options for managing the adequacy of third-party cybersecurity practices include contractual cybersecurity requirements and confidentiality/nondisclosure agreements

How does your state manage the adequacy of third-party (contractor, service provider, business partner) cybersecurity practices? (48 respondents)



Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

Privacy and identity access management (IAM)

Though CISOs now demonstrate greater confidence and control over many potential threats, the 2018 survey results show that the emerging issues of privacy and enterprise IAM have not gained much traction. Five additional states have appointed a CPO since the 2016 survey, representing a slow establishment of this role (only 14 states have a CPO.) Still, our 2018 survey found that states are making incremental improvements in their privacy programs, including establishing formal policies on the destruction of personal infor-

mation and programs for managing privacy compliance.

The adoption of enterprisewide IAM faces many barriers. Only 42 percent of our state respondents provide enterprisewide IAM solutions either to all or some agencies under the governor’s authority. Competing or higher priorities constitute the top barrier to IAM adoption, as in 2016. The next biggest barriers are cost at second place, followed by the decentralized environment of the state and the complexity of integrating with legacy systems tied for third place.

The top audit finding reported by our respondents was in the access control category.

Yet IAM was not one of the top five cybersecurity initiatives reported by the states for 2018/2019. States should do more in the area of IAM to not only reduce the number of audit

findings, but also to establish IAM as a strategic enabler of business initiatives to improve citizens' experience of dealing with government using modern authentication methods.

FIGURE 33

More than half of states do not have a program for managing privacy compliance and a formal process for dealing with complaints about information privacy

Does your state have the following?

		Yes	No	N/A or do not know
A program for managing privacy compliance (49 respondents)	2018	27%	61%	12%
	2016	21%	60%	19%
A written privacy, fair information practices, or data collection policy in place (49 respondents)	2018	47%	37%	16%
	2016	58%	27%	15%
Formal policies in place with respect to the destruction of personal information (49 respondents)	2018	82%	10%	8%
	2016	71%	19%	10%
A formal process in place to deal with complaints about handling privacy of information (such as a privacy hotline) (48 respondents)	2018	25%	54%	21%
	2016	28%	46%	17%
A formal incident response process (notifications, hotline) for breach of privacy (48 respondents)	2018	58%	31%	10%
	2016	69%	21%	10%

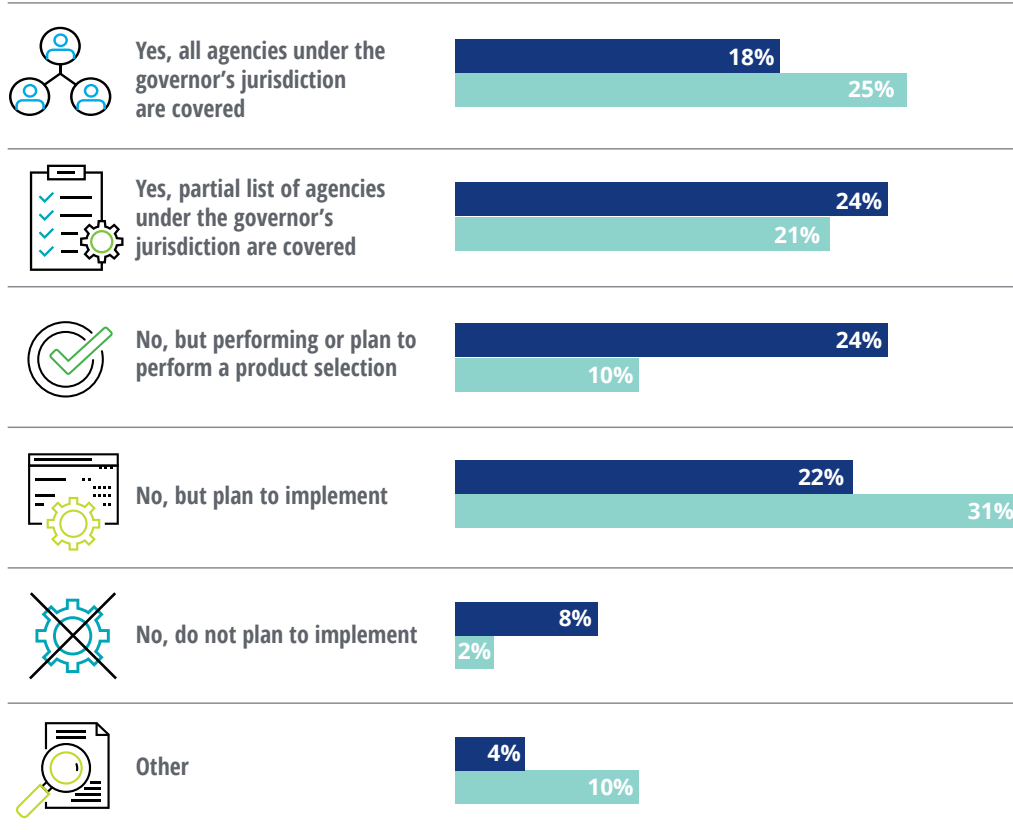
Source: 2016 and 2018 Deloitte-NASCI0 Cybersecurity Studies.

FIGURE 34

Thirty-three states have either established an enterprise IAM solution or plan to perform a product selection

Does your state provide an enterprisewide IAM solution? (50 respondents)

■ 2018 ■ 2016

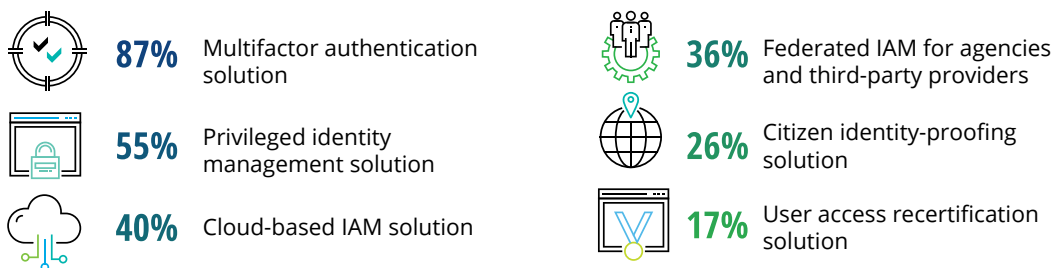


Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 35

Multifactor authentication, privileged identity management, and cloud-based IAM solutions are CISOs' leading IAM initiatives

What are your current IAM initiatives? (47 respondents)



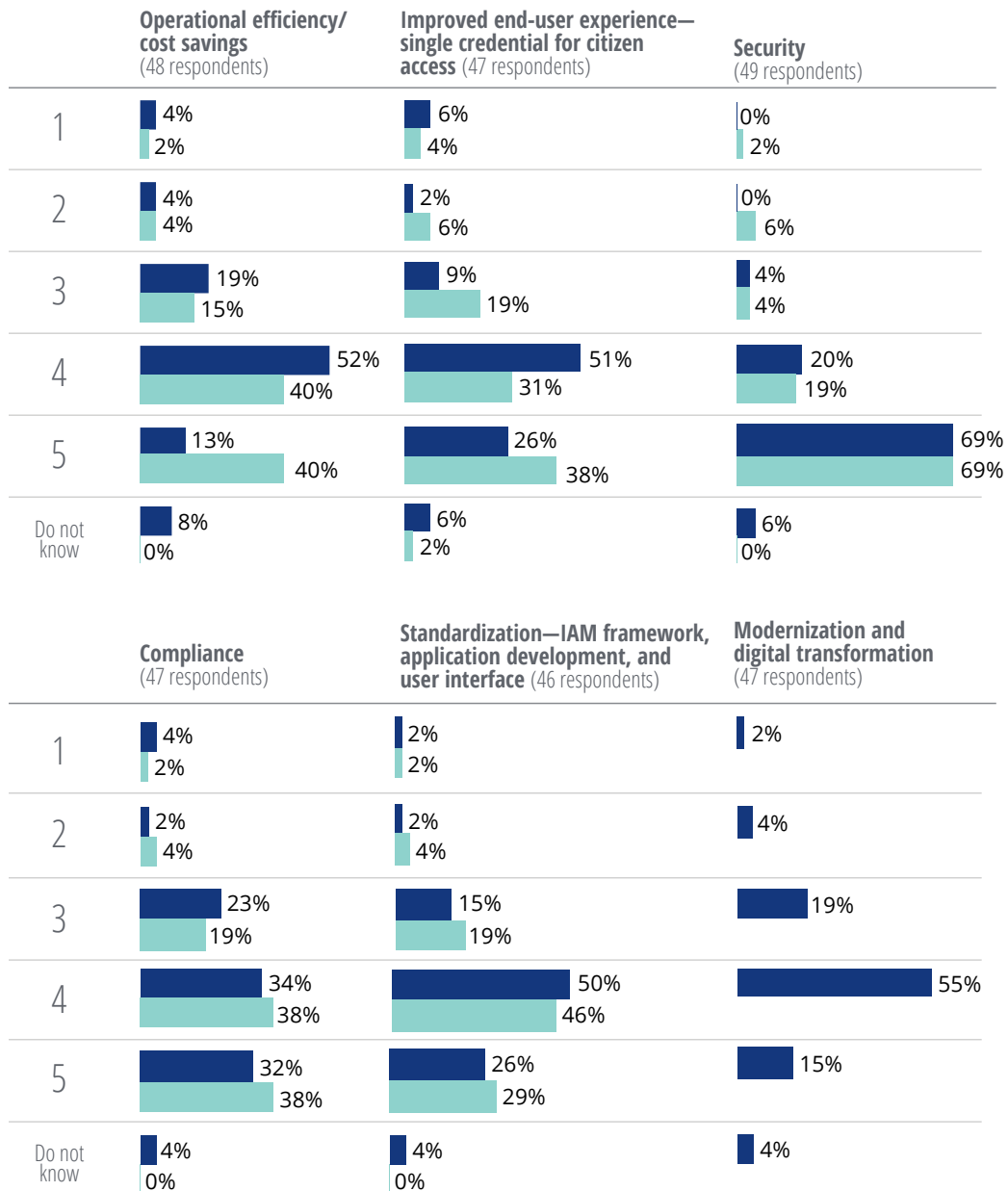
Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 36

Security is the most important reason for making IAM investment decisions

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

■ 2018 ■ 2016



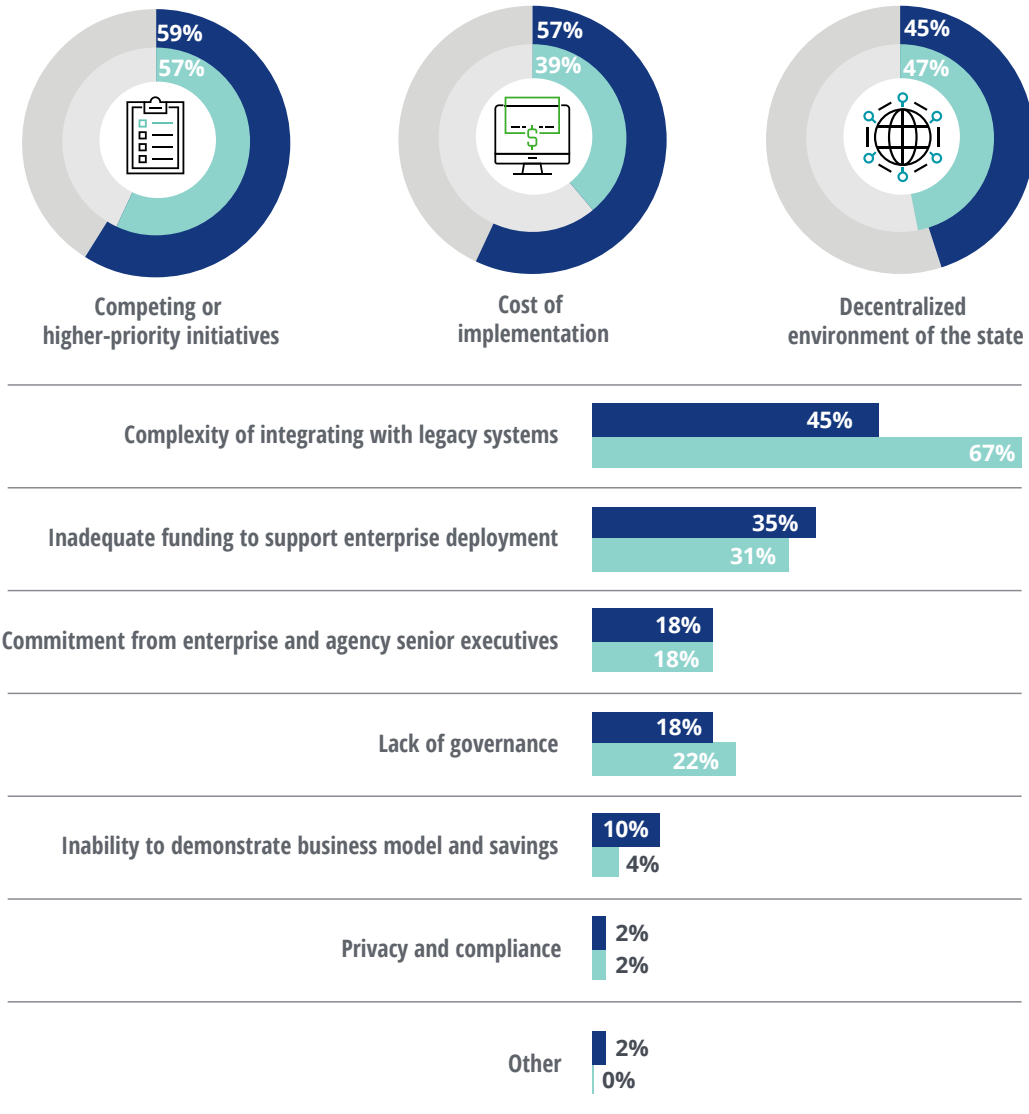
Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

FIGURE 37

Cost of implementation has risen as a top barrier to adopting an enterprise IAM approach

What are the top three barriers that your state faces in adopting an enterprise IAM approach? (49 respondents)

■ 2018 ■ 2016



Source: 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

Appendix: Acknowledgments and survey methodology

The 2018 Deloitte-NASCIO Cybersecurity Study uses survey responses from:

- US state enterprise-level CISOs, with additional input from agency CISOs and security staff members within state governments. CISO participants answered 56 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Participation was high: responses were received from all 50 states. Figures 38 through 40 illustrate the CISO participants' demographic profile and that of their states.
- US state (business) officials, who responded to a survey designed to help characterize how the state government enterprise views, formulates, implements, and maintains its security programs. The results help

FIGURE 38

Survey respondents' job title

CISO or equivalent	40
CIO or equivalent	5
Other	5

Source: 2018 Deloitte-NASCIO Cybersecurity Study.

provide valuable insights into state business stakeholder perspectives.

The two surveys gave survey 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

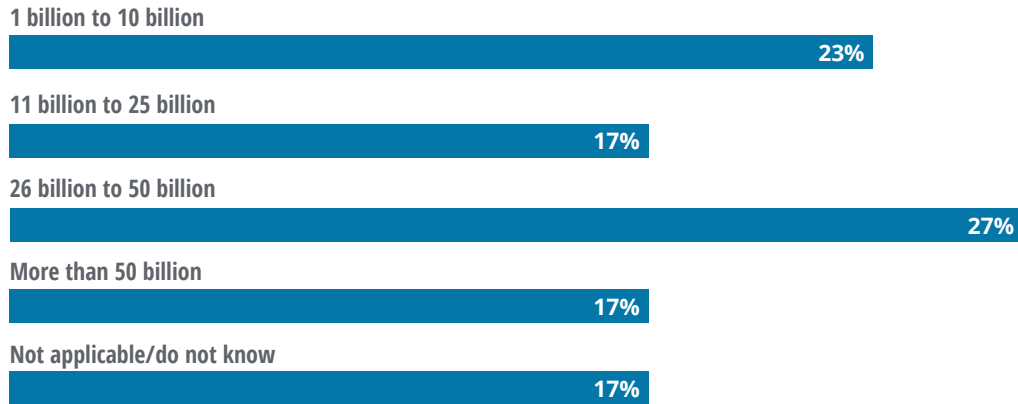
Number of state government employees (excluding higher education employees)



Source: 2018 Deloitte-NASCIO Cybersecurity Study.

FIGURE 40

Approximate annual state budget for current budget year (US\$)



Source: 2018 Deloitte-NASCIO Cybersecurity Study.

Endnotes

1. Office of Management and Budget, *An American budget: Analytical perspectives*, 2018, pp. 273–288.
2. Forrester Research, Inc., *The US Healthcare Security Benchmark 2017 To 2018*, January 17, 2018.
3. Centers for Medicare and Medicaid Services, “SMD #16-009 re: Mechanized claims processing and information retrieval systems—APD requirements,” June 27, 2016.

About the authors

SRINI SUBRAMANIAN is a principal in Deloitte & Touche LLP's Cyber Risk Services practice and leads the State, Local, and Higher Ed sector for Risk and Financial Advisory Services in the Government & Public Services industry. He has more than 31 years of IT experience and more than 20 years of security and privacy experience in the areas of information security strategy, innovation, governance, identity, access management, and shared services. Subramanian actively participates in the National Governors Association (NGA), NASCIO, and state committees to elevate cyber risk awareness in government.

DOUG ROBINSON has served as executive director of the National Association of State Chief Information Officers (NASCIO) since 2004. His career spans over 40 years in public sector information technology, including positions in state government, higher education, and IT consulting. Prior to joining NASCIO, Robinson served as executive director in the Governor's Office for Technology, Commonwealth of Kentucky. As a senior IT executive in the state CIO office, he led IT strategic planning, enterprise architecture, policy, and research initiatives. Robinson is a frequent speaker, panelist, author, and recognized national expert representing state CIOs, policy issues, priorities, and trends in state government IT. In addition, he represents NASCIO on several national councils, boards, and advisory committees.

Acknowledgments

We thank the NASCIO and Deloitte professionals who helped to develop the survey and execute, analyze, and create the report.

NASCIO

- **Doug Robinson**, Executive Director
- **Meredith Ward**, Senior Policy Analyst

STATE CISO SURVEY REVIEW TEAM

- **Elayne Starkey**, State of Delaware (retired)
- **Rajiv Das**, State of Michigan
- **Stan Gatewood**, State of Georgia
- **Mark Gower**, State of Oklahoma
- **Michael Roling**, State of Missouri
- **Nancy Rainosek**, State of Texas

DELOITTE SUBJECT MATTER SPECIALIST CONTRIBUTORS

- **Bharane Balasubramanian**, Deloitte & Touche LLP
- **Bharath Chari**, Deloitte & Touche LLP
- **Clayton Frick**, Deloitte & Touche LLP
- **Deborah Golden**, Deloitte & Touche LLP
- **John O'Leary**, Deloitte Services LP
- **Art Stephens**, Deloitte Consulting LLP
- **Srini Subramanian**, Deloitte & Touche LLP
- **Mike Wyatt**, Deloitte & Touche LLP

DELOITTE SURVEY TEAM, DATA ANALYSIS, AND BENCHMARKS

- **Sushumna Agarwal**, Deloitte Services LP
- **Divya Nayak**, Deloitte & Touche LLP
- **Akash Keyal**, Deloitte Services LP
- **Alex Vilkin**, Deloitte & Touche LLP
- **Susan Watts**, Deloitte & Touche LLP

MARKETING

- **Annette Evans**, Deloitte Services LP
- **Anudeep Gurram**, Deloitte Services LP
- **Catherine Yang**, Writer

About Deloitte

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte’s cyber risk services help complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation, and performance objectives through proactive management of the associated cyber risks. Deloitte provides advisory, implementation, and managed cybersecurity services to help our government clients lead the way with a collaborative threat intelligence strategy. Deloitte’s demonstrated approach and methodology help our clients better align security investments with risk priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to deliver services in the face of cyber incidents.

The Deloitte Center for Government Insights produces groundbreaking research to help government solve its most complex problems. Through 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, publications, briefings, and government affairs, NASCIO is the premier network and resource for state CIOs.

For more information, visit www.nascio.org.

Contacts

NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

Doug Robinson

Executive Director
+1 859 514 9153
drobinson@nascio.org

Meredith Ward

Senior Policy Analyst
+1 859 514 9209
mward@nascio.org

DELOITTE

Dan Helfrich

Principal, Government &
Public Services Leader
Deloitte Consulting LLP
+1 571 882 8308
dhelfrich@deloitte.com

Srini Subramanian

Principal, Deloitte Risk and
Financial Advisory
State, Local & Higher Education Leader
Deloitte & Touche LLP
+1 717 651 6277
ssubramanian@deloitte.com

Jason Salzetti

Principal, State, Local & Higher
Education Sector Leader
Deloitte Consulting LLP
+1 415 328 9348
jsalzetti@deloitte.com

Mike Wyatt

Principal, Deloitte Risk and
Financial Advisory
Deloitte & Touche LLP
+1 512 226 4171
miwyatt@deloitte.com

Deborah Golden

Principal, Government & Public
Services, Cyber Risk Services Leader
Deloitte & Touche LLP
+1 571 882 5106
debgolden@deloitte.com

Bharane Balasubramanian

Senior Manager, Deloitte Risk
and Financial Advisory
Deloitte & Touche LLP
+1 512 226 4049
bbharanedaran@deloitte.com

Deloitte.

Insights

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



Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Junko Kaji, Aditi Rao, Preetha Devan, and Abrar Khan

Creative: Emily Moreano, Kevin Weier, Sonya Vasilieff, and Tushar Barman

Promotion: Nikita Garia

Cover artwork: Taylor Callery

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 Deloitte and NASCIO are not, 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 business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this publication contains the results of a survey conducted by Deloitte and NASCIO. The information obtained during the survey was taken "as is" and was not validated or confirmed by Deloitte or NASCIO.

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

Copyright © 2018 Deloitte Development LLC. All rights reserved.