Deloitte. University Press

NASCIO Representing Chief Information Officers of the States

2016 Deloitte-NASCIO Cybersecurity Study

State governments at risk: Turning strategy and awareness into progress

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

CONTENTS

Message from NASCIO President

Each year, the National Association of State Chief Information Officers (NASCIO) conducts a survey of state chief information officers (CIOs) to identify and prioritize the top policy and technology issues facing state government. State CIOs ranked cybersecurity as their top priority in 2014, 2015, and 2016. Considering that it seems that cybersecurity breaches in both the public and private sector are consistently splashed across the news, this is understandable.

In the 2016 Deloitte-NASCIO Cybersecurity Study, we asked state chief information security officers (CISOs) about the status of cybersecurity in their states, as well as their perspectives and insights. We have compiled and highlighted those findings here. Importantly, we have found that the message that "cybersecurity is everyone's responsibility" is seeing some traction. Specifically:

- Cyber risks and mitigations now have more attention at the governor level and are increasingly on the governor's agenda
- Cybersecurity has been woven into the fabric of government operations and sustainability
- Most states indicate an increase in budget; however, funding remains the biggest challenge
- Finding talent is still a challenge, but states are working to win the hearts and minds of their cyber workforce

In other words, cybersecurity is a team sport, but the game is not over. Yes, there continue to be challenges with proper funding, finding qualified talent, and training and awareness. But the good news is that we are seeing positive indications that CISOs and CIOs are having a strong impact, as communication and collaboration among agencies and all levels of state government is increasing.

NASCIO will continue to use the findings in this report and other work to advocate for increased funding, a qualified workforce, and all resources necessary for states to maintain effectiveness and elevate their cybersecurity efforts.

Darryl Ackley

NASCIO President and Cabinet Secretary and CIO for the
New Mexico Department of Information Technology

Foreword

TODAY, no one disputes that state governments need to be concerned with cyber risk. The 2016 Deloitte-NASCIO Cybersecurity Study shows that cyber risk has risen in importance in the eyes of governors and other state executives. For CIOs and CISOs, this governor-level attention is encouraging news and an opportunity to secure resources and support for state cybersecurity programs.

Given its current trajectory, cyber risk in state governments is unlikely to dissipate, and may even grow—largely a result of the increase in innovation and use of technology and data. State governments have rapidly adopted new technology to better serve constituents and reduce dependency on legacy systems that are difficult to maintain. Ironically, the very steps governments have taken to embrace these new innovations add to the cyber risks. This is why we need to begin viewing the management of cyber risk as a core function of running government operations.

Since 2010, Deloitte and NASCIO have been conducting biennial surveys of CISOs and state officials to explore how states are managing cyber risk. In our fourth survey to date, we found that even as the importance of cybersecurity has gained ascendancy, many of the issues CISOs are grappling with are stubbornly persistent. Following are some of the top takeaways from the 2016 survey:

Governor-level awareness is on the rise. The survey results indicate that governors and other state officials are receiving more frequent reports from CIOs/CISOs. Initiatives such as the National Governors Association (NGA) "Call to Action" seem to be helping to maintain the prominence of cybersecurity on executive agendas.

Cybersecurity is becoming part of the fabric of government operations. For the first time, all respondents report having an enterprise-level CISO position. The CISO role itself has become more consistent in terms of responsibilities and span of oversight. CISOs are also focusing their energies more on what they can control.

A formal strategy and better communications lead to greater command of resources. Securing sufficient resources—both funding and talent—remains a top challenge for CISOs. This year, we found evidence that states that take a proactive approach to strategy setting and communication are more likely to see improvements in funding and access to talent.

We believe that, overall, the survey results spell out a clear message for CISOs: **State leaders are paying attention. Take advantage of this focus to make substantial progress.**

Finally, we would like to thank participants in this year's survey: the 49 CISOs who responded to the longer version of the survey—24 of whom were new to their role—and the 96 state officials who responded to the accompanying state officials survey. Your time and commitment will help states in their efforts to effectively manage cyber risk and protect citizen data.

AUTHORS OF THE SURVEY

Doug Robinson
Executive Director, NASCIO

Srini Subramanian
Principal, Deloitte & Touche LLP

Governor-level awareness is on the rise

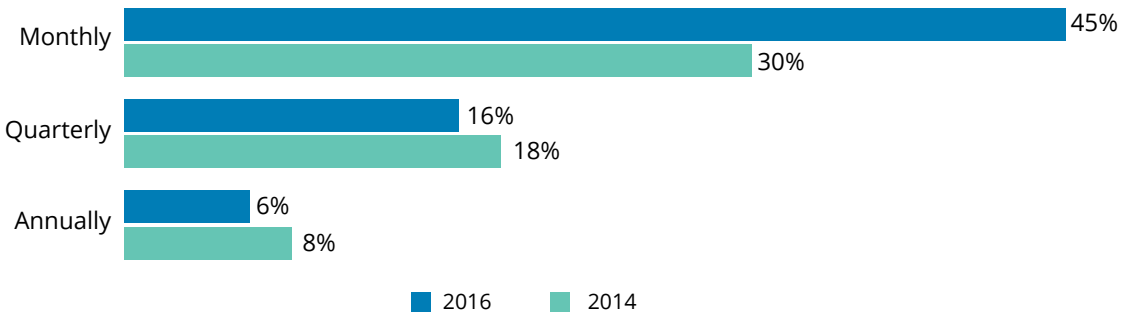
THE critical nature of cybersecurity has not been lost on governors and other state officials. The state officials survey this year shows that over 90 percent say that cybersecurity is important to their state, and over 94 percent say that it is important to their individual agency. Cybersecurity is also a more frequent topic of discussion at state executive leadership meetings (figure 1). More than three-fifths (61 percent) of state officials say that cybersecurity is discussed at executive leadership meetings at least quarterly, compared with less than half (48 percent) in 2014.

Governors are receiving more frequent briefings on cybersecurity. Nearly a third (29 percent) of CISOs provide their governors with monthly reports on cybersecurity, compared with only 17 percent in 2014 (figure 2). However, this level of communication has not extended to state legislatures. Nearly a third of respondents say that they never communicate with their legislatures, unchanged from 2014. This is an important consideration, given the legislature's role in appropriating funds.

Despite increased executive-level awareness of cybersecurity, there remains a "confidence gap" in terms of how well CISOs versus state officials think security threats can be handled by their states. For instance, two-thirds (66 percent) of state officials say they are very or extremely confident that adequate measures are in place to protect information assets from externally originating cyberthreats, compared with only a quarter (27 percent) of CISOs. These findings, which are similar to those from our 2014 study, indicate that CISOs may need to take a different approach when communicating the severity of cyberthreats to state officials.

States are also starting to act and make progress in areas visible to governors. Since the NGA issued its "Act and Adjust: A Call to Action for

Figure 1. How often is the topic of cybersecurity presented or discussed at your agency/office executive leadership meetings?



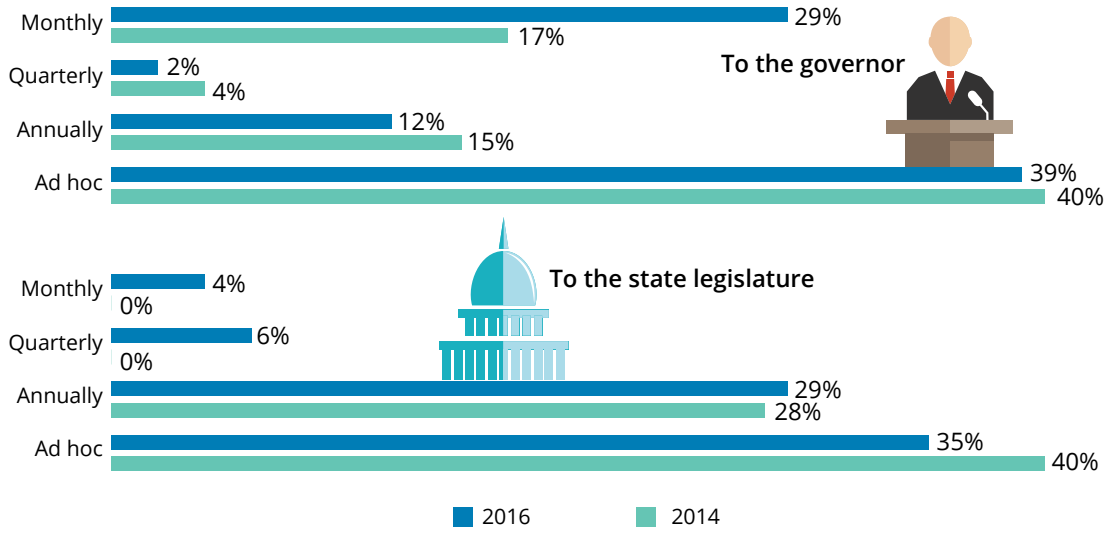
Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Governors for Cybersecurity" in 2013, more than half (54 percent) of respondents say that they have implemented at least some of the NGA's recommendations, compared with only a third (33 percent) in 2014 (figure 3). In fact, governors have launched initiatives ranging from state cyber academies and public-private partnerships to dashboards and preparedness and response plans.[1]

See survey analysis section for more data.

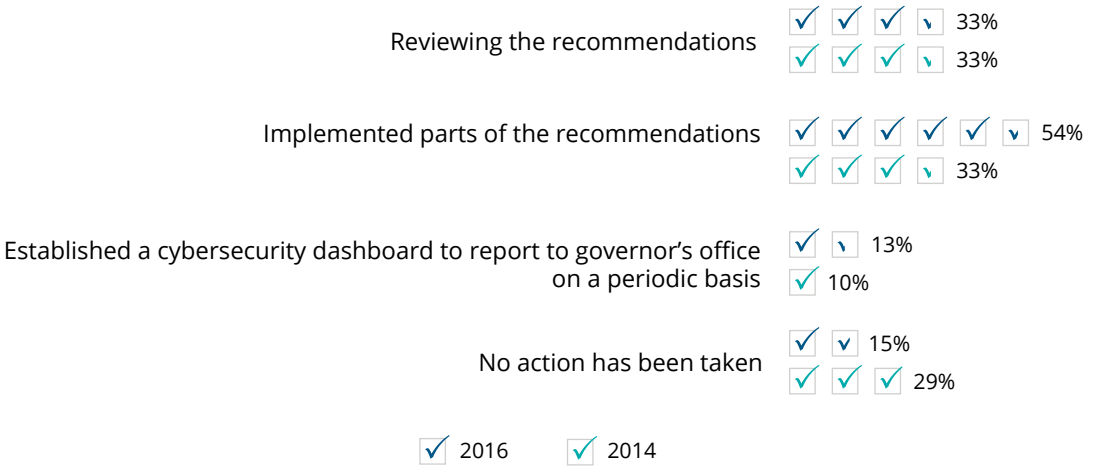
Figure 2. To what extent are you required to provide reports on cybersecurity status or posture of the enterprise to the following positions?



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 3. How do you characterize your state's adoption of NGA's "Act and Adjust" report? (select all that apply)



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Cybersecurity is becoming part of the fabric of government operations

CISOs have begun to take a more programmatic approach to managing cyber risk and are starting to concentrate on areas that are in their control (figure 4). Only 45 percent of CISOs cited the "growing sophistication of threats" as a barrier to addressing cybersecurity challenges, down from 61 percent in 2014. CISOs are focusing on areas where they can take proactive steps to better manage risks. Some of the top areas CISOs say are within their purview include audit logs and security event monitoring, strategy and planning, and vulnerability management (figure 5).

The CISO role itself is now a well-established position in state government. For the first time, all respondents report having an enterprise-level CISO position, an indication that states

Figure 4. Top cybersecurity initiatives for 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 5. Top CISO functions

The survey respondents indicated that the top five functions within the scope of the CISO included:

*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

consider protecting information assets—including citizen data—from cyber-threats to be an important government responsibility. CISOs' responsibilities and top priorities have remained consistent over the past two years, a sign that the role is solidifying. This conclusion is supported by the fact that some 50 percent (24 individuals) are new to the role—yet they say their responsibilities are the same as those who have held their position for several years.

In terms of priorities, three initiatives that made the top five—training and awareness (39 percent), monitoring and SOCs (37 percent), and strategy (29 percent)—were also among the top five in 2014 (figure 4).

The mechanisms by which CISOs' authority over other organizational entities is established have not changed significantly since 2014. In addition, alignment of cybersecurity initiatives with business initiatives has increased, with 29 percent of respondents reporting appropriate alignment, versus only 14 percent in 2014. However, we continue to see CISOs having challenges in making progress on enterprise-wide initiatives in a largely federated model of governance with the agencies. For example, our results show challenges in operationalizing state-wide identity and access management (IAM) implementations. To overcome these challenges and help close the confidence gap that we continue to see, more will need to be done to elevate the authority and influence of the CISO role. CISOs need to improve communications around risks and metrics to better inform agency business executives and help promote their agendas.

See survey analysis section for more data.

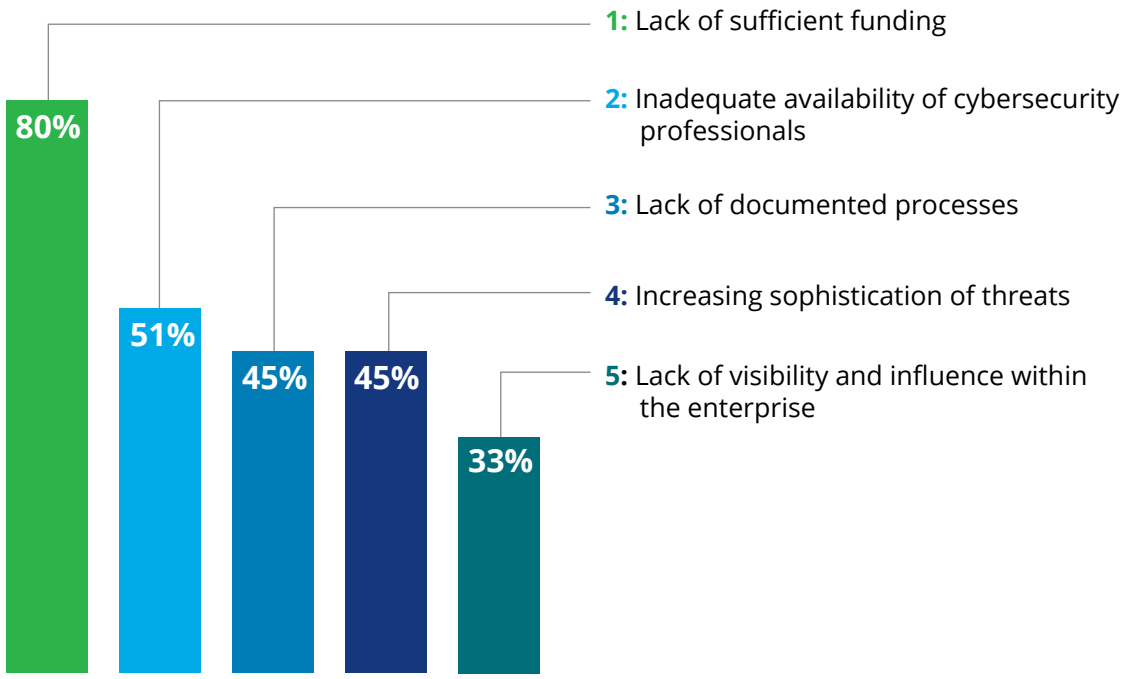
A formal strategy can lead to more resources

EVEN as CISOs better define their roles and become an integral part of state government, they continue to face challenges, particularly in securing the resources they need to combat ever-evolving cybersecurity threats. Four-fifths (80 percent) of respondents say inadequate funding is one of the top barriers to effectively address cybersecurity threats, while more than half (51 percent) cite inadequate availability of cybersecurity professionals (figure 6).

Survey evidence suggests that when CISOs develop and document strategies—and get those strategies approved—they can command greater budgets and attract or build staff with the necessary competencies. A direct correlation can be seen between having an established strategy and obtaining more full-time equivalents (FTEs) dedicated to cybersecurity, as well as year-over-year budget increases (figure 7). For example, 11 out of 33 states that have an approved strategy reported

Figure 6. Top five barriers in addressing cybersecurity challenges

Funding still remains at the top of the list, with cybersecurity professionals next in line.



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

they have more than 15 FTEs dedicated to cybersecurity, and 16 out of 33 states with an approved strategy reported they had an increase in budget. An approved and proactively communicated strategy can also help CISOs overcome another barrier: "lack of visibility and influence in the enterprise," an ongoing challenge in the largely federated governance model in state government.

See survey analysis section for more data.

Figure 7. Intersection of approved strategy and resources

	More than 15 dedicated FTEs for cybersecurity	Staff has required competencies	Increase in budget	Cyber budget more than 2% of IT budget	Alignment of cyber and business programs
Approved strategy (33 states)	11 (33%)	16 (48%)	16 (48%)	10 (30%)	12 (36%)
No approved strategy (16 states)	1 (6%)	3 (19%)	5 (31%)	0 (0%)	2 (12%)

Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

Key takeaways overview

Executive AWARENESS

Governors and state officials are paying more attention to cyber risk . . .

. . . but compared to CISOs, state officials still overestimate how well they think states can handle security threats

CISOs have an opportunity to make significant progress in educating stakeholders about the true magnitude of cyber risk to gain elusive support

Operational INTEGRATION

Cybersecurity is becoming part of the fabric of government operations . . .

. . . but the largely federated model of governance makes it challenging for the CISO to exercise influence and authority across the enterprise

Effective collaboration across agencies, legislators, and federal partners is key to effective cyber risk management

Formal STRATEGY

The top challenges of lack of funding and finding talent for cybersecurity continue at the same intensity . . .

. . . but CISOs with a formal, approved cybersecurity strategy are more likely to secure funding and talent

CISOs should formalize their cybersecurity strategy and communicate its urgency to the stakeholders who need to approve it

Survey data analysis

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

Strategy and governance

Strategy is central to driving states' cybersecurity direction, which makes it especially important for CISOs to push for approval of their strategies. This year's survey shows that more CISOs are making progress in this regard: Two-thirds (67 percent) had cybersecurity strategies that were both documented and approved, compared with 55 percent in 2014 (figure 8). From a governance perspective, most states' security functions use a largely federated model of governance, which makes it even more important for CISOs to be effective in influencing agency business and technology stakeholders and getting their buy-in for the strategy.

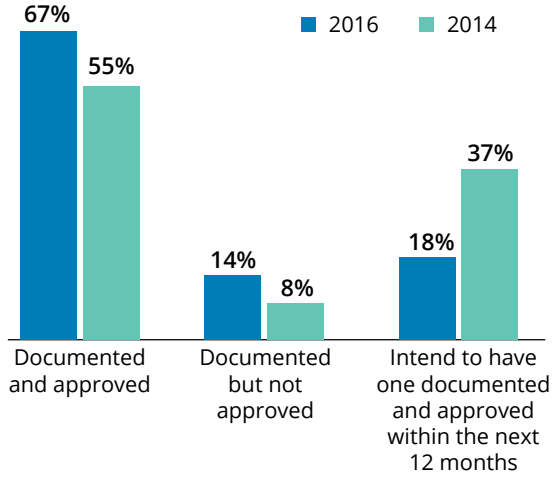
Strategies continue to involve both lines of business and technology decision makers; however, significant confidence gaps continue from the 2014 study, signifying that improvements need to be made in defining the priorities, risks, and strategies in place. A disconnect can also be seen between senior-level commitment and adequate funding (figure 9).

Collaboration across state lines and with federal agencies is also part of respondents' strategies, and it is an important means of sharing practices for addressing cybersecurity challenges (figure 10). This year, almost all respondents say that they are collaborating with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the United States Department of Homeland Security (DHS)/fusion centers.

CISOs are expressing a growing concern about the security practices of third parties, including those of contractors, service providers, and business partners. Nearly a quarter (22 percent) of CISOs say they are not very confident in this regard (figure 11). CISOs indicate that addressing cybersecurity in the contract is their leading option for managing

Figure 8. States' progress in maintaining cybersecurity strategy

States are making progress in getting their strategy approved. A third of the states continue to work on getting their strategy approved.

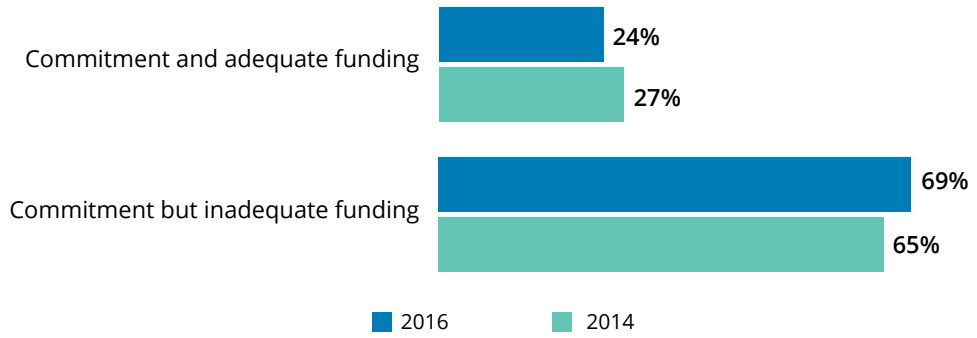


Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 9. Senior executive support (governor's office, agency secretary, or CIO) for security projects to effectively address regulatory or legal requirements

State cybersecurity projects continue to have the appropriate level of executive commitment, but lack the required funding.

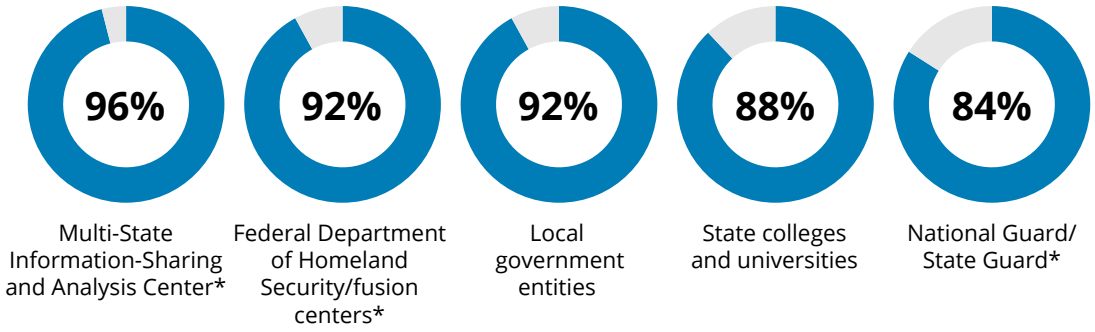


Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 10. Collaboration trends as part of the states' cybersecurity program

Collaboration is becoming central to state government strategy. Increased collaboration is an area to watch as states establish their security operations centers.

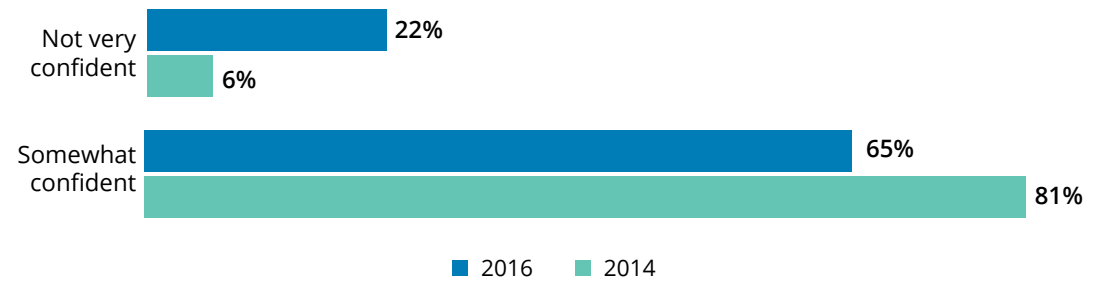


*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 11. CISOs' confidence levels in cybersecurity practices followed by third parties (contractors, service providers, business partners)

CISOs' confidence level in third-party security management practices continues to be a struggle.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 12. States' leading methods to manage adequacy of third-party (contractors, service providers, business partners, cybersecurity practices)

Ways to manage the adequacy of third-party cybersecurity practices (top five)	2016
Address cybersecurity issues in the contract	84%
Sign confidentiality and/or non-disclosure agreements	80%
Impose enterprise's cybersecurity policy and controls on third party	71%
Where allowed, perform background verification checks on select high-risk third-party employees	61%
Monitor and control third-party access to your systems and data	61%

Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

the cybersecurity practices of third-party organizations (figure 12).

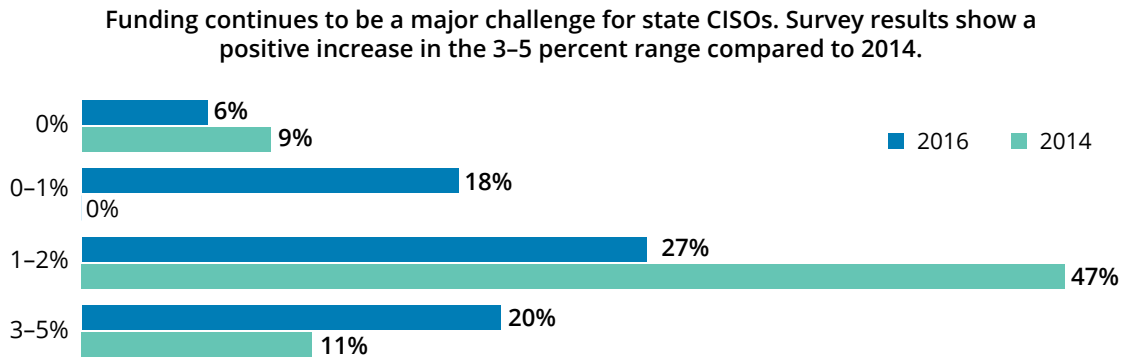
Budget and funding

Lack of sufficient funding remained the most significant challenge for CISOs in 2016. The majority of respondents continue to indicate that their cybersecurity budgets were only between 0-2 percent of their state's overall IT budget (figure 13). The results did show an increase over 2014 in the 3–5 percent range of the state's overall IT budget. From a year-over-year budget perspective, 33 percent of respondents note that their budgets have remained the same (figure 14). Of the 43 percent of respondents with an increase, most of them noted increases only in the 1–5 percent range. In contrast, the federal cybersecurity budget has seen an increase of 35 percent over the 2016-enacted level.[2]

Looking at the top items covered within a budget, this year's survey shows incident response as the most frequently cited (figure 15). Cybersecurity research and development and audit and certification costs moved up significantly from 2014.

Given cybersecurity's status as a national issue, states are able to tap into a range of state and

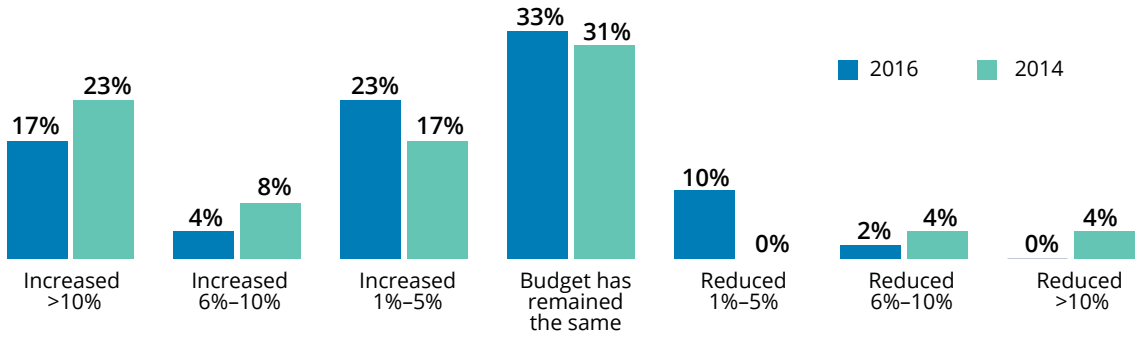
Figure 13. Percentage of state's cybersecurity allocation as part of the overall IT budget



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies. Graphic: Deloitte University Press | DUPress.com

Figure 14. Year-over-year trending of the state cybersecurity budget for the years 2014–2016

State cybersecurity budgets have largely remained stagnant when compared with the federal cybersecurity budget.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 15. Areas covered under the cybersecurity budget

Since 2014, the top areas supported by the cybersecurity budget have changed. Logical access control, research and development, and audit/recertification have made their way into the top five.

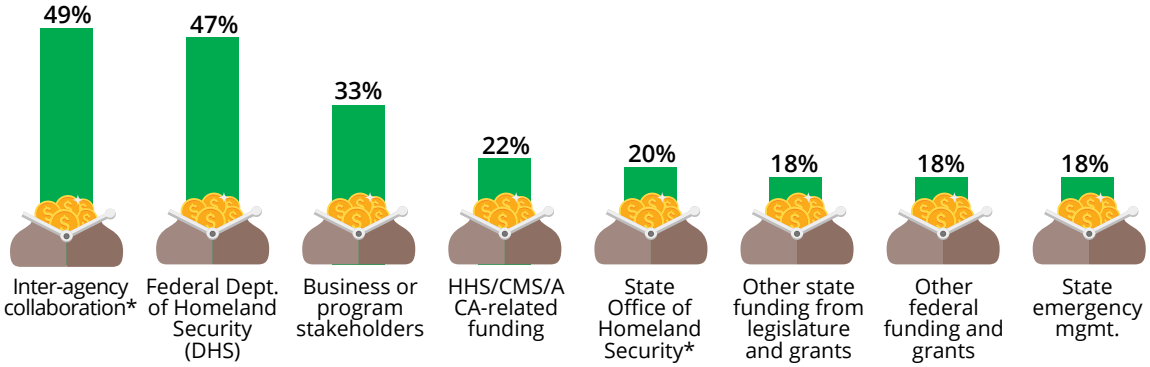
Top areas covered under the cybersecurity budget	2016	2014	Trend
Incident response	83%	69%	↑
Logical access control	79%	51%	↑
Compliance and risk management	69%	74%	↓
Cybersecurity research and development	57%	37%	↑
Audit or certification costs	48%	31%	↑
Infrastructure protection devices	40%	61%	↓
Awareness/communication costs	30%	78%	↓
Security consultants	26%	53%	↓

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 16. Additional funding sources for cybersecurity initiatives

State CISOs have started looking at alternate sources of funding, both inside and outside their states. Inter-agency collaboration and the Department of Homeland Security are their leading sources of additional funding.



*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

federal programs and initiatives to secure additional funding (figure 16). Although limited, these are important avenues for CISOs as they build strategies to bridge the funding gap.

Talent

In 2016, the cybersecurity talent crisis continues. Overall, the size of state cybersecurity staff moved up slightly, consistent with budgets (figure 17)—but not to the levels seen in the private sector or at federal agencies, which may have well over 100 FTEs handling cybersecurity. CISOs cite the inadequate availability of cybersecurity professionals as one of their biggest challenges, second only to obtaining sufficient funding, and note salary and competition with the private sector as the top factors negatively impacting their workforce strategies (figure 18).

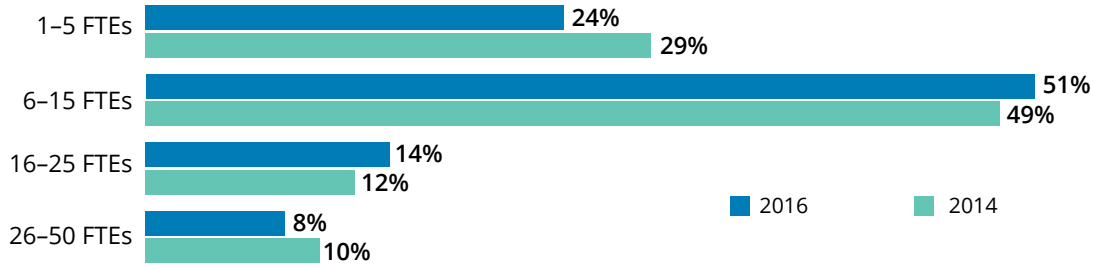
For many CISOs, their challenges are exacerbated by underfunded pension plans and budget constraints that have forced states to change retirement plans for those now entering the workforce. Attractive benefit plans, historically one of the "carrots" of a state government career, are no longer a given, and retirement packages are being restructured to more closely resemble those found in the private sector.[3] In addition, private sector salaries for information security professionals have risen dramatically in recent years, making state government less competitive on the compensation side.

CISOs are therefore looking for other ways to win the hearts and minds of prospective employees. While more than half say that job stability is one of the top three ways to attract and retain cybersecurity talent, nearly as many point to the opportunity to serve as an important factor as well (figure 19). Promoting the potential to "give back" may be an especially effective way to attract Millennial talent, and should be built into talent acquisition plans.

The majority of states (56 percent) see a gap in required competencies (figure 20). To close the cybersecurity competency gap, states are using a range of strategies, including providing training, enlisting outside specialists, and outsourcing certain functional areas (figure 21). Training and awareness, the top initiative reported by states in 2016, has improved since 2014, with more respondents saying that

Figure 17. Dedicated cybersecurity professionals employed by the state's enterprise security office

The majority of states have enterprise cybersecurity teams of between 6 and 15 full-time equivalents (FTEs). Overall team size continues to show a small increase year over year.

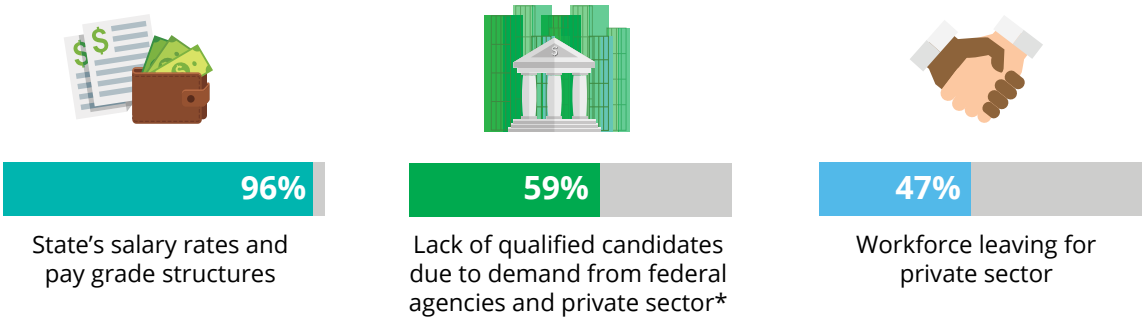


Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 18. Top three human resources factors that negatively impact the CISO's ability to develop, support, and maintain cybersecurity workforce

State CISOs continue to identify inadequate availability of cybersecurity talent as a top barrier. The ability to attract and retain cybersecurity professionals is impacted by pay grade structures as well as by competition from the federal government and the private sector.

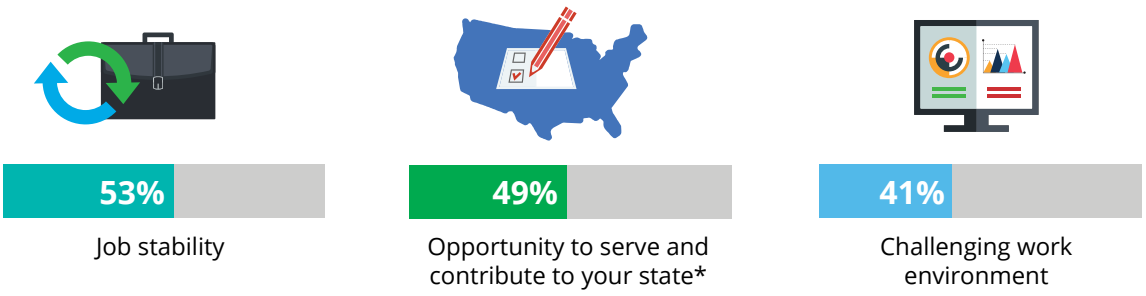


*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 19. Top three factors that CISOs employ to attract and retain cybersecurity talent

State CISOs are still grappling with the cybersecurity talent gap. Job stability, the opportunity to serve, and a challenging work environment are the top factors for attracting and retaining talent.



*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 20. State internal cybersecurity professional competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements

The majority of states say their staff have gaps in cybersecurity competencies. Training, outsourcing, and staff augmentation are the leading ways that CISOs bridge the talent gap.

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 21. Top outsourced cybersecurity functions

States' leading outsourced functions continue to focus on threat management services.

Outsourced functions (top five)	2016	2014
Cyber threat risk assessments	54%	37%
Forensics/legal support	44%	39%
Cyber threat management and monitoring services	35%	37%
Vulnerability management	27%	18%
Audit log analysis and reports	23%	18%

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 22. Cybersecurity training trends for employees based on job role and function

States have made strides in increasing the breadth of security awareness training.

Provide required training to	Change from 2014 to 2016
Executives	↑
People handling sensitive information	↑
IT application developers and programmers	↑
System administrators	↑
IT infrastructure	↑
Business and program stakeholders	↑
General state workforce	↑
Third-party workforce (vendors, contractors, consultants, business partners)	↓

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

they train a broad range of employees, from systems administrators and programmers to executives and those handling sensitive information (figure 22).

Emerging trends

IDENTITY AND ACCESS MANAGEMENT (IAM)

More states in 2016 (47 percent) than in 2014 (33 percent) have an enterprise IAM solution that covers some or all of the agencies under the governor's jurisdiction. However, CISOs continue to face the same barriers to implementing enterprise IAM solutions, including the complexity of integrating with legacy systems, cost, competing or higher-priority initiatives, and the states' decentralized IT environment (figure 23). Similar to 2014, CISOs are focusing on implementation of multifactor authentication, federated IAM, and privileged identity management solutions. Cloud-based IAM solutions and citizen identity proofing solutions follow closely as leading initiatives (figure 24).

Figure 23. Top five barriers to an enterprise IAM approach

Barriers	2016
Complexity of integrating with legacy systems	67%
Competing or higher-priority initiatives*	57%
Decentralized environment of state	47%
Cost of implementation	39%
Inadequate funding to support enterprise deployment*	31%

*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 24. States' current IAM initiatives

IAM initiatives	2016
Multifactor authentication	77%
Federated IAM for agency and third party*	48%
Privileged identity management solution	37%
Cloud-based IAM solution	27%
Citizen identity proofing solution*	15%

*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

CYBERTHREATS

CISOs view threats targeted at employees—including phishing, pharming, social engineering, and ransomware—as likely to be the most prevalent in the coming year (figure 25). This is a change from 2014, when attacks exploiting various vulnerabilities and foreign-sponsored espionage topped the list. CISOs continue to be "somewhat confident" in their states' abilities to protect against cyberthreats (figure 26). They appear most confident in their ability to protect against internal threats and least confident when it comes to threats originating from emerging technologies.

ASSESSMENTS

The majority of the states continue to perform ad-hoc assessments to evaluate their cybersecurity posture (figure 27). More frequent assessments could provide a better baseline for determining the effectiveness of cybersecurity controls.

CYBERSECURITY TECHNOLOGY ADOPTION

More states have adopted traditional cybersecurity solutions such as firewalls and

antivirus software (figure 28). CISOs indicate that security compliance, network behavior analysis, data protection, and IAM solutions lead the next wave of enterprise adoption.

CYBER LEGISLATION

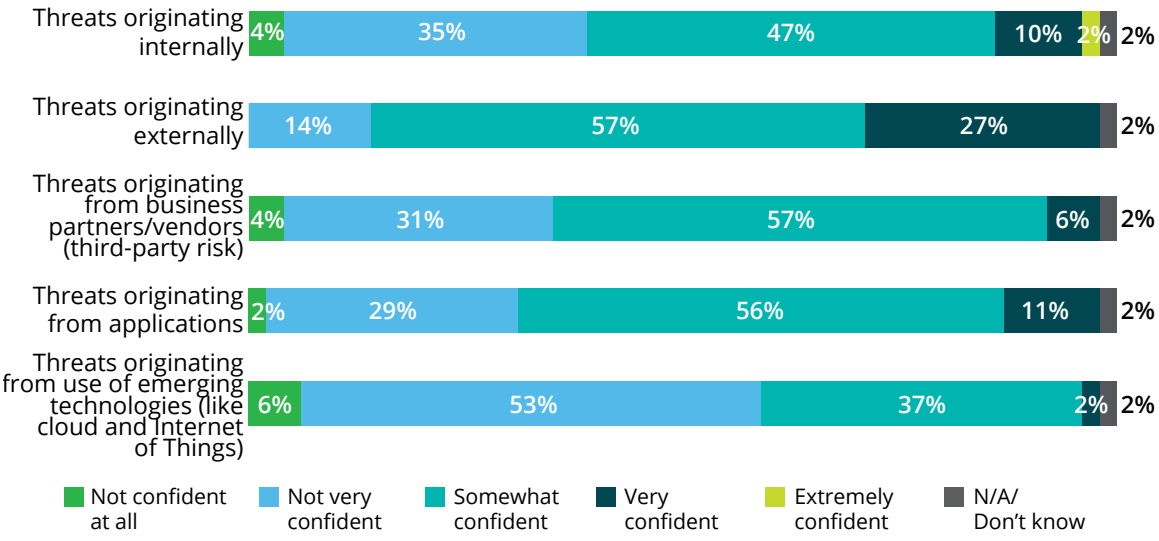
Several state legislatures have been active in providing guidance to CISOs regarding implementation of cybersecurity measures—particularly in the areas of data breach reporting and notification. However, most states do not have established cybersecurity legislation in place (figure 29). More than a quarter (29 percent) of states have reported an increase in funding from legislation and grant sources.

Figure 25. Prevalence of cyberthreats across state governments

	Somewhat higher threat	Very high threat
Phishing, pharming, and other related variants	35%	47%
Social engineering	31%	42%
Ransomware	43%	29%
Increasing sophistication and proliferation of threats (e.g., viruses, worms, and malware)	51%	14%
Exploits of vulnerabilities from unsecured code	45%	8%

Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

Figure 26. CISOs' confidence levels in protecting their state's information assets from cyber threats



Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

Figure 27. Frequency of cybersecurity assessments

	Monthly	Quarterly	Semi-annually	Annually	Ad hoc
Security code review	6%	2%	0%	8%	63%
Security risk assessment	0%	2%	2%	33%	54%
Internal penetration testing	17%	4%	4%	15%	52%
Application security vulnerability testing	13%	13%	2%	17%	50%
Cyber threat intelligence analytics	35%	2%	0%	2%	48%
External penetration testing	13%	2%	0%	29%	46%
Penetration testing conducted by third party	4%	6%	0%	33%	46%
Privacy impact assessment	0%	0%	2%	13%	44%
Cyber incident simulation or wargaming (to prepare for a cyberattack) and business continuity exercises	2%	6%	10%	33%	33%
Annual disaster recovery exercises and tests	2%	0%	10%	50%	29%
Security events monitoring/ security operations center	60%	0%	0%	6%	23%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 28. Top emerging technologies

		Plan to fully deploy or pilot within the next 12 months	Currently piloting	Fully deployed
Leading technologies being deployed or piloted in the next 12 months	Security compliance tools	**52%**	6%	21%
	Multifactor authentication	**49%**	14%	22%
	Federated identity management	**38%**	19%	19%
Leading technologies that are currently being piloted	Biometric technologies for user authentication	8%	**25%**	4%
	Network behavior analysis	29%	**21%**	27%
	Data loss prevention technology	37%	**20%**	25%
Leading technologies that are fully deployed	Firewalls	2%	0%	**96%**
	Antivirus	4%	0%	**92%**
	Spam filtering solutions	2%	2%	**90%**

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 29. Provisions of states' cyber legislation/statutes

	Established and funded	Established and not funded	In progress	Not in place
Cybersecurity incident/data breach reporting and handling	43%	21%	4%	32%
Data breach notification	41%	35%	2%	23%
Role and authority of the enterprise CISO or equivalent	40%	4%	2%	54%
Continuity of government/continuity of operations	35%	13%	4%	48%
Cybersecurity awareness	31%	4%	2%	63%
Data privacy provisions: authority and purpose; collection, storage, use, and sharing limitations	27%	21%	2%	50%
State-level cybersecurity program and framework for enterprise risk management	27%	17%	8%	48%
Cybersecurity budget allocation and review	26%	0%	4%	70%
Cyber threat information-sharing program between state agencies, law enforcement, and private entities	21%	10%	6%	63%
Public-private partnerships or council to support the state's cybersecurity programs	13%	2%	4%	81%
Cybersecurity workforce development and training	11%	4%	4%	81%
Cybersecurity legislative council or equivalent to do a periodic review, steer the state's cybersecurity posture, and allocate funding	11%	10%	6%	73%
Role and authority of the enterprise chief privacy officer (CPO) or equivalent	6%	2%	2%	90%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Moving forward

In the past two years, CISOs have moved their states forward in the fight against cyber risk. But the threat environment is so complex and evolving that many challenges remain. States faced with a myriad of priorities and ongoing resource constraints may be hard-pressed to allocate sufficient funding to cybersecurity initiatives. Competition for top talent can make it difficult to attract the professionals needed to effectively combat constantly evolving threats.

But CISOs do have one thing in their favor: State executives, including governors, are starting to pay more attention to the issue of cybersecurity. Those who are able to harness this attention have an opportunity to garner more resources and support for their initiatives. In order to make further progress, CISOs should think about the following:

- **Strategy:** Document and formalize the cybersecurity strategy. Going through the process of socializing the strategy with a broad range of stakeholders has a number of benefits. It ensures input from each of these parties, improving the overall strategy as a result. It strengthens collaborative relationships with other state agencies and departments. It raises awareness of cybersecurity issues. And finally, as our results have shown, it increases the chances of garnering more funding.
- **Funding:** Work with stakeholders to make cybersecurity a significant line item on state IT and business initiative budgets. For most states, cybersecurity is less than 2 percent of the overall IT budget. Cybersecurity is a business risk to state government, and funding should be commensurate with the risk.
- **Communications:** Use metrics and numbers to tell a compelling story about cyber risk. The fact that state officials are significantly more confident than CISOs about their states' ability to protect against cyber risk indicates that the right message still may not be getting across. State officials' lack of insight into the true business risks of cyberthreats could even affect funding. It is important for CISOs to step up the frequency of their communications—especially with agency business executives and legislators—and to communicate the risks more effectively.
- **Talent:** Promote the right benefits, modernize your workplace culture, and better define required skills to attract the right talent. The nature of what states have to offer workers has changed—which can be an advantage if positioned correctly. Millennials are not necessarily attracted by the promise of a secure retirement—something fewer states today are able to offer. Many of them find the prospect of "giving back" to be a more compelling reason to gravitate toward an employer. This, along with a rich training and development program, can serve as the basis for a campaign to recruit Millennial talent.

States should consider these components as they better define their strategy and look to create a higher level of awareness. These approaches can help CISOs continue their progress in combating cyber risks.

Appendix: Survey methodology

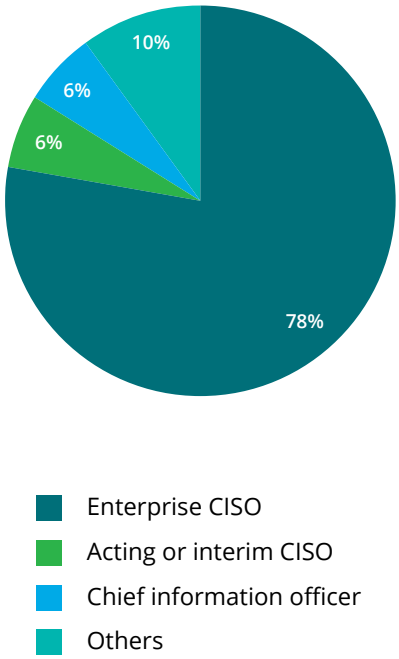
THE 2016 Deloitte-NASCIO cybersecurity study uses survey responses from:

- US state enterprise-level CISOs, with additional input from state agency CISOs and security staff members
- US state (business) officials, using a survey designed to help characterize how the state government enterprise views, formulates, implements, and maintains its security programs

CISO profile

CISO participants answered 59 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Participation was high: Responses were received from 49 states and territories. Figures 30–32 illustrate the CISO participants' demographic profile.

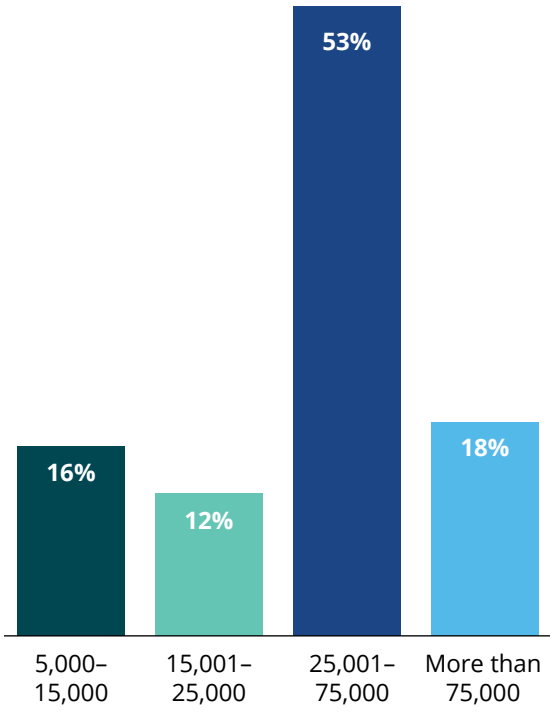
Figure 30. CISO survey respondent designation



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 31. Number of government employees in your state (excluding higher education employees)



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

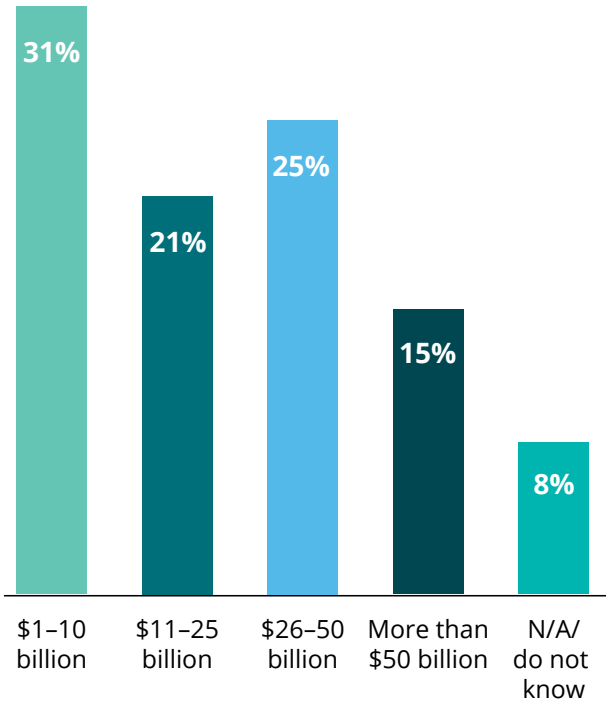
State official profile

Ninety-six state business and elected officials answered 15 questions, providing valuable insight into state business stakeholder perspectives. The participant affiliations included the following associations:

- National Association of State Budget Officers (NASBO)
- National Association of State Auditors, Comptrollers, and Treasurers (NASACT)
- National Association of Attorneys General (NAAG)
- National Association of Secretaries of State (NASS)
- National Association of State Personnel Executives (NASPE)
- National Association of State Chief Administrators (NASCA)
- National Association of State Procurement Officials (NASPO)
- National Association of Medicaid Directors (NAMD)
- National Emergency Management Association (NEMA)
- Federation of Tax Administrators (FTA)
- Governors Homeland Security Advisors Council (GHSAC)
- International Association of Chiefs of Police (IACP)—Division of State and Provincial Police (S&P)

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

Figure 32. Approximate annual budget of the respondent states (USD)



How Deloitte and NASCIO designed, implemented, and evaluated the survey

Deloitte and NASCIO collaborated to produce the 2016 Deloitte-NASCIO Cybersecurity Study. Working with NASCIO and several senior state government security leaders, Deloitte developed a questionnaire to probe key aspects of information security within state government. A CISO survey review team, consisting of the members of the NASCIO Cybersecurity Committee, evaluated the survey questions and assisted in further refining the survey questions.

In most cases, respondents completed the surveys using a secure online tool. Respondents were asked to answer questions to the best of their knowledge and had the option to skip a question if they did not feel comfortable answering it. Each participant's response is

confidential, and any identifying information was deleted after the preparation of the survey reports.

The data collection and analysis was conducted by DeloitteDEX, Deloitte's proprietary survey and benchmarking service. Results of the survey have been analyzed according to industry-leading practices and reviewed by senior members of Deloitte's Cyber Risk Services practice, the Deloitte Center for Government Insights, and Deloitte's Technology and Human Capital practices. In some cases, in order to identify trends or unique themes, data were also compared to prior surveys and additional research. Results on some charts may not total 100 percent based on answer choices such as "not applicable," "do not know," or "other."

Due to the volume of questions, and for better readability, this document reports only the data points deemed to be most important at the aggregate level. A companion report, including all questions and benchmarked responses, has been provided individually to the state CISO survey respondents.

ENDNOTES

1. National Governors Association, “Resource center for state cybersecurity,” http://www.nga.org/cms/statecyber, accessed September 10, 2016.

2. ITDashboard.gov, https://itdashboard.gov/; The White House, *President’s IT budget for FY 2017*, https://www.whitehouse.gov/sites/default/files/omb/egov/documents/fy17_agency_submission_topline.pdf.

3. Steven Greenhouse, “Pension funds strained, states look at 401(k) plans,” *New York Times*, February 28, 2011, http://www.nytimes.com/2011/03/01/business/01pension.html?_r=0.

AUTHORS

SRINI SUBRAMANIAN

Srini Subramanian is a principal in Deloitte & Touche LLP's Cyber Risk Services practice, and leads the Risk Advisory practice for state government. He has more than 27 years of IT experience and more than 16 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 NGA, NASCIO, and state committees to elevate cyber risk awareness in government.

DOUG ROBINSON

Doug Robinson has served as executive director of the National Association of State Chief Information Officers (NASCIO) since 2004. Founded in 1969, NASCIO is the only national organization representing state chief information officers of the 50 states and territories. His career spans over 35 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 for state government. 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.

CONTRIBUTORS

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

MEMBERS OF THE STATE CISO SURVEY REVIEW TEAM

Maria Thompson, State of North Carolina
Agnes Kirk, State of Washington
Marcos Vieyra, State of South Carolina
Erik Avakian, Commonwealth of Pennsylvania
Jim Edman, State of South Dakota
Elayne Starkey, State of Delaware
Deborah Blythe, State of Colorado

DELOITTE SUBJECT MATTER SPECIALIST CONTRIBUTORS

Bharane Balasubramanian, Deloitte & Touche LLP
Bill Eggers, Deloitte Services LP
Art Stephens, Deloitte Consulting LLP
Srini Subramanian, Deloitte & Touche LLP
John O'Leary, Deloitte Services LP
Peter Viechnicki, Deloitte Services LP
Mike Wyatt, Deloitte & Touche LLP

DELOITTE SURVEY TEAM, DATA ANALYSIS, AND BENCHMARKS

Balaji Kannan, Deloitte & Touche LLP
Pankaj Kamleshkumar, Deloitte Support Services India Private Limited

MARKETING

Annette Evans, Deloitte Services LP

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

Mark Price
US Public Sector Industry Leader
Deloitte LLP
1 617 585 5984
maprice@deloitte.com

Srini Subramanian
Leader, State Sector Risk Advisory Services
Deloitte & Touche LLP
1 717 651 6277
ssubramanian@deloitte.com

Ed Powers
National Managing Principal
Cyber Risk Services
Deloitte & Touche LLP
1 212 436 5599
epowers@deloitte.com

Mike Wyatt
Leader, State Cyber Risk Programs
Deloitte & Touche LLP
1 512 226 4171
miwyatt@deloitte.com

ABOUT DELOITTE AND NASCIO

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 the legal structure of Deloitte LLP and its subsidiaries. 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 transform legacy security programs to "Secure.Vigilant.Resilient.™" cyber risk programs. Deloitte's demonstrated approach and methodology helps its clients better align security investments with risk priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to thrive 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 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.

Deloitte.
University Press

Follow @DU_Press

Sign up for Deloitte University Press updates at DUPress.com.

Follow @NASCIO, #stateofcyber

About Deloitte University Press
Deloitte University Press 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 University Press is an imprint of Deloitte Development LLC.

About this publication

Cover art by Kotryna Zukauskaite