Handout #2

Deloitte.

NASCIO
Representing Chief Information Officers of the States

2014 Deloitte-NASCIO Cybersecurity Study

State governments at risk: Time to move forward

A publication of Deloitte and the National Association of State Chief Information Officers (NASCIO)

Contents

Message from NASCIO President

State Chief Information Officers (CIOs) consistently rank cybersecurity as a primary concern and priority—in light of the numerous cyber attacks on state and private sector systems, that ranking is not surprising. In the 2014 Deloitte-NASCIO Cybersecurity Study we asked state Chief Information Security Officers (CISOs) about those concerns and we have highlighted them here. What we found is that insufficient funding, sophisticated threats, and shortage of skilled talent threaten security and put state governments at risk.

For example:

- Although nearly half of the CISOs reported incremental increases to cybersecurity budgets, insufficient funding remains the leading barrier to battling cyber threats
- Further, approximately 6 in 10 CISOs cited an increase in sophistication of threats, up from roughly half in our 2012 survey
- Finally, the number citing a shortage of qualified cybersecurity professionals jumped to 59% in 2014 from 46% in 2012

Because of these challenges and the growing number of threats, CISO roles and responsibilities have changed in just the past two years – the position is maturing. However, in spite of roadblocks, CISOs continue to launch broad-based awareness campaigns, look for qualified talent and homogenize security practices. CISOs also continue to collaborate with their CIOs, state business leaders and the private sector.

The national survey data and recommendations for moving forward provide state CISOs and CIOs with information they need to work through the hurdles they face on a daily basis. Likewise, moving forward, NASCIO will continue to identify cybersecurity as a critical concern and priority of state CIOs, support a policy research agenda, advocate for increased funding and education on threat trends, and aid states in strategies to attract and retain qualified talent.

Craig P. Orgeron, PhD
NASCIO President and CIO, State of Mississippi

Foreword

Today's media headlines are filled with stories of cybersecurity incidents and their disturbing impact. Despite heightened attention and unprecedented levels of security investment, the number of cyber incidents, their associated costs, and their impact on the lives of U.S. citizens continue to rise. Cyber threats now permeate every aspect of life, and have become an important focus for Chief Executive Officers (CEOs) and board members of private corporations. As we embrace emerging technologies beyond cloud and mobile, such as wearable technology and internet-of-things (IOT), cybersecurity will continue to be critical to business.

States have also witnessed an increase of high-impact cybersecurity incidents since 2012 – incidents that have attracted public, media, and legislative attention. As a result, governors in affected states had to respond quickly to restore public trust. In 2013, the National Governors Association (NGA) established a resource center for cybersecurity as well as a policy council to advise state governors.

Since 2010, Deloitte and NASCIO have conducted biennial surveys of the state government enterprise CISOs to take the pulse of this critical issue. In the 2014 survey, our third to date, we see evidence of states' growing focus on improving their cybersecurity posture by placing more responsibility in the hands of CIOs and CISOs. State CIOs and CISOs continue to improve and standardize security services, launch broad-based awareness campaigns, and look for ways to attract the right talent to join them in their fight against cyber threats.

However, such advances are inadequate. In light of the increasing severity, volume and sophistication of cyber threats, compounded by lagging discovery times and longer restoration periods, states are becoming more vulnerable to cyber attacks. It is more important now than ever that they continue to identify collaborative approaches for addressing cyber threats. Consider the following:

- **States are facing persistent challenges:** CISOs continue to be impeded by constrained budgets, increasing sophistication of threats, and lack of cybersecurity professionals. These remain their top three barriers to fighting cyber threats.
- **State officials are more confident than CISOs:** An accompanying survey of state business and elected officials found that 60% had a high level of confidence in the ability of states to protect and defend against external cyber threats. Contrast that to the considerably smaller percentage – only a quarter of state CISOs, expressing a similar level of confidence. State leaders need to be better informed regarding the gravity of the situation. This disconnect may significantly undermine the CISOs' ability to gain funding and support for cybersecurity programs.
- **CISO role is maturing as well as expanding:** Results show that even as CISO responsibilities are evolving to encompass some of the more traditional responsibilities of a corporate risk and compliance executive, many CISOs are also becoming accountable for a range of other areas. CIOs and state leaders need to consider creative ways of allocating and managing these expanding responsibilities. A multi-pronged approach involving Chief Privacy Officers (CPOs), security technology leaders, agency business executives, and governors' offices, all working with the CISOs could help gain more executive accountability and support.

In this report, we offer thought-provoking suggestions for tackling cybersecurity challenges. It is our hope that states consider these ideas as they evolve and improve their cybersecurity programs.

Finally, we would like to acknowledge the support of all those who participated in the 2014 survey as reflected in the outstanding response rate:

- **49 state CISOs or their equivalents responded to the long version of the CISO survey**
- **186 state officials responded to the accompanying state officials survey**

Thank you for your continued recognition and efforts in aid of this important issue, and your commitment to helping states protect citizens' information and maintain the public trust.

Srini Subramanian
Principal
Deloitte & Touche LLP

Doug Robinson
Executive Director
NASCIO

Time to Move Forward

Trends and Challenges

CISO role maturing
98.0% have CISO role;
89.8% of CISOs report to CIO

Budget disconnect
47.9% have budget increases (YoY);
75.5% cited lack of sufficient budget as top challenge

Approved strategies are still largely missing

45% Absence of approved strategy

Role standardization
Over **96%** of CISOs shared similar top five functions

Confidence Gap
Ability to protect against external attacks;
Only 24% CISOs vs. 60% State officials

State officials

CISOs

Cyber threats
Increasing sophistication of threats **#2** barrier;
74.5% malicious code top external data breach

Talent crisis
59% of CISOs choose talent as #3 top barrier;
9 out of 10 choose salary as top barrier to staffing

Call to Action

Define and establish new executive roles
Support responsibilities with CPO and security technology roles

Communicate risks and impacts
Periodically communcate to business leaders to obtain commitment and funding

Document and approve
Define cybersecurity strategy to obtain appropriate funding

Define and measure
Establish metrics, align them to business values

Periodically assess security
Stay abreast of emerging technologies and threats; build vigilant and resilient capabilities

Collaborate with HR
Establish millenials-focused talent management

Embrace outsourcing of cybersecurity functions
Bridge the talent inadequacy

Key findings

Security is the top priority for state CIOs. While security has always been a priority it has never been at the top of the list – until 2014. Once considered just another item on state officials' busy to-do lists, cybersecurity has moved front and center, an issue that is increasingly drawing the attention not just of Information Technology (IT) departments, but state agency heads, legislators, and governors. The results of the 2014 Deloitte-NASCIO Cybersecurity Study confirm the growing importance of cybersecurity for states. The following key themes emerged from our analysis:

- **Maturing role of the CISO:** State CISO role continues to gain legitimacy in authority and reporting relationships. The responsibilities of the position are becoming more consistent across states, yet expanding. CISOs today are responsible for establishing a strategy, execution of that strategy, risk management, communicating effectively with senior executives and business leaders, complying with regulators, and leading the charge against escalating cyber threats using various security technologies.

- **Continuing budget-strategy disconnect:** The improving economy and states' growing commitment to cybersecurity have led to an increase – albeit small, in budgets. CISOs have also been successful at tapping supplemental resources, whether from other state agencies, federal funding, or various agency and business leaders. Nevertheless, budgets are still not sufficient to fully implement effective cybersecurity programs – it continues to be the top barrier for CISOs according to the survey results. In addition, survey responses show that there may be additional barriers to securing the budget: namely the lack of well-thought-out and fully vetted cybersecurity strategy. Without solid strategies to help them prioritize their activities, and program metrics that can track their progress, CISOs appear to struggle to gain the financial commitment of business leaders.

- **Cyber complexity challenge:** State information systems house a wide range of sensitive citizen data, making them especially attractive targets for cyber attacks. CISOs are concerned about the intensity, volume and complexity of cyber threats that run the gamut from malicious code to zero-day attacks. They need to stay abreast of existing and developing threats and increasing regulations to establish and maintain the security of an information environment that now increasingly extends from internal networks to cloud and mobile devices. Additionally, state officials appear more confident than CISOs in the safeguards against external cyber threats, perhaps a result of ineffective communication of risks and impacts.

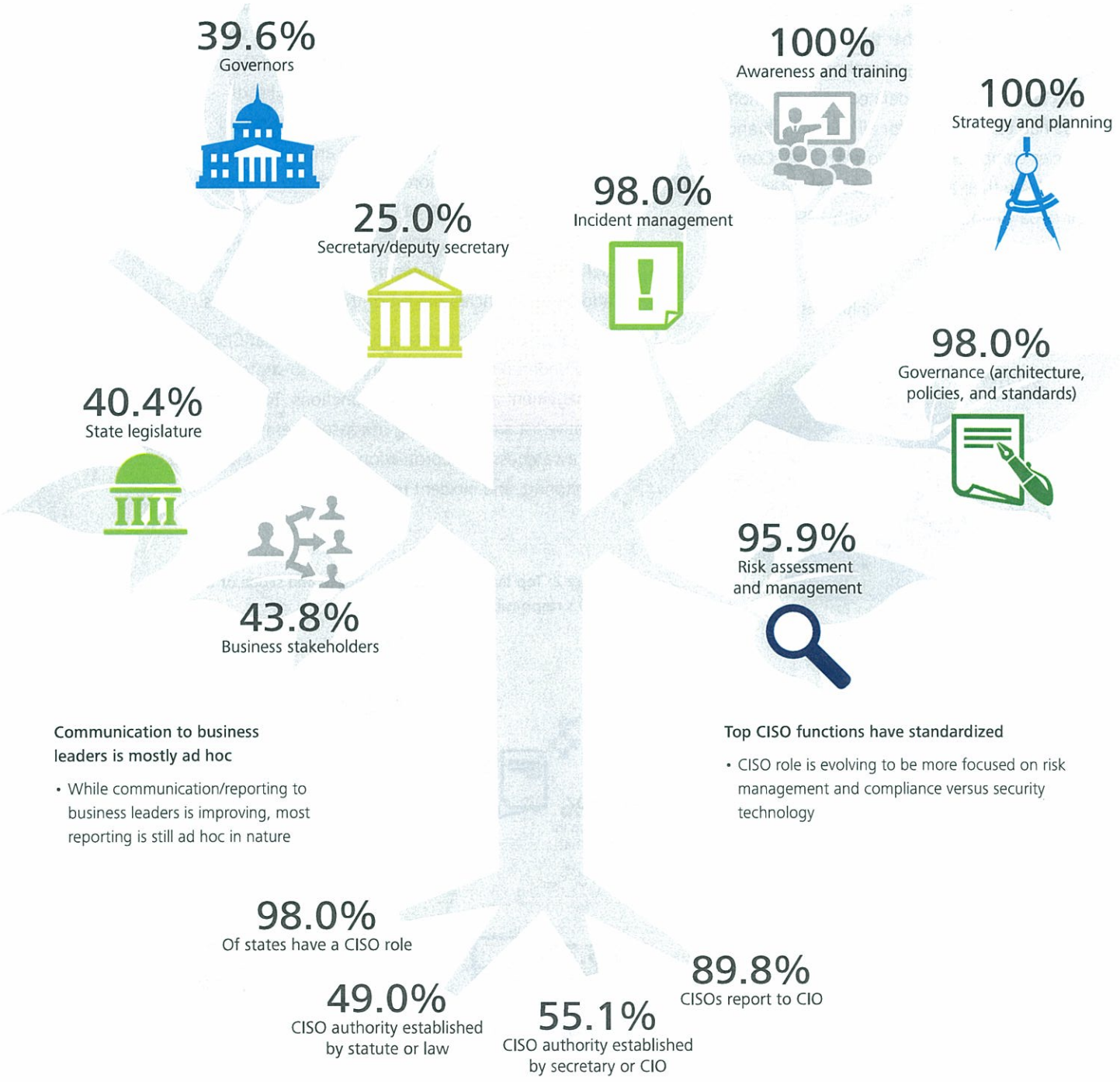
- **Talent crisis:** The skill sets needed for effective cybersecurity protection and monitoring are in heavy demand across all sectors. Private sector opportunities and salaries are traditionally better than those offered by government. Not surprisingly, state CISOs are struggling to recruit and retain people with the right skills, and they will need to establish career growth paths and find creative ways to build their cybersecurity teams. Furthermore, as states turn to outsourcing and specialist staff augmentation as a means to bridge their cybersecurity talent gaps, it's imperative for CISOs to manage third-party risks effectively.

The study compares the responses from CISOs and state officials, along with relevant results from the 2010 and 2012 Deloitte-NASCIO cybersecurity studies. These comparisons provide additional context for evaluating the implications of this year's results.

I. Maturing role of the CISO

Given the enormous array of cyber threats that impact state governments, it is apparent that the state CIOs are looking to the top professional charged with protecting their information assets – the CISO. As a result, the CISO position is gaining in importance, becoming better defined, and calling for more consistent capabilities.

Maturing role of the CISO

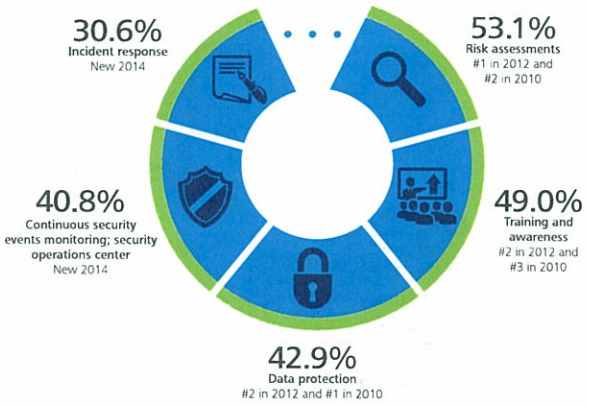


CISO role has gained legitimacy

Ninety-eight percent of states have established an enterprise CISO role. Today, nine out of ten CISOs report to the CIO or equivalent versus about three-quarters in 2012.

In a further indication that states are acknowledging the importance of CISOs, the position is increasingly being established by either the agency secretary and/or by statute. The scope of authority for state CISOs is also becoming better defined. In 2014, more CISOs had responsibility for all executive branch agencies compared with two years ago. Conversely, only 2% say their authority does not extend beyond their department, compared with 12% two years ago.

Figure 1: Top five cybersecurity initiatives for 2014

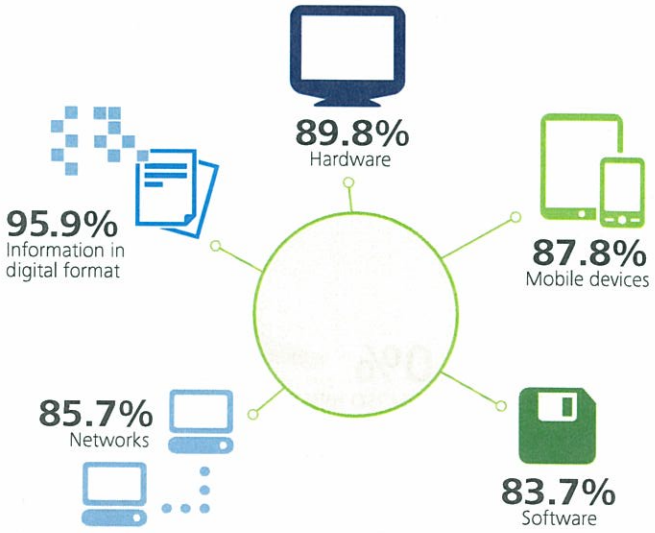


Responsibilities are becoming more standardized

Within the past two years, the CISO role has become better defined – position descriptions are more standardized, and expectations across the different states are more consistent. At the same time, the responsibilities associated with the CISO position are expanding rapidly. Compared with 2012, we found that a much higher percentage of CISOs are performing similar functions in a long list of responsibilities. For example, all respondents said they were responsible for strategy and planning, as well as training. Yet, more CISOs indicate they have also taken on oversight of various technical security functions since 2012, including network security and perimeter defense and vulnerability management– adding to the increasing list of their responsibilities.

The range of top cybersecurity initiatives that CISOs have undertaken indicate more focus to strategy, risk management and compliance functions. Top on their initiative list are performing risk assessments, training and awareness, data protection, continuous event monitoring, and incident response.

Figure 2: Top five areas within mandate and scope of the CISO's responsibility



Communication has increased, but there is more to do

An important component of the CISO's job is communicating with stakeholders – from the general public to the governor. Due to the increased visibility of cyber incidents, governors and legislators are requesting formal reports on cybercrime and what is being done to combat it. Nearly four out of five CISOs now send reports to the governors, versus only three out of five in 2012 – likewise, the number who send reports to their state legislature has also increased significantly. To satisfy this growing demand for information on cybersecurity, CISOs will need to find better ways to collect and use metrics for monitoring the intensity and frequency of threats, as well as for evaluating the effectiveness of their strategies.

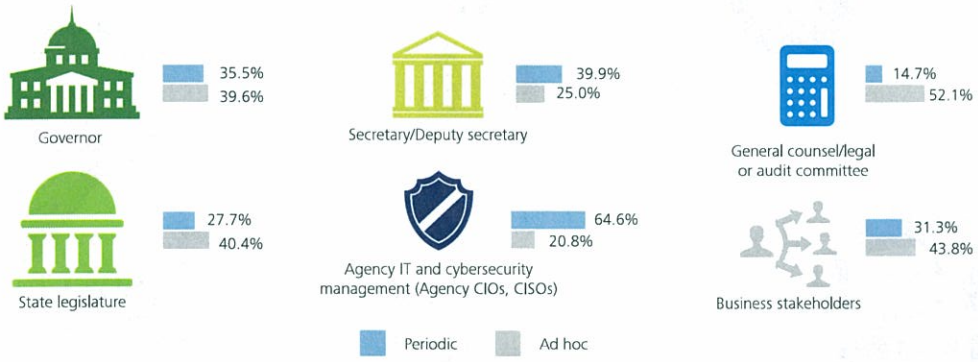
CPOs to complement CISOs?

Increasingly, states have begun to establish the position of CPO – 30% of the states reported that they have a CPO, compared to 18% in 2012. This is an encouraging trend because it helps CISOs focus on their mission, while the CPOs aid in communication to business leaders in their citizen privacy and trust advocacy role. Given that CISOs' responsibilities include governance, risk management, and compliance, there will be a need for collaboration between CISOs and CPOs on strategy, reporting to business leaders and legislatures, and measurement.

Figure 4: States with enterprise CISO and CPO roles

	2014	2012
CISO	98.0%	96.0%
CPO	29.2%	18.0%

Figure 3: While reporting has improved, it is still largely ad hoc in nature



Moving forward

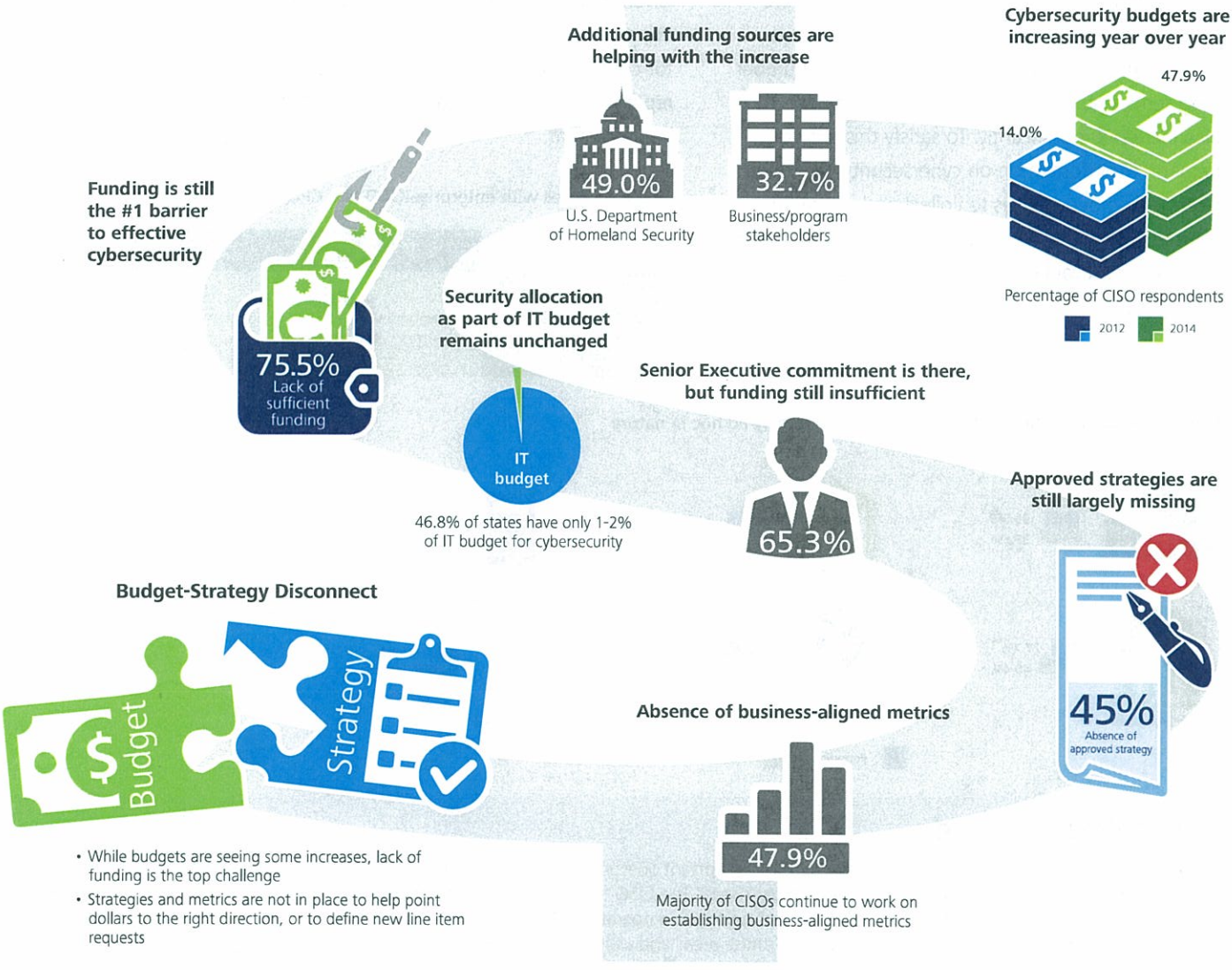
As CISOs take on more and more responsibilities, an important question arises: Have the responsibilities become too diversified for one executive to handle? If so, what priorities take a back seat? The CISO function might evolve to manage three broad areas: a) governance, risk, and compliance; b) privacy; and c) security technology and operations. While one or more positions may still report to an elevated CISO position, having leaders who specialize in each of these areas and assigning them resources can help improve program efficiency.

- CISOs could continue to manage the strategic, risk management, and regulatory/compliance functions that have always been core to the role. Improving communication with elected and appointed business leaders and agency/program leaders regarding risks, and navigating the increasingly complex regulatory environment, will also be important to their role.
- Enterprise-level privacy officers can help determine which data needs to be protected and why. They also play an important role safeguarding citizen privacy and restoring trust when an incident occurs. Working together, privacy officers and CISOs are better positioned to gain business leadership support for their programs.
- The technical and operational aspects of security management are a better fit for a security executive with a deeper IT infrastructure and operations background.

II. Budget-strategy disconnect

Budgets are the financial manifestation of an organization's strategy. CISOs acknowledge that their budgets have increased from past years, but believe they are still insufficient to establish a strong security posture for their states. CISOs continued to cite the lack of adequate funding as the top barrier to program effectiveness, consistent with both the 2010 and 2012 surveys.

Budget-strategy disconnect



- While budgets are seeing some increases, lack of funding is the top challenge
- Strategies and metrics are not in place to help point dollars to the right direction, or to define new line item requests

The budget landscape is improving

After years of strapped budgets, states are allocating more money for cybersecurity. Almost half of the states report increases in year-over-year budgets. This is in contrast to 2012, when more than three-quarters of respondents said their budgets were either decreasing or staying the same.

Figure 5: Cybersecurity budgets have increased (YoY)

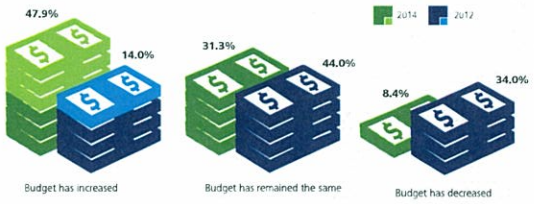
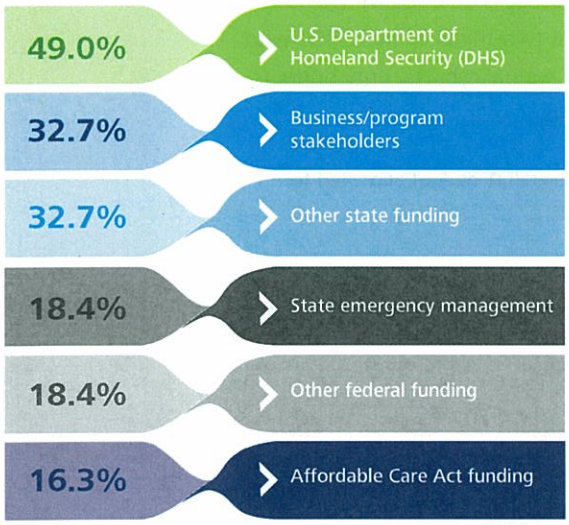
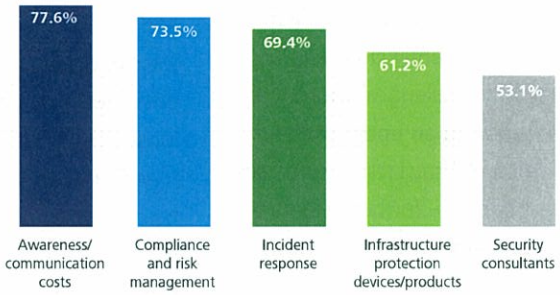


Figure 6: Additional sources that contribute to fund cybersecurity initiatives



CISOs also reported that they have been effective in identifying other sources of funding for cybersecurity initiatives. The majority of CISOs find additional support through such channels as the U.S. Department of Homeland Security, business or program stakeholders, and other state funding sources, as well as Affordable Care Act-related funds.

Figure 7: Top five areas covered within cybersecurity budgets

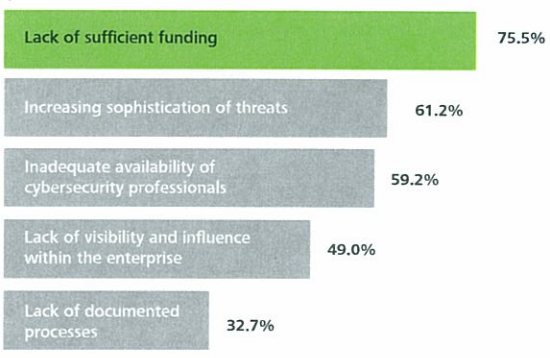


Yet, budget continues to be the top barrier...

Despite some improvement, cybersecurity still makes up a relatively small portion of states' overall IT budgets – just under half of respondents place it between 1% and 2%, while an additional 11% say it commands between 3% and 5%. About three-quarters of the CISOs cite the lack of sufficient funding as a major barrier to addressing cybersecurity challenges in their states. Business leaders concur with the CISOs' assessment: lack of funding was the most frequently cited barrier to addressing cybersecurity challenges. More than half of the states that reported an uptick in their annual budget since 2012 still say lack of sufficient funding is their biggest barrier – further evidence that budgets need to increase substantially to be sufficient.

One reason CISOs may be especially concerned about the adequacy of budgets is that they are beginning to take on a broader mission with an increased range of activities. In others words, CISOs are taking on more initiatives with budgets that were already inadequate. CISOs indicate that the leading areas covered in cybersecurity budgets include awareness/communication, compliance and risk management, and incident response. Compared to 2012, more CISOs accept these areas as part of their cybersecurity budgets. As cybersecurity needs increase, there is also greater competition for resources among these different initiatives, forcing a need to prioritize. Budgets will certainly need to grow if states are to appropriately fund all the areas encompassed by CISOs' expanding missions.

Figure 8: Lack of sufficient funding continues to be the #1 barrier since 2010

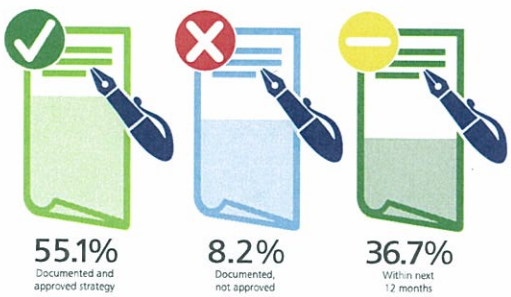


Strategy still lags

Let's face it. Considering that lack of budget has been cited as a top barrier since this survey's inception in 2010, and that security spending as a percentage of IT still is in the 1% to 2% range, funding will probably always be an issue unless CIOs and CISOs take deliberate actions. Since increasing their budgets is a top priority for CISOs, they need better ways to convince business executives to loosen their purse strings. Yet without a strategic roadmap that is aligned to program priorities, it is hard for them to garner funding from key decision makers. In fact, the survey data suggests that having an approved strategy is an effective way to increase funding. About two-thirds of the CISOs who indicated a rise in their annual cybersecurity budgets had an approved strategy.

Figure 9: Percentage of overall IT budget allocated to cybersecurity

Figure 10: Half of the states maintain a cybersecurity strategy



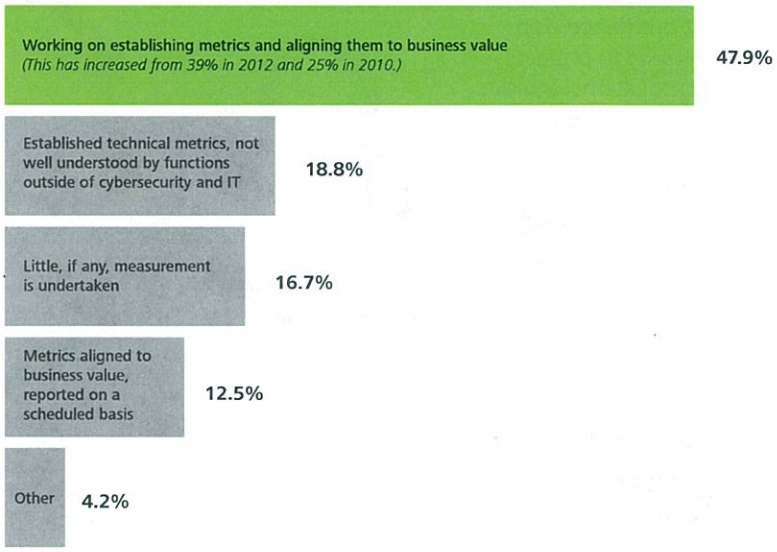
Measurement is a work in progress

In addition to strategy, it is important for CISOs to be able to gauge whether cybersecurity programs are effective. But for this, they need tools such as key risk indicators and metrics, dashboards, and benchmarking to help them assess and report on performance to business leaders. Most CISOs say that measuring and demonstrating effectiveness is a work in progress. While the number of states that have established and regularly report performance metrics has increased slightly, such concrete evaluation is still lacking. About half of CISOs say they are working on establishing metrics, a modest increase from 2012. Clearly, this is a significant development opportunity.

Improvement is also needed when it comes to conducting assessments of states' cybersecurity risk posture. Although the number of states that perform scheduled reviews is increasing, the majority of the CISOs continue to indicate that any reviews they perform are ad hoc in nature. While the number of states that conduct application security vulnerability testing and code reviews on a quarterly basis has nearly doubled since 2012, this still constitutes only about a quarter of states. Frequent communication with business stakeholders regarding cyber risks or system vulnerabilities is a sign of improving program maturity.

Another important aspect of measurement is assessing the financial impact of security breaches. More states have begun to calculate the cost of breaches. In 2012, three-fifths of respondents said they either didn't measure monetary damages or didn't know; by 2014, that number had shrunk to a third.

Figure 11: Majority of CISOs indicate that they continue to work on establishing metrics and aligning them to business value



Moving forward

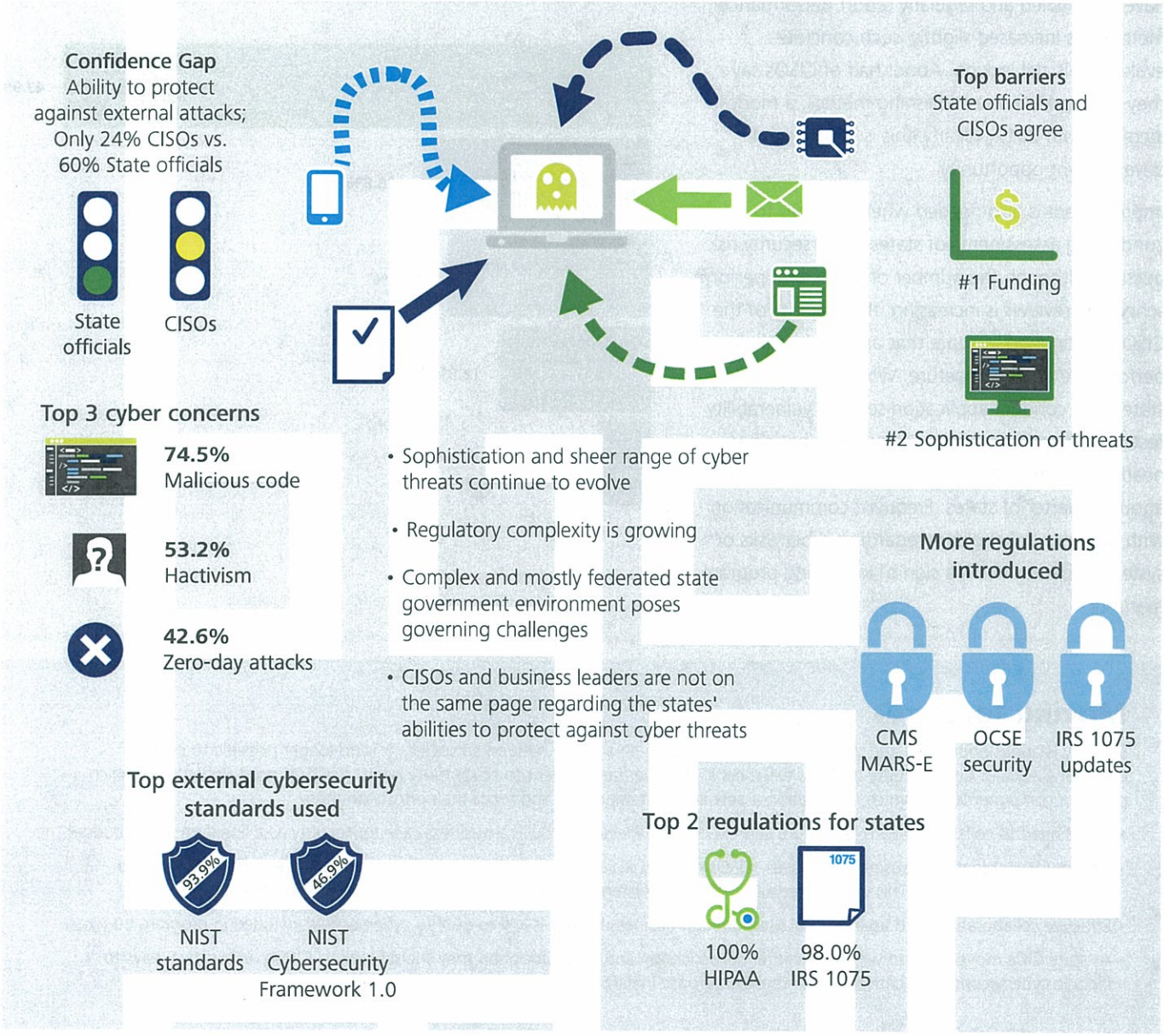
Strategy is about prioritizing and deliberately choosing paths. In a highly networked society, it is no longer possible to protect everything equally. Cybersecurity budgets will most likely never be sufficient to cover every need, so CISOs must understand which program components and which information assets are most important and focus their efforts on these.

- CISOs need to collaborate with legislators and executive leadership to build a business case for security as a line item in the budget.
- For new technology and business initiatives, CISOs need to work with state CIOs to allocate a reasonable percentage of their budgets to cybersecurity. This will help ensure that future systems incorporate the appropriate cybersecurity measures.
- Effective collaboration with agency-level program and business leaders is key to getting cybersecurity included in program budgets.
- As state CIOs move forward with data center consolidation and cloud adoption they should look to CISOs for creative ways to include cybersecurity as a critical part of these enterprise initiatives.

III. Cyber complexity challenge

States today are subject to a growing number of sophisticated cyber attacks that range from data breaches to the political protests of hacktivists —individuals who break into computer networks to promote their political agendas. Within just the past few years, a number of high-profile attacks on states have resulted in loss of Personally Identifiable Information (PII) of millions of citizens, including social security numbers, payment card records, dates of birth, driver's license numbers, and tax data. These incidents have cost states millions of dollars in clean-up costs, as well as loss of both revenues and public trust.[1] The problem is not likely to go away any time soon, as cybercriminals continue to be drawn to the wealth of data residing within each state.

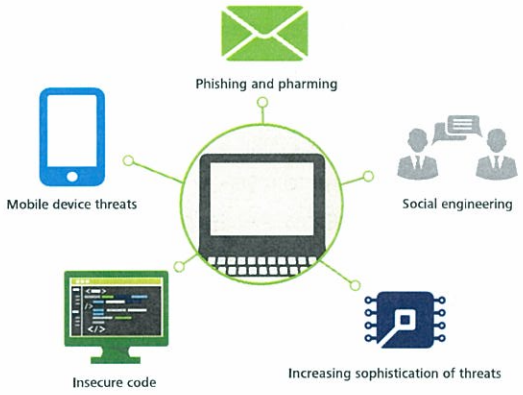
Cyber complexity challenge



Cyber threats are a moving target

The sophistication and sheer range of cyber threats continue to evolve rapidly, making the CISO's job of safeguarding the state's information assets extremely difficult. Staying current on emerging technologies and the cyber threat landscape is a significant challenge for CISOs; in fact, three out of five survey respondents cited the increasing sophistication of threats as a major barrier to addressing cybersecurity in their states. Layer on budget and talent constraints, and it's even more of an uphill battle.

Figure 12: Top cyber threats that the CISOs are most concerned with



CISOs are especially concerned with activities that prey on vulnerable users of information systems. Eighty percent agree that the next 12 months will bring an increased threat of pharming and phishing scams, while 72% believe the same of social engineering schemes. Another top concern for CISOs is threats that exploit vulnerabilities in mobile devices. It is clear that a focus on end-user education is a priority.

Malicious code continues to be the CISO's most dreaded channel for a data breach. But in 2014, two other cyber threats newly added to our list claimed second and third place: hacktivism and zero-day attacks—the latter referring to security risks as yet unknown to hardware and software vendors.

Figure 13: Adoption of NIST Cybersecurity Framework 1.0

Regulatory complexity is growing

In an effort to protect citizen data from cyber threats, federal and state governments have passed a spate of new regulations that stipulate the timeframe for notifying legislators, citizens, and federal agencies when there is a breach. For example, the Internal Revenue Service (IRS) requires incident notification within 24 hours, and the Centers for Medicare and Medicaid Services (CMS) incident notification requirement is an hour from the time a state agency detects an incident has occurred. Within the past two years, CISOs have attempted to address additional security requirements from new regulations, including the CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E), new updates to the Internal Revenue Service (IRS) 1075 publication and the Office of Child Support Enforcement (OCSE) security requirements.

Most states adhere to the Commerce Department's National Institute of Standards and Technology (NIST) guidelines. In February 2014, NIST released Version 1.0 of its Cybersecurity Framework to help organizations that oversee the country's financial, energy, health care, and other critical systems secure their information against cyber attacks.[2] The Framework is beginning to gain traction. Nearly two out of five CISOs say they are currently reviewing the Framework, with an additional 47% saying they plan to leverage it within the next six months to a year.

Most states appear relatively watchful about reviewing their cybersecurity policies for compliance with regulations and alignment with industry standards. Seventy-five percent of respondents indicated a review within the past year. Both internal and external security audits continue to reveal a number of gaps in state cybersecurity measures. According to the survey, the most frequent gaps are access control, risk assessment, and configuration management. Nearly half of the respondents (49%) indicate a lack of visibility and influence within the enterprise as one of their top barriers, impacting the ability of CISOs to enforce compliance measures consistently across the agencies.

Figure 14: Leading regulations with which states need to comply

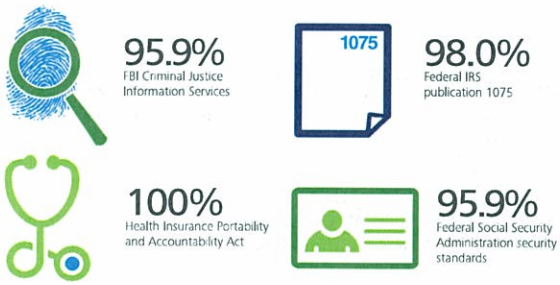
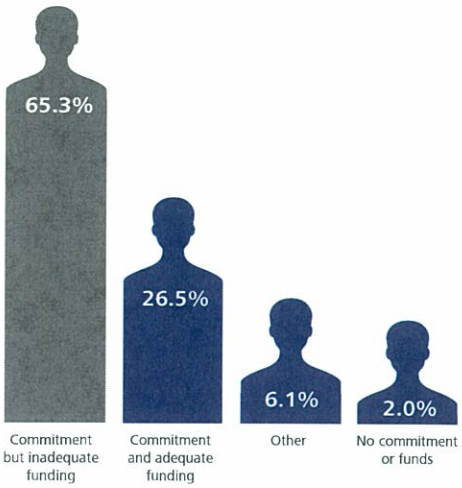


Figure 15: Senior executive support (Governor's office or CIO) to address cybersecurity regulatory and legal requirements

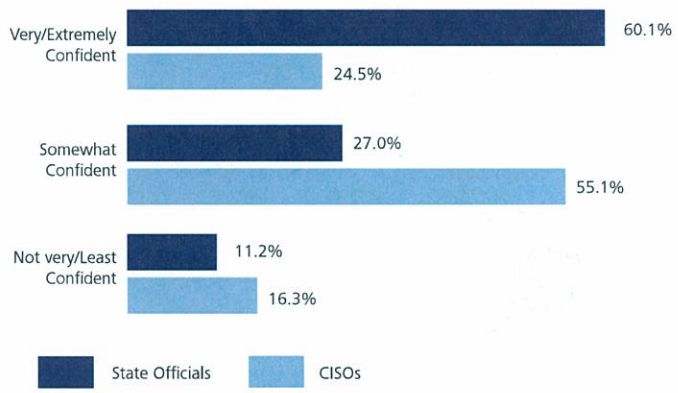


CISOs and business leaders have a confidence gap

The mostly federated and agency program-driven governance of states makes it a challenge to forge a strong alliance with business, program and elected leaders. Furthermore, regular changes to the appointed and elected leadership is the norm in states which necessitates a deliberate focus on leadership relationship management. The complexity of the state government environment makes CISO/CIO communication with the business leaders a continuing challenge.

Consider how the challenge is manifesting in a communication gap. As CISOs continue to battle the wide-ranging cyber threats bearing down on their states. There appears to be a discrepancy between them and business stakeholders when it comes to how confident they are that their efforts are succeeding against these continueing threats. A high percentage of state official respondents (60%) indicated that they are very or extremely confident that their state's information assets were protected against external cyber threats. However, only 24% of the CISO survey respondents expressed a similar sentiment. The higher degree of confidence among business leaders indicates the need for state CISOs to do a better job of communicating risks and potential impacts to business stakeholders. Improving this communication and closing the confidence gap will likely help address the budget challenge as well.

Figure 16: State officials and CISOs are not aligned in their level of confidence of the states' abilities to protect against external cyber threats



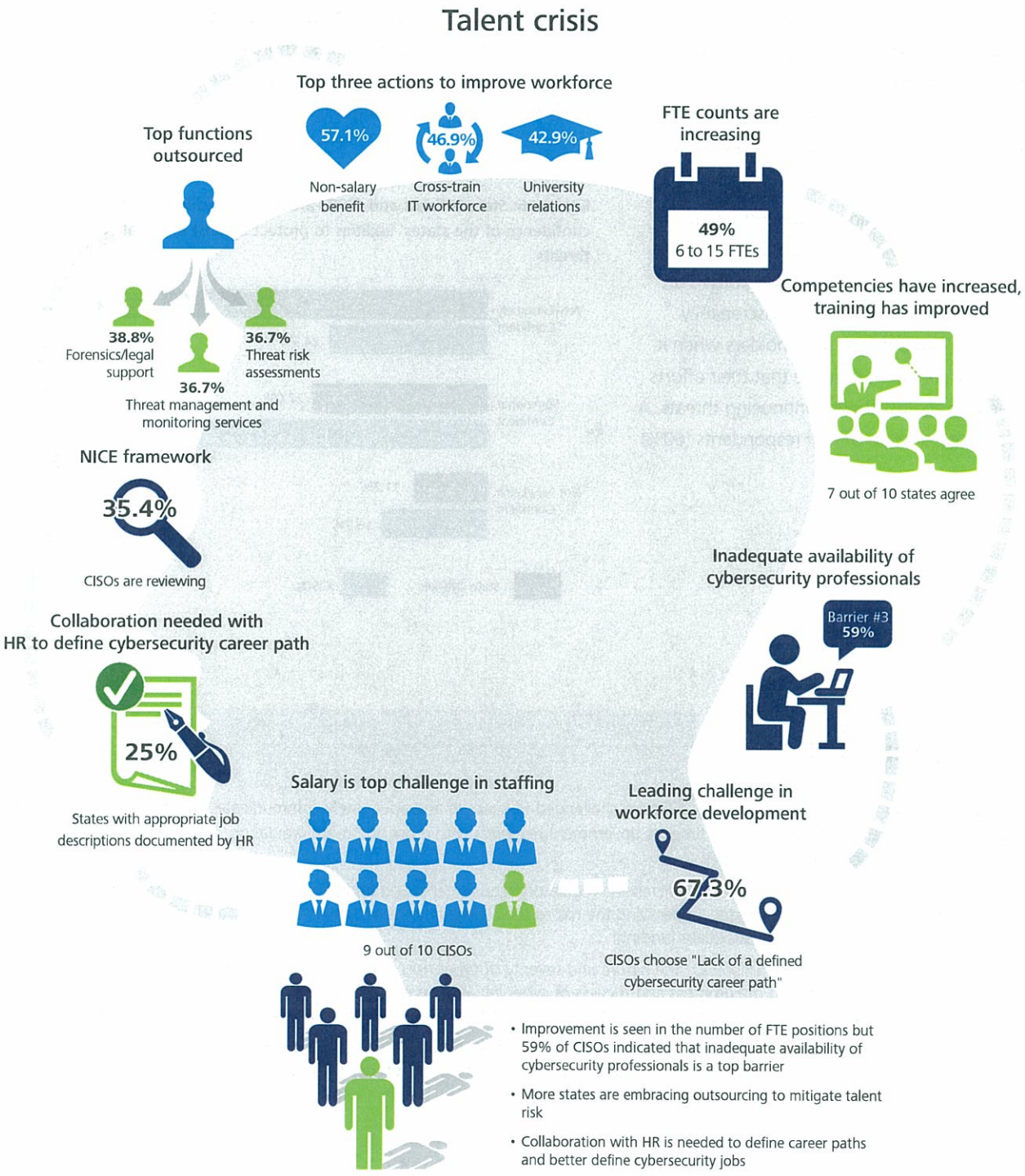
Moving forward

As the complexity of cyber threats increases, CISOs are challenged to keep up and adequately communicate with stakeholders about the critical nature of these threats. At the same time, as government responds with more and more regulation, CISOs will have to devote significant resources to compliance activities.

- There is an opportunity for CISOs to use both increasing regulatory requirements and audit findings to gain the attention of business and program executives. Business stakeholders understand the risk to their program mission when regulatory and audit issues are not addressed and are more likely to respond with adequate funding.
- It is critical for CISOs to clearly communicate the nature and severity of cyber risks to business, agency program, and legislative leaders and stakeholders. Simply reporting on the progress and success of cyber initiatives is not enough. In fact, it seems to be resulting in unwarranted complacency on the part of business leaders, who are more confident than CISOs in their state's ability to protect against threats.
- The defense mechanisms need to evolve – they can't rely on protection of the perimeter alone. CISOs need to develop threat-monitoring plans for early detection of incidents and be prepared to respond when incidents do occur. They also need effective recovery plans so that operations can be up and running quickly after a cyber incident.

IV. Talent crisis

To keep information safe, organizations need employees with skills in cybersecurity – skills that require continual updating as cyber-threat actors develop ever-more sophisticated ways of infiltrating IT infrastructures. Government agencies at the federal, state, and local levels are hard-pressed to compete against the private sector for technology talent. As cybersecurity threats increase for private companies and government alike, the need for employees with coveted cybersecurity skills is likely to become even more acute.



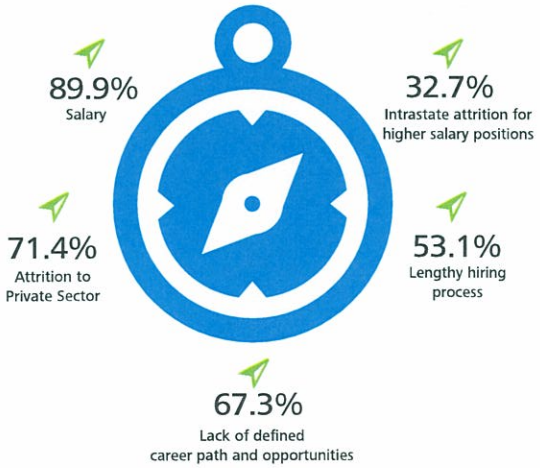
The right talent is hard to find

Despite the fact that only 2% of CISOs point to talent management as a top priority, down from 10% in 2012, CISOs believe that the scarcity of qualified professionals willing to work in the public sector is one of the biggest barriers to effectively addressing cybersecurity challenges.

According to nine in ten respondents, the biggest challenge in attracting talent to state cybersecurity positions comes down to salary, hardly surprising in this seller's market for cybersecurity talent. Lack of a clear career path and the lengthy state hiring process were also cited as obstacles by a large percentage of respondents. What's more, only a quarter of respondents say their states have adequately documented the required competencies for cybersecurity positions as part of job descriptions, which may further hinder their ability to attract the appropriate talent. Even when states are successful at recruiting top talent; however, the lure of the private sector often makes them difficult to retain.

Nevertheless, CISOs are doing their best to both grow and strengthen their organizations. Nearly half of states now have cybersecurity staffs numbering 6 to 15 FTEs compared with less than two-fifths in 2012, while the number with smaller staffs of 1 to 5 FTEs has fallen significantly.

Figure 17: Top five challenges in attracting and retaining talent



CISOs say their states use a variety of strategies to attract cybersecurity employees, including promoting non-salary benefits, cross-training and developing other state IT employees, fostering relationships with state universities, and communicating such benefits as job stability compared with the private sector.

Collaboration with state HR departments to develop better ways to attract and retain talent is a growing necessity. CISOs feel that their state HR departments need to establish cybersecurity career paths and improve job descriptions to attract employees whose skills are aligned with cybersecurity priorities.

Figure 18: Number of dedicated cybersecurity professionals in the state's enterprise security office

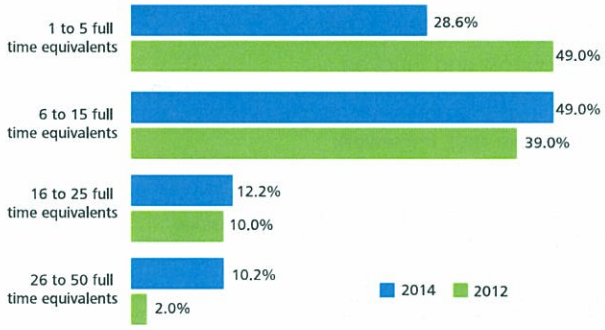


Figure 19: Top four state strategies to retain cybersecurity talent

Training has become a priority

CISOs are gaining more confidence in their staffs. Only one in ten said employees have large gaps in competencies versus nearly a quarter in 2012, and a greater percentage said their employees are up to the job compared with two years ago. CISOs are also becoming more proactive about closing competency gaps, and cybersecurity training is a priority. Almost all CISOs said they provide annual or more frequent training to employees and contractors, up significantly from 2012. Furthermore, CISOs say their departments have become much more self-sufficient in providing cybersecurity awareness to their employees based on job role and function.

A majority of CISOs indicated that they are either reviewing or implementing portions of the NIST National Initiative for Cybersecurity Education (NICE) Framework to prepare, educate, recruit, train, develop, and retain a diverse cybersecurity workforce.[3]

Figure 20: States' adoption of NICE framework

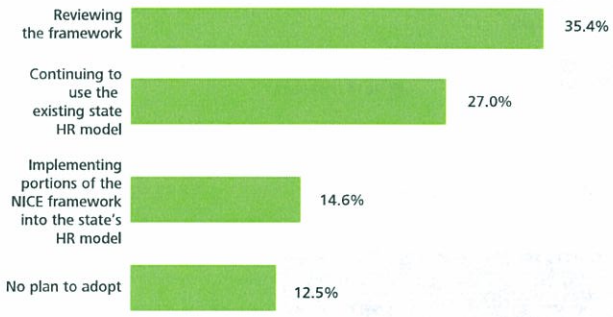
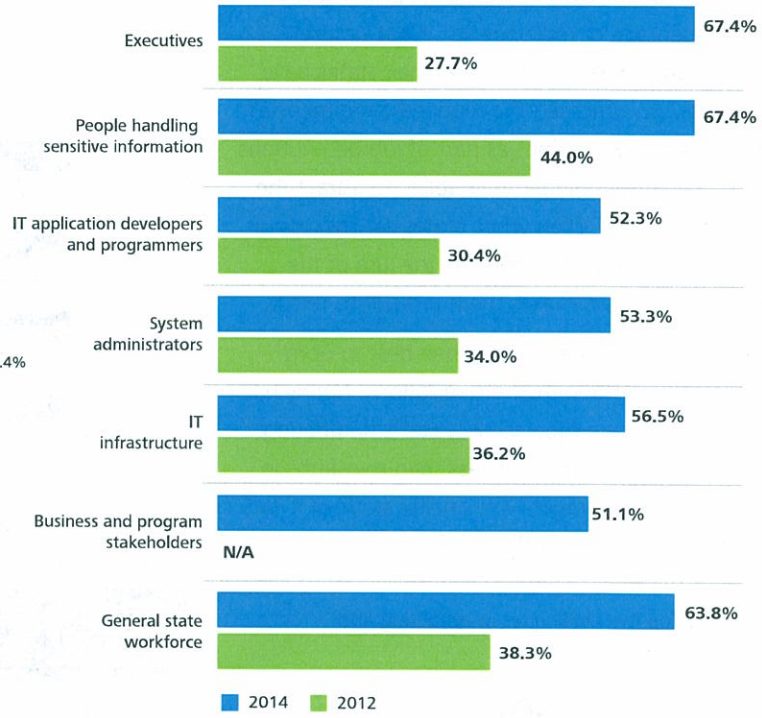


Figure 21: States have significantly increased training for their staff



Outsourcing has become more accepted

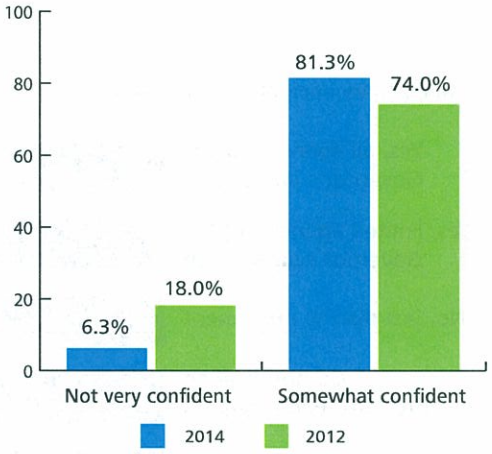
Outsourcing is one way to compensate for talent gaps. For CISOs who are restricted in their ability to hire workers, or who are having trouble attracting employees with the required skill sets, outsourcing certain aspects of cybersecurity work is an option. The most frequently outsourced functions include forensic and legal support, risk assessment, and threat management and monitoring.

About a third of CISOs said they do have knowledge of third-party cybersecurity capabilities and have identified controls and agency dependencies. However, only a minority review and test them regularly. The majority of states are managing third parties' performances by requiring that they adhere to state cybersecurity policy and controls.

Somewhat disturbingly, most CISOs said they are only somewhat confident in the cybersecurity practices of third parties, suggesting that more needs to be done to evaluate and maintain the adequacy of cybersecurity practices of third parties.

Figure 22: Leading outsourced cybersecurity functions

Figure 23: CISOs confidence levels in cybersecurity practices of third parties



Moving forward

State governments are in a difficult position when it comes to competing with the private sector for cybersecurity talent. CISOs need to look at more creative ways to build their teams and ensure that they enlist the support of people with cutting-edge skills in cybersecurity.[4]

- The scarcity of talent means that private sector partnership will likely need to be part of the talent mix. CISOs should provide training to their staff to effectively manage teams that may include members from third parties. Third-party partnerships may cover activities ranging from managing security functions to providing specialist augmentation.
- Millennials are likely to be an important source of talent in the cybersecurity arena. Attracting Millennials is a whole new ballgame; factors that motivate them are often different from what has appealed to previous generations. Rather than job stability and money, Millennials tend to look for work that "makes a difference," a more entrepreneurial work environment, and job variety and flexibility. Cybersecurity work certainly fits the bill for making a difference, and CISOs need to make sure this message is adequately communicated.
- The skill sets required for cybersecurity work are unique. States need to do a better job of mapping these competencies and creating well-documented job descriptions. There is a need for dedicated HR professionals who can partner with CISOs to ensure the right talent is coming in the door. Knowledgeable HR professionals can also work with CISOs to redefine the cybersecurity career path and create strong learning programs that develop and grow the right talent from the start.

Emerging Trends

Enterprise Identity and Access Management (IAM)

Enterprise IAM solutions are important for states. They provide data access rights to the right individuals and help organizations comply with increasingly stringent compliance standards related to the management of digital identities.

While about a third of states have some form of an enterprise IAM solution, over half have yet to implement one. For states that have not adopted an approach to IAM, results show the primary barriers to implementation are a decentralized environment, the complexity of integrating with legacy systems, and lack of governance. CISOs say their states are involved in a range of initiatives, including multi-factor authentication, federated IAM for agencies and third-party providers, and implementing privileged identity management solutions.

Figure 24: Adoption of enterprise IAM solution

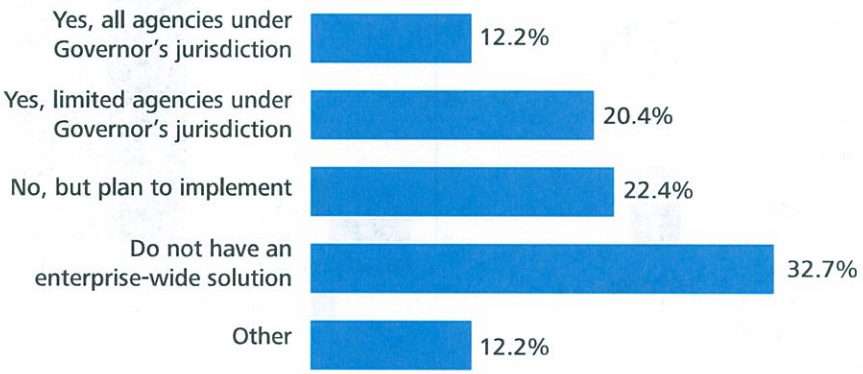
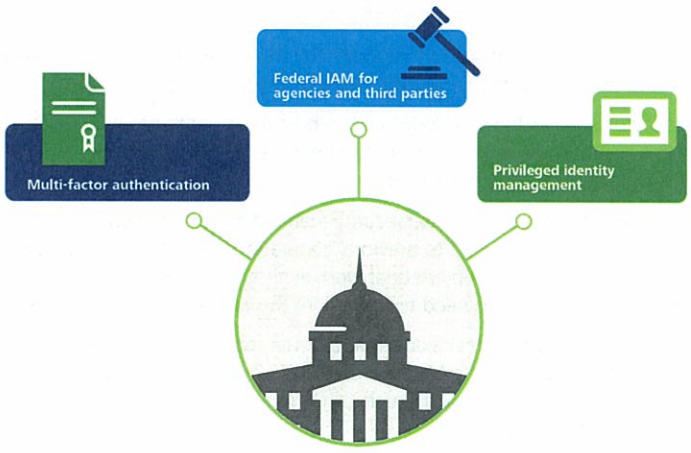


Figure 25: Leading IAM initiatives in states



Privacy

The unprecedented growth of social media, paired with a series of high-profile stories on government accessing citizens' personal information, has made privacy a hot-button issue. CISOs cite a wide range of privacy concerns, most prominently unauthorized access to personal information, compliance with privacy statutes, and managing information sharing with third parties.

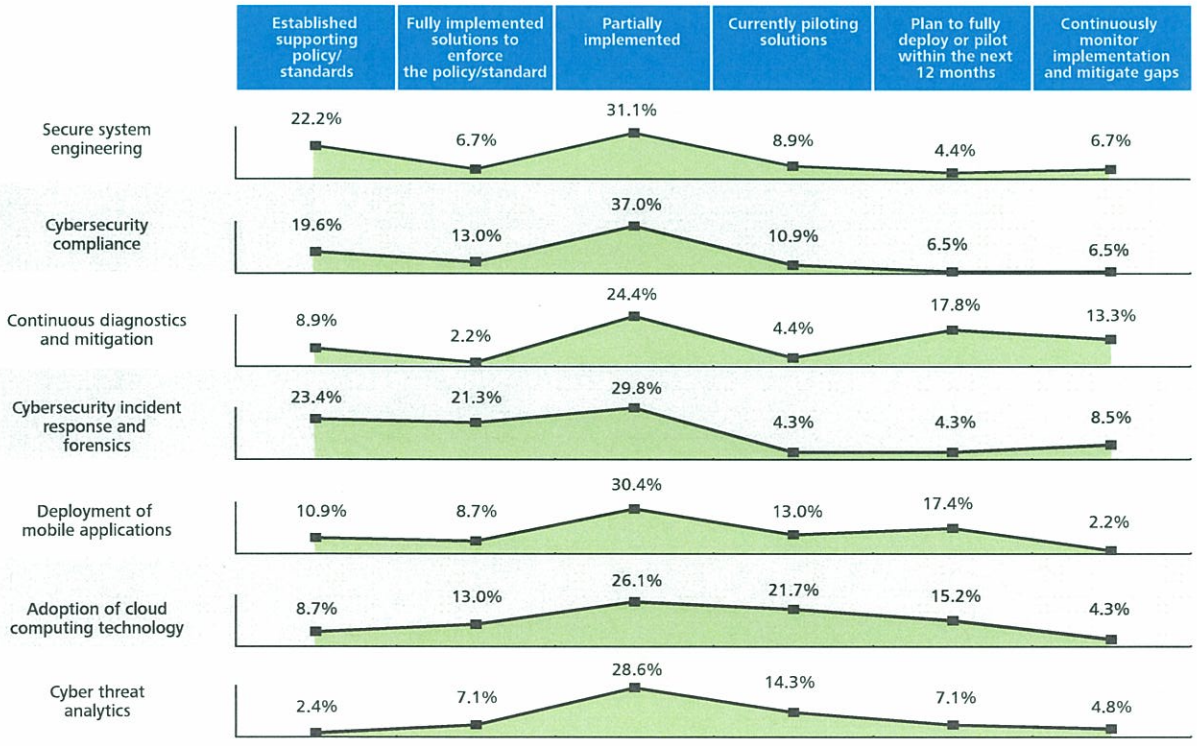
Both the federal government and most states have enacted privacy laws, and complying with them requires both resources and careful planning. Yet, only a third of states have programs for managing privacy compliance, and only two fifths have a formal process in place to handle complaints about information privacy. This may be one reason why states have decided to establish a separate position of CPO. The position now exists in nearly a third of states, up from two years ago.

Figure 26: Leading privacy concerns

NASCIO Core Security Services Taxonomy

Consistent with the 2012 Deloitte-NASCIO Cybersecurity Study, we asked the CISOs to perform a self-evaluation of maturity across a range of core security services.[5] The responses provided greater insight into the maturity of select cybersecurity program elements as highlighted in Figure 27.

Figure 27: Status of Core Security Services Taxonomy

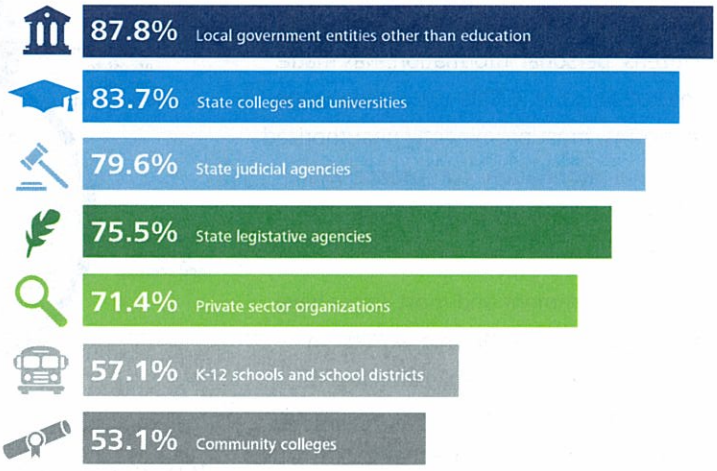


Collaboration with non-governmental entities

State CISOs are collaborating with other state agencies and various outside entities, especially in the areas of cybersecurity awareness and providing supporting policies and standards. The vast majority of CISOs indicated that they collaborated with local governmental entities, state colleges and universities, and state judicial agencies as part of their security programs.

States are also welcoming guidance from leading public sector leadership organizations, including NASCIO, the National Governors Association (NGA), and NIST. For example, more than two-thirds of CISOs indicated that they are either reviewing or working on recommendations provided by NGA's "Act and Adjust" report.[6] Similarly, NIST-provided cybersecurity standards and the NIST Cybersecurity Framework 1.0 are the leading choices for CISOs when establishing their cybersecurity programs.

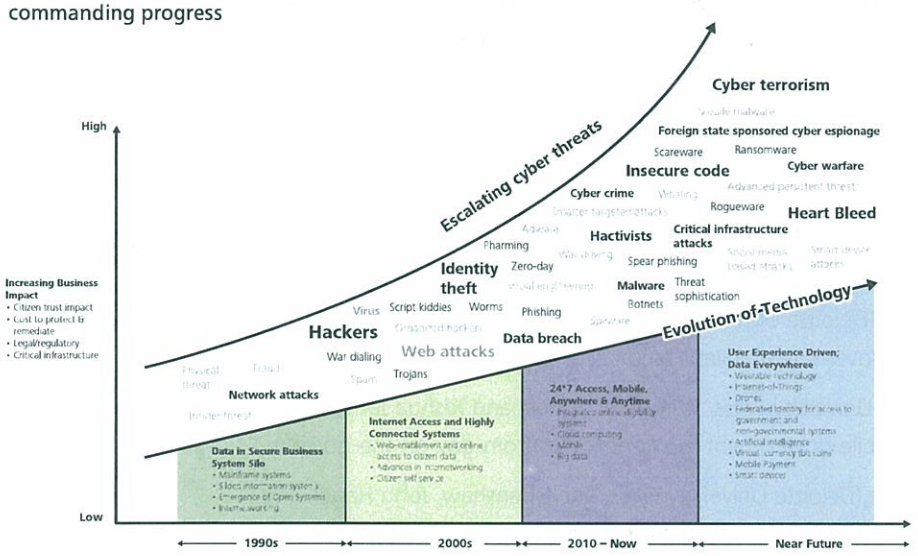
Figure 28: States collaboration with non-governmental entities



Moving forward…

It is clear that cybersecurity threats are increasing – in sophistication, intensity, diversity, and volume – and that they are not going away anytime soon. Consider the evolution of the environment, and threat and impact from 1990s to today and in the foreseeable future (Figure 29). While states have made incremental improvements, there is still more to do to mitigate the mounting threats and disruption to business when attacks succeed.

Figure 29: Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress



The information environment for states is becoming more difficult to protect as they increase their use of on-line services, both to save money and in response to citizen demands. Agencies and citizens are also clamoring for more mobile services, increasing the complexity of security. Cloud computing is another way states are looking to capture cost efficiencies, but the move brings a host of security concerns. Finally, the rise of information sharing across state and federal networks, aimed at solving some of the problems that arise from silos, including poor communication, has the potential to create more vulnerabilities. The business need to adopt technology advances and the increasing sophistication of cyber threats are posing a daunting challenge. Cybersecurity must become an enterprise business imperative for states.

All of this leads to the stark conclusion that the states must embrace cybersecurity as part of our business and technology culture. As the states move forward with a renewed emphasis, they also need to consider the approach to security. The traditional approach to managing security through preventive and risk-based protective measures, while important and necessary, is no longer enough. States today must add two other elements to the mix: vigilance – continuous monitoring for threats that gives them early detection capabilities and resilience – the ability to respond and recover. Achieving greater effectiveness with modest budgets depends on taking a threat-aware, risk-based approach. Additionally, states need to determine the right balance of secure, vigilant, and resilient capabilities needed to support the various programs, agencies and operational activities of state government. Making a secure, vigilant, and resilient approach a business imperative means every new technology project or system implementation must include funding to incorporate these elements. Implementing this approach will call for creative partnerships and collaboration with the private sector, other states and the federal government. Only by making cybersecurity a priority for business leaders, embarking on innovative collaborations with public and private sector entities and covering all three bases, will states be in a position to address the continuing onslaught of cybersecurity risks.

Sources

[1] SC data security efforts, monitoring may cross $27M; Seanna Adcox – Associated Press, April 20, 2014, http://www.washingtontimes.com/news/2014/apr/20/sc-data-security-efforts-monitoring-may-cost-27m/

[2] NIST released Version 1.0 of its Cybersecurity Framework; Framework for Improving Critical Infrastructure Cybersecurity (National Institute for Standards and Technology, Version 1.0, February 12, 2014, http://www.nist.gov/cyberframework/)

[3] National Initiative for Cybersecurity Education (NICE) Framework; National Cybersecurity Workforce Framework (National Initiative for Cybersecurity Education, http://csrc.nist.gov/nice/framework/)

[4] Talent Crisis Moving Forward section was derived from the following sources:

- Global Human Capital Trends 2014: Engaging the 21st-century workforce. (Deloitte University Press, http://www2.deloitte.com/global/en/pages/human-capital/articles/human-capital-trends-2014.html)
- Gen Y and technology in today's workplace: Talent and the Generations (Part 1). (Alexandra Levit, Dorie Clark, and John Hagel, March 3, 2013, http://dupress.com/articles/talent-the-generations-part-1/)
- Introduction: Government's talent factor (Deloitte University Press, William D. Eggers, February 20, 2014, http://dupress.com/articles/introduction-governments-talent-factor/?coll=4602)
- The mobile government worker (Deloitte University Press, William D. Eggers and Joshua Jaffe, July 17, 2013, http://dupress.com/articles/the-mobile-government-worker-excerpt-from-gov-on-the-go/?ind=)
- From invisible to visible . . . to measurable (Deloitte University Press, Eric Openshaw, John Hagel, and John Seely Brown, March 10, 2014, http://dupress.com/articles/from-invisible-to-visible/?top=7)
- Predictions for 2014: Building a Strong Talent Pipeline for the Global Economic Recovery (Bersin by Deloitte, Josh Bersin, December 2013, http://marketing.bersin.com/predictions-for-2014.html)

[5] "The Heart of the Matter: A Core Services Taxonomy for State IT Security Programs." NASCIO. October 2011

[6] Act and Adjust: A Call to Action for Governors for Cybersecurity. (National Governors Association, September 26, 2013, http://www.nga.org/cms/home/nga-center-for-best-practices/center-publications/page-hsps-publications/col2-content/main-content-list/act-and-adjust-a-call-to-action.html)

Appendix

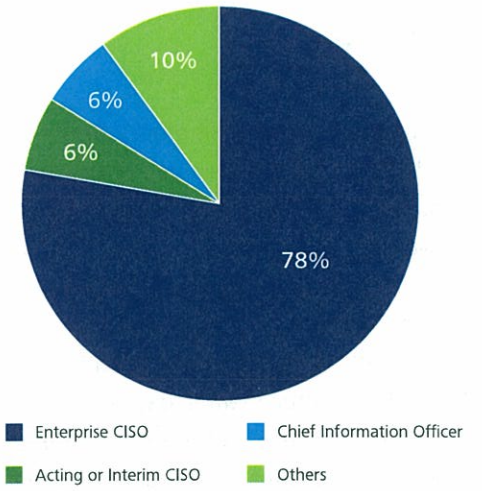
The 2014 Deloitte-NASCIO Cybersecurity Study uses survey responses from:

- U.S. state enterprise-level CISOs, with additional input from agency CISOs and security staff members within state governments.
- U.S. 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 58 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Participation was high – responses were received from 49 states. Figures 30 to 32 illustrate the CISO participants' demographic profile.

Figure 30: CISO survey respondent designation



State Official Profile

One hundred eighty-six (186) state officials answered 14 questions, providing valuable insight into states' business stakeholder perspectives. The participant affiliations included the following associations:

- National Association of State Auditors, Controllers and Treasures (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 Budget Officers (NASBO)
- National Association of State Procurement Officials (NASPO)
- American Association of Motor Vehicle Administrators (AAMVA)
- National Association of Medicaid Directors (NAMD)
- National Emergency Management Association (NEMA)
- Adjutant General Association of the United States (AGAUS)
- Governors Homeland Security Advisors Council (GHSAC)
- Federation of Tax Administrators (FTA)
- International Association of Chiefs of Police (IACP) – Division of State and Provincial Police (S&P)

The two surveys provided space for respondents' comments when they wanted to explain "N/A" or "other" responses. A number of participant provided comments that offered further insight. Some of these comments may have been included in this report, but the respondents have not been cited for confidentiality reasons.

Figure 31: Approximate annual budget of the respondent states ($USD)

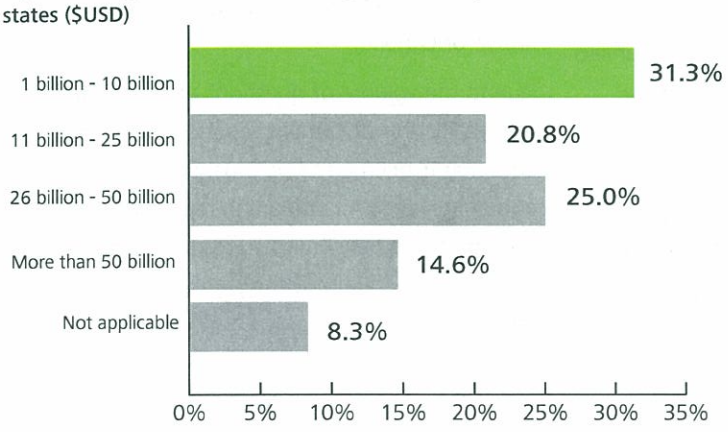
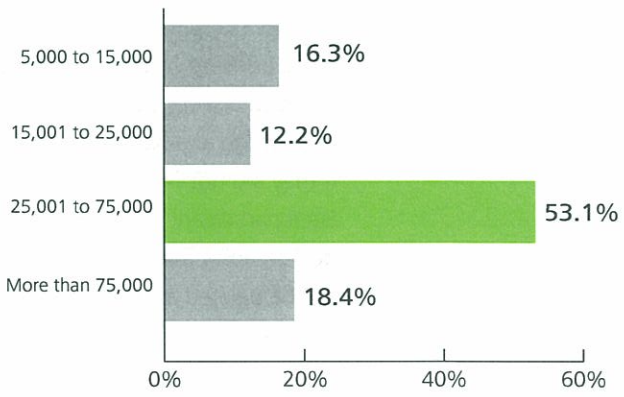


Figure 32: Number of employees in your state
(excluding higher education employees)



Acknowledgements

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

NASCIO
Doug Robinson, Executive Director
Meredith Ward, Senior Policy Analyst

Security and Privacy Committee Co-Chairs and Members

State CISO Survey Review Team
Brian Engle, State of Texas
Chris Buse, State of Minnesota
Dan Lohrmann, State of Michigan
Elayne Starkey, State of Delaware
Elliot Schlanger, State of Maryland
Erik Avakian, Commonwealth of Pennsylvania
Michele Robinson, State of California

Deloitte subject matter specialist contributors
Art Stephens, Deloitte Consulting LLP
Ed Powers, Deloitte & Touche LLP
Libby Bacon, Deloitte Consulting LLP
Mike Wyatt, Deloitte & Touche LLP
Srini Subramanian, Deloitte & Touche LLP

Deloitte survey team, data analysis, and benchmarks
Bharane Balasubramanian, Deloitte & Touche LLP
Ruth Williams, Communications Consultant

Marketing
Annette Evans, Deloitte Services LP
Beth Ruck, Deloitte Services LP
Shawn Vaughn, NASCIO
Suzanne Love Beck, Deloitte Services LP

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

Deloitte and NASCIO collaborated to produce the 2014 Deloitte-NASCIO Cybersecurity Study. Working with NASCIO and several senior state government security leaders, and Deloitte's security survey questionnaire used for other security surveys, 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 Security & Privacy Committee, reviewed 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 demographic information of the survey content will be deleted after the preparation of the survey reports.

The data collection and analysis process 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 and Human Capital specialists. In some cases, in order to identify trends or unique themes, data was also compared to prior surveys and additional research. Results on some charts may not total 100 percent based on the analysis of the comments related to 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 on the data points deemed to be most important at the aggregate level. A companion report including the questions and benchmarked responses has been provided individually to the state CISO survey respondents.

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's practitioners provide advisory, implementation, and managed services to help transform legacy IT security programs into proactive *Secure.Vigilant.Resilient.* cyber risk programs that 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.

For more information visit **www.deloitte.com**.

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, 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

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

Jessica Blume
US Public Sector Industry Leader
Deloitte LLP
1 813 273 8320
jblume@deloitte.com

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

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

Mike Wyatt
State Sector Cyber Risk Program Services Leader
Deloitte & Touche LLP
1 512 226 4171
miwyatt@deloitte.com