Deloitte.

NASCIO
Representing Chief Information Officers of the States

2012 Deloitte-NASCIO Cybersecurity Study

State governments at risk: a call for collaboration and compliance

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

Contents

Executive summary 2

Key findings 4

1. The cybersecurity budget-strategy connection 5

2. Cybersecurity authority and governance 10

3. Preparedness for emerging threats 15

4. Compliance—a lever for CISO leadership 18

Trends 23

A call to action for states 26

Appendix 28

Additional thought leadership 30

About the survey 32

Sources/Footnotes 33

Acknowledgements 34

About Deloitte & NASCIO 35

Contacts 36

In light of the sophisticated threats to state networks, NASCIO continues to identify cybersecurity as a critical concern of state CIOs, and to advocate for additional funding and support for state security programs. The 2012 Deloitte-NASCIO cybersecurity study highlights challenges that state enterprises and security personnel face in protecting states' critically important systems and data, the lifeblood of our operations.

In a period of continuing fiscal constraints, the challenges we face are daunting. The study portrays a powerful image of the current information security landscape. States must remain vigilant—we are targeted by millions of security threats each week. States need more qualified cybersecurity professionals. It is evident we must prepare for emerging threats and do a better job of monitoring compliance. The survey responses provide a foundation for building greater insight into the maturity of state cybersecurity programs.

One of the greatest concerns of State CIOs and CISOs is that security does not fail gracefully. Every CIO and CISO wakes up each day knowing that if they don't get security right and breaches are suffered, their programs can be perceived to be ineffective, and their citizens may suffer direct harm. This reality must drive us to constantly focus on achieving adequate levels of risk and security in our programs. For that reason, the recommendations and findings in this report set a roadmap that states must pursue to mitigate risks and advance an action agenda for cybersecurity initiatives.

Brenda L. Decker

NASCIO President and CIO, State of Nebraska

Executive summary

Cybersecurity continues to be one of the most pressing challenges facing State Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) today. Security threats to states have been widely reported, however the nature of the game has changed. Cybercriminals and hacktivists—a new breed of hacker with a political or social agenda—use increasingly sophisticated methods involving rapidly evolving technologies to target cyber infrastructure for monetary gain and to make political statements.

As states progress towards a future of internet-hosted applications using new technologies, like big data, mobile solutions, and cloud computing, and continue to grow their electronic repositories of valuable citizen data, addressing the issue of protecting personally identifiable information (PII) and state systems is of utmost importance.

Consider the staggering statistics:

- Government agencies have lost more than 94 million records of citizens since 2009, according to a recent Rapid7 report on the "Data Breaches in the Government Sector."[1]
- The average cost per lost or breached record is $194 per the Ponemon Institute's 2011 Cost of Data Breach Study.[2]

Recognizing that security breaches can be far more costly than cybersecurity programs—especially when coupled with the incalculable cost of regaining lost citizen trust—government leaders must focus their attention on developing and implementing proactive and innovative approaches and solutions.

In these times of escalating threats and increasing accountability, the 2012 Deloitte-NASCIO Cybersecurity survey identified three significant core findings:

- **Problems persist:** As in our 2010 report, CISOs recognize the importance of cybersecurity, but continue to struggle to gain adequate budgets and stakeholder buy-in. Cybersecurity governance and strategy continue to challenge states.
- **People change but results have not:** Despite 31 new state CIOs and 22 new state CISOs since 2010, the challenges reported in this survey are consistent with the 2010 survey results, highlighting ongoing problems.
- **State officials acknowledge the importance of security:** In a parallel survey targeting a limited cross-section of state business and elected officials, 92% of respondents ranked cybersecurity as "most important (81%)," or "very important (11%)."

The results of the 2012 Deloitte-NASCIO Cybersecurity survey show clear evidence of commitment and support from public sector business leaders. CIOs/CISOs must leverage this support by better articulating the risks and impacts to overcome the challenges related to governance, authority and budget—and effectively tackle cyber threats.

In this report, we propose a set of strategic action items for states, in addition to a compelling business case based on survey findings. CIOs and CISOs are encouraged to use these recommendations to build greater awareness and support at each level of state government. We hope this document is a catalyst for CIOs/CISOs and their state official partners to drive their mutual cybersecurity initiatives to even greater success.

In closing, we acknowledge the efforts of the state CIOs and CISOs in their endeavor to protect data and champion the topic. Consider the impressive response to this 2012 survey:

- **50 CISOs (48 states and two territories) or their equivalents responded to the long version of the CISO survey, which also included a self-assessment to measure the maturity of cybersecurity services in their states**
- **63 responses to the state officials survey that resulted in a broader understanding of the business stakeholder perspective**

Congratulations on your dedication and accomplishments to foster a more secure future.

Srini Subramanian
Principal
Deloitte & Touche LLP

Doug Robinson
Executive Director
NASCIO

States at risk – A call for action

Cybersecurity challenges continue in 2012 amidst escalating threats

92% State officials feel cybersecurity is very important for the state

50% CISOs manage a team of one to five cybersecurity professionals only

Only 14% CISOs feel that they receive appropriate executive commitment and adequate funding for cybersecurity

70% CISOs have reported a breach

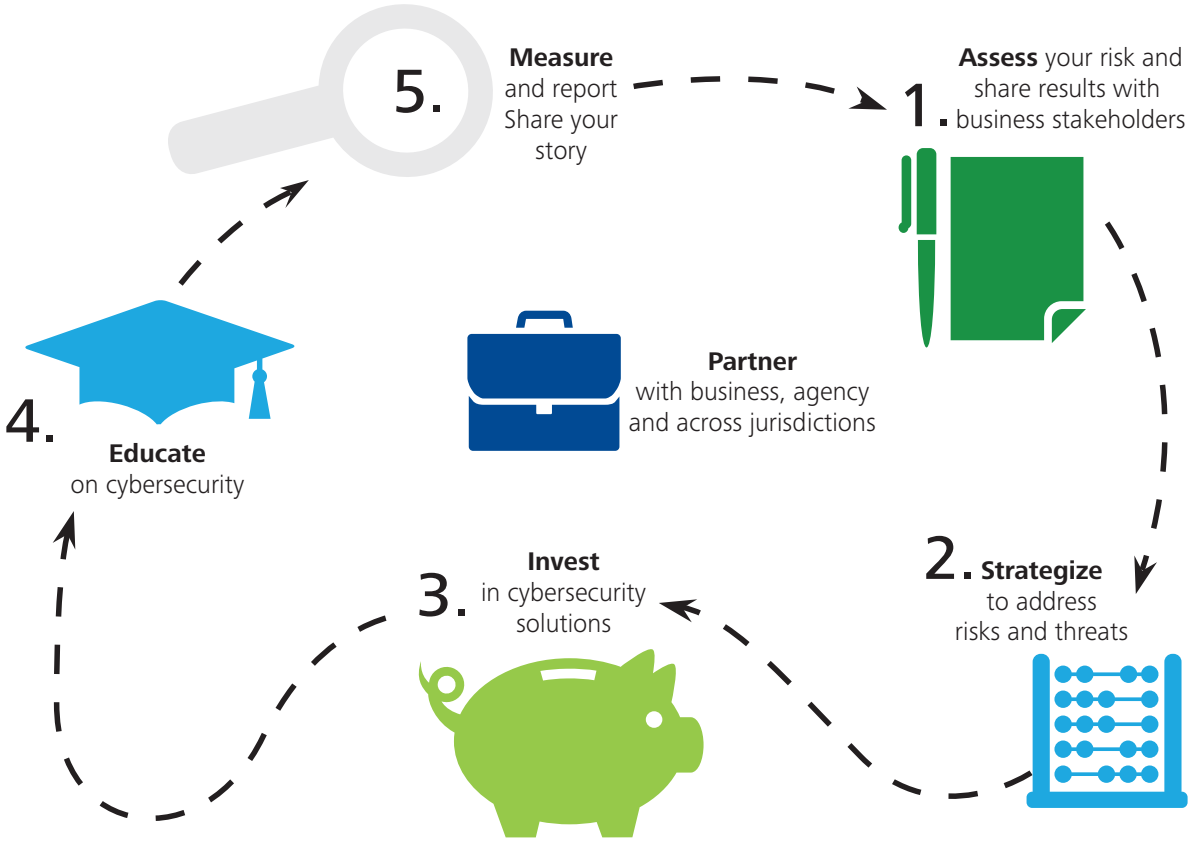
CISOs are very confident in protecting state's assets against external threats **Only 24%**

CISOs feel that staff have the required cybersecurity competency **Only 32%**

CISOs indicate "Lack of sufficient funding" is the key barrier to address cybersecurity **86%**

CISOs feel "phishing and pharming" as their top cybersecurity threat **82%**

An urgent call to execute on a robust cybersecurity strategy, with strong governance and compliance monitoring measures



Key findings

As in the previous survey, the 2012 Deloitte-NASCIO Cybersecurity Study asked state information security representatives an encompassing set of questions regarding current cybersecurity practices. In 2012, a new, parallel survey for state officials focused on their views on the importance of cybersecurity, barriers to achieving security goals, and the alignment of business and cybersecurity initiatives.

This report analyzes responses to both surveys and focuses on four key areas:

1. **The cybersecurity budget-strategy connection:** Insufficient funding is still the greatest hurdle CISOs face. CISOs must continue to build business stakeholder advocacy for cybersecurity initiatives by communicating strategies and reporting on risks, progress, and results. In addition, CISOs can take a leadership role in creating competency centers and shared service approaches to facilitate sharing of scarce resources across agency siloes.

2. **Cybersecurity authority and governance:** Many CISOs operate in a highly distributed model with little direct authority over agency security strategies, activities, or resources. This makes the creation of enterprise governance more critical as a means of boosting coordination of cross-agency resources. Governance must extend to third-party service providers, too. States and their partners share security risk, which makes it critical that roles and responsibilities be clearly defined and processes regularly assessed.

3. **Preparedness for emerging threats:** The wealth of personally identifiable information (PII) and sensitive business data makes states attractive targets for cybercriminals and hacktivists. Business transformation initiatives and innovations, like cloud technology and mobile solutions, are introducing new security challenges and can be potential opportunities for CIOs/CISOs to bring business visibility and support for embracing the new technologies.

4. **Compliance—a lever for CISO leadership:** The stream of new cybersecurity regulatory requirements is endless—and so are the audits that inevitably follow. CISOs can help guide state agencies in meeting standards by promoting a common framework based on the National Institute of Standards and Technology (NIST) standards. Better communicating compliance issues and audit findings and enabling business leaders to make more informed decisions will help CISOs gain stronger support and funding for their security programs. In addition, many states have not named an enterprise-wide chief privacy officer as the single point of authority on what information must be protected.

This study compares the responses from the CISOs and state officials, along with the relevant results from the 2010 Deloitte-NASCIO Cybersecurity Study and the 2012 Deloitte Touche Tohmatsu security survey of the global financial services industry (GFSI). These comparisons provide additional context for assessing the impact and meaning of the survey results.

1. The cybersecurity budget-strategy connection

Lack of funding is cybersecurity's Achilles heel—putting states at risk as citizen information held by states becomes a more attractive target.

Bottom line

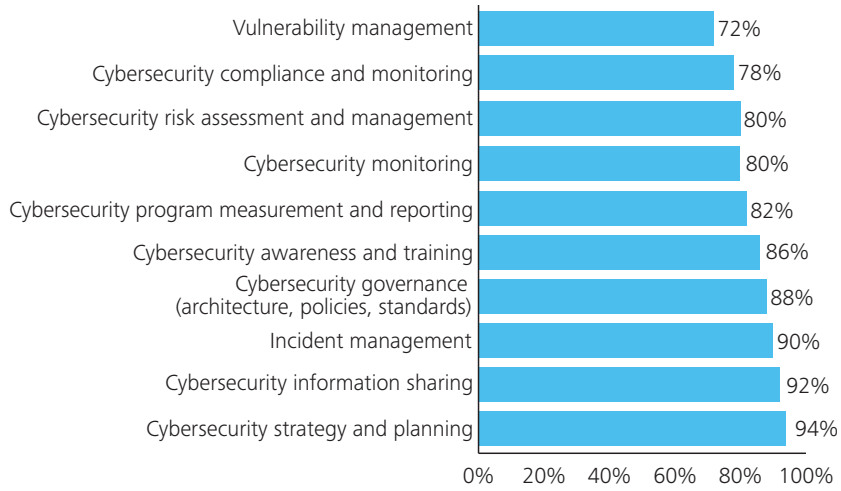
There is evidence that state officials are increasingly seeing information security as very important to state government and their agencies. CISOs should capitalize on this trend and enlist the support of business stakeholders in advocating for cybersecurity funding. A thoughtfully developed and communicated cybersecurity strategy, complemented by measurement and reporting across the enterprise, is critical to this effort.

Despite the fact that revenues are slowly recovering from the effects of the recession, states continue to face fiscal pressures and must carefully prioritize spending. Cybersecurity programs are feeling the pinch. At the same time, the wealth of citizen data that states store presents an attractive target for attack. It is vitally important that CIOs and CISOs make the case for adequate security funding with a sound strategy.

Budget basics

Any examination of budget must begin with an understanding of the functions and assets included in the CISOs' mandate. As illustrated in Figures 1 and 2 CISOs may lay claim to a wide range of functions—from highly strategic to tactical.

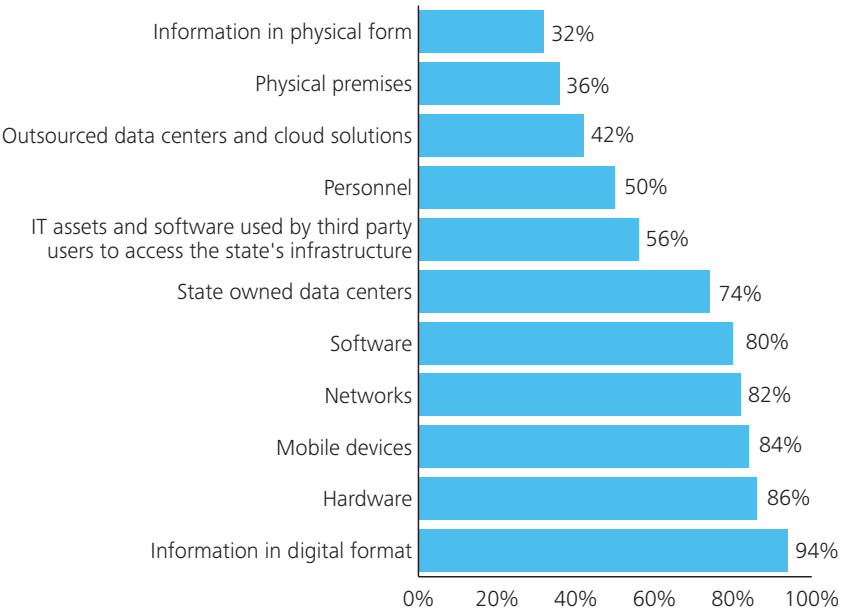
Figure 1. Top functions of the CISO or equivalent



Key takeaway

Positive trend: 82% of CISOs say cybersecurity program measurement and reporting are within their scope of responsibilities. That's a notable increase from 67% in 2010.

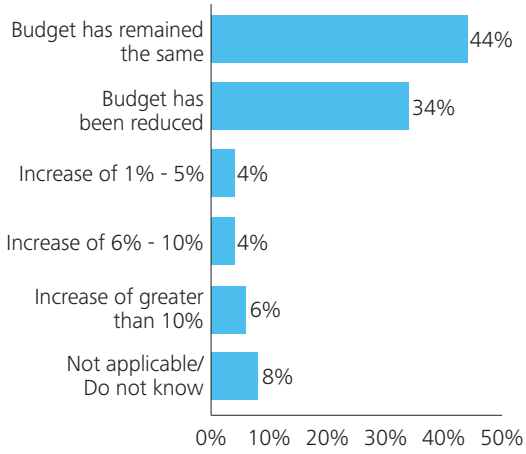
Figure 2. Assets within mandate of CISO or equivalent



Key takeaway

CISOs believe they own securing "everything electronic," while there is evidence of a growing trend toward convergence of physical and electronic security functions.

Figure 3. Year-over-year trend of cybersecurity budget for years 2010 and 2011



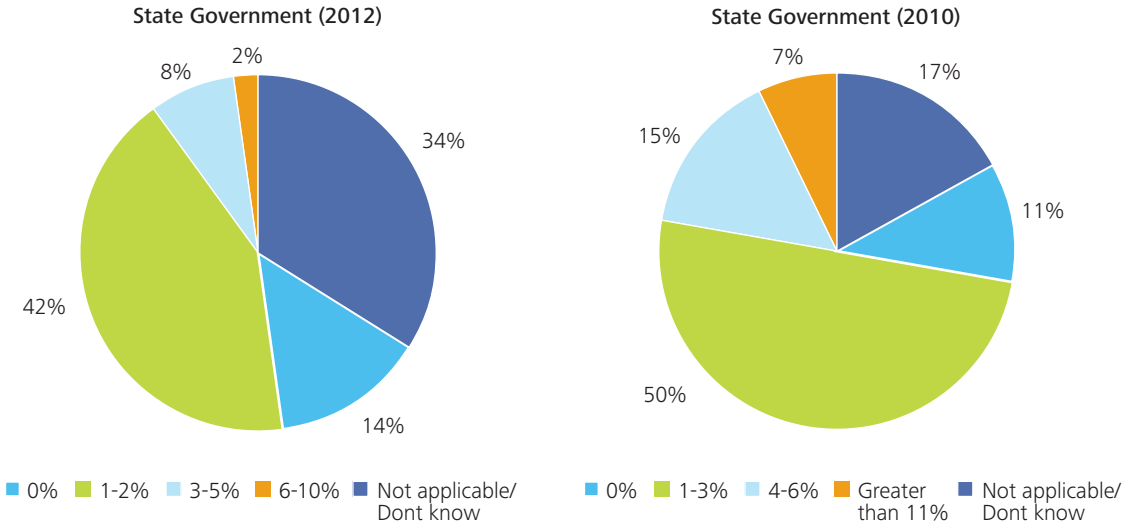
The budget discussion is complicated by the fact that most CISOs' budgets are only a portion of the total security spend across the enterprise. In fact, 56% of respondents operate in a federated model and hold responsibility for centralized common services—with assigned services specific to each agency.

The question of what percentage of the state IT budget is devoted to cybersecurity was modified in the 2012 survey to narrow the ranges, starting with one to two percent (versus one to three percent in 2010). The results support the comments from 2010 responders—41% indicated the figure was one to two percent of the overall IT budget (Figure 4).

Key takeaway

14% of respondents reported a budget increase between 2010 and 2011. However, the majority weren't as fortunate.

Figure 4. Comparison of budget allocation to cybersecurity (2012 vs. 2010)



Key takeaway

Only a small portion of the overall IT budget is devoted to cybersecurity—most state security budgets are in the 1-2% range.

Lack of sufficient funding and skilled staff remain the top CISO concern

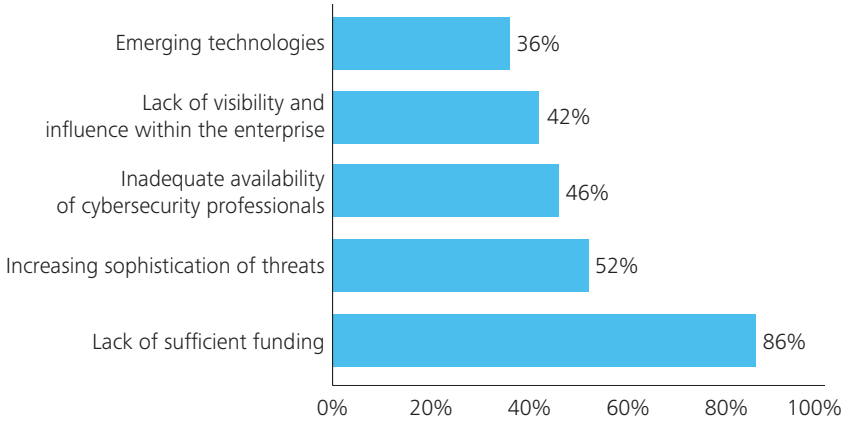
While CISOs continue to cite "lack of sufficient funding" as the top barrier in the survey (Figure 5), many state officials cited information security as "extremely important" (81%) or "very important" (11%). The CISO survey also shows that 74% of respondents felt that there is executive support but not adequate funding (Figure 6).

There's never been a better opportunity for CISOs to partner with business stakeholders—and advocate jointly for increases in cybersecurity budgets through well-articulated strategies, measures, and outcomes.

These results are evidence that state officials understand the importance of information security, but may not realize the need or significance of funding a particular initiative or project. There's never been a better opportunity for CISOs to partner with business stakeholders—and advocate jointly for increases in cybersecurity budgets through well-articulated strategies, measures, and outcomes.

In addition, the majority of respondents to the CISO and state officials surveys agree that business and cybersecurity initiatives are aligned to some degree—with only 10% reporting no synchronization. This is an indication that many CISOs are taking positive steps to help make sure roadmap alignment and involvement with the business—a bottom line recommendation from the 2010 report.

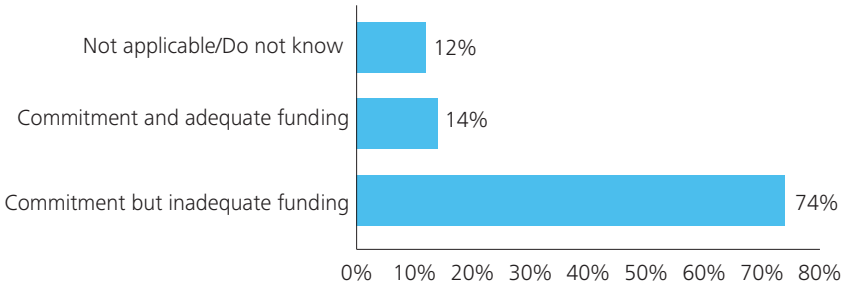
Figure 5. Top five barriers faced in addressing cybersecurity



Key takeaway

The top five barriers paint a powerful picture of the challenges CISOs face today. Insufficient resources against growing sophistication of threats and emerging technologies make the need to raise stakeholder awareness to gain their support and funding more critical.

Figure 6. Senior executive support (Governor's Office/CIO) for security projects to address regulatory/legal requirements



Key takeaway

74% of CISO respondents have executive commitment—but that has not translated into adequate funding in the majority of cases.

82% **vs.** **8%**

82% of CISOs are responsible for cybersecurity measurement and reporting.

Only 8% are currently measuring the value and effectiveness of their enterprise cybersecurity organization's activities.

Strategy and measurement—essential to better communication with business

A cybersecurity policy strategy is key to building support for increased funding. When budgets are tight, a strategic plan is essential to beginning to gain acceptance and support. This is an area of significant focus for CISOs:

- 46% already have a documented and approved strategy.
- 6% have a documented strategy that requires approval.
- 30% intend to develop one in the next 12 months.

What else could CISOs be doing to build support? They can pursue more cybersecurity program measurement and reporting. CISOs need to demonstrate results from their strategy in order to increase support and funding. Fortunately, this is squarely on the CISOs' to-do list with 82% citing measurement and reporting as a key responsibility—up from 67% in 2010.

There is an urgent need to address measurement and reporting. Only 8% of respondents currently track the value and effectiveness of enterprise cybersecurity activities. What's more, reporting on cybersecurity status and posture should be expanded beyond agency IT and cybersecurity groups to include business stakeholders, legal, the legislature, and the governor—and should ideally be performed on a semi-annual or annual basis.

Shared security services must be an integral part of the strategy

Given the fact that cybersecurity professionals are at a premium and the significant costs associated with security technologies, products, and operations, part of a strategy should include the potential to effectively share technology and people assets.

- A shared services model could make highly skilled, but underutilized, security personnel in one agency available to others—providing a greater level of service at no additional cost.
- Agencies could specialize in a particular area, such as security strategy, security framework and assessment automation, or identity and access management, and lend their knowledge and skills to other agencies as competency centers in a shared services model.

Case in point: States are creating health insurance exchanges (HIXs) in response to the federal Affordable Care Act—and they are receiving millions in federal funds to help with these projects. Enterprise CIOs and CISOs should reach out to health and human services officials to help make sure that adequate security and privacy requirements are integrated into the solution.

Through these joint efforts, CISOs may find that their states' health and human services agencies develop new competencies, such as in identity and access management (IAM) tools and processes. This knowledge, which was developed while using federal funds, could be extended to other agencies via a competency center approach and an auditable chargeback mechanism to sustain the operations of the shared services.

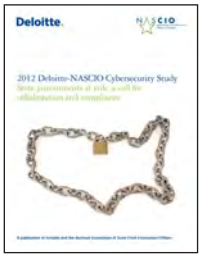
The creation of a security services taxonomy, as recommended in the 2010 Deloitte-NASCIO Cybersecurity Study as defined by the NASCIO Security and Privacy Committee in 2011, can be a key enabler for a shared services model.[9]

Leading practice highlight

Pennsylvania does more with less via competency centers and shared-services models

The Commonwealth of Pennsylvania recognized that, in a federated model of agency governance, shared service, and a competency center approach can help promote and mature security services. Pennsylvania's Identity and Access Management (IAM) program leverages a Department of Public Welfare-led offering for "Identity repository (Directory)" services, while the CISO retains governance and coordination responsibility with the agencies. In addition, Pennsylvania's automated user provisioning project—executed as part of the enterprise IAM program—highlights the success of the individual-agency-funded rollout of the provisioning implementation.

Comparing State Government and Global Financial Services Industry (GFSI) Responses.



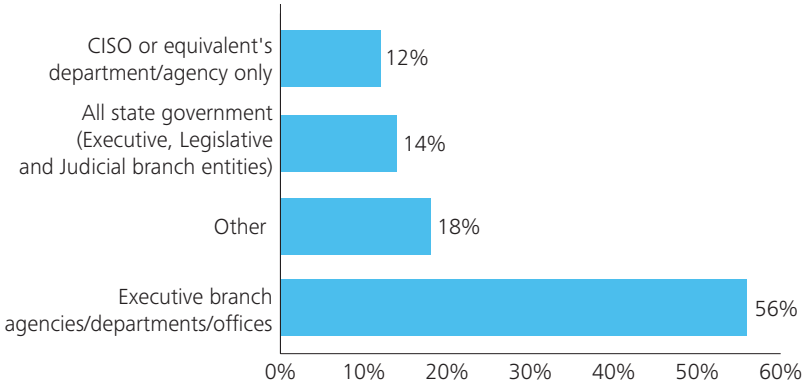
	2012 Deloitte-NASCIO Cybersecurity Study	2012 DTTL GFSI Security Study (large organizations)
Security budget has increased	14%	> 60%
Year-over-year trending	4% report an increase of 1-5%	39% report an increase of 1-5%
Dedicated security professionals	50% have 1-5 FTEs	47% have >100 FTEs

2. Cybersecurity authority and governance

Lack of enterprise authority and visibility is a challenge that is unlikely to change in the near future.

Most CISOs operate in a federated or distributed environment where IT and security resources are dispersed across various state agencies and departments. The majority report having authority over only executive branch agencies, departments, and offices (Figure 7).

Figure 7. Scope of CISO authority



Bottom line

CISOs need to creatively evolve their role in a mostly federated governance model. States are doing more to improve in-house staff skills, but continue to rely on third-party resources. States must establish clear security policies and an associated framework and routinely confirm compliance of outsourced third-party-managed projects—rather than relying on contract terms alone.

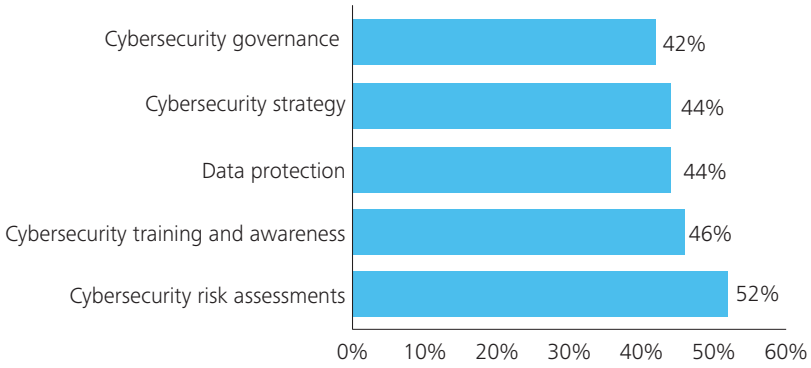
Key takeaways

The good news: The enterprise CISO position is now firmly entrenched in states—with 96% of respondents reporting that the position or its equivalent is present.

The not-so-good news: The enterprise CISO position is one of coordinating cross-agency resources, rather than holding state-wide authority.

CISOs must redouble their efforts to collaborate with security functions across the enterprise in order to positively influence governance practices. And the fact that 92% either has defined governance for cybersecurity or plans to create policies in the next 12 months serves as an important means to communicate across the enterprise. Another positive note—more than two-thirds of those with documented, approved governance have updated the policy in the last two years.

Figure 8. Top five cybersecurity initiatives for 2012



Key takeaway

CISOs place renewed emphasis on "Governance" and "Strategy" by bringing them to the top five initiatives in 2012.

Leading practice highlight

California's enterprise CISO-agency ISO model

In a move that shows acceptance of the fact that a federated model will persist, California passed a law in 2010 requiring each of its 120 state agencies to name an information security officer (ISO). The position reports to the CISO and establishes a structure to be certain that the applicable skills are in place across the enterprise for effective governance of the security function.

Before the law took effect, about 60% of state agencies had ISOs. Now every agency has one, and the enterprise CISO oversees training programs to help make sure these ISOs possess the qualifications and skills needed to manage agencies' information security programs.

The foundational governance model will help to elevate the visibility of cyber initiatives and issues across the state, in addition to serving as a great mechanism to promote future shared security services and collaboration across agencies.

Cyber skills are at a premium

Staffing levels remain an issue, with "inadequate availability of cybersecurity professionals" ranking as number three on the list of barriers to addressing security. A recent NASCIO report, *State IT Workforce: Under Pressure,*[3] confirms this challenge—listing security as the top area where states struggle to attract and retain IT employees.

In addition, states run very lean cybersecurity staffs. Half of the respondents report five or fewer cybersecurity professionals on their teams and 38% report six to 15 FTEs—numbers that are nearly identical to the 2010 study. It is likely that state agencies operating in a federated model have additional security FTEs not reporting to the state CISOs, emphasizing the need for collaboration. In contrast, Deloitte's 2012 GFSI Survey found that 47% of financial service industry organizations of similar size have more than 100 FTEs.

Leading practice highlight

Michigan elevates cybersecurity visibility to executives

By integrating cyber and physical security, the State of Michigan has bridged a traditional divide using a comprehensive approach to risk. The state created a new organization—Cybersecurity and Infrastructure Protection (CIP)—and appointed an enterprise Chief Security Officer (CSO). The goals? Reduce redundancy by eliminating overlapping duties and maximize security coordination and responsiveness across the enterprise.

The new approach has led to improvements in governance, procedures, operations, and risk management outcomes. For example, it has returned hard savings of at least $500,000 on emergency management staffing functions and positioned the CIP to gain better access to federal funds available from the Department of Homeland Security.

Most notably, this success would not have been possible without sponsorship for the new approach from executives, the governor, CIO, and budget director.

Staff competency is another area of concern. The survey shows that CISOs are seeing more shortfalls in security professional skill sets than in 2010, but they are also doing more to close the gap through training and employee development activities (Figure 9). In addition, the 2012 responses show a significant increase in the use of outsourcing and staff augmentation as a way to bring more security skills to bear.

Figure 9. Internal cybersecurity professionals competency—2012 vs. 2010

	2010	2012
Closing the gaps by outsourcing the affected areas	9%	12%
Staff has large gaps in competencies	17%	24%
Closing the gaps through staff augmentation (e.g. consultants and contractors)	22%	28%
Staff has all the required competencies	25%	32%
Closing the gaps through adequate training to staff for developing required competencies	35%	50%

Key takeaway

CISOs are doing more staff development and using more outside resources to close the cybersecurity skills gap.

The evolution of cybersecurity governance, combined with a strategy to promote collaboration and shared services, will help CISOs find ways to do more with existing cybersecurity resources across the enterprise. As mentioned in the previous section's highlight, an agency with the resources and skill sets for a particular security service could become a competency center for the enterprise. CISOs can demonstrate leadership by efficiently adding enterprise security services to their security service catalogs and rapidly executing on their strategies.

Leading practice highlight

Cyber competency starts at the top in Delaware with ISO certification

Every state organization in Delaware is required to designate one to three information security officers (ISOs) who are responsible for security matters. In recognition of the critical nature of the role—and the fact that the security landscape is always changing—a firm commitment was made to provide the tools and training ISOs need to achieve and stay current with required competencies.

Going beyond simply offering a range of courses, ISOs can take advantage of a comprehensive, two-year certification program that enables them to formally demonstrate their knowledge of information security. This certification not only enhances the ISOs' credentials, but also shows a security commitment to their leadership. In the spring of 2012, the governor recognized the first group of ISOs to complete the two-year program. Certified ISOs in turn, are helping achieve wider coverage of employees in the mandatory cybersecurity training to the employees and contractors as seen by the improved results in 2012.

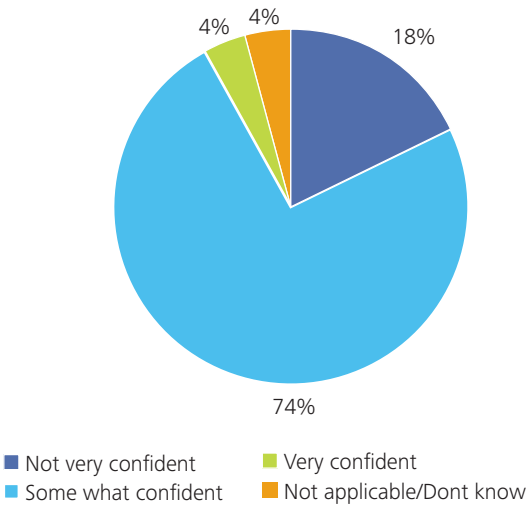
A call to improve security management of third-party service providers

Fiscal constraints and the inability to attract and retain talent, combined with the demand for rapid innovation, put increased pressure on states to outsource services. Numerous states have outsourced information systems of entire programs such as Medicaid Management Information Systems (MMIS) and data center services.

With the advent of cloud-based services, a number of states are moving their core enterprise technology services, such as email, storage and disaster recovery, to cloud and/or outsourced service providers. In addition, states routinely engage service providers to develop and maintain large applications for agencies, such as Health and Human Services, Revenue, Education, and Transportation.

Many of these third parties manage their own networks, receive delegated user management for state-run systems, and have access to state-owned sensitive PII and personal health information (PHI). Increasingly, states are tapping or considering the use of third-party resources for a variety of cybersecurity functions, with threat management and monitoring, threat risk assessments, and forensic/legal support most commonly cited (see Figure 10a on page 14).

Figure 10. State CISO confidence in in cybersecurity practices of their third party service providers

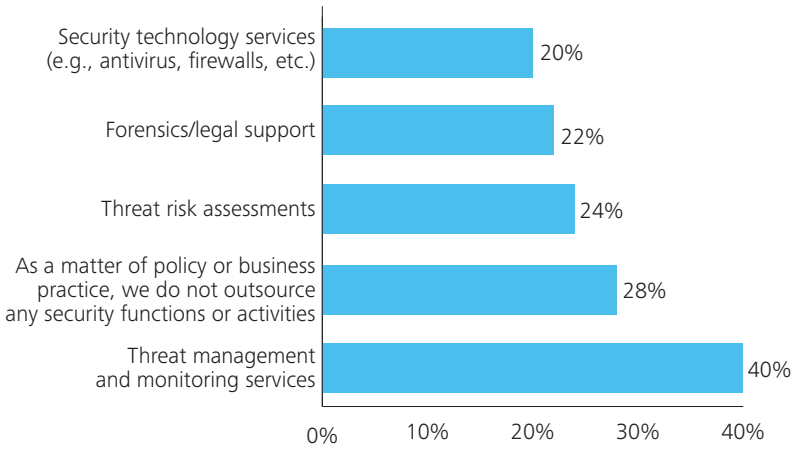


Key takeaway

As in 2010, state CISOs continue to be concerned about security practices of third party providers, when outsourcing is on the rise.

Outsourcing business and security functions raises the issue of how states determine the adequacy of security practices on the part of contractors, service providers, and other business partners. This is a challenging area and one where CISOs continue to rely heavily on contractual measures. As in 2010, a great majority of respondents attempt to address the issue in contracts and/or through confidentiality and non-disclosure agreements (NDAs). Just 12% report that they regularly monitor and review third-party services—down from 25% in 2010.

Figure 10a. Outsourcing of cybersecurity functions



Key takeaway

More states are using outsourced resources to perform threat risk assessments. An independent review and report on risks is a wise investment to build a case for the funds to address cybersecurity shortfalls.

It is also evident that CISOs are wary about the use of third-party cybersecurity services. For example, 28% of respondents report that they do not outsource as a matter of policy or business practice. Only 4% report that they are very confident in the cybersecurity practices of their partners.

When "paper" (aka contracts and NDAs) is used as the primary means of mandating third-party cybersecurity practices, there is the potential for a range of negative side effects:

- Transferring security risk and practices as part of the contract only can complicate the contracting process and lengthen negotiations, with no assurance of the service provider following the contract terms.
- Contract fees can be significantly greater as vendors increase their price to cover the cost of assumed risk.
- Transferring risk to a third party does not change the fact that states are responsible for protecting data—and that's especially apparent if a partner falls short and state executives are left to explain the incident to the public.

Given the need to gain access to specialized security skills and services, the use of outsourcing will continue—and some transfer of risk is inevitable. Therefore, it's up to states to move beyond paper to practice by clearly defining cybersecurity measures and expectations, and then routinely inspecting third parties for compliance.

3. Preparedness for emerging threats

Emerging threats are opportunities to build stronger business partnerships

Bottom line

States are stewards of sensitive citizen and business data—making it more important that CISOs and agency stakeholders collaborate regarding the protection of information. CISOs can raise the visibility of security as a key enabler for innovation. By helping business leaders embrace new technologies and practices such as cloud, big data, and mobile solutions, CISOs can forge lasting business partnerships and support.

States have a goldmine of medical, financial, and other PII, as well as sensitive business and financial data.

When PII goes public, it can spur some of the most heated citizen outrage and damning media attention.

A stolen laptop with social security numbers…a printing error that sends medical statements to the wrong people…malware, like Flame, that steals data. Whether the exposure is inadvertent or malicious, states have a duty to do everything in their power to protect information.

The economic costs from breaches are substantial. The annual Ponemon study[5] puts the organizational cost per breach at $5.5 million—a hefty penalty that financially strapped states can little afford.

Emerging threats equal emerging opportunities

2012 is the first year the survey included mobile devices as a choice in the question of "What threats will have the greatest impact over the next 12 months?" And, it made the top four. This is no surprise as the movement to mobile is very active in state government.

94 million

The number of Americans' files in which personal information has been exposed to potential identity theft through data breaches at government agencies since 2009.[4]

680%

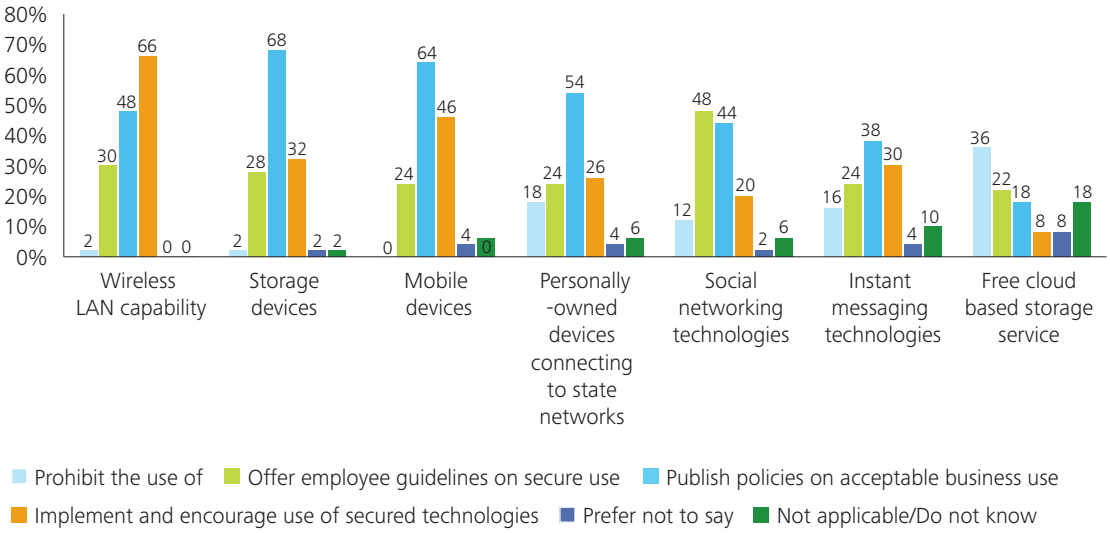
The increase in significant cybersecurity threats against U.S. government systems from 2006 to 2011.[6]

CISOs ranked mobile devices in the top four of threats with the greatest impact over the next 12 months.

Social media, cloud, mobile, and whatever comes next—there are always business transformation initiatives and new technologies in play. The CISO challenge is preventing these opportunities from turning into cybersecurity risks. The study shows there's no one-size-fits-all approach regarding guidelines and usage policies for technology (Figure 11). In fact, states selectively deploy a range of tactics. For example:

- 36% ***prohibit*** the use of free, cloud-based storage services.
- 48% ***offer employee guidelines*** on social networking technologies.
- 68% ***publish policies on acceptable*** use of storage devices, such as USBs and portable media players.
- 66% ***implement and encourage the use of secured technologies***, like wireless LANs.

Figure 11. Security enables the adoption of new technologies



Key takeaway

States must accept the inevitability of new technologies entering their physical and virtual borders—and quickly define and adopt policies to address them.

By forming partnerships with agencies and working collaboratively on business transformation projects, CISOs can make security an integral part of new initiatives. By doing so, CISOs can gain support and funding to implement appropriate security measures and encourage the use of security technologies.

Improved IAM as a program integrity measure

States routinely disburse billions of dollars through state and federally funded programs. They are looking at ways to reduce fraud, waste, and abuse in a tough economic environment where the schemes to exploit weaknesses get more sophisticated and brazen every day. Whether it is someone cashing another person's unemployment or disability payments, "trading" their electronic benefit transfer (EBT) card for cash, or a provider charging the state for services not delivered, there has never been a greater need to confirm the identity of the person using government funds.

A cybersecurity framework, tools and modern identity management techniques can be effective measures in supporting agency program integrity initiatives. As such, they present an excellent opportunity for CIOs and CISOs to better connect with the program executives leading these initiatives. Identity-proofing techniques employed during online access to citizen applications and a secure identity credential to identify both the individual receiving services and the service provider can help make sure proper benefit delivery. Strong authentication measures can also be an effective means to track worker actions and deter fraud. NASCIO's State Digital Identity Working Group has recently published the *State Identity Credential and Access Management (SICAM) guidance and roadmap*[7] which provides guidance to states on navigating the challenges associated with trust, interoperability, security, and process improvement.

External threats are evolving

The incidence of the most common external breaches declined from 2010 (see Figure 12), which shows that traditional means of securing the boundaries of the enterprise are having a positive and sustained impact.

Figure 12. The changing face of external breaches 2010 vs. 2012

	2010	2012	Change
Malicious software	68%	58%	↓
Web	55%	30%	↓
Hackers	45%	30%	↓
Physical attack, such as stolen laptop	36%	20%	↓
Foreign state-sponsored espionage	6%	12%	↑
External financial fraud	4%	12%	↑

Key takeaway

Emerging cybercrime and state-sponsored threats will require a strong response from states.

4. Compliance—a lever for CISO leadership

Regulatory compliance should be used to better communicate risks to business stakeholders and drive home the need for support to improve information security. An enterprise privacy officer, when states can make a case to have one appointed, will be a key ally.

Bottom line

State agencies need to conform to a growing body of more stringent cybersecurity regulatory requirements with reduced funding. CISOs need to look for innovative methods to continuously monitor the state's cybersecurity compliance and join hands with state officials to secure sufficient resources. CIOs and CISOs should use compliance measures and audit findings to better articulate cybersecurity risks to business stakeholders and make a compelling business case. An important element is missing—determining who owns privacy. CIOs and CISOs need a go-to source for direction on what to protect, and it is important for state executives to consider establishing a chief privacy officer role to complement the CIOs/CISOs function.

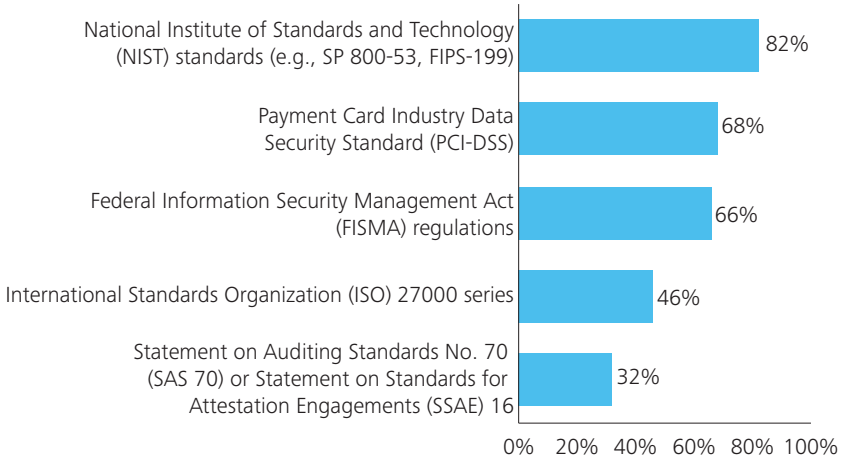
Regulatory audits are a routine occurrence in state agencies. And, survey respondents indicate that internal and external audit findings are also routine. Yet, due to the federated and distributed model that most states follow, enterprise CISOs are hard pressed to gain visibility into a states' overall regulatory postures and audit findings.

Regulatory frameworks used by states

There is a substantial body of federal laws and regulations with which state agencies must comply. For example, nearly 100% of respondents cited the need to comply with the Health Insurance Portability and Accountability Act (HIPAA), Federal IRS Publication 1075, and the Criminal Justice Information Services (CJIS) Security Policy.

CISOs know that the adoption of security standards can help to guide state agencies in their quest to satisfy regulatory mandates. And most respondents indicate a preference for NIST SP800-53 as the foundation for enterprise-wide security policies, standards, and procedures (Figure 13).

Figure 13. External cybersecurity standards, regulations, frameworks and guidance you rely on to comply or carry out information security programs



Key takeaway

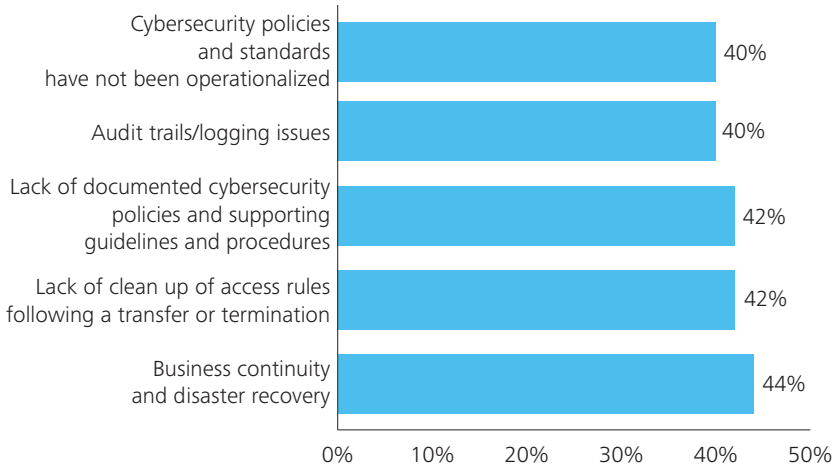
Given that NIST SP800-53 is the base standard for several key federal cybersecurity regulations, states are encouraged to adopt it as the common framework.

States also face regulatory audit findings; the key is to bring the visibility of these findings and risk of non-compliance to state leaders

While states do not have a compliance mandate like FISMA, state agencies undergo routine audits by a number of federal and other organizations. Key points to consider include:

- 45 CISO respondents report at least one regulatory audit finding.
- Given the current federated and decentralized model of governance, CISOs lack visibility into agency-level regulatory audits and findings.
- Business leaders understand and own the risks of non-compliance—and federal and state regulators expect these stakeholders to meet compliance requirements.
- CISOs must relate the risks of non-compliance to cybersecurity issues and use that to gain support for enterprise standards and solutions.

Figure 14. Internal/external audit findings within your state over the past 12 months



Key takeaway

State agencies are routinely audited and the findings can help CISOs highlight risks to business stakeholders.

Regulation helped banks gain executive visibility and support

"Over the past several years, regulation has been an important driver of banks' investment in security and IT risk. As a result, we've seen notable improvement and maturity of capability at many of the largest financial institutions. While some question the return on compliance investments, these more mature organizations have generally fared better than their less well prepared competitors in the face of real world cyber-attacks and security incidents. It is clear that regulation, among other drivers, has helped to elevate security concerns to executive management and boards, resulting in more visibility, broader support, and more significant investments that are creating benefit for the banks."

Ed Powers
US Financial Services Leader for Deloitte's Security & Privacy practice

Responses to the State Officials Survey indicate that CISOs are not alone in the pursuit to secure information IT assets. These stakeholders understand the cybersecurity risks and consider this a critical matter for the state. In fact, they feel the pain directly because audit findings are reported to the heads of individual agencies—and they own the risk of non-compliance and are responsible for determining how to address shortcomings.

Therefore, state CISOs can leverage regulations and audit results as a way to better articulate cybersecurity risks due to non-compliance and obtain sufficient cybersecurity funding.

Better communicate compliance issues

As explained in the previous section, despite the federated model, enterprise CISOs can establish their authority over cybersecurity governance and define a strategy to implement and prioritize enterprise security projects based on regulatory requirements. In this process, it is essential to recruit agency CISOs or their equivalent to support the effort.

To improve the chances that this joint effort will be a success, CISOs must step up reporting and encourage their agency counterparts to do the same. As shown in Figure 15, cybersecurity reporting is primarily performed on an ad-hoc basis, and limited to agency IT and security staff.

Figure 15. Nature and frequency of reporting from State CISOs

	Never	Monthly	Quarterly	Annually	Other
Governor	40.4	17	6.4	19.1	17
State Legislature	55.3	4.3	6.4	23.4	10.6
Secretary/Deputy Secretary	39.1	19.6	6.5	13	21.7
Agency IT and cybersecurity management (Agency CIOs, CISOs)	22.9	39.6	8.3	12.5	16.7
General Counsel/Legal or Audit Committee	46.7	4.4	4.4	22.2	22.2
Business Stakeholders	54.3	2.2	6.5	13	23.9
Other	61.9	14.3	4.8	4.8	14.3

Key takeaway

CISOs must communicate more broadly and with greater regularity in order to raise cybersecurity visibility and drive support for greater funding.

Leading practice highlight

West Virginia's risk management initiative

In West Virginia, a combination of legislation and an Executive Order helped to define and require the development of Executive-wide policy, training, audit for compliance, and mitigation of vulnerabilities. In addition, Executive Order 6-06 called for the formation of an Executive Branch Information Security Team and a Privacy Management Team. The Governor's Executive Information Security Team (GEIST) was subsequently established which enlisted high-level departmental operatives to extend the reach of the Office of Information Security and Controls.

An Information Security Strategic Plan was developed and, over time, resources and tools have been acquired to focus on the information and cybersecurity challenge of overall risk reduction through strong controls and heightened awareness. In addition, an audit function was established at the Office of Technology; the Office of Technology will have a base audit that can satisfy requirements of multiple audits conducted throughout the year, saving significant time for repeated audits on the same control set.

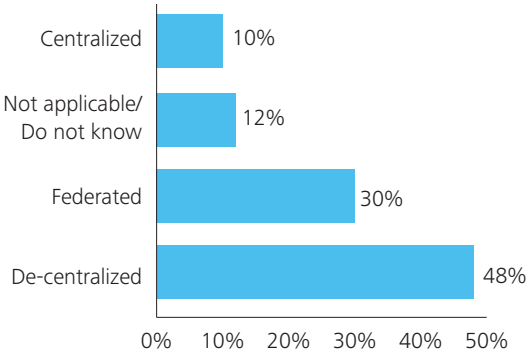
CIOs and CISOs own the information security domain, not privacy

Protection of PII is a hot-button topic—with 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands having enacted legislation requiring notification of security breaches involving personal information.[8]

There's an important distinction between privacy and cybersecurity functions. Privacy personnel focus on the protection of citizen rights and are charged with saying what to protect. Once the what is defined, CISOs and other cybersecurity staff can determine the how (i.e., what measures should be taken to protect that information).

Only 18% of states report having an official responsible for privacy, such as a Chief Privacy Officer. Of course, this doesn't mean no one is looking out for privacy. It's hugely important to such agencies as health and human services and public safety. And the survey bears this out with the majority of respondents saying their states follow a decentralized or federated model for privacy (Figure 16).

Figure 16. Structure of state's privacy function



Key takeaway

The lack of a centralized privacy function places added pressure on CIOs and CISOs who seem to inherit the privacy function by default.

How can CISOs be certain the risk of PII exposure is properly mitigated when there is no single point of authority responsible for determining what needs to be protected?

Until the Chief Privacy Officer position becomes prevalent in state government, CIOs could compensate by appointing their general counsel or senior staff member as a privacy liaison with the responsibility of finding and working with privacy personnel in the various agencies and departments. This will not only serve to strengthen PII protection; it can also be a means of joining forces to advocate for more business stakeholder support to improve privacy measures.

Share lessons learned and leading practices

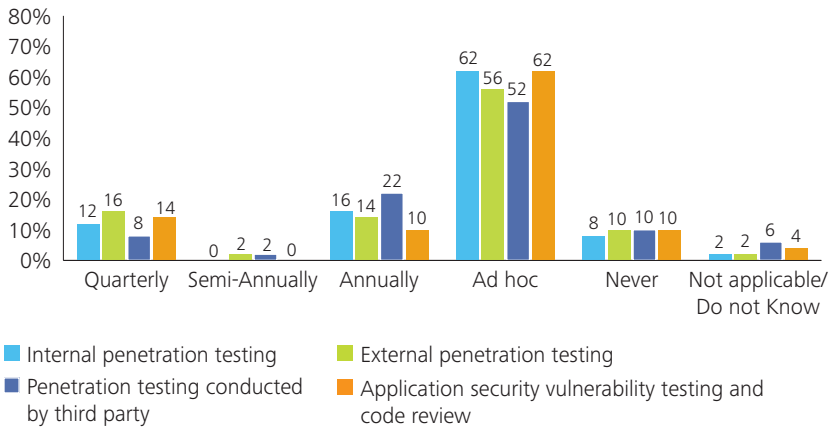
Enterprise CISOs have the opportunity to look across state governments and identify agencies that are doing exceptionally well in one or more security disciplines, such as identity and access management, threat assessment and mitigation, or protection of PII. As such, CISOs are in an ideal position to foster efficient information sharing of leading practices from these top performers to other agencies—and perhaps build a Center of Excellence model to formalize the process.

Trends

Vulnerability testing frequency

The 2012 study shows that the majority of states continue to conduct internal and external system penetration testing on an ad-hoc basis only. In fact, the number that test on a quarterly basis has fallen slightly since 2010.

Figure 17. Frequency of testing and review



Leading practice highlight

A showcase for effective, enterprise-wide vulnerability management in North Carolina

Vulnerability management is complex and time consuming. For example, software and hardware vulnerabilities are identified at different times of the year, pose different threats, and are typically announced either monthly or quarterly, based on the vendor. The effort to apply thousands of patches (fixes) is immense. However, the longer an issue remains unresolved, the greater the likelihood of compromise—and a security incident.

In North Carolina, the Office of Information Technology Services (ITS), the State's central IT services provider, patches platform vulnerabilities, while client agencies, which own their respective business applications, patch their application vulnerabilities.

In an innovative project to streamline the process across the enterprise, ITS leverages open-source tools to capture scanning results from several system platforms, load them into a centrally managed database, strip out false positives, and immediately provide the results to agency customers. As a result, agency personnel can assess, validate, and address the vulnerabilities—and report back to ITS on the current status of any vulnerabilities.

This enterprise-wide initiative has reduced the "time to vulnerability closure" from weeks to days. What's more, the use of open-source tools eliminated licensing fees for the commercially provided vulnerability management solution. And, three positions were repurposed for other activities, saving the state more than $250,000 annually.

Key takeaway

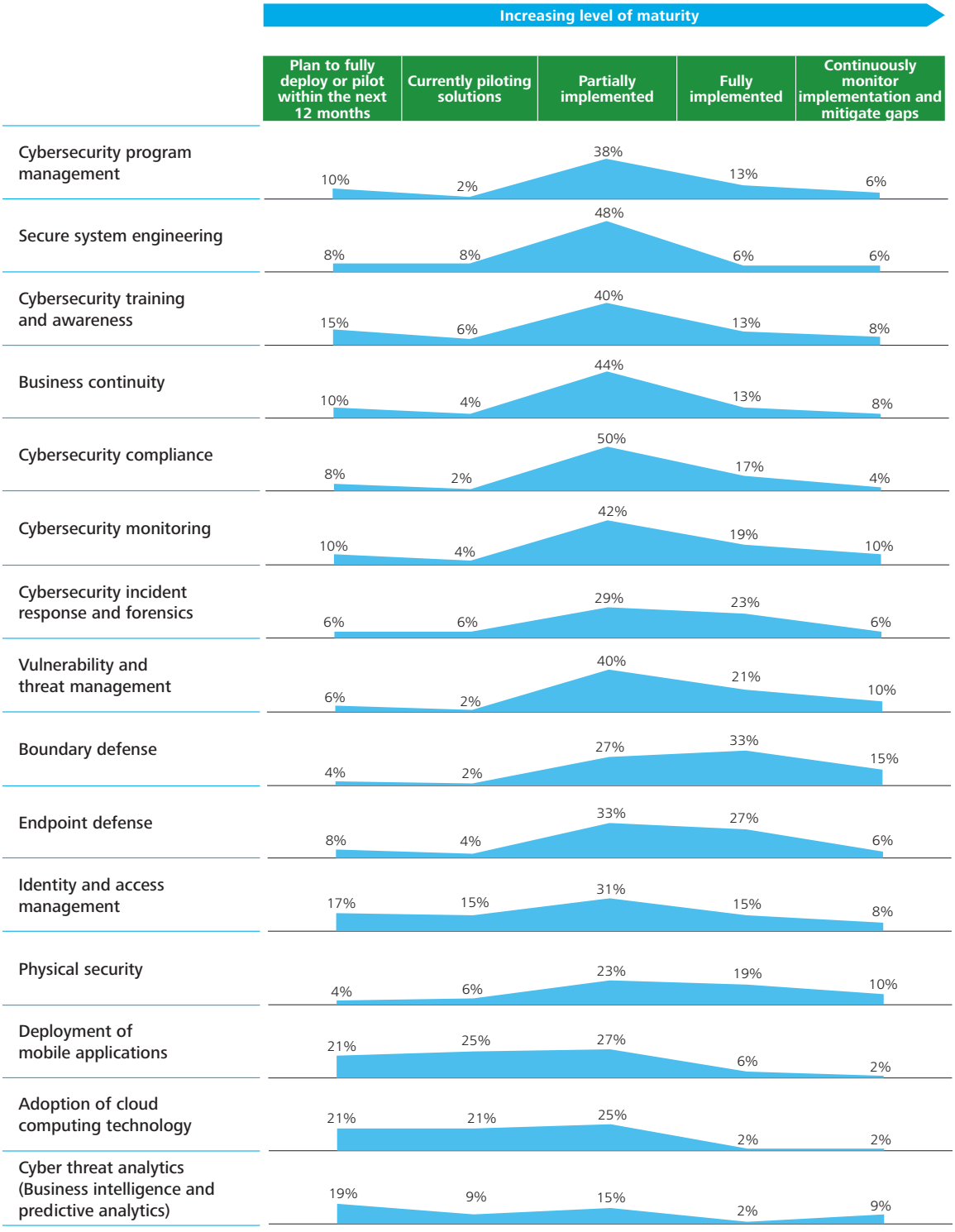
Because vulnerability tests are fundamental "security 101" tasks, the recommended approach is to plan and conduct them on a quarterly or semi-annual basis.

Maturity of cybersecurity practices

The 2012 Deloitte-NASCIO Cybersecurity Study CISO questionnaire included a new section asking participants to conduct a detailed self-evaluation across a range of core security services. The responses provide a foundation for building greater insight into the maturity of states' cybersecurity programs. The 2012 responses, in combination with those in the years to come, will serve to highlight areas where states are performing well, as well as opportunities for improvement.

In an October 2011 issue brief, *The Heart of the Matter*,[9] NASCIO recommended that states identify a taxonomy of core, critical cybersecurity services to help make sure that IT security remains robust—regardless of fiscal challenges. The responses to two of the questions related to core services are highlighted in Figure 18 and Figure 19 on pages 26 and 27.

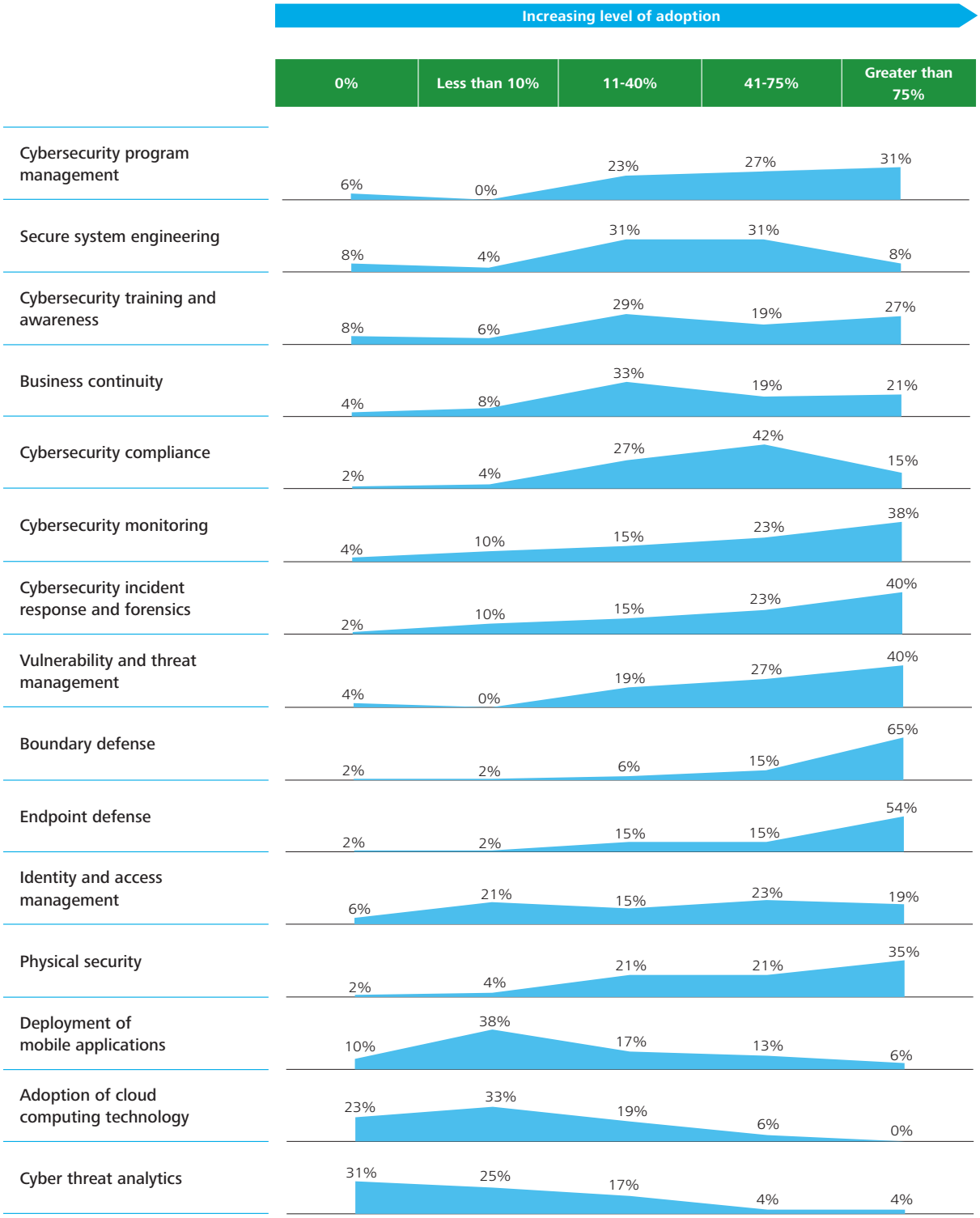
Figure 18. Extent of enterprise cybersecurity services implementation



Key takeaway

CISOs have historically focused on perimeter-security-related services, such as boundary and endpoint defense. Business initiatives that drive the use of new technologies, like cloud and mobile, must include core security services adoption as an integral part of projects from day one.

Figure 19. Extent of enterprise level adoption of cybersecurity services



Key takeaway

Boundary and endpoint defense services are implemented on an enterprise-wide basis and have gained broad acceptance. The more complicated functions and emerging technologies have a low rate of adoption—an indication that they could be prime candidates for a shared services delivery model.

A call to action for states

The 2012 Deloitte-NASCIO Cybersecurity Study shows that, while CIOs and CISOs recognize the risks inherent in securing information, much work remains to overcome their challenges. Many business official respondents report that cybersecurity is very or extremely important to their states and individual agencies. As such, CIOs and CISOs have a green light to push for the funding, resources, and stakeholder support needed to further cybersecurity initiatives.

Based on survey results, the following checklist highlights actions states can take to mitigate risks and move the needle forward on cybersecurity programs and objectives.

- ✓ **Assess and communicate security risks:** Adopt a uniform security framework such as the Federal NIST standard, perform regular compliance assessments against the framework across agencies, and communicate risks to relevant business stakeholders.

- ✓ **Better articulate risks and audit findings with business stakeholders:** Routine reporting of cybersecurity threats, projects, and status is essential to building support for security and privacy initiatives.

- ✓ **Explore creative paths to improve cybersecurity effectiveness within states' current federated governance models:** Create cybersecurity competency centers or pursue a shared services model to maximize the use of scarce qualified personnel resources, technology, and dollars to avoid duplication of effort across agencies and departments.

- ✓ **Focus on audit and continuous monitoring of third-party compliance:** With greater use of outsourcing, more needs to be done to manage the growing shared risk. States must communicate cybersecurity policies and practices to partners, including local governments, and regularly use specific metrics to assess how well these protective measures are being followed.

- ✓ **Raise stakeholder awareness to combat accidental data breaches:** Better, more effective user education is a huge opportunity—because the number one cause of security breaches is user error. Balance the cost of education and the disruption to individuals against the benefit of keeping the state out of the headlines—and it's clear the investment is a sound one.

- ✓ **Aggressively explore alternative funding sources including collaboration with other entities:** Leave no stone unturned in the hunt for additional funding for security and privacy initiatives. Identify agency initiatives with federal funding and help make sure cybersecurity requirements are considered and addressed. Use what's learned to benefit state agencies and their partners.

- ✓ **Make better security an enabler of the use of emerging technologies:** Leverage the strong motivation of business leaders to embrace new technology to improve program effectiveness by building effective security measures and using them as an enabler. Identify and agree on a core security services taxonomy to serve as a common vocabulary for describing services that must be provided to meet the requirements of security standards frameworks defined by the federal government and various standards bodies.

Appendix

Participant profile

The 2012 Deloitte-NASCIO Cybersecurity Study targeted two audiences:

- 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 participants answered 64 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Participation was high—representatives from 48 states and two territories responded to the survey. Figure 20, Figure 21 and Figure 22 illustrate the CISO participants' demographic profile.

Figure 20. CISO survey respondent designation

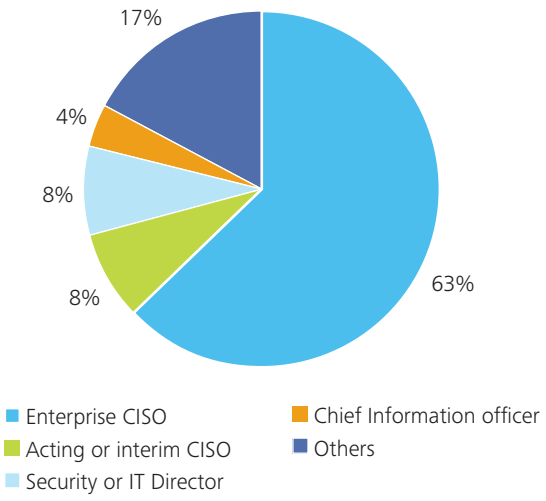


Figure 21. Number of employees in respondent states (excluding higher education employees)

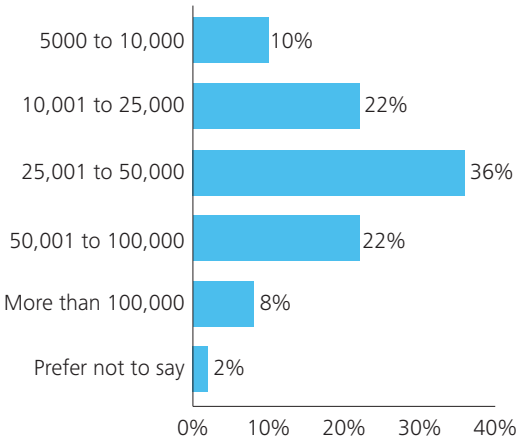
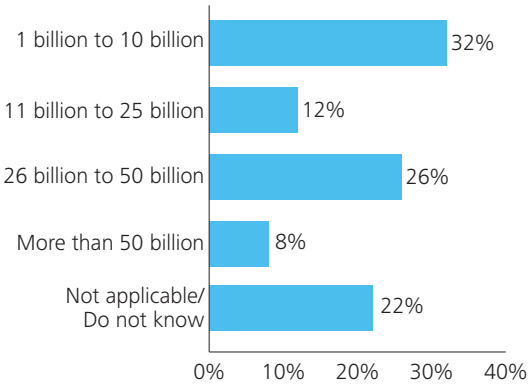


Figure 22. Approximate budget of the respondent states



Sixty-three state officials answered 17 questions to provide insight into states business stakeholders' perspectives. The participant affiliations included the following associations:

- National Association of State Auditors, Controllers 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).

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 have been included in this report, but the respondents have not been cited for confidentiality reasons.

Additional thought leadership reference materials

For more information and perspectives about cybersecurity challenges, solutions, and best practices, readers are encouraged to explore these resources:

NASCIO

- Capitals in the Clouds: The Case for Cloud Computing in State Government Part I: Definitions and Principles
- The Heart of the Matter: A Core Services Taxonomy for State IT Security Programs
- Security at the Edge, Protecting Mobile Computing Devices
- The State Identity Credential and Access Management Guidance and Roadmap (SICAM)
- State IT Workforce: Under Pressure

Deloitte

- 2012 Global Financial Services Industry Security Survey
- Cloud Computing: Forecasting Change
- Cloud Computing
- Tech Trends 2012


0 1 1
0 1 0
0 1 0

About the survey

How Deloitte and NASCIO designed, implemented and evaluated the survey

Deloitte and NASCIO collaborated to produce the 2012 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. Each participant's response is confidential and demographics information of the survey content will be deleted after the preparation of the survey reports.

The data collection, analysis and validation 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 Technology Risk Services. 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 to 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 was provided individually to the enterprise CISO survey respondents.

Sources/Footnotes

[1] "Rapid7 Report: Data Breaches in the Government Sector." Rapid7. September 6, 2012.

[2] "2011 Cost of Data Breach Study: Global." Ponemon Institute. March 2012.

[3] "State IT Workforce: Under Pressure." NASCIO. January 2011.

[4] "Rapid7 Report: Data Breaches in the Government Sector." Rapid7. September 6, 2012.

[5] "2011 Cost of Data Breach Study: Global." Ponemon Institute. March 2012.

[6] Gregory Wilshusen. Testimony before the House Homeland Security Committee's subcommittee on Oversight, Investigations and Management. April 2012

[7] "The State Identity Credential and Access Management Guidance and Roadmap (SICAM)", NASCIO, September 2012.

[8] http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx National Conference of State Legislatures. August 2012.

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

Acknowledgements

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

NASCIO
Charles Robb, Senior Policy Analyst
Doug Robinson, Executive Director

Security and Privacy Committee Co-Chairs and Members

State CISO Survey Review Team
Chris Buse, State of Minnesota
Dan Lohrmann, State of Michigan
Elayne Starkey, State of Delaware
Erik Avakian, Commonwealth of Pennsylvania
Mike Russo, State of Florida

Deloitte subject matter specialist contributors
Art Stephens, Deloitte Consulting LLP
Kristen Miller, 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
Cynthia O'Brien, Deloitte & Touche LLP
Olivier Curet, Deloitte & Touche LLP
Sheila Celata, Deloitte & Touche LLP
Susan Supernavage, Launch International, Inc.

Marketing
Germaine Henry, Deloitte Services LP
Pamela Williams, Deloitte Services LP
Suzanne Love Beck, Deloitte Services LP
Shawn Vaughn, NASCIO

About Deloitte and NASCIO

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate.

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

National Association of Chief Information Officers (NASCIO)

Doug Robinson
Executive Director
1 859-514-9153
drobinson@AMRms.com

Charles Robb
Senior Policy Analyst
1 859-514-9209
crobb@AMRms.com

Deloitte

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

Rhoda Woo
Managing Director
Security & Privacy
Deloitte & Touche LLP
1 214-436-3388
rwoo@deloitte.com

Srini Subramanian
Principal
Leader, State Sector Security & Privacy
Deloitte & Touche LLP
1 717-651-6277
ssubramanian@deloitte.com

About this publication

About Deloitte