Deloitte.

NASCIO
Representing Chief Information Officers of the States

State governments at risk
A call to secure citizen data and inspire public trust

The 2010 Deloitte-NASCIO Cybersecurity Study
A publication of Deloitte and the National Association of State Chief Information Officers

Contents

Cybersecurity: State leadership and the protection of personal data

As states confront the worst economic crisis since the Great Depression, governors across the country find themselves forced to cut many vital programs and services. Against this backdrop, it's difficult to encourage new investment; however, there is one issue that is too crucial to ignore: cybersecurity.

Cybercrime – the term used for any computer hacking, identity theft, fraud and other Internet related prohibited activities—is more prevalent, more insidious than any other crime, yet it remains an invisible threat that is easy to overlook. Cyber criminals are more organized and more effective than ever, and they now use sophisticated tools and resources freely traded on the black market to help them steal valuable constituent, business, and government data that are highly desired by domestic and global criminals, terrorists and foreign states acting with harmful intent.

At the federal level, the President and his Cabinet have made cybersecurity a national priority with the goal of better managing risks to national security posed by cyber terrorism and cyber warfare threats. However, the effort to protect the data of governments and citizens cannot be addressed by the federal government alone. It is a national mission, not a federal one, a responsibility that requires us to work to enlist the leadership, innovative ideas and resources at the state level.

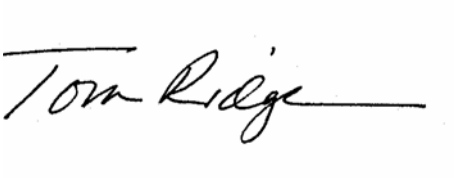
The 2010 Deloitte-NASCIO[1] Cybersecurity Study confirms that large amounts of Personally Identifiable Information (PII) that the states maintain may be at risk, but barriers identified in the study make securing PII a daunting task.

In the current environment of elevated cyber threats, states are faced with circumstances that have the potential to produce a perfect storm:

- States hold the most comprehensive collection of PII about constituents, spanning from birth to death.
- States routinely rely on the Internet to better serve constituents and increase efficiency. Moreover, health care reform promises to increase collection, storage, sharing and usage of people's personal information.
- Along with the federal government and financial, energy and health care sectors, states must shore up defenses to protect critical data systems.

State executives have worked hard to leverage the Internet and improve constituent services. Unfortunately, it appears that cyber criminals also are working hard to develop new Internet-based attacks and scams.

To keep up with these threats, we must step up our actions. State and local governments, federal agencies and the private sector now must work together to implement tougher security safeguards, thwart these threats, and be ready to respond when an attack occurs. It's a battle that we can win, but we must make cybersecurity a priority – before others make us a target.



The Honorable Tom Ridge
First Secretary of the U.S. Department of Homeland Security
Former Governor of Pennsylvania

Harry D. Raduege, Lieutenant General, USAF (Ret)
Chairman, Deloitte Center for Cyber Innovation
Deloitte Services LP
Co-chairman for the Center for Strategic and International Study's (CSIS's) Commission on Cybersecurity for the 44th Presidency
Former Director, Department of Defense,
Defense Information System Agency

Foreword

People put a lot of trust in state governments to collect, maintain and protect the appropriate information necessary to execute their programs, protect individual rights, and ensure public safety. The volume of that information expands at an ever-increasing pace, and maintenance and protection of that information, particularly where it involves Personally Identifiable Information (PII) and Personal Health Information (PHI), becomes more and more challenging. The 2010 Deloitte-NASCIO Cybersecurity Study finds that states need to do more to secure citizen data and maintain public trust.

These developments come at a time when cyber threats are increasing in sophistication and force. The threat of participation of some foreign governments and organized crime has added another element to the array of cyber risks; potential traps for sensitive consumer information seemingly are multiplying.

We launched the 2010 Deloitte-NASCIO Cybersecurity Study to assist state leaders in making informed decisions related to cybersecurity threats, risks, programs, and strategies. Survey questions pertained to areas such as information security governance, investments, use of security technologies, quality of operations, privacy, and identity and access management.

We extend our sincere thanks to the Chief Information Security Officer (CISO), designates and security teams who took time out from their busy days to respond to this survey. We had an outstanding participation, with 49 of the 50 states responding to the survey. Without their valuable input and insight, this study would not have been possible.

In September 2006, NASCIO conducted a study of state CISOs. Data from that effort highlighted the key needs for sufficient staffing, adequate funding, and executive support. More recently, the 2010 Deloitte-NASCIO Cybersecurity Study finds that while State CISOs have done an excellent job at evolving their roles, educating stakeholders and seeking legislative support, they only can do so much with the resources and influence they currently possess.

The 2010 Deloitte-NASCIO Cybersecurity Study highlights that State CISOs substantially lack the funding, programs, resources, and tools available to CISOs of comparable private-sector enterprises. More significant, the study indicates that most State CISOs do not have the enterprise authority to manage the risks that threaten critical information assets spread across multiple agencies, departments, boards, and other organizations which make up state government.

The issues outlined above are not unique to state government; the private sector and federal government also grapple with them. At the federal level, the President has recognized the critical nature of the problem with the appointment of a cybersecurity coordinator. It behooves the governors to make cybersecurity a priority for the states to bolster the state CIOs and CISOs efforts.

Srini Subramanian
Director
Deloitte & Touche LLP

Doug Robinson
Executive Director
NASCIO

"In recent years, NASCIO has identified cybersecurity as one of the most critical concerns of state CIOs and made obtaining additional funding and support for state-level security programs a top priority. While states have established chief information security officer (CISO) positions over the last decade and worked hard to secure state-maintained networks and systems, the ever-increasing number and nature of threats have led to an evolving landscape in which vulnerabilities continue to threaten the security of state government. Most salient among the findings are that CIOs and CISOs continue to need greater authority and resources in this tough economy. Unprecedented budgetary cuts across state governments and growing reliance on contractors and outsourced IT services are creating an environment that is even harder to secure, and the report highlights the growing concerns of CISOs in this regard."

Steve Fletcher

NASCIO President & CIO of the State of Utah

Key Findings

There has been progress on many fronts since the 2006 NASCIO CISO study but concrete actions on key information security threats and risks remain an elusive goal.

Four years ago, the 2006 NASCIO survey of State CISOs described the "increasingly complex and threatening world" of cybersecurity and the challenges inherent therein. The 2010 Deloitte-NASCIO Cybersecurity Study underscores the continuing challenges, and details an environment in which the sophistication and proliferation of threats are escalating.

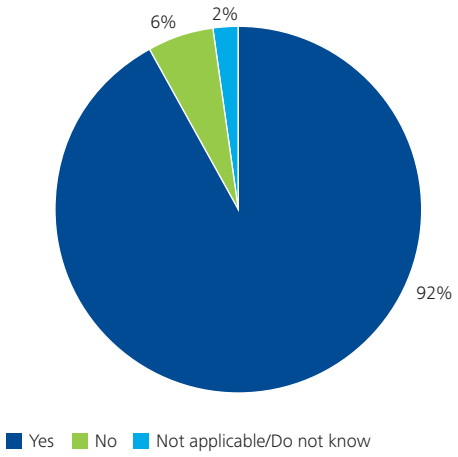
The 2010 Deloitte-NASCIO Cybersecurity Study asked state representatives an encompassing set of questions regarding their current practices pertaining to cybersecurity. This report analyzes their responses and focuses on five key areas:

1. **Governance:** The Enterprise CISO position is firmly established in the majority of states. To be successful, CISOs must continue to evolve this position to garner enterprise visibility, authority, executive support, and business involvement.
2. **Strategy:** States increasingly are embracing strategic planning as part of their cybersecurity approaches and are converging on the National Institute of Standards and Technology (NIST) risk assessment framework for strategic alignment. However, without compliance audit and enforcement mandate such as the Federal Information Security Management Act (FISMA) at the Federal level, compliance to the NIST framework across the enterprise is not likely to be achieved.
3. **Budget:** Security budgets and resources available to State CISOs lag behind those of their private-sector counterparts. In tough economic times the gap may be widening as the private sector is increasing its investment in security.
4. **Internal, External Threats and creating a cyber mindset:** Threats to PII and PHI are growing—both from the inside and the outside. States are still in the early stages of establishing programs and deploying technology to protect this sensitive data. Further, CISOs expect to face a host of threats over the next 12 months, ranging from "zombie" networks to social engineering and employee lapses. For this reason, CISOs recognize the importance of creating a "cyber mindset" within their respective enterprises, and are turning to education and awareness to combat these threats.
5. **Security of Third Party Providers:** States use the services of contractors, managed service providers, and other third parties to deliver sensitive and critical constituent services; managing the security of these third-party providers may not be keeping pace with the escalation of threats.

The 2010 Deloitte-NASCIO Cybersecurity Study compares state responses against Deloitte's bellwether survey in the financial services industry, as well as against other external sources and benchmarks. These comparisons serve to demonstrate the divide that exists between the private sector and the states.

1. Cybersecurity Governance
Taking a page from the private sector will be a step in the right direction

Figure 1. Does your State have the position of enterprise Chief Information Security Officer (CISO) or equivalent?



State governments are obviously composed of three different branches (executive, legislative and judicial); and within each branch, there exists a multitude of agencies, departments and boards, some of which do not fall under the state governor's jurisdiction. Most of these organizations have their own Information Technology (IT) departments; many have their own directors and information security officers. Respondents to the 2010 Deloitte-NASCIO Cybersecurity Study indicated that 92 percent of states have an Enterprise CISO role. This represents an increase from 83 percent from the 2006 NASCIO CISO survey.

According to the most recent study results, the majority (51 percent) of Enterprise CISO respondents indicated that their state follows a federated information security model, meaning that while the CISO is responsible for the enterprise, the agencies also may have a separate IT/security structure. Study results also revealed that the Enterprise CISO is most commonly (63 percent) responsible for the executive branch of the state, and only 10 percent of the respondents had authority over the executive, legislative and judicial branches.

The Enterprise CISO has a broad portfolio of functions to manage in both policy and operational security areas.

While it is encouraging that 92 percent of the responding states reported having CISOs, and scope of their function has broadened, we find that Enterprise CISOs lack the visibility and authority to effectively drive security down to the individual agency level.

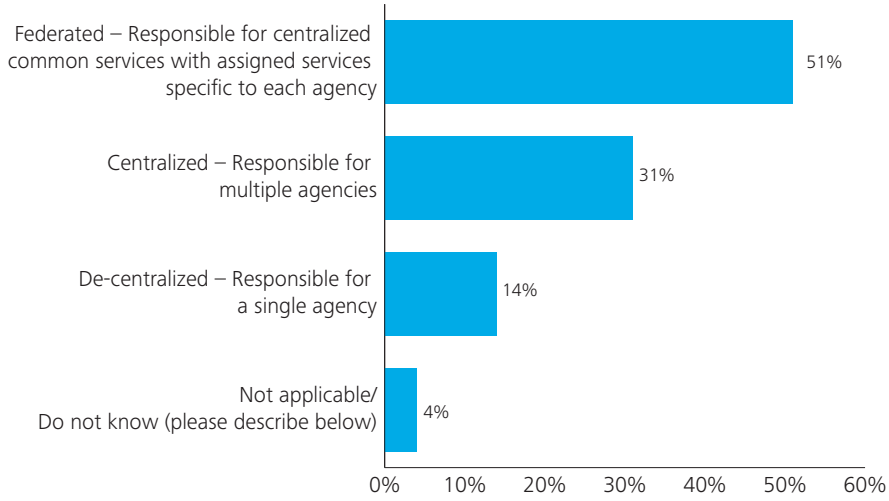
The CISO reporting relationship

The 2010 Deloitte-NASCIO Cybersecurity Study indicated that a majority of CISOs (76 percent) report to the CIO, the state IT Director or the equivalent. While this represents a healthy increase of 22 percent from the September 2006 NASCIO survey, we believe that the role of a state CISO is still evolving from technologist to enterprise risk management executive.

CISO direct reports

State CISOs fare worse than their financial services industry counterparts when it comes to employee resources. Nearly half of the respondents (47 percent) in the 2010 Deloitte-NASCIO Cybersecurity Study reported a staff of one to five full-time equivalent (FTE) information security professionals within their states or agencies. When compared to the 2010 Deloitte Global Financial Services Industry (GFSI)

Figure 2. How is your state's information security model structured?



Security Study[2], the difference is dramatic; more than 100 full-time professionals report to CISOs in financial organizations of similar size to that of an average state.

While the states' federated model may explain how more security professionals are working within individual agencies, CISOs still will be strongly challenged to implement consistent security measures across the board. As an example, one agency may be adequately addressing its risk and exposure, while another agency, lacking comparable security resources, may be exposing the state at the enterprise level to sizable risk.

Combating cybercrime through a multi-disciplinary approach

Cybersecurity should be a priority for Governors' cabinet members, legislators, and the judiciary. The state leadership should play a fundamental role in enabling Enterprise CISOs to exercise the right authority and influence within state government.

Figure 3. Scope of authority: For which of the following organizational entities does your State's CISO or equivalent have responsibility?

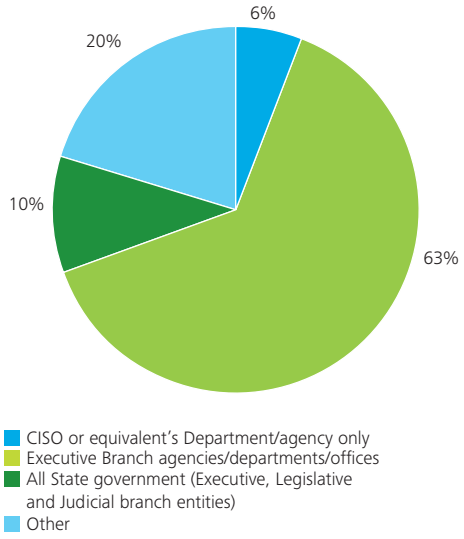


Figure 4. Which functions are within the scope of the CISO or equivalent official?

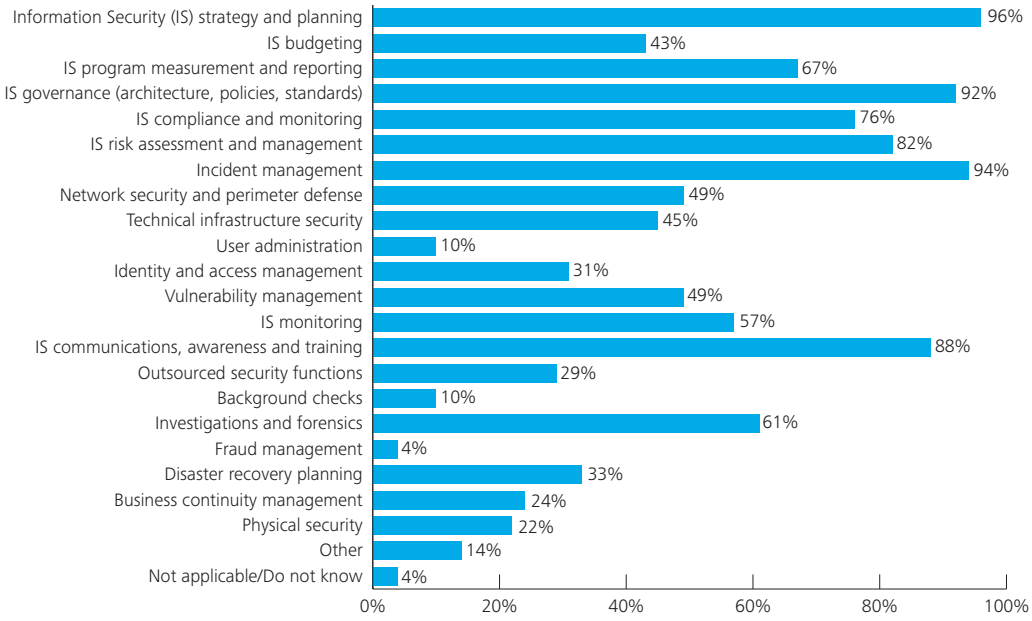


Figure 5. To whom does your State's CISO, or equivalent responsible for information security, report?

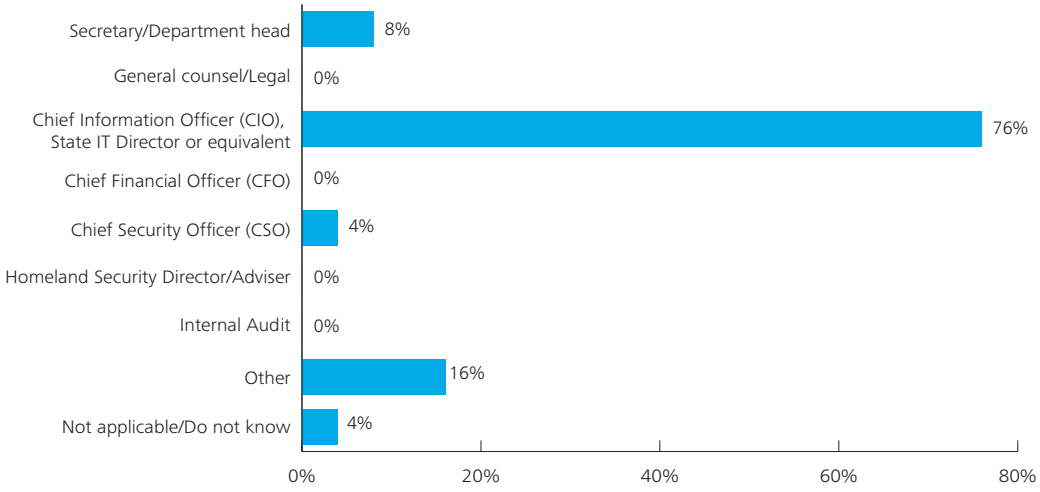


Figure 6. Comparison of number of information security FTEs in state versus financial services organizations of comparable size.

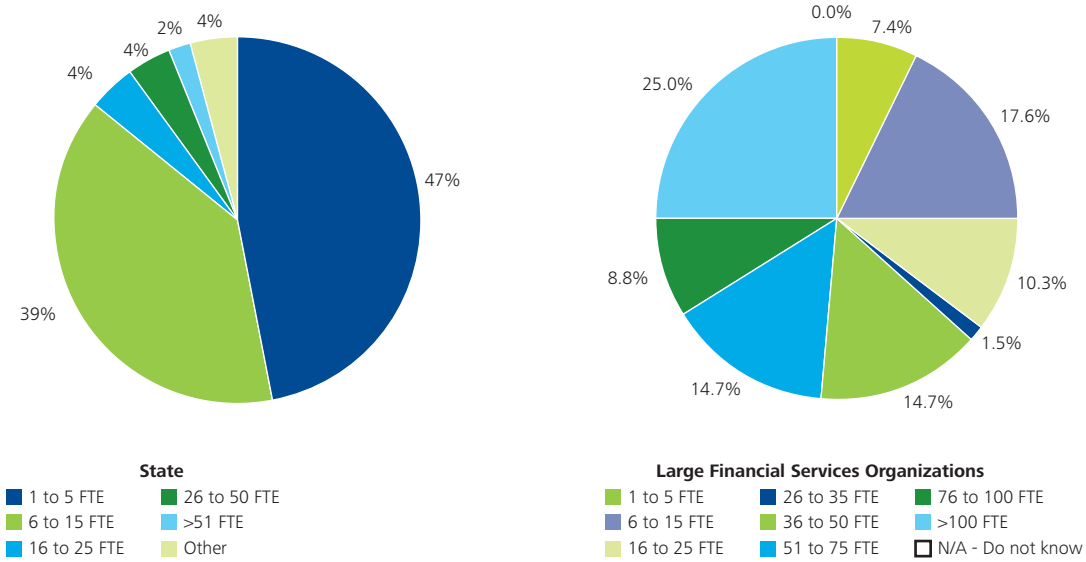
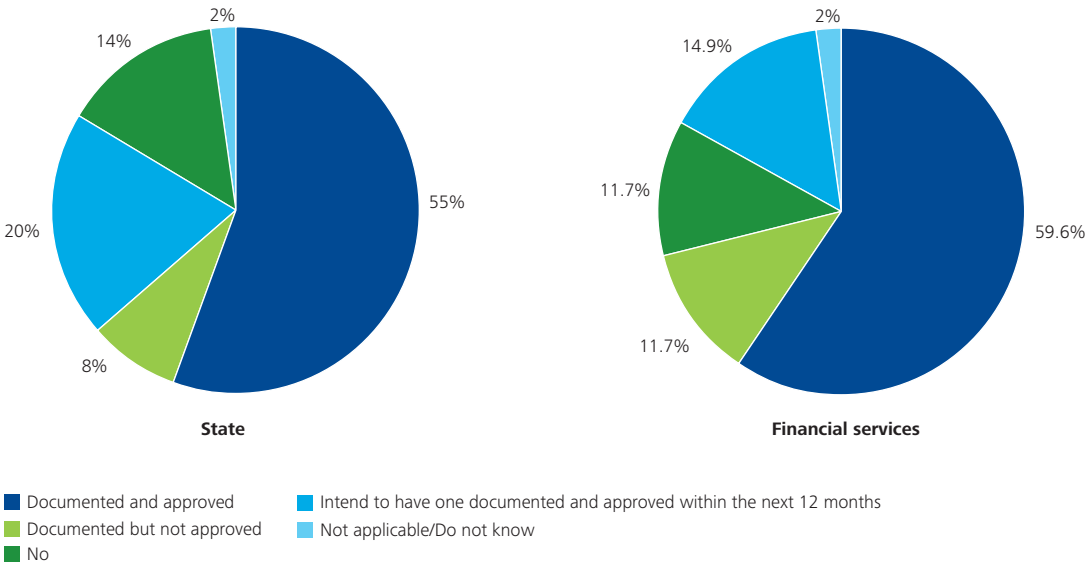


Figure 7. Comparison of security strategy across state governments and financial services organizations. Does your State (or agency) have a documented and approved information security strategy?



Joining forces?

State Attorneys General (AGs) are also actively are engaged in combating identity theft and cybercrime, raising cyber awareness, and fighting identity theft under resource constraints similar to the CISO. Joining forces with AGs, Homeland security, Federal and local agencies may help raise the bar for information protection in state government. This is just one option; states need to get creative to holistically combat cybersecurity risks.

Bottom Line

Continued progress in enterprise governance and risk management processes that fully integrate business and technology is necessary to manage the security function effectively. State governments need creative and collaborative approaches to be more effective in combating risks. State leadership plays an important role in striving to establish a situation in which cybersecurity has top visibility and CISOs have the authority to be effective.

"A common misconception made by government leaders and policymakers is that CISOs spend most of their time developing and enforcing security controls. But the fact of the matter is that security is only one factor in the success equation. State CISOs also need to be highly skilled at driving policies, standards, and complex enterprise solutions through a complicated governance processes, often dominated by individuals who are reluctant to change, provide funding support, or concerned of losing control. Furthermore, State CISOs must be masters at human and financial resource management, constantly selling the value proposition of security to people who control the purse strings. If any one of these three critical success factors is not in place, State CISOs simply will not be able to position their program to appropriately address the barrage of cyber threats all governments face each day. And that is what makes the job of a State CISO so difficult and why there has been only marginal success across our nation."

A State CISO

Figure 8. Comparison of security governance (defined roles, responsibilities, policies and procedures) across state governments and financial services organizations. Does your State (or agency) have a documented and approved governance for information security (i.e. defined responsibilities, policies and procedures)?

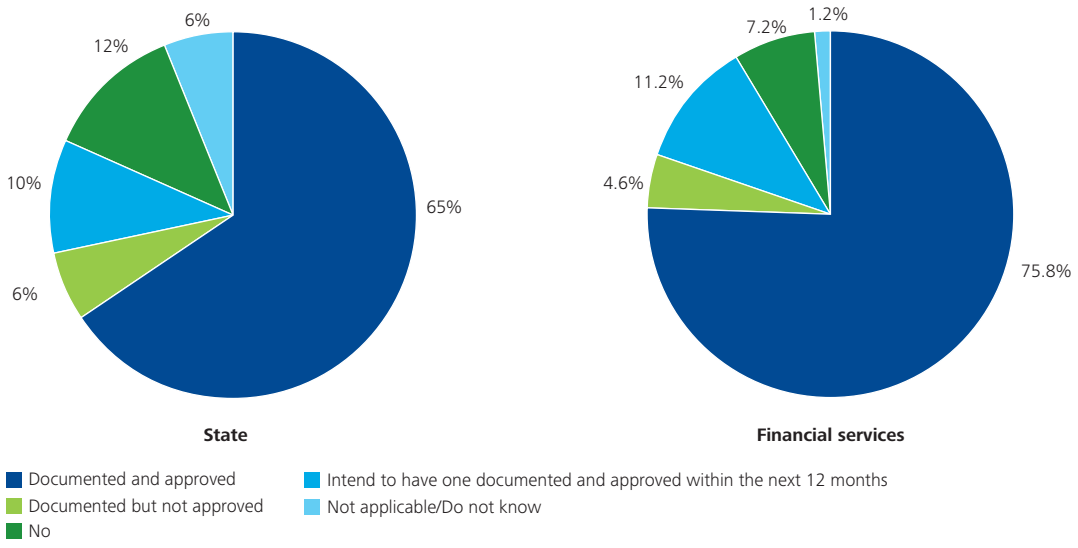
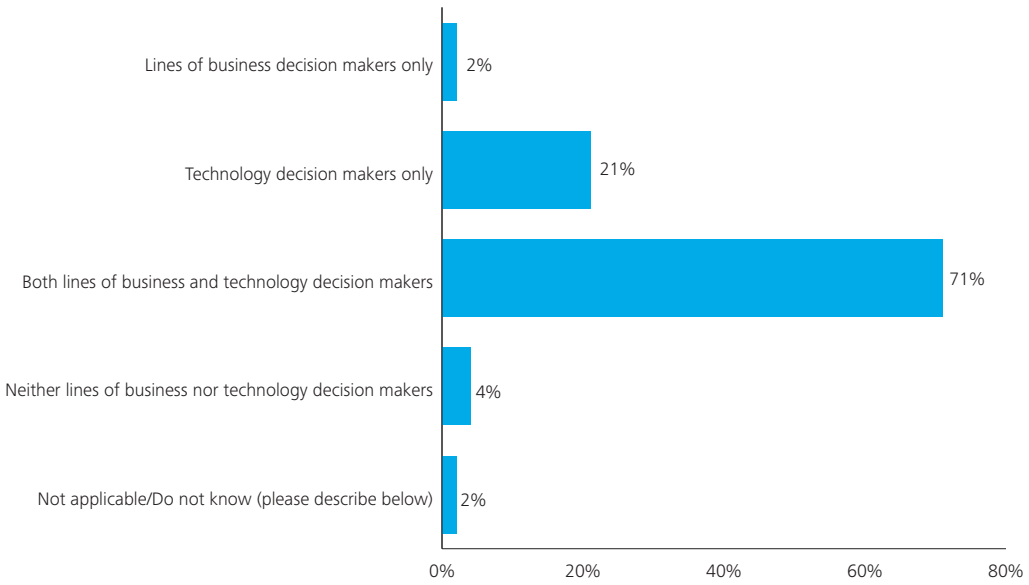


Figure 9. Does your State (or agency) actively engage both business stakeholders and technology decision makers in identifying requirements for the State's (or agency's) information security strategy?

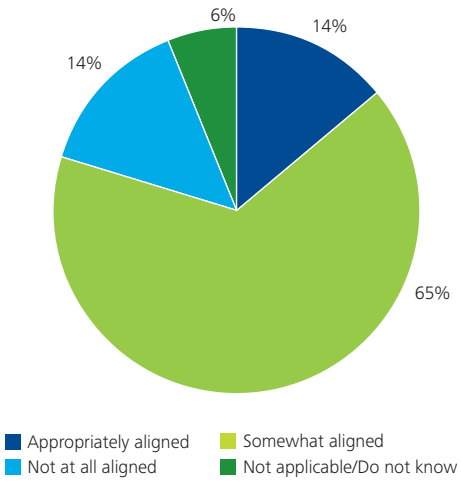


2. Information Security Strategy
States have the strategic plans; the challenge is in the execution

According to respondents of the 2010 Deloitte-NASCIO Cybersecurity Study, many states have documented enterprise-level security strategic plans. In general, these plans have helped CISOs establish consistent tone, set security priorities, and facilitate coordination among the many stakeholders within the state. A majority (83 percent) of responding State CISOs indicated that they have or intend to have a documented and/or approved information security strategy in the next 12 months. Similarly, 81 percent of respondents said they have or intend to have enterprise-level information security responsibilities, policies, and procedures defined and documented. These numbers are impressive and comparable to the 2010 Deloitte GFSI study when it comes to documented and approved strategy and governance. Figures 7 and 8 compare states with comparably sized financial services organizations for these two factors.

Many CISOs responding to the 2010 Deloitte-NASCIO Cybersecurity Study noted the importance of a security strategic plan to help engage executive state leadership in meaningful dialogue about enterprise risks. Overall, 71 percent of respondents said that both business and technology decision-makers provided input to their state Information Security strategies.

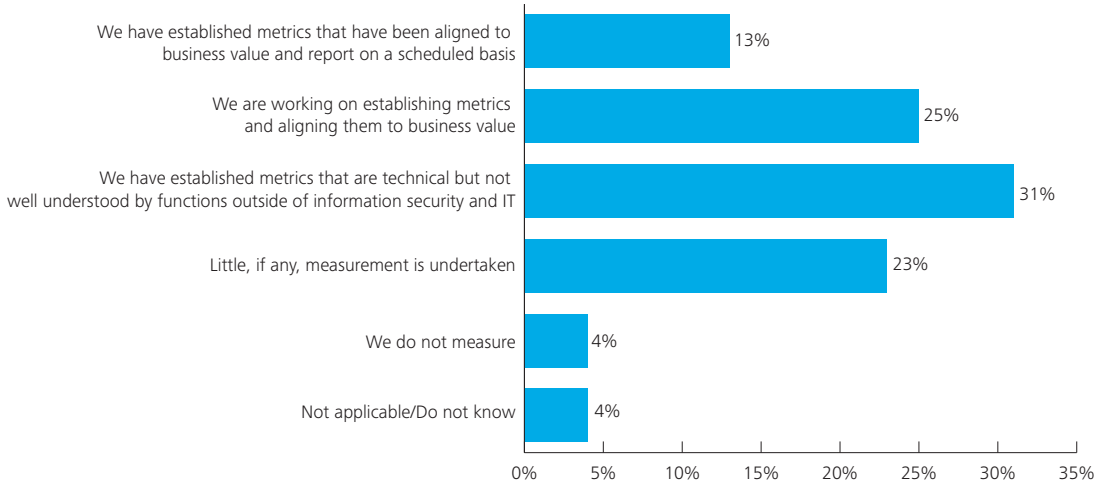
Figure 10. To what extent are business and information security initiatives aligned with each other in your State (agency)?



Seventy-nine percent of study respondents also indicated that security initiatives are "aligned" (14 percent) or "somewhat aligned" (65 percent) with business drivers.

Still, not every number was encouraging. Figure 11 summarizes how respondents revealed information security is measured and demonstrated to the business; only 13 percent of participating states indicated the existence of established metrics aligned to business value, and 23 percent reported little to no measurement at all.

Figure 11. Which statement best represents how you measure and demonstrate the value and effectiveness of your information security organization's activities?



There are two sides to achieving security alignment. CISOs need to articulate how they are adding value by protecting the business. And business leaders cannot be missing in action; they need to define what risks they have and what needs to be protected.

Security standards and frameworks

Respondents to the 2010 Deloitte-NASCIO Cybersecurity Study indicated a variety of information security standards, regulations, and/or frameworks in use within their information security programs. The NIST framework is the most prevalent; 90 percent of study respondents tabbed it toward the top. A variety of other standards and frameworks are also in use, ranging from the prescriptive Payment Card Industry Data Security Standards (PCI-DSS), to the Statement on Auditing Standards No.70 (SAS-70), which is more flexible in scope and approach. The range of standards or frameworks in use may represent funding-related requirements of different programs (for example, FISMA requirements for federal funds), as well as the unique nature of various state programs.

In the absence of overarching regulatory requirements, most states lack the impetus to adopt rigorous compliance with a chosen framework. Simply put, without a strong regulatory framework, associated compliance reporting, or funding, CISOs find it challenging to enact consistent security measures state-wide. "Desperately Seeking Security Frameworks – A Roadmap for State CIOs," a NASCIO brief published in March 2009[3], articulates the challenge for state government in the lack of a consistent risk compliance framework.

Figure 12. Which of the following external security standards, regulations, frameworks or guidance does your State (or agencies) choose to adhere to, comply with, or rely on, in carrying out its information security program?

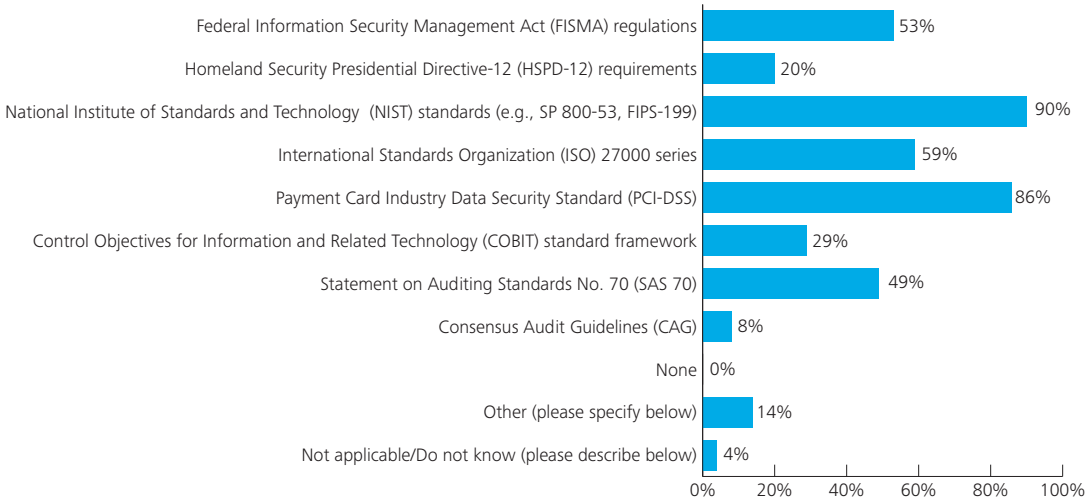
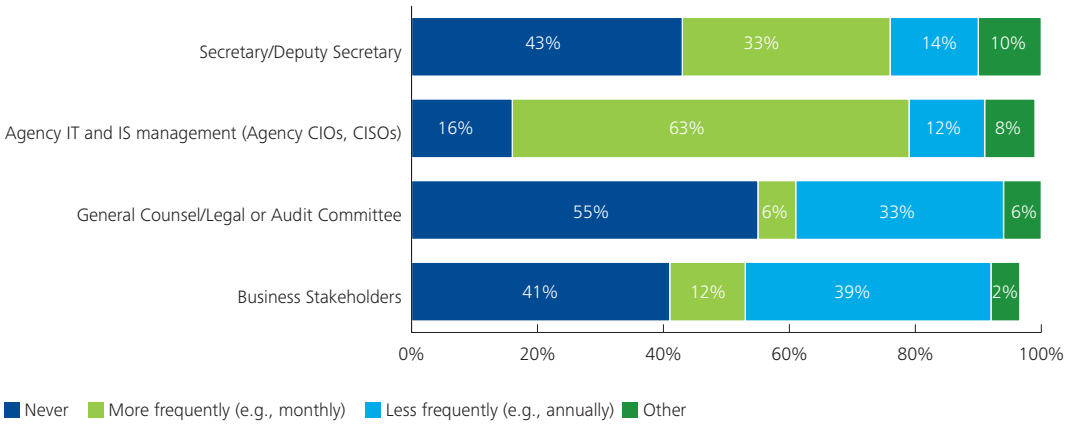


Figure 13. To what extent are you required to provide a report on information security status, or posture of the enterprise, to the following positions?



Executive Reporting

The execution of strategy, particularly when it requires the coordination of many different stakeholders, requires regular and transparent communication. About 63 percent of respondents to the 2010 Deloitte-NASCIO Cybersecurity Study indicated that they report data about information security to IT management on a frequent (e.g. monthly) basis. Respondents reported that communication with the State Secretary or Deputy Secretary, General Counsel/Legal, Audit Committee, and other business stakeholders is less frequent.

Compliance requirements have moved the private sector toward adoption of common, consistent security frameworks; they also have helped bring their CISOs into conversations about reporting and metrics with a broader set of organizational decision makers. The lack of similar compliance and reporting requirements is a handicap for the State CISOs. Regular briefings on the state of cybersecurity to the executive leadership and legislature will help bring visibility to the strategy and advance the execution.

Bottom Line

Sound security strategy is not enough; it must be supported by an executable roadmap that is aligned to (and involves) the business. State CISOs face an added challenge of bringing state leaders into security discussions in the absence of consistent regulatory security requirements that are common across the enterprise.

3. The Budgetary Trend
Declining security budgets are a dangerous trend, aggravated by economic conditions and competing state priorities

Tough economic times have debilitated the state governments, and many states are still reeling under budget deficits. The 2010 Deloitte-NASCIO Cybersecurity Study uncovered that State CISOs overwhelmingly (88 percent) consider "lack of sufficient funding" to be the greatest barrier to information security. A high number of respondents (79 percent) also said their information security budgets have been reduced or remained the same.

This financial picture is in contrast to the 2010 Deloitte GFSI Security Study, which notes, "During the worst economic downturn in recent memory, when so many budgets are being cut, information security budgets are safe for the most part and many have increased."

Research suggests that in lackluster economies, the security environment gets more dangerous. With this in mind, it may not be the right time to cut security funding, given current risks.

Information security as a percentage of IT budget
Current spending on information security has not kept up with the increased threats. Half of the survey respondents (50 percent) indicated that their information security budget is one to three percent of their overall IT budgets. States need to take a risk-based approach to determine the right percentage by agency/program, and continually monitor risks and make necessary adjustments.

The National Governors Association recognizes that states are prime threats for external and internal cyber threats. Their policy position statement on cybersecurity[4] states, "One of our critical infrastructure assets, our state networks, are attacked on a daily basis. The failure

Figure 14. What major barriers does your State (or agency) face in addressing information security?

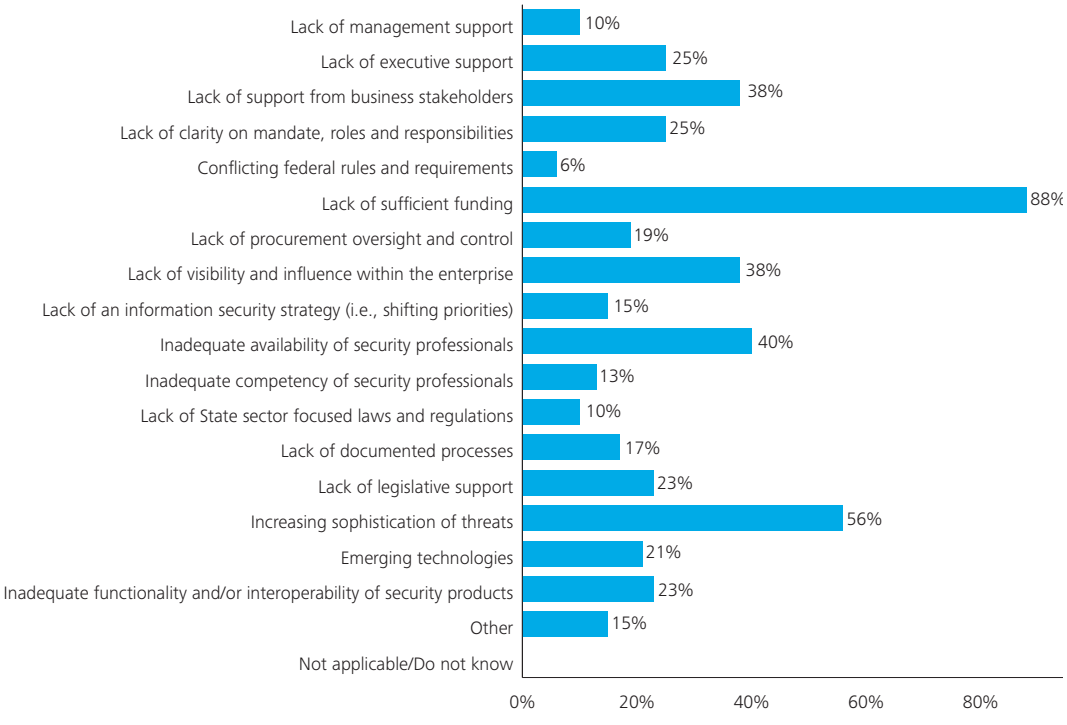
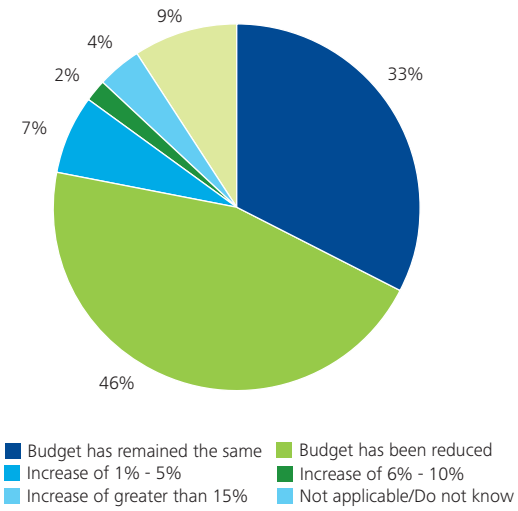
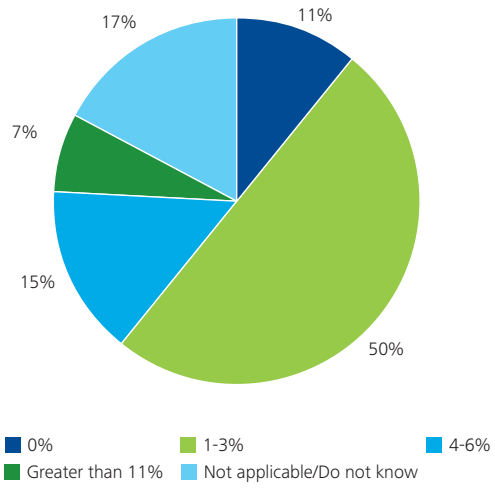


Figure 15. Characterize the year-over-year trending in your information security budget for years 2009 and 2010.



to secure these networks has serious implications for national security, including continuity of government, the operations of critical infrastructure and the health, safety, and general welfare of citizens. Cyber attacks have disrupted state government networks, systems and operations, and potentially could impact first-responder communications during an attack on our homeland."

Figure 16. What percentage of your department's overall IT budget is allocated to information security?



While states are pursuing strategies to gain efficiencies by promoting more online access and self-service, cutting information security budgets is a dangerous trend.

How CISOs are bridging the budget gap

Data from the 2010 Deloitte-NASCIO Cybersecurity Study indicates that, at least in the current economic climate, many states are looking for other means to secure information security funding. Organizations such as NASCIO and the Multi-State Information Sharing and Analysis Center (MS-ISAC) provide states with collaboration opportunities, information resources, and training opportunities to help bridge state funding gaps.

Help may be on the way. The federal government is increasing funding opportunities; one example is the Department of Homeland Security (DHS) grants available for state-level cybersecurity initiatives. Some states have leveraged DHS grants to do cybersecurity risk assessments, and to roll out training programs. CISOs must continue to look for innovative funding avenues by engaging state and federal leaders, legislators, and private-public stakeholders.

CISOs also must play a key role in budget requests and IT initiatives at the agency-level to see that adequate information security measures are accounted for. Eventually, this will help improve the percentage of IT budget allocated to information security.

Bottom Line

While security spending falls short of what is required to defend state citizens and public services infrastructure, the situation will not change overnight. Seeking out collaborative partnerships and additional funding is critical to mitigate security risks in the near term.

4. Internal and External Threats
States collect, store, use, and share enormous amounts of citizens PII. These "pots of gold" must be better protected

State agencies possess treasure-troves of medical, financial, and other personally identifiable information, not to mention sensitive business data and information relevant to national security – this information is under direct and focused attack.

A scan of public data loss notification websites indicates that more than one-fifth of reported data breaches in 2009 occurred in the state and local government sectors.

> "State governments' receipt of dollars from ARRA, HITECH, and other significant federal sources inextricably is tied to their ability to demonstrate strong information security controls. The role of state government in health information exchanges depends fundamentally on whether the public believes they can trust state government with their medical data."
>
> **Bob Campbell**
> **State Sector Leader**
> **Deloitte LLP**

Instances of medical identity theft and Medicaid fraud are also on the rise. The public impact from these scenarios is very real: More than 1.4 million people have been victimized by medical identity theft, according to an Experian-sponsored Ponemon Institute study published in February 2010[5]. The study estimates that victims pay about $20,000 each to resolve their cases. Nearly half of victims also lost health coverage due to the fraud, and nearly one-third said their health premiums rose after they were victimized. Fewer than 10 percent say their incidents were completely resolved.

The economic costs from reported breaches in the U.S. are well understood. The benchmark annual Ponemon study[6] estimated the average total per-incident cost in 2009 at $6.75 million.

Protecting PII

In the U.S., 46 of 50 states have enacted privacy laws guiding the definition and use of sensitive information. Nationwide trends point to more regulations in the future, including increased rules around the protection and use of health information as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act. New security and privacy laws will continue to impact the states significantly over the coming years. In response to complex global, federal and state regulations, private companies increasingly are hiring Chief Privacy Officers (CPOs) to help manage PII. The 2010 Deloitte GFSI study indicated that, in the U.S., 77 percent of the respondents had at least one or more executives responsible for privacy. In contrast, the 2010 Deloitte-NASCIO Cybersecurity Study found that only 18 percent of state respondents indicated having an enterprise level official responsible for privacy (such as a CPO) or equivalent. 24 percent of study respondents also indicated they have an enterprise privacy program in place.

Figure 17. Does your State have an official responsible for privacy (e.g., Chief Privacy Officer or equivalent)?

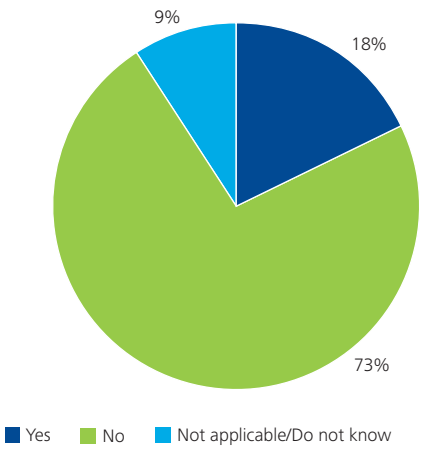
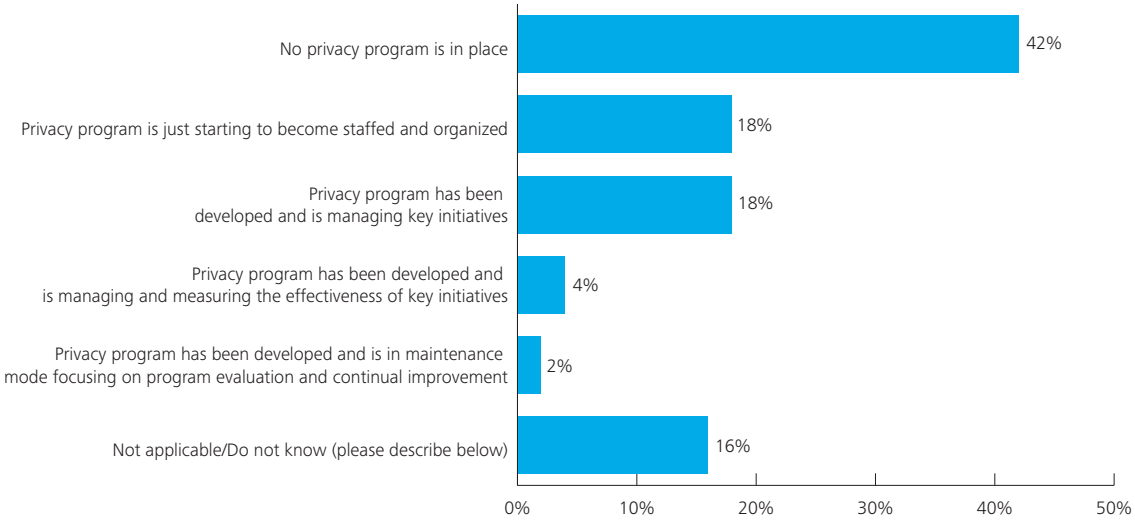


Figure 18. How would you describe the state of maturity of your organization's privacy program?



While we recongize that most states have privacy officers as part of their large agencies such as health and human services and education, the absence of a single point of enterprise accountability for privacy function is a risk.

Internal threats

Traditionally, states have focused on strengthening the perimeters of their networks to keep cyber criminals out. According to the 2010 Deloitte-NASCIO Cybersecurity Study, respondents expressed lower confidence in their ability to prevent internal threats when compared to external threats.

Respondents also reported that the majority (55 percent) of internal breaches over the past 12 months were a result of accidental breach of information, such as the accidental loss of an unencrypted laptop or hard drive. Many of these breaches can be traced to either the malicious or inadvertent behavior of employees. The findings underscore the importance of improving employee accountability with adequate checks and balances and cybersecurity awareness within state organizations.

Identity and Access Management (IAM)

Digital identity management is a significant business imperative for state agencies providing online access to information and services. The lack of an interoperable identity management framework across the state agencies and states has resulted in the use of disparate approaches for identity-proofing, credentialing and access to information. This has resulted in an inconsistent and costly implementation of digital identity management solutions. A number of initiatives, such as the NASCIO's State Digital Identity Working Group, are attempting to tackle this complex issue.

"The sources of threats to my state are widespread. On any given day, I deal with new viruses, zombie networks, phishing and pharming scams, foreign espionage, financial fraud, and serious vulnerabilities introduced from the latest social networking or technological gadget on the market. My day feels like an over-the-top suspense movie."

A State CISO

Figure 19. Level of confidence in protecting information assets from threats

Using a scale from 0-5 indicate your level of confidence that your organization's information assets are protected from threats	Not confident at all	Not very confident	Somewhat confident	Very confident	Extremely confident	Not applicable/ Do not know
Attacks originating internally	6%	19%	57%	11%	2%	4%
Attacks originating externally	4%	13%	45%	26%	9%	4%

Managing user access across diverse user populations that include business partners (third party), citizens, and employees has increasingly become a critical security concern and a source of significant costs. Respondents to the 2010 Deloitte-NASCIO Cybersecurity Study ranked security as the primary influencing factor (63 percent) in their IAM investments followed by operational efficiency, compliance and improved end-user experience.

External threats

Over the past decade, states have begun to meet citizen demand for online access to government services. While this strategy increases flexibility, in the age of cyber warfare it is also a source of significant risk. As states increasingly put services online and collect store, use, and share citizen data through public networks, the risk of exposing these assets to unlawful elements increases.

Survey respondents indicated that the primary cause (68 percent) for external breaches in the past 12 months was due to malicious software originating from outside the enterprise. Breaches from other sources, including website defacement (55 percent), hackers (45 percent), and stolen devices (36 percent) were not far behind.

Bottom Line

States are struggling to keep up with security threats from organized and sophisticated cybercrime rings. Preventing intentional and accidental breaches from insiders is high on the list of near-term priorities, as well. Solutions must involve not just technical tools, but also process improvement, fail-safe protection, and training and awareness programs.

Figure 20. In terms of the following internal breaches over the last 12 months, which of the following apply to your agency?

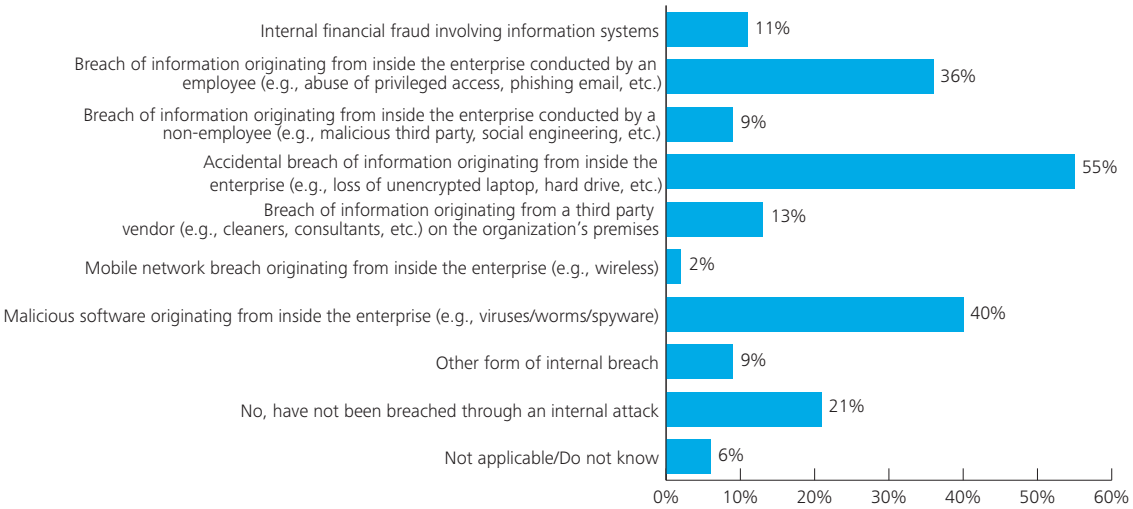


Figure 21. On a scale of 1 to 5 how important are the following reasons to your IAM investment decisions? (1 = (Least Important), 5 = (Most Important))

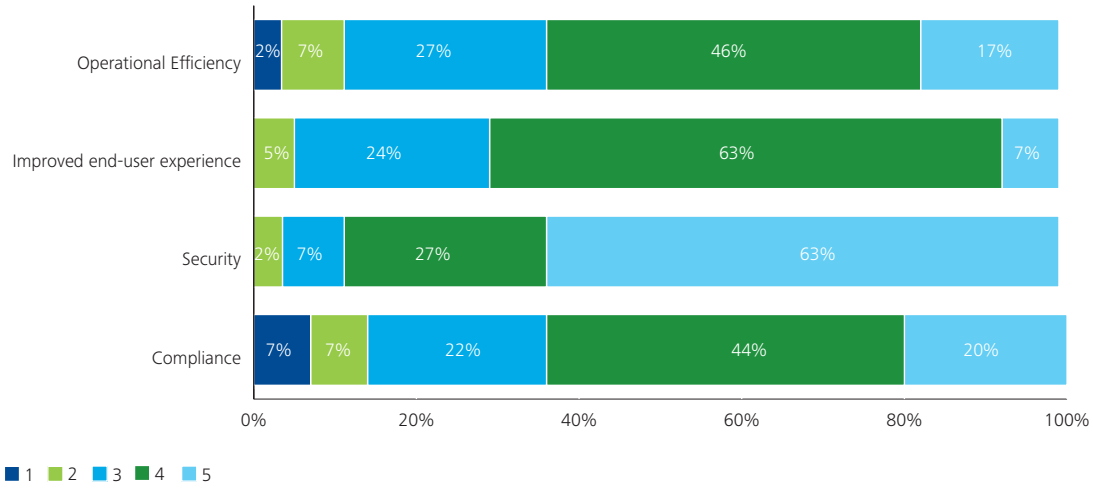
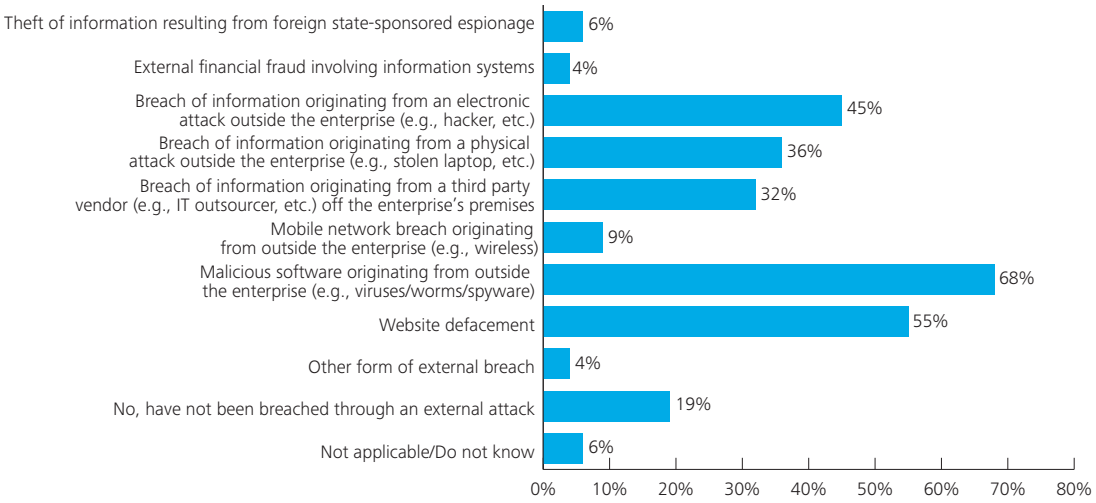


Figure 22. In terms of external breaches over the past 12 months, which of the following apply to your State (or agency)?



5. Security of Third-Party Providers
States must enforce better third-party security

State agencies rely heavily on the services and data-sharing capabilities of third-party service providers, contractors, business partners, and community organizations. Many of these third parties manage their own networks, receive delegated user management capabilities for state-run systems, and have access to sensitive information and equipment of state agencies. While third parties bring specialization, innovation, and flexibility to government, they can be the weak links in today's networked environment.

Data from the 2010 Deloitte-NASCIO Cybersecurity Study supported this claim. A full 20 percent of the respondents reported they were "not very confident" at all in the information security practices of their third parties, and 69 percent of the survey respondents indicated they were only "somewhat confident."

Figure 23. How confident are you in the information security practices of your third parties (contractors, service providers, business partners)?

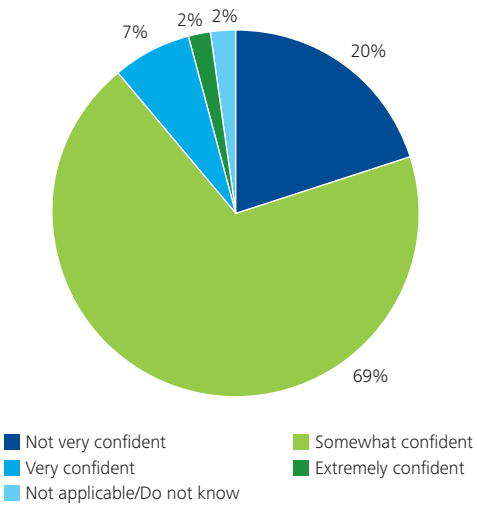


Figure 24 illustrates just how much CISOs know about third-party security capabilities and controls. Nearly one-fourth of respondents (23 percent) said they don't know their third-parties' security capabilities and controls at all.

When asked how they address the adequacy of third-party information security practices, respondents indicated their top three practices as follows:

1. Confidentiality and/or Non-Disclosure Agreements (77 percent)
2. State security policy and controls imposed on third-party (75 percent)
3. Address security issues in contract (68 percent)

While these are important controls to manage third-party relationships, they primarily transfer risk without effective ways to monitor for compliance. Often those third-party employees who are responsible for carrying out key aspects of security contracts are not familiar with associated security requirements or policies. A more proactive approach to managing risks would require states to have independent attestations, and necessitate that they regularly monitor and review third-party services with periodic and random audits.

Bottom Line

Reduced budgets, combined with the demand for rapid innovation, put increased pressure on states to outsource services and rely on third-party service providers to reach their goals. It is imperative that agencies put their third parties through an effective verification and compliance program in order to keep data safe.

Figure 24. Which statement best describes the level at which your agency handles third-party (contractors, service providers, business partners) security capabilities, controls and agency dependencies?

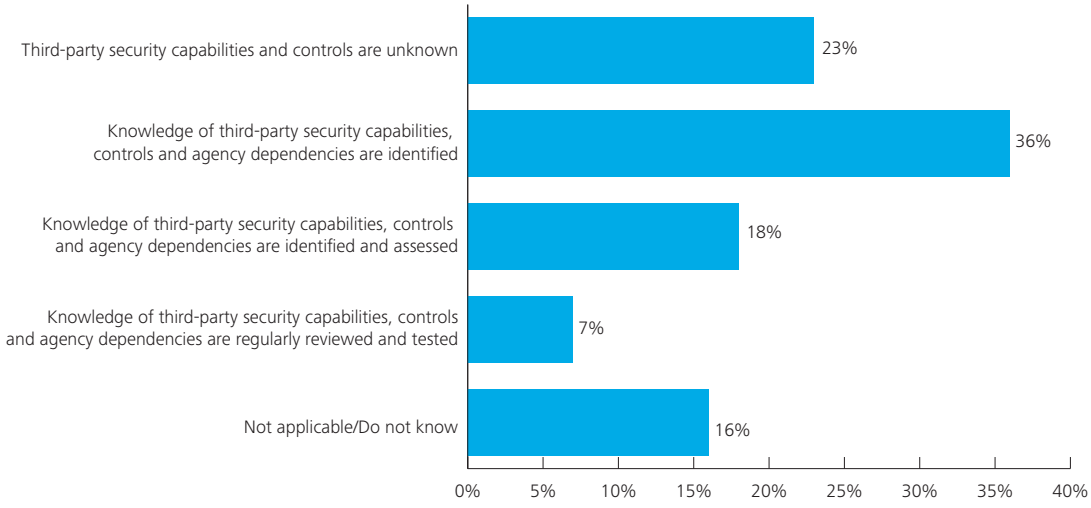
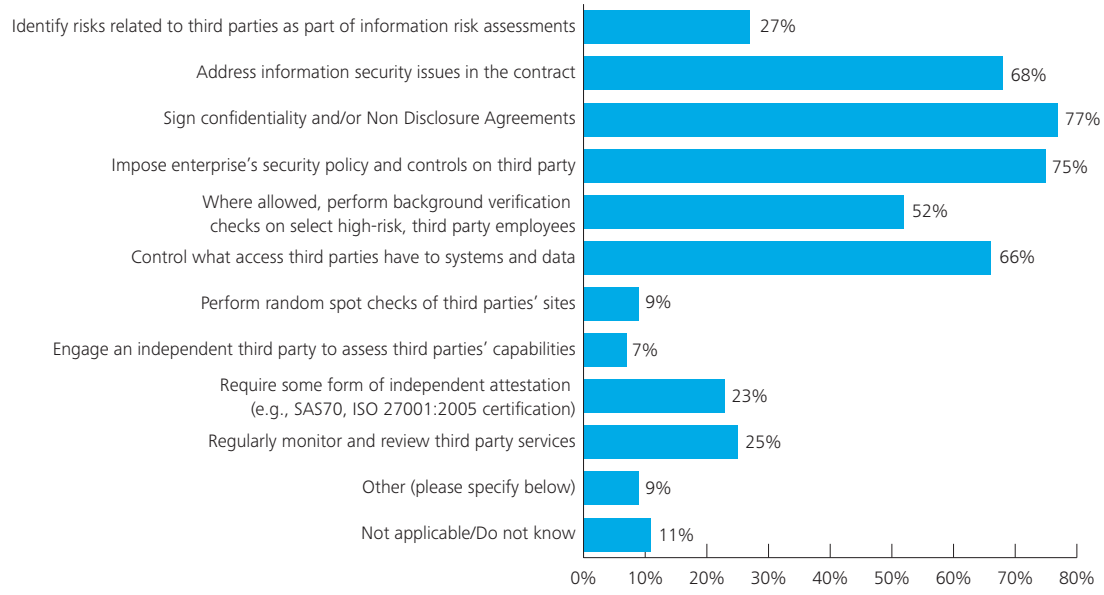


Figure 25. How do you address the adequacy of third party (contractors, service providers, business partners) information security practices?



Trends

In this section we provide general cybersecurity policy and technology findings from the 2010 Deloitte-NASCIO Cybersecurity Study.

Outsourcing

Outsourcing is a rising trend in state government. Respondents to the 2010 Deloitte-NASCIO Cybersecurity Study indicate a variety of security functions that they outsource, with 24 percent of respondents reporting threat and vulnerability monitoring services as the most common function they outsource. Still, not every state outsources – 18 percent of respondents indicated their states do not outsource security functions.

Security Initiatives for 2010

Survey respondents chose data protection (60 percent), risk assessments (58 percent), training and awareness (54 percent), application security (42 percent) and security measurement/reporting (42 percent) as their top five initiatives for 2010.

Figure 26. Does your agency outsource any of the following security functions?

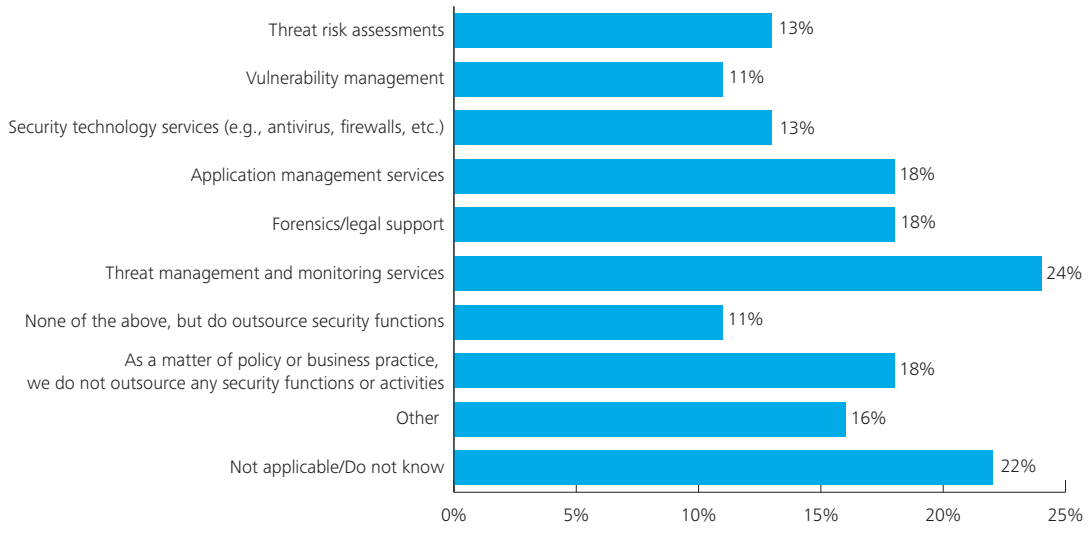


Figure 26-a. What are your State's top five (5) security initiatives for 2010?

We've seen an evolution in the private sector where security "detaches" from the infrastructure and "travels" with increasingly mobile data (via PDAs, memory sticks, and tools like those). Data loss prevention (DLP) strategies and technologies focus on securing data regardless of where it is, whether its misuse is for malicious purposes or an unintended lapse of judgment.

Ted DeZabala
Security and Privacy Leader
Deloitte & Touche LLP

Figure 27. How do you characterize the adoption of the following technologies (at either enterprise or agency level)?

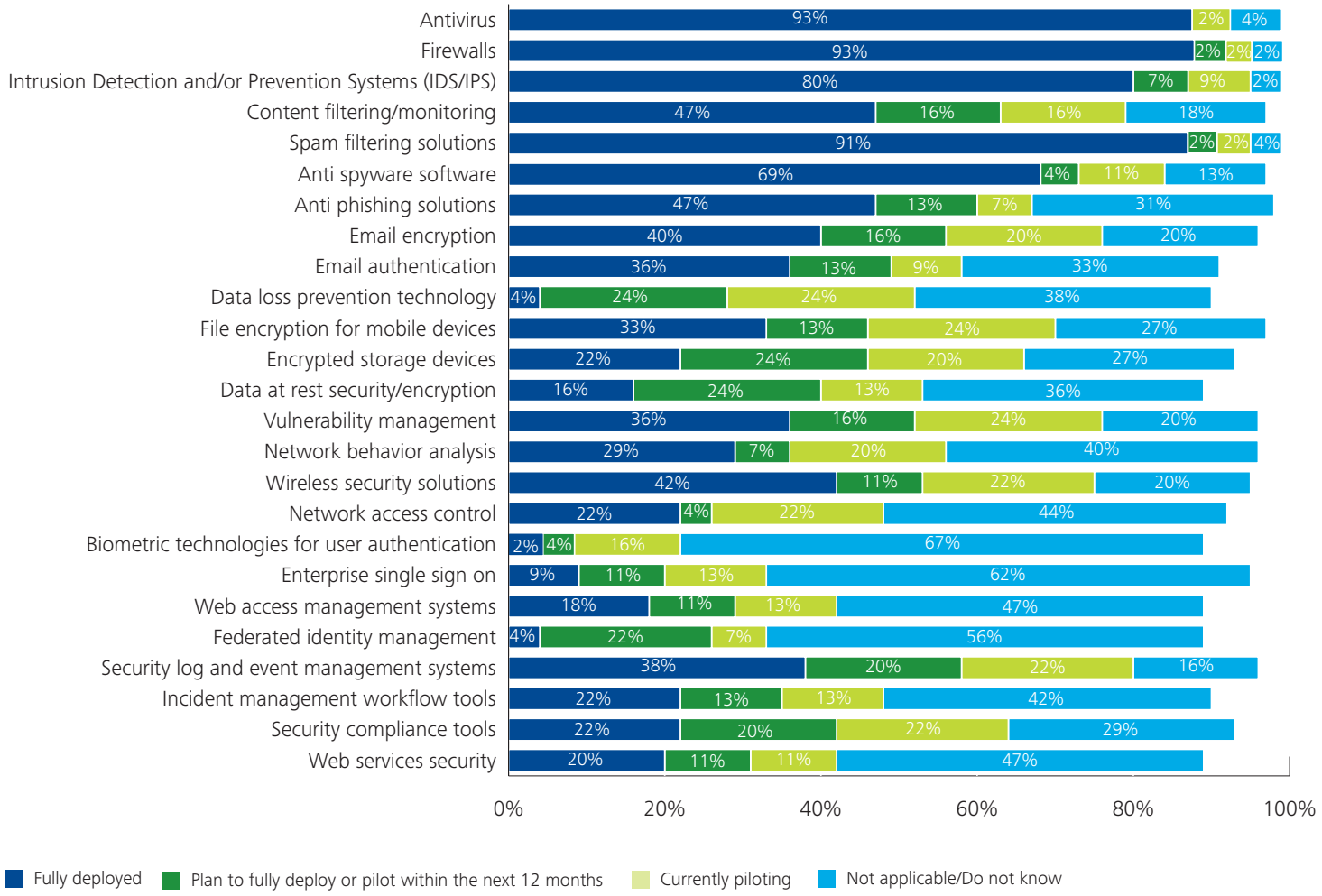


Figure 28. Security Testing: How often does your State conduct the following:

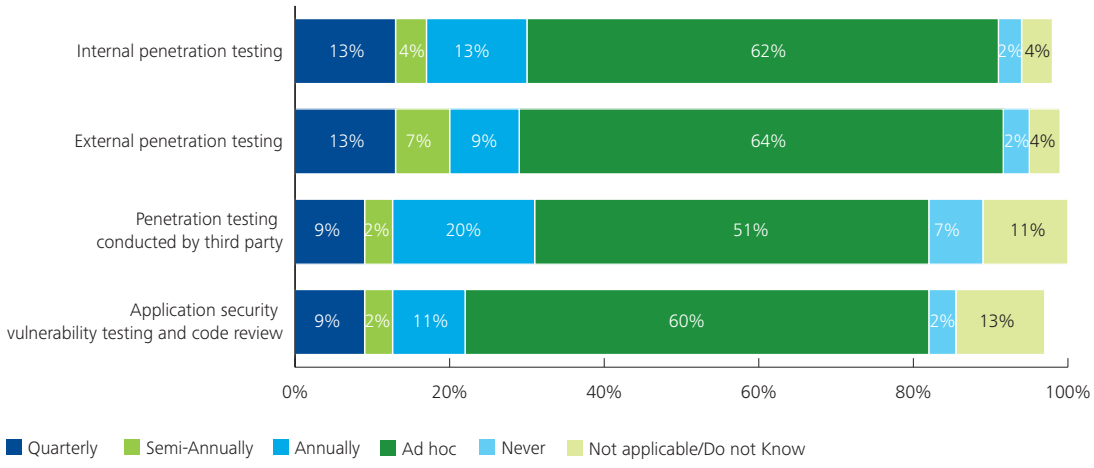
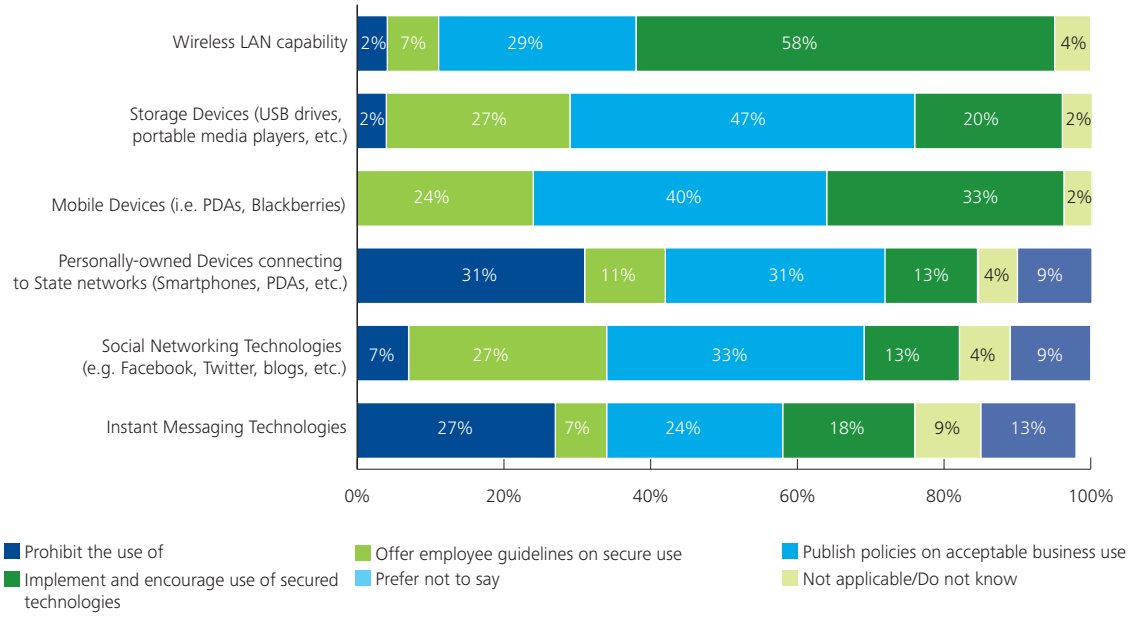


Figure 29. Does your State (or agency) have:



Security Technology Adoption

Study respondents reported a wide variety of technologies in deployment or planned for deployment within the next 12 months. While more than 80 percent of agencies have fully deployed antivirus, firewall, and Intrusion Detection and/or Prevention Systems (IDS/IPS), approximately one quarter (25 percent) of respondents indicated that they were expected to pilot mobile device file encryption, vulnerability management, and data loss prevention technologies as well.

Vulnerability Testing Frequency

The majority of respondents to the 2010 Deloitte-NASCIO Cybersecurity Study indicated that system penetration testing occurs on an ad-hoc basis only. This is not necessarily surprising; if states are aware of security weaknesses in their environment, a penetration test only confirms that fact. Still, it is important to note that penetration testing is a requirement for various security standards, including PCI-DSS and NIST. Many states have penetration testing as a requirement within their individual state security policies. It also has become a key component of many states' system development and acquisition processes.

Policies on the Use of Technologies

Data from the 2010 Deloitte-NASCIO Cybersecurity Study indicates that states take a mixed approach to offering guidelines and usage policies, or prohibiting use of certain technologies all together. For instance, 27 percent of responding states prohibit the use of instant messaging technologies. Seven percent of the responding states prohibit the use of social networking technologies. When it comes to these popular new technologies, CISOs must walk a fine line. Denying use may fail to meet citizen expectations, frustrate new employees or simply be ignored; encouraging use can help attract a technology-savvy talent pool to the states, spark local economies, and help innovate governments with new ways of delivering efficient, effective services to the public.

Action Items for States

The 2010 Deloitte-NASCIO Cybersecurity Study reveals some significant improvements from the 2006 report, but there is more that needs to be done. Responses to the more recent study showed that CISOs recognize the risks inherent in securing information. Data also indicates that CISOs recognize there are significant limitations to how they can address those risks effectively. Perhaps the most troubling trend was that, despite what is in many cases an enterprise-level title, CISOs do not have enough authority in state agencies to carry out their role properly.

Based on survey results, here is an initial checklist to help states take action to mitigate present day cybersecurity risks.

- ☑ Enlist executive and legislative leadership in establishing cybersecurity as a state priority. CISOs should seek out the support of leadership across all branches of government, as well as influencers and other private-public stakeholders to advance the discussions.
- ☑ Governors should follow the lead of the federal government and private industry when it comes to making information security a priority. The best way to show it is a top priority is to make it a top priority for the highest executive office of the state.
- ☑ Business and security must be better aligned from strategy through to execution. This makes it critical for the CISOs to fulfill their enterprise-wide risk management role. Regular reporting and metrics are key parts of achieving this alignment.
- ☑ Though there is no mandated, state compliance platform to drive consistent security programs, adopting an understood, comprehensive, and repeatable framework state-wide will enable improved alignment between state agencies and business, technology, and security leaders.
- ☑ State security spending falls short of industry benchmarks and CISOs face a tough battle in protecting state services from daily threats. Although there undoubtedly will be tradeoffs, states should re-evaluate their security spending annually based on risks as they change.
- ☑ Unintentional or malicious acts from inside an organization are just as potentially dangerous as external breaches. States need a holistic approach to deal with both types of threats.
- ☑ States need to monitor and assess security capabilities of third-party providers. Information security risks from these outside parties will only increase in the future.

Participant Profile

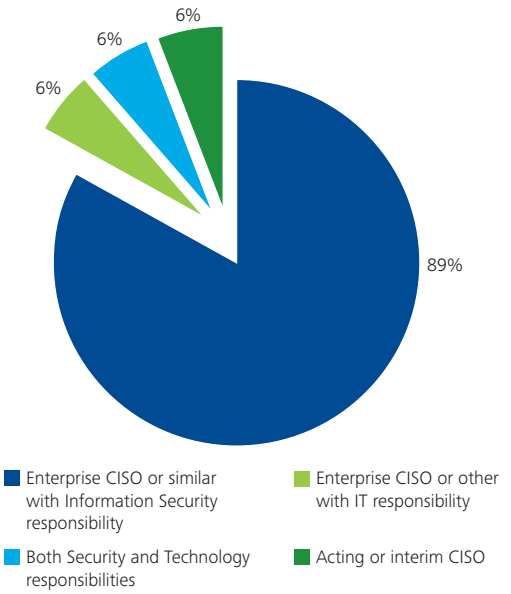
The 2010 Deloitte-NASCIO Cybersecurity Study was targeted at U.S. state enterprise- level CISOs, with additional input from agency CISOs and security staff members within state governments. Participants answered 57 questions designed to characterize the enterprise level strategy, governance, and operation of security programs. The topic clearly seemed to resonate, as representatives from **49 of the 50 states responded to the survey.**

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

Respondents' Positions in State Government

Most of the people who responded to the survey were State CISOs or individuals with similar titles within the enterprise information security infrastructure. Others identified themselves as acting or interim CISOs, or as "dual-title" positions that included both IT and security components. Six percent of respondents held the CIO title or a similar position indicating primarily IT responsibilities. The breakdown of respondents' positions is as follows:

Figure 30. Survey Respondents' Positions



Budget of Respondent Organizations

While the majority of the survey respondents indicated an annual state budget of less than $25 billion, one-third of the respondents indicated a 2009 budget of $10 to $25 billion. Figure 31 indicates the respondent breakdown.

Number of Employees in Respondent Organizations

- More than one-third of respondents indicated between 25,000 and 50,000 state employees. Figure 32 indicates the respondent breakdown.

Figure 31. Indicate the approximate annual budget of your State for the current budget year ($USD)?

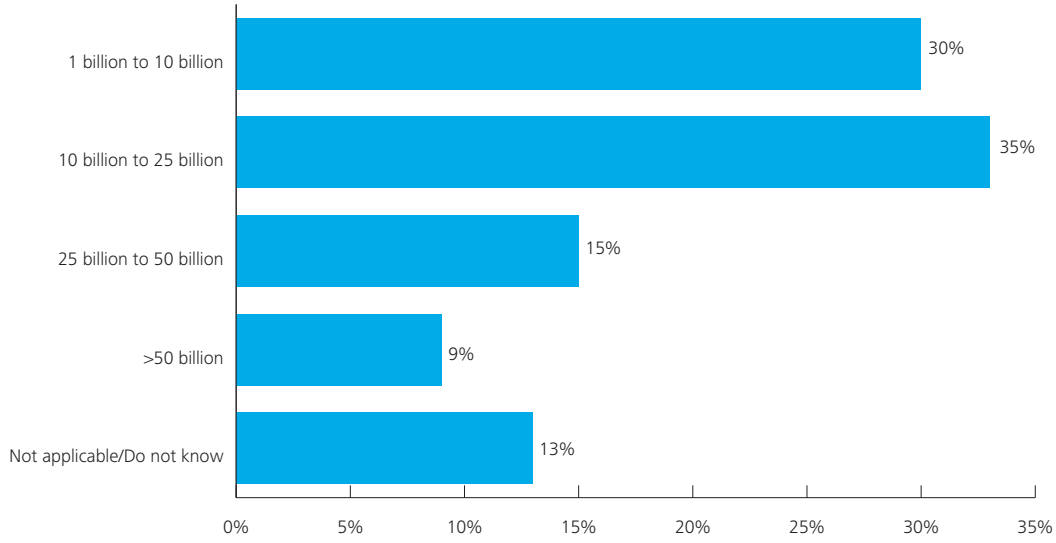
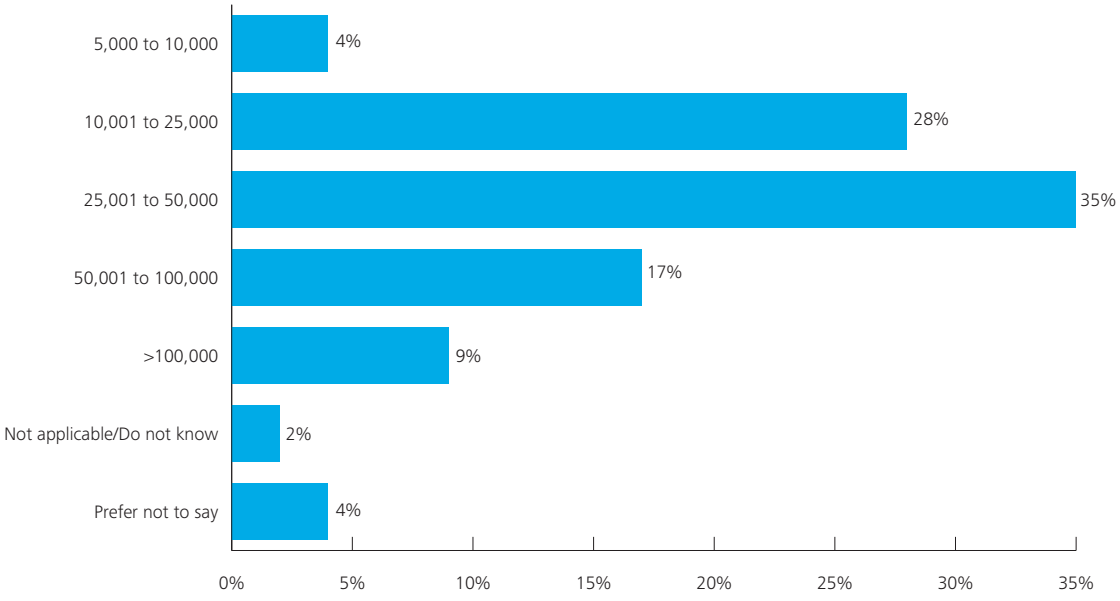


Figure 32. Number of employees in your State (excluding higher education employees)?



About the survey

How Deloitte and NASCIO designed, implemented and evaluated the survey

Deloitte and NASCIO collaborated to produce the 2010 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 State 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".

Additional insights

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 all questions and benchmarked responses was provided individually to the survey respondents.

Sources/Footnotes

1 The National Association of State Chief Information Officers

2 Deloitte Global Financial Services Industry (GFSI) Security Study, 2010, download at **http://www.deloitte.com/view/en_GX/global/industries/financial- services/article/2ac300d256409210VgnVCM100000ba42f00aRCRD.htm**

3 NASCIO Brief - Desperately Seeking Security Frameworks – A Roadmap for State CIOs, **http://www.nascio.org/publications/documents/NASCIO-SecurityFrameworks.pdf**

4 National Governors Association (NGA) Policy Position on Cybersecurity **http://www.nga.org/portal/site/nga/menuitem.8358ec82f5b198d18a278110501010a0/ ?vgnextoid=6ee0863754047210VgnVCM1000005e00100aRCRD**

5 **http://www.experian.com/assets/data-breach/white-papers/experian-medical-id-theft- healthcare.pdf**
http://news.cnet.com/8301-27080_3-10460902-245.html

6 Ponemon Survey report **http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_01220 9_sec.pdf**

Acknowledgements

We thank the NASCIO and Deloitte professionals who helped to develop the survey, execute, analyse 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
Ken Ontko, State of Oklahoma
Karen Sorady, CSCIC, State of New York
Elayne Starkey, State of Delaware
Mark Weatherford, Formerly with the State of California

Deloitte subject matter specialist contributors
Bob Campbell, Deloitte LLP
Alex Contreras, Deloitte & Touche LLP
Ted DeZabala, Deloitte & Touche LLP
Mark Ford, Deloitte & Touche LLP
Rene Hoffman, Deloitte & Touche LLP
Russell Jones, Deloitte & Touche LLP
Kristen Miller, Deloitte Consulting LLP
J.R. Regan, Deloitte & Touche LLP
Srini Subramanian, Deloitte & Touche LLP
Mike Wyatt, Deloitte & Touche LLP

Deloitte Survey team
Bharanedaran Balasubramanian, Deloitte & Touche LLP
Suna Taymaz, Deloitte & Touche LLP
Srini Subramanian, Deloitte & Touche LLP

Data collection & benchmarks
Andrei Kananovich, Deloitte Canada

Marketing
Justine Brown, Deloitte Services LP, State Government National Marketing
Karen Walsh Deloitte Services LP, State Government National Marketing
Pam Williams, Deloitte Services LP, National Marketing

About Deloitte & NASCIO

About Deloitte

"Deloitte" is the brand under which thousands of dedicated professionals in independent member firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, and tax services to selected clients. In the United States, Deloitte has 45,000 professionals with a single focus: serving our clients and helping them solve their toughest problems. Leveraging an industry focus, Deloitte's public sector practitioners have helped provide solutions to areas crucial to local, state, and federal government agencies for more than 45 years.

Deloitte delivers services, research, and solutions for government to help serve the 21st Century Citizen, including the information security, privacy, risk and vulnerability management, and identity management related topics.

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

Bob Campbell
State Sector Managing Principal
Deloitte LLP
1 512-226-4210
bcampbell@deloitte.com

Ted DeZabala
National Managing Principal
Security & Privacy
Deloitte & Touche LLP
1 212-436-2957
tdezabala@deloitte.com

Rene Hoffman
AERS State Sector Leader, Principal
Deloitte & Touche LLP
1 412-338-7302
rehoffman@deloitte.com

Srini Subramanian
Director
Security & Privacy
Deloitte & Touche LLP
1 717-651-6277
ssubramanian@deloitte.com

JR Reagan
Federal Solutions Lead, Principal
Deloitte & Touche LLP
1 571-882-5870
jreagan@deloitte.com