NASCIO Representing Chief Information Officers of the States

Research Brief

July 2006

NASCIO Staff Contact: Mary Gay Whitmer, mwhitmer@amrms.com or (859) 514-9209.

Born of Necessity: The CISO Evolution

Bringing the Technical and the Policy Together

As the recent exposure of approximately 26 million records of U.S. veterans has proven, what may seem like a simple and harmless act—taking a laptop computer home to work on a project—can quickly turn into a disaster, exposing millions to potential identity theft. Creating a negative image of government's ability to protect the citizens it serves, this incident demonstrated in a very public way that a federal agency's security policies and practices were not sufficient enough to stop an employee from taking home a laptop with sensitive information on it without the proper authorization. Statistics from current surveys reflect the fact that citizens' trust in the government's ability to keep their personal information private is relatively low.[1]

For state CIOs, a security breach like the one described above is one of many information security concerns. Such threats exist within states in the form of negligent or even malicious employees. States also face external threats ranging from hackers to spyware purveyors to malevolent individuals who seek to either cripple state IT systems or gain access to sensitive homeland security-related information. In order to properly identify (and even anticipate) these and other IT threats and then implement risk-based security protections to avert them, the state CIO typically has on staff a state Chief Information Security Officer (CISO) or position with a similar title who is responsible for ensuring the security of state IT systems and the information within them. The importance of a leader with respect to IT security was highlighted in recent GAO testimony regarding the recent exposure of veterans' personal information. That testimony specifically cited "strong leadership" as needed to improve IT security within the Veterans Administration.[2] ***This brief examines the role of the state CISO as it has evolved in response to the growing complexities of the IT threat environment, homeland security concerns, and growing demands for enhanced citizen services.***

While the brief covers the many facets of the evolving CISO role below, it seeks to highlight that the CISO is not merely a technical position involved in the operational aspects of IT security. Instead, the CISO is evolving as an IT security policy leader. A state CISO's responsibilities involve educating others, including those within the Governor's office, state agency leaders, legislators, and others outside of government to help ensure adequate funding for security. ***The ability of the CISO to form and maintain good relationships with state homeland security and emergency management***

[1] "Privacy Trust Survey of the United States Government," the Ponemon Institute and the CIO Institute at Carnegie Mellon University, January 31, 2004, <http://cioi.web.cmu.edu/research/2004PrivacyTrustSurveyoftheUnitedStatesGovernmentExecutiveSummaryV.6.pdf>.

[2] "Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs," Testimony before the Subcommittees on Disability Assistance and Memorial Affairs and on Economic Opportunity, Committee on Veterans Affairs, House of Representatives, GAO-06-897T, June 20, 2006, <http://www.gao.gov/highlights/d06897thigh.pdf>.

leaders, and even state auditors, is now a vital part of ensuring that the technology underlying even the most basic government function is secured to protect against risks that might reasonably occur.[3] Within this context, this brief takes a look at:

- The environmental drivers for the evolving role of the state CISO (Section I)
- Variations in the CISO title (Section II)
- The critical success factors for state CISOs (Section III)
- Governance and reporting structures (Section IV)
- The breadth and depth of CISO authority (Section V)
- The array of CISO responsibilities (Section VI)
- The growing importance of the CISO's relationships inside and outside of the state (Section VII)
- The CISO's involvement in information privacy issues (Section VIII)
- Typical CISO education, experience, certification and compensation (Section IX)
- What state CISO's really need to do their jobs (Section X)
- A few predictions about the future of the state CISO position (Section XI)
- What CIOs need to know and do about the state CISO position (Section XII).

I. It's a Jungle Out (and In) There: Concerns of the State CISO

The Concerns from Within:

One House, Many Doors and Windows: The nature of the state environment presents inherent security concerns. State governments are comprised of many employees that are spread across a myriad of agencies, boards, commissions and other governmental entities. This creates an environment in which there are many windows and doors through which risks can enter the state IT environment and potentially threaten the entire state network.

Everyone's a Techie: More technology savvy employees are introducing their personal technological devices into the state workplace. This opens up threats of downloading sensitive workplace data onto iPods (called "pod-slurping") or PDAs. Use of consumer-grade Instant Messaging (IM) services by employees at work also can introduce worms, viruses and other unwanted cyber-creatures into the state IT environment through bypassing the state's firewall protection.

Me? Violating State Policy? Unaware employees who do not realize the risks they present by violating state IT security policies, either knowingly or negligently, are a continuing concern. An example would be an employee who takes a laptop with sensitive information downloaded onto it home in violation of state policy, thereby presenting the risk of theft of the laptop and/or the sensitive information on it.

Outside Help: Many states use contractors from the private sector to provide targeted, specialized expertise at a reasonable cost. Contractors likely use and/or have access to state IT resources. They also may have access to sensitive information held by the state or may even work on IT-related

[3] The role of the university CISO is also evolving in a similar manner as the state CISO. According to a 2006 study by Educause, all of the fourteen surveyed universities have a lead administrator on information security and the vast majority of university CISOs report to a senior IT executive. "Effective Management of Information Security and Privacy," Alicia Anderson, Educause Quarterly, Number 1, 2006, <http://www.educause.edu/ir/library/pdf/eqm0614.pdf>.

projects. However, contractors introduce risks similar to those created by state employees regarding the potential for violation of state IT security policies and/or procedures.

The Legal Framework from Within: Each state has a variety of laws and regulations dealing with information security. The state CISO must understand those legal requirements and help ensure that the state's information security program is consistent with them.

The Concerns from Outside:

Ever-Mutating Threats: From viruses to worms to spyware to botnets, the IT threats continue to evolve and morph quickly in response to the implementation of security measures to avert them. Moreover, these creatures of the Internet underworld can target new technologies as they emerge. For example, viruses and worms are now targeting Instant Messaging communications. Some worry that these threats will also migrate to impact users of smart phones and other devices with merged voice and data capabilities.

More Services, Please: As citizens conduct more and more business online with vendors ranging from banks to Internet booksellers, citizens expect similar online avenues of services to be offered by the state. States now report hundreds of online services from filing taxes online to applying for hunting and fishing licenses. With each online application or enhancement to an existing application, there are security risks that must be addressed.

Who's a Citizen to Trust? With headlines in mainstream news outlets about both public and private sector data breaches, citizen trust may slowly erode and citizens may gradually turn away from enhanced online services offered by the state for fear that the state will not be able to protect their personal or financial information. Current statistics suggest that citizens are concerned with the government's ability to protect their personal information.[4]

The Legal Framework from Without: In addition to state legal requirements, CISOs must also understand the federal regulatory framework, including HIPAA (the Health Insurance Portability and Accountability Act). While some federal laws, such as Sarbanes-Oxley and FISMA (the Federal Information Security Management Act), may not apply directly to the states, CISOs must still understand their potential influence regarding information security.

Homeland Security Concerns: In the post-9/11 world, states' IT infrastructure may be at risk from terrorists and other malevolent individuals who want to cause harm to the U.S. Sensitive homeland security-related information held within state agencies must also be protected.

[4] "Privacy Trust Survey of the United States Government," the Ponemon Institute and the CIO Institute at Carnegie Mellon University, January 31, 2004, <http://cioi.web.cmu.edu/research/2004PrivacyTrustSurveyoftheUnitedStatesGovernmentExecutiveSummaryV.6.pdf>.

Threats Facing Any Given State on Any Given Day: Below is an example from the state of Michigan's website that describes the types of threats that the state must avert on a typical day:

- 2200 e-mail viruses
- 200 scans/probe attempts (internal/external users scanning the network for unauthorized access)
- 140 web defacement attempts
- 15 computer hi-jack attempts (remote control/trojans)
- Illegal/inappropriate activity
- Child pornography
- Copyright violations
- Pirated software, music, and movies
- SPAM (sent)--visiting inappropriate websites (gambling, pornography).[5]

In light of the current IT threat environment, states need the CISO or equivalent position to strategically address these threats by creating and executing policies on an enterprise level, and to provide guidance to the state CIO and state agencies.

The State of the State CISO: ***According to NASCIO's 2004-2005 Compendium of Digital Government in the States, 29 states reported having a Chief Security Officer or similar position.*** However, 2004 marked a slight decline in the number of states with this response from the previous year's survey.[6] A more recent survey conducted by NASCIO of state CISOs reflects that this number has remained relatively steady as of summer 2006. ***The aggregated results of this NASCIO survey will be released later in 2006.***

II. What's in a Title? Variations on a Throne

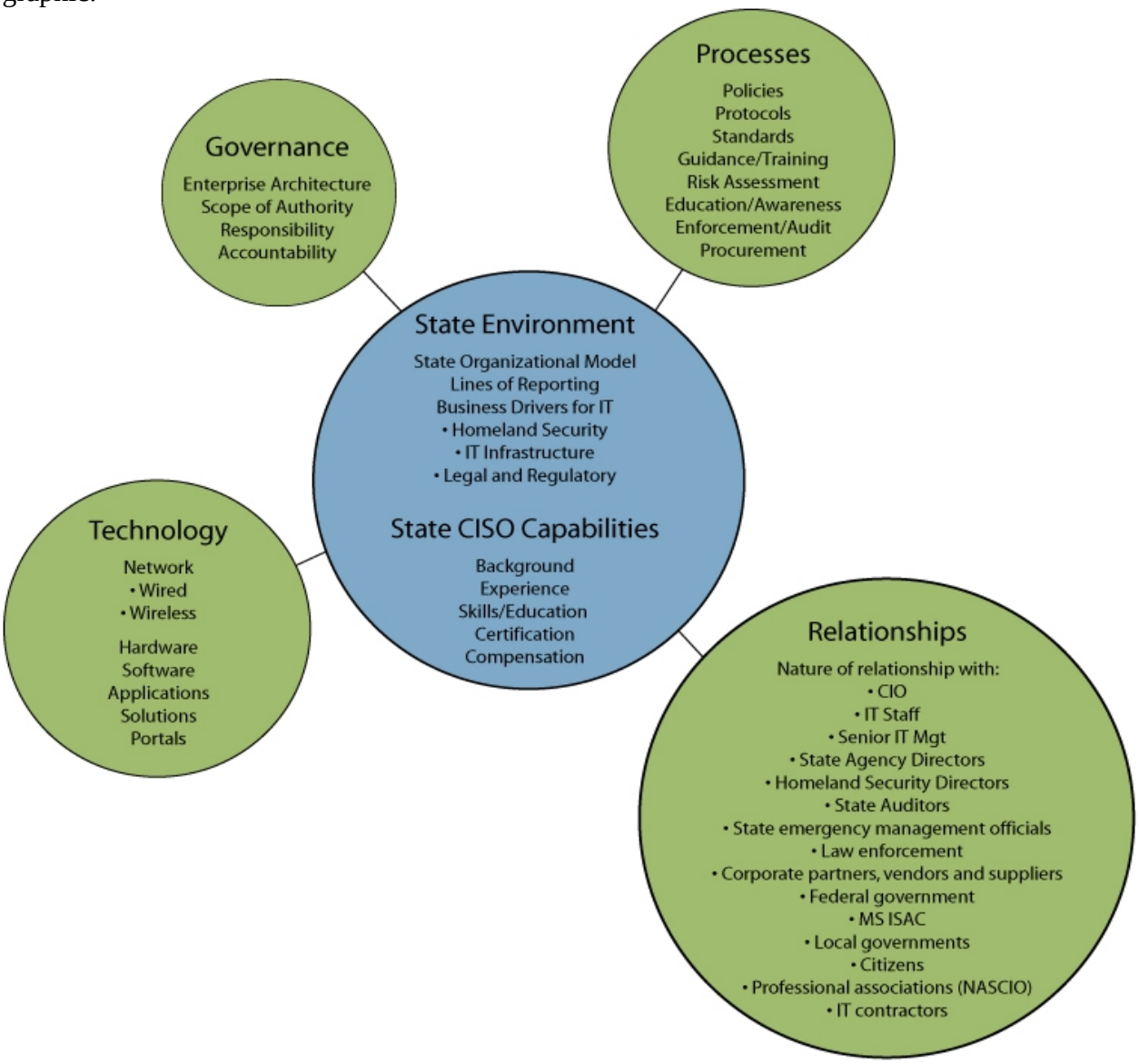
While authority and responsibility levels should be the focus of an enterprise IT security leader, the title may vary from state-to-state. Variations on the CISO title include Chief Security Officer (CSO), Manager/Director of Security, and even Chief Risk Officer (CRO). According to a 2005 survey of both public and private sector entities by CSO Research Reports, the predominant titles are the CISO, Manager of Security, and Director of Security. The title of CRO has diminished greatly.[7] Of note, many CISOs are the first to hold the title. For example, based upon the 2005 CSO Research Reports survey of public and private sector CSOs, 71% of the survey respondents were the first to hold their title, reflecting the fact that the CISO position is a relatively new one for many organizations.[8] Based on NASCIO's forthcoming publication of its aggregated CISO survey results, the most common state title is CISO. However, other common titles include CSO and variations of Director of Information Security or Information Security Officer. Unique titles include Homeland Security Technology Manager and Cyber Protection Officer.

[5] "Understanding Security at Work," State of Michigan IT Security Website, May 26, 2006, <http://www.michigan.gov/cybersecurity/0,1607,7-217-34395-108237--,00.html>.
[6] NASCIO 2004-2005 Compendium of Digital Government in the States, NASCIO, 2005, <http://www.nascio.org/publications/compendium.cfm>.
[7] "The State of the CSO—Part I," Julie Hanson, CSO Research Reports, June 1, 2005, <http://www.csoonline.com/csoresearch/report89.html>.
[8] Ibid.

Variations in title can reflect variations in responsibilities. For example, a person with a CSO title, as opposed to the CISO title, may be more likely to have physical security responsibilities. Typical responsibilities of the CISO are discussed in Section VI of this brief.

III. Critical Success Factors for the State CISO: A World of Complexity

: The graphic below is a visual representation of the state CISO's world and identifies some of the major factors that are critical to a CISO's success. As will be discussed in Section VII of this brief, the CISO's relationship with people inside and outside of government is a piece that is critical to a CISO's ability to secure IT. The ability of the state CISO to articulate the need for security, build trusting relationships and work with stakeholders to accomplish business needs while providing good security measures comes into play with the "relationships" aspect of this graphic.



IV. Governance/Reporting Structures for State CISOs

Current State Trend: ***The prevailing trend in states with a CISO or equivalent position is to have that position report to the state CIO.*** States such as Michigan, Kansas, Louisiana, Delaware, Arkansas, Texas, Virginia, and Iowa are following this model. One advantage of this model is that it helps to ensure that the CISO position is not buried within the state IT organization. By reporting to the state CIO, the state CISO can derive the needed authority to help to ensure that agencies understand the importance of IT security. This approach at the state level follows the overall trend in the private sector. According to a 2005 CSO Research Reports survey, the CISO increasingly reports to an organization's CIO or CTO. In 2005, the prevalence of this reporting structure increased to 38% of survey respondents, up from 29%.[9] According to a forthcoming NASCIO survey of state CISOs, the second most prevalent approach in the states is for the state CISO to report to an administrative agency or department head. Another approach, though less common, is for the state CISO to report to the Governor or an official within the Governor's office.

An Emerging Trend in the CISO Reporting Structure: Although the current trend is for a CISO to report to an organization's CIO, questions have been raised about whether this reporting structure creates an inherent conflict of interest by having those who manage an organization's IT also oversee the security of it. For a state's IT projects, does the fact that the state CIO has a responsibility to bring those projects in on-time and within budget compromise security if the state CISO reports to the CIO? For those with concerns about this potential conflict of interest, the proposed solution is to provide the state CISO with a degree of independence. Suggested ways of making the CISO more independent, particularly in the private sector, are to have the position report to the Chief Operating Officer (COO), the Chief Financial Officer (CFO), or even the CEO.

While the state trend indicates that many CISOs report to their CIO, both Colorado and California have created CISO positions that do not report to the state CIO. In Colorado, this position is located in the Governor's office and reports to the Governor's Chief of Staff. California has taken a different approach, locating the position in the state's Department of Finance and structuring the position to report to the department chief. Other potential methods of building-in CISO independence include the formulation of strong policies, requirements to report all breaches to the COO or equivalent, and a position in the IT department for an independent auditor.[10] Potential benefits of increased independence for the CISO position include an increased ability to have an enterprise-wide view, being able to advocate tough security measures, reporting to an authority within the organization that is higher than the CIO, and increased ability to create policies with an understanding of the criminal mind.[11]

While the reporting structure of the CISO position could evolve over time, the current state government trend of placement of the CISO position within the office of the state CIO may have germinated in part out of the fact that many state CIOs have responsibility in statute or Executive Order for securing the state's IT systems. Even if not specifically set out in statute, security is normally within a state CIO's purview. Hence, the CIO and CISO must work closely together in order to help ensure sufficient IT security. Moreover, security is based upon the implementation and

[9] Ibid.
[10] "Hand Over Security," Christopher Koch, CIO Magazine, April 15, 2004, <http://www.cio.com/archive/041504/homeland.html>.
[11] Ibid.

execution of solid practices and procedures. If there is a conflict between security and efficiency concerns, then the CIO should point this out and help determine the best balance between efficiency and security.

Importance of an Elevated CISO Position: Regardless of the model that a state chooses for a reporting structure, the CISO position must be elevated to a level that will allow the CISO to properly carry out his or her duties to help to ensure enterprise IT security, including developing solid relationships with state agencies and being able to provide guidance at the highest levels of state government. A heightened CISO position will also demonstrate through its placement within government that IT security is a priority.

V. Breadth and Depth of CISO Authority

The Breadth of CISO Authority: The possible breadth of CISO authority ranges from only certain specified state agencies to all three branches of government. According to *NASCIO's Compendium of Digital Government in the States*, generally, those states that reported having a CISO or the equivalent have an enterprise-wide CISO who develops and promulgates security policies and procedures for a federated organization.[12] A recent NASCIO survey of CISOs indicates that it may be more common for a state CISO to have authority with respect to the executive branch of government, while CISOs with "statewide" authority extending into the legislative and/or judicial branches of government are somewhat less common. However, Colorado and Delaware have CISOs with responsibility for security of shared state services within all three branches of government, with some exceptions. Depending upon the state, the CISO also may or may not have authority with respect to elected officials, such as an elected state auditor, or independent boards and commissions. Authority over educational institutions, such as K-12 and higher education, varies according to state as well. Louisiana and Arkansas have CISOs with authority that encompasses higher education. Finally, Delaware is an example of a state in which the CISO has authority with respect to all three branches of government plus K-12.

While it is more common for the CISO to have authority primarily over executive branch agencies, some states may have an organized council or forum to coordinate among the various state IT officials within the other branches of state government. For example, Kansas' CISO chairs its statewide Security Council that is comprised of security officials throughout the state. The Security Council recommends policies to the state's IT Executive Council that has members from all branches of government and local and law enforcement representatives. Moreover, even for state CISOs with authority primarily over the executive branch, there may exist some implicit authority over governmental or educational entities that are on the state network. This implicit authority may be derived if the CISO has the ability to curtail any entity's use of the state network if it compromises other agencies that are on the network.

The Depth of CISO Authority: The prevailing model in the states appears to be federated in nature with agencies having an Information Security Officer (ISO) that reports to the agency head. For smaller agencies that may not be large enough to support an ISO position, the state CISO usually requires a point of contact that can be reached day or night. The agency ISOs or points of contact

[12] NASCIO 2004-2005 Compendium of Digital Government in the States, NASCIO, 2005, <http://www.nascio.org/publications/compendium.cfm>.

appear to have somewhat of a "dotted-line" authority back to the state CISO. However, some states, including Kansas and Arkansas, take a more collaborative approach in which the agencies recognize the authority of the CISO although it may not be formalized in statute. To bring state agency ISOs and other IT security officials together, states including Texas and Arkansas have executive branch security work groups to coordinate the sharing of best practices and to improve the consistency of IT security. Delaware's CISO is embarking on an effort to provide agency ISOs with tools and other assistance to heighten their levels of responsibility and accountability.

VI. The Array of CISO Responsibilities

The CISO as an Enterprise Strategist: As the CISO position has evolved in both the private and public sectors, its focus has shifted from a concentration on perimeter defense to strategy, policy, and business process enablement. The enactment of business process regulations such as HIPAA (the Health Insurance Portability and Accountability Act) and Sarbanes-Oxley, have increased the focus on business processes and how security can help both enable those processes while protecting an organization's IT infrastructure and information assets.[13] This shift is supported by the findings of a 2005 CSO Research Reports survey in which 58% of survey respondents (combined from both the private and public sectors) said that they play a strategic role within their respective organizations.[14]

This overall trend toward the CISO as a strategist is reflected in state government with a shift in focus of the CISO from purely operational duties, such as perimeter defense, to enterprise policy and a strategic direction for security for the entire state enterprise. According to a forthcoming NASCIO survey, the vast majority of state CISOs has policy responsibilities—some have a mix of policy and operational duties, while others have primarily policy duties. Many state CISOs develop IT security policies and procedures for the state enterprise. Those policies and procedures are then implemented by agencies, sometimes with the assistance of a state's IT operations department. While a CISO likely develops enterprise security policies, there are variations across the states regarding the enforcement of those policies. While the state trend may lean toward providing the state CISO with enforcement responsibility with respect to IT security policies, such as in Michigan, Delaware, and Colorado, some states handle IT security policy enforcement through the state auditor's office, possibly in coordination with the state CISO and/or CIO, or an auditing division housed within the state legislature. Regardless of where the enforcement authority is housed within the state, the CISO plays an important role in understanding when agencies are in compliance with those policies. The state CISO also likely has a role in granting waivers to agencies that request exemptions from an enterprise IT security policy.

An Overview of State CIO IT Security-Related Offerings: For state CIOs that have security duties within their purview and may have a CISO as a staff member, *NASCIO's Compendium of Digital Government in the States* provides insight into the rising importance of a CIO's IT security-related duties regarding the state enterprise. The Compendium reflects that significant majorities of the nation's CIOs have already begun offering a variety of security-related services to the enterprise. The most common offering is alerting of cyber-threats. Every category saw 5%-10% increases in the number of states responding affirmatively over 2003.

---

[13] "Q & A: What Makes a Good Chief Information Security Officer?" Matthew Schwartz, CSO Magazine, December 26, 2005, <http://www.esj.com/Security/article.aspx?EditorialsID=1569>.

[14] "The State of the CSO—Part II," Julie Hanson, CSO Research Reports, June 29, 2005 <http://www.csoonline.com/csoresearch/report90.html>.

- Cyber-alerting: 45 states
- Audit/assessment of systems: 39 states
- Collection or analysis of incidents or violations: 41 states
- Coordination with national defense/security agencies: 39 states
- Response to and remedies for cyber-threats and violations: 40 states
- Training: 35 states.[15]

CISO Duties and Responsibilities: Though CISO duties across the states vary, a CISO may be tasked with the following types of duties:

- Enterprise IT security program and policy development
- Draft and edit cybersecurity regulations and legislative initiatives
- Management of specific operational areas (monitoring and perimeter defense of the state network)
- Development of the business case for continuing investment in IT security (including assisting agencies with their IT security business cases)
- Review of agency IT projects for compliance with security policies
- Agency risk and/or vulnerability assessments or audits (may be mandatory or voluntary) and involvement in SAS 70 Type II audits
- Agency security training and awareness, including IT security newsletters and websites and security exercises
- Risk and incident management and response
- Patch management
- IT forensics and investigations
- Crisis communications and management for IT incidences.

A Note on Physical Security and the Role of the CISO: Physical security measures can come into play when a state must secure its data center and other IT systems and infrastructure. Within the private sector, the title of CSO may reflect responsibility for not only information security but also for physical security measures as well. In the states, CISO responsibility for physical security measures varies with some state CISOs having responsibility for physical security where it relates to securing a state's IT assets. However, other state CISOs must coordinate with their state facilities management officials or others in law enforcement with that responsibility.

VII. The Increasing Importance of the CISO's Relationships Inside and Outside of the State

As the state CISO's role has evolved in importance, so has the importance of the CISO's role in coordinating with many internal and external IT security stakeholders. The CISO must not only be knowledgeable regarding information security, but must also be able to effectively communicate with those who are unfamiliar with IT security and build trusting relationships with them. Within a state, the CISO may coordinate with other agencies to leverage internal business processes with the ultimate goal of enhancing IT security. These agencies may include procurement, budget/finance, human resources, and the auditor's office. The state CISO also may play a key role in cybersecurity

[15] NASCIO 2004-2005 Compendium of Digital Government in the States, NASCIO, 2005, <http://www.nascio.org/publications/compendium.cfm>.

and a state's efforts regarding homeland security, critical infrastructure protection, and emergency management. Many critical homeland security and public safety functions rely on information and communications systems that must work properly in times of crisis. Given the importance of these systems in protecting state citizens from harm resulting from attacks or acts of nature, the state CISO's role in this area is likely to increase in prominence.

The variety of stakeholders with whom a state CISO may coordinate includes those from within as well as outside of state government. The list below provides an overview of the many stakeholders with which a state CISO may need to coordinate in order to further state IT security measures.

Internal Stakeholders:

- Coordinating council or body of agency information security officers
- State agencies (incidence and violation reporting, consultation, etc.)
- Consultation with and/or testimony before state legislature
- Enterprise architecture working groups (including security architecture)
- State portal activities
- State privacy officials
- State homeland security
- State critical infrastructure protection
- Emergency management
- Disaster recovery and business continuity
- Facilities management
- State institutions of higher education

External Stakeholders:

- Federal government agencies, including:
  - Homeland Security
  - US-CERT
  - FBI
  - NIST
- Local governments, including law enforcement agencies
- Alerting entities
- MS-ISAC
- Other sector ISACs
- Private sector partners
- Professional and trade associations, including NASCIO
- Citizens, including security awareness efforts and Internet fraud avoidance

A Note on the MS-ISAC:
One organization with which state CISOs participate is the Multi-State Information Sharing and Analysis Center (MS-ISAC), the only ISAC that specifically represents state governments. The mission of the MS-ISAC, consistent with the objectives of the National Strategy to Secure Cyberspace, is to provide a common mechanism for raising the level of cyber security readiness and response in each state and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the states and providing two-way sharing of information between and among the states and with local government. It is a voluntary and collaborative organization with participation from all 50 states and the District of Columbia. For more information about the MS-ISAC, please see: www.msisac.org.

VIII. The CISO's Involvement in Information Privacy Issues

To understand the state CISO's responsibility with respect to privacy issues, one must understand the relationship between the security and privacy disciplines. Privacy policies address how information and data are collected, used, accessed and retained. Security policies and procedures provide mechanisms for ensuring that the information is protected from unauthorized access or alteration/deletion. Privacy cannot be ensured without effective security policies and measures.

Information Privacy in the State Enterprise: As of 2004, 18 states reported to NASCIO that they have a CPO or similar position for the enterprise. These positions generally develop and promulgate privacy policies and procedures for a federated state enterprise. [16] West Virginia stands as an example of a state that has an enterprise Chief Privacy Officer. In addition, California has an Office of Privacy Protection, which is located within the state's Department of Consumer Affairs. Much less common methods of handling privacy are privacy oversight commissions or special legislative committees—three states reported having an oversight commission and three indicated a special legislative committee. Twenty-one other states reported an "other" mechanism for addressing privacy. Most of these states indicated that this mechanism involved consensus-building in the development of privacy policies for the federated enterprise.

As data breaches and health information efforts grow in importance, mechanisms for addressing information privacy issues appear to be springing-up in a somewhat organic fashion at the agency-level. HIPAA-covered entities must have a privacy officer, while many state Attorney General Offices deal with privacy from a consumer protection perspective. With the privacy field's emphasis on examining existing privacy laws and the need for privacy policies or laws that address contemporary issues, such as identity theft, attorneys may hold these positions, as opposed to technologists.

The Role of the CISO in Privacy: Since many states are still in the process of understanding how best to address information privacy issues, the role of the CISO regarding privacy varies according to the state. Some state CISOs, such as Delaware's, have responsibility for handling privacy strategy and issues on a statewide basis. Delaware's approval process for standards and policies gives other departments and branches of government the opportunity to comment before the standards/policies are finalized Other state CISOs may handle privacy issues, though on a less formal basis or may liaison with agency-level privacy officers on an as-needed basis at the intersection of security and privacy. As both positions evolve in light of increased data breaches and citizen awareness of the potential for identity theft, the relationship between the two positions will evolve.

[16] NASCIO 2004-2005 Compendium of Digital Government in the States, NASCIO, 2005, <http://www.nascio.org/publications/compendium.cfm>.

IX. Typical CISO Education, Experience, Certification and Compensation

The background for a CISO, whether public or private sector, requires less of a technical background and more of a business, audit, law enforcement, business or security background. According to a CSO Research Reports survey, there has been an increase in military, local law enforcement and corporate security officials as CSOs.[17] The 2005 version of this survey reflected a 2% decrease in CSOs with an information security background. However, there were increases in CSOs with audit, business operations and law enforcement backgrounds.[18] Hence, a CISO may be knowledgeable about IT and security, but may also have either law enforcement or business operations experience.

Education: Increasingly, public and private sector CSOs have degrees. A 2005 CSO study found that 57% of survey respondents have degrees—a 5% increase from the previous year. [19] While this number may be on the rise, holding a degree does not appear to be the determinative factor in the hiring of CISOs. Background, the right mix of skills and possibly a security certification appear to be the more important factors. For those CISOs who hold degrees, there does not appear to be any one degree that is preferred over all others. While technical degrees, such as computer science, information systems, math and even engineering, may be more prevalent, other business-related degrees could be growing in importance. For example, an MBA or a degree in decision information sciences may be appropriate for a CISO.

Certifications: The past several years have seen increases in CISOs obtaining security certifications. Popular certifications include the CISSP and CISA certifications. In 2005, a CSO survey found that 34% of respondents held a CISSP certification.[20]

At the state level, there is an increasing interest in security certifications. Some certifications are specific to a particular vendor, such as Cisco or Microsoft, while others are not. More common certifications that CISOs may pursue include:

- **CISSP** (Certified Information Systems Security Professional): Offered by (ISC)2
- **CISA** (Certified Information Security Auditor): Offered by Information Systems Audit and Control Association (ISACA)
- **CISM** (Certified Information Security Manager): Offered by ISACA
- **GIAC** (Global Information Assurance Certification): Offered by SANS Institute along with other security and IT-related certifications.

As in other sectors, the CISSP and CISM are common certifications for public sector CISOs. While not a requirement to be a state CISO, these and other certifications can provide a broad base of knowledge upon which a CISO can overlay practical information security experience.

[17] "The State of the CSO 2004," Lorraine Cosgrove Ware, CSO Research Reports, June 1, 2004, <http://www.csoonline.com/csoresearch/report72.html>.
[18] "The State of the CSO—Part I," Julie Hanson, CSO Research Reports, June 1, 2005, <http://www.csoonline.com/csoresearch/report89.html>.
[19] Ibid.
[20] Ibid.

Important CISO Qualities: The CISO position requires a unique balance of technical knowledge of IT and security along with the ability to communicate effectively and build strong relationships across the state enterprise. State CISOs must be able to understand the technical, while translating that into "English" for those with non-technical backgrounds. This skill is particularly important in educating state agencies about IT security and in persuading state leaders that IT security must be adequately funded on an ongoing basis. Below are some of the important skills and characteristics that NASCIO has identified.

Technical Skills:

- Well-rounded IT background
- Experience in network, database, and application security and access controls
- An appreciation for how fast IT advances
- Ability to keep pace with quickly changing threats and increasingly inventive hackers
- Ability to analyze both security and business needs

"Business"-Related Skills:

- Good communications and decision-making skills
- Being a "bridge-builder" with agencies to gain their trust and educate them
- Ability to influence a team of people who don't necessarily report to you
- Understanding the legal framework of both state and federal laws, such as HIPAA and Sarbanes-Oxley, that impact state IT resources
- Understanding the importance of collaboration with others across the state enterprise and with private sector partners and professional associations (NASCIO, etc.)
- Ability to negotiate, know when to compromise, and when to stand your ground

Important CISO Characteristics:

- Emphasizing the positive to stakeholders
- Being proactive in the face of emerging IT threats
- Having a vision for state IT security
- Viewing the CISO position as not just a job, but as a vocation you love!

A Note on CISO Compensation and Retention: As is more broadly the case with state government positions, private sector salaries for CISOs are likely higher than those in the government sector. For example, the 2005 version of CSO's survey of both public and private sector CSOs found that 27% reported salaries between $124,999 and $199,999, which was a 4% increase from the previous year. An additional 23% reported salaries between $75,000 and $99,999.[21] The generally higher salaries of the private sector have created a drain on state IT security personnel. A state may invest time, training and resources into its IT security staff members, only to find that the private sector can offer them better compensation. Potential ways of countering this effect include increasing the pay scale for state IT security to be commensurate to the private sector or marketing other benefits, such as better quality of life and retirement benefits, as an enticement for state IT security positions.

[21] Ibid.

X. What State CISOs Really Need to do Their Jobs

In conjunction with preparing this brief, NASCIO conducted a survey of state CISOs and other IT security personnel. One question contained in the survey asked the state CISOs to choose the top three items/resources they need to do their jobs. Among the top selections were:

- Adequate staffing/personnel
- Support of the State CIO (or equivalent)
- Support of state agencies
- Adequate funding
- Support of the Governor or other senior state management leaders.

Other selections that were cited by the survey respondents, included:

- Support of the state legislature
- Adequate authority
- Enforcement ability
- Incorporation of security into state enterprise architecture
- An effective IT governance structure.

XI. Perspectives on the Future of the State CISO Position

Emerging Drivers of the CISO Position: As the state government workforce becomes more mobile and acclimated to wireless laptops, PDAs and other converged devices, state CISOs will have to deal with the difficulties of securing those devices and the sensitive information on them while preserving the conveniences that those devices bring to state workers. A continuing driver behind the evolving role of the CISO will be the rapidly changing IT threat environment. Predictions include increased concern with securing systems against terrorists, increasingly organized hackers, negligent or malicious insiders, and attacks aimed at the application level or to exploit existing vulnerabilities. Recent federal legislation, such as REAL ID and proposed legislation on data breach notification and information security, could also shape the responsibilities of state CISOs. A few final drivers are likely to be states' exploration of Service Oriented Architecture (SOA) and the increased need for IT systems that are designed to be collaborative in nature and bring together diverse groups of stakeholders with differing business needs.

A Few Predictions: Much like gazing into a crystal ball, there is a sense of how the CISO position may evolve, but changing circumstances will act as drivers in how the position continues to take shape in state government. However, we can make a few generalized predictions. They are as follows:

- **State IT Governance:** While sufficient funding for IT security positions is likely to remain a challenge for states, more states are likely to have a CISO position or its equivalent. With improved methods of measuring effectiveness and value, the state CISO will be better able to demonstrate the importance of the position. As the importance of security, especially regarding the handling of personal information increases, the authority of the state CISO will increase. States also will consolidate IT security to help ensure that all agencies—from large to small—are secured in ways that are cost-effective and reliable. This fact will also serve to increase state CISO authority. Other trends within states are likely to have a similar effect, including Enterprise Resource Planning (ERP) efforts, enterprise identity and access management initiatives, information assurance and data classification activities, and Service Oriented Architecture (SOA).

As part of this evolution, the position could move out from under the state CIO in some states and/or be combined with physical security.

- **Security as a Business Enabler:** In the face of continuing cyber-related threats and data breaches, state CISOs will support their case for adequate IT security measures by demonstrating ways in which IT security can be a business enabler, instead of just another requirement.
- **State CISOs as Collaborators:** As the authority and purview of the state CISO increases, so will the need to collaborate within the broad reaches of state government and beyond to other states and even internationally. Efforts such as sharing IT threat information and the development of cooperative agreements for disaster recovery hot sites could be drivers for this.

XII. What CIOs Need to Know and Do About the State CISO Position

- **The Role of the CIO Regarding Security:** While part of an executive team that may include the CISO, the CIO is ultimately accountable for information security.
- **The Emerging Role of the CISO as Security Strategist and Business Enabler:** As IT security has increased in importance, so have the policy and strategy-related duties of the state CISO. The position has evolved from operations to more of a policy and security-strategy position. The state CISO may also seek to build support from others within the state by demonstrating how IT security can actually enable improved business processes and services.
- **An Elevated Position:** CISOs need visibility and the support of senior management--do not bury the position! While the trend appears to be for the CISO to report to the state CIO or equivalent, state CIOs should be aware that there is an emerging theory supporting the placement of the CISO under an official other than the CIO to avoid potential conflicts of interest. If a state is deciding where to place the position of CISO, this could be a proposed option. The CIO should understand the supporting arguments behind that option and ways that potential conflicts of interest can be mitigated if the CISO reports to the CIO.
- **Depth and Breadth of CISO Authority:** State CISOs normally have authority at least with respect to the executive branch of government, if not for the entire state government enterprise, including other branches of government. Regarding state agencies, many states take a "federated" approach, with state agencies having an information security officer or an IT security point of contact that may report to the agency head.
- **Relationships Matter:** As a result of the increasingly prevalent role of the CISO as a strategist for state IT security, it has become important for CISOs to develop strong relationships with many stakeholders inside and outside of state government. In particular, state CISOs are likely to become more involved in state homeland security, critical infrastructure and emergency management efforts as they relate to state IT systems and cybersecurity. In addition, the state CISO may also need to leverage relationships with other state agencies and processes, including procurement, budget and human resources.
- **What's Privacy Got to do With It?** States are still determining where best to address the information privacy function regarding personal or sensitive information within state IT systems. Some state CISOs may handle privacy-related issues, while others may not. As the privacy function emerges and takes shape within the states, so will the CISO's relationship with state privacy officers or the equivalent.
- **The Compensation Challenge:** Compensation for CISOs can be a challenge. One option is to pay them as close to commensurate with the private sector as possible. Other options include an emphasis to potential job applicants on quality of life and good retirement packages.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

- **CISO Skills:** As opposed to a purely technical position, state CISOs now have a balance of technical, policy and "business" related skills. Important skills are communications, building relationships and understanding security and security management.
- **It's Worth Looking Into:** Because of the level of integrity and responsibility required for state CISOs and other state IT security personnel, states should conduct background and credit checks on candidates for those positions.

A Word about Background and Credit Checks: The responsibilities of state CISOs and other state IT security personnel require a high level of integrity. Background and credit checks conducted prior to the hiring of a state CISO or other IT security official can help to ensure that the position is occupied by an individual who will not breach his or her duty to the citizens to protect state information systems and uphold the highest levels of professional ethics. Background checks can reveal prior incidences that may serve as indicators of a job applicant's ethics, integrity and professionalism. Credit checks can be useful in revealing a job applicant's financial problems, which could create a situation that is ripe for fraud, embezzlement or other financially-motivated misconduct or criminal activity.

- **Too Many Chiefs?** For states that are attempting to create a CISO position or ensure the continued existence of the position, the state CIO should be prepared for the possibility of encountering concerns from government leaders that there are "too many chiefs." The argument stems from the fact that there may be many state positions that are "chiefs," such as the "Chief" Information Officer, the "Chief" Financial Officer, the "Chief" Technology Officer, the "Chief" Enterprise Architect, etc. In such cases, it may be of assistance to point out that it's the function and authority of the CISO, not the title, that is important in securing state IT resources.
- **Accountability:** Collecting and analyzing state data is an important way to measure CISO success and outcomes.
- **Training & Continuing Education:** It is important for state CIOs to have the resources for ongoing, specialized training for state CISOs and IT security staff members.
- **Sharing Best Practices:** As the CISO position continues to evolve and becomes solidified, the opportunity to share best practices will likely increase. State CISOs may consider opportunities to share best practices on an intrastate, interstate and even international basis as well as with private sector partners.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

Appendix A: Learning More--Additional Resources

NASCIO:
"The IT Security Business Case: Sustainable Funding to Manage the Risks," NASCIO, May 2006, http://www.nascio.org/nascioCommittees/securityPrivacy/public/NASCIO%20IT%20Security%20Business%20Case%20Brief.pdf.

NASCIO Security and Privacy Committee Webpage:
http://www.nascio.org/nascioCommittees/securityPrivacy/members/.

Other Publications and Resources:
"Effective Management of Information Security and Privacy," Alicia Anderson, Educause Quarterly, November 1, 2006, http://www.educause.edu/ir/library/pdf/EQM0614.pdf.

"The National Strategy to Secure Cyberspace," A White House Report, February 2003, http://www.whitehouse.gov/pcipb/.

United States Computer Emergency Readiness Team (US CERT):
http://www.us-cert.gov/.

National Institute of Standards and Technology (NIST), Computer Security Division:
http://csrc.nist.gov/.

The Federal Information Security Management Act (FISMA):
http://csrc.nist.gov/policies/FISMA-final.pdf.

Sarbanes Oxley Act:
http://www.sec.gov/spotlight/sarbanes-oxley.htm.

Infragard:
http://www.infragard.net/.

Multi-State ISAC:
www.msisac.org.

IT ISAC:
https://www.it-isac.org/#.

International Systems Security Association (ISSA):
http://www.issa.org/.

Global Security Working Group:
http://it.ojp.gov/topic.jsp?topic_id=58.

Internet Education Foundation:
http://getnetwise.org/.

National Cyber Security Partnership:
http://www.cyberpartnership.org/.

SANS Technology Institute:
http://www.sans.edu/.

CSO Magazine:
http://www.csoonline.com/.

Select State Security Websites:

Arizona:
http://gita.state.az.us/security/.

Arizona Security Architecture:
http://gita.state.az.us/enterprise%5Farchitecture/NEW/Security%5FArch/.

Arkansas:
http://www.itsecurity.state.ar.us/.

California:
http://www.dof.ca.gov/OTROS/SecurityProgram/SecurityProgram.asp.

Colorado:
http://www.colorado.gov/cybersecurity/index.html.

Delaware:
http://dti.delaware.gov/cybersecurity.

Florida:
http://www.secureflorida.org/.

Georgia:
http://gta.georgia.gov/00/channel_modifieddate/0,2096,1070969_7295376,00.html.

Kansas:
http://www.da.ks.gov/itec/ITSec/default.htm (IT Security Council).

Kentucky:
http://cot.ky.gov/security/.

Louisiana:
http://www.doa.state.la.us/oit/securityoffice/index.htm#.

Maryland:
http://dbm.maryland.gov/portal.

Michigan:
http://www.michigan.gov/dit/0,1607,7-139-30639_30656---,00.html.

Nevada:
http://infosec.nv.gov/.

North Carolina:
http://www.iso.scio.nc.gov/.

Texas:
http://www.dir.state.tx.us/security/index.htm.

South Carolina:
http://www.secure.sc.gov/site/default.asp.

Virginia:
http://www.vita.virginia.gov/security/security.cfm.

West Virginia:
http://www.state.wv.us/got/security.cfm.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org