NASCIO
Representing Chief Information Officers of the States

Moving Forward: Leadership Toolkit for State CISOs

NASCIO staff contact:

Meredith Ward
Senior Policy Analyst
201 East Main Street, Suite 1405, Lexington, KY 40507 USA

Phone 859.514.9153 | FAX 859.514.9166 | mward@NASCIO.org | www.NASCIO.org

TABLE OF CONTENTS

NASCIO
Representing Chief Information Officers of the States

About the National Association of State Chief Information Officers

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs. For more information, visit www.NASCIO.org.

Executive Summary

In 2006, the National Association of State Chief Information Officers (NASCIO) surveyed state chief information security officers (CISOs) and released a report titled, A Current View of the State CISO: A National Survey Assessment. The report called for a heightened role of state CISOs as cybersecurity continues to be an important issue to states and state chief information officers (CIOs). Fast forward nearly 10 years and cybersecurity is not only "an" important issue but "the" issue of most importance to state CIOs.

Each year NASCIO conducts a survey of the state CIOs to identify and prioritize the top policy and technology issues facing state government. The CIOs top ten priorities are identified and used as input for NASCIO's programs, conference sessions and publications. In recent history, CIOs have consistently ranked cybersecurity as the top concern for state CIOs:

> **Security:** risk assessment, governance, budget and resource requirements, security frameworks, data protection, training and awareness, insider threats, third party security practices as outsourcing increases, determining what constitutes "due care" or "reasonable" (www.NASCIO.org/topten)

Because of this ranking and the numerous cyber attacks on state enterprise systems, it is imperative that states have the right policies and the right people in place to combat and prevent these attacks. In the 2014 Deloitte-NASCIO Cybersecurity Study, we asked CISOs about those concerns and we found that insufficient funding, sophisticated threats and shortage of skilled talent threaten security and put state governments at risk:

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

Because of these challenges and the growing number of threats, state CISO roles and responsibilities have changed in just the past two years—the position is maturing. That's why NASCIO, via the Security and Privacy Committee, is releasing this first ever toolkit for state CISOs. In the summer of 2015, we asked state CISOs about critical leadership traits, how state CISOs and private sector CISOs differ and also gauged the tenure of state CISOs.

Survey Participants

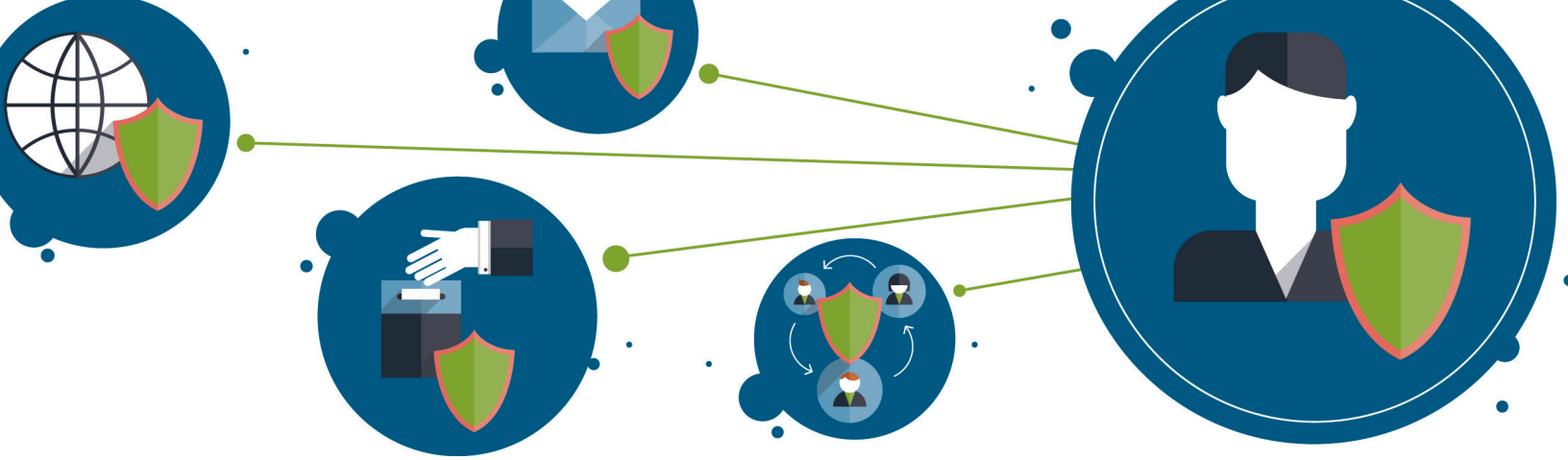
In the 2006 NASCIO CISO survey, 83% of responding states had a CISO or the equivalent of that position. In 2015, 100% of states have a CISO or equivalent position. Forty-four states completed the 2015 survey. Three states did not have the CISO position filled at the time of the survey, so a representative from the state CIO's office provided a response.

1. Alabama
2. Alaska
3. Arizona
4. Arkansas
5. California
6. Colorado
7. Connecticut
8. Delaware
9. Florida
10. Georgia
11. Illinois*
12. Indiana
13. Iowa
14. Kansas
15. Kentucky
16. Louisiana
17. Maine
18. Maryland
19. Massachusetts
20. Michigan
21. Minnesota
22. Mississippi
23. Missouri
24. Montana
25. Nebraska
26. Nevada*
27. New Hampshire
28. New Jersey
29. New Mexico
30. North Carolina
31. North Dakota
32. Ohio
33. Oklahoma
34. Oregon
35. Pennsylvania
36. Rhode Island
37. South Carolina
38. South Dakota
39. Tennessee
40. Texas
41. Utah
42. Vermont*
43. Virginia
44. Washington
45. West Virginia
46. Wisconsin
47. Wyoming

*No CISO at time of survey

We also wanted to gauge state CISO tenure and found the average tenure in 2015 is 39 months, compared to 25 months for state CIOs.

This toolkit will examine the survey responses, give "advice from the trenches" and detail other critical success factors for state CISOs.



State CISO Leadership Traits

In the 2006 NASCIO CISO survey, the evolving role of the state CISO is described in this manner:

> The state 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. The 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 leaders, and even state auditors, is now a vital part of ensuring that the technology underlying the most basic government function is secured to protect against risks that might reasonably occur.

It is safe to say that this description is still fairly accurate and with this evolving role has come a brighter spotlight on the CISO position.

While this is a positive thing, state CIOs must now be surer than ever that the right person is in the CISO position. And, for state CIOs, finding the right cybersecurity talent has been a challenge. In the 2014 Deloitte-NASCIO Cybersecurity Study, this was one of the major obstacles for state cybersecurity maturity:

> The skill sets needed for effective cybersecurity protection and monitoring are in heavy demand across all sectors. Private sector opportunities and salaries are traditionally better than those offered by government. Not surprisingly, state CISOs are struggling to recruit and retain people with the right skills, and they will need to establish career growth paths and find creative ways to build their cybersecurity teams.

Understanding these challenges, the first thing we asked of respondents was to rank the most important leadership traits or attributes for state CISOs. The top five responses were: strategist, communicator, relationship manager, educator and facilitator. Strategist and communicator were only separated by one vote, so we will consider them the two most important responses.

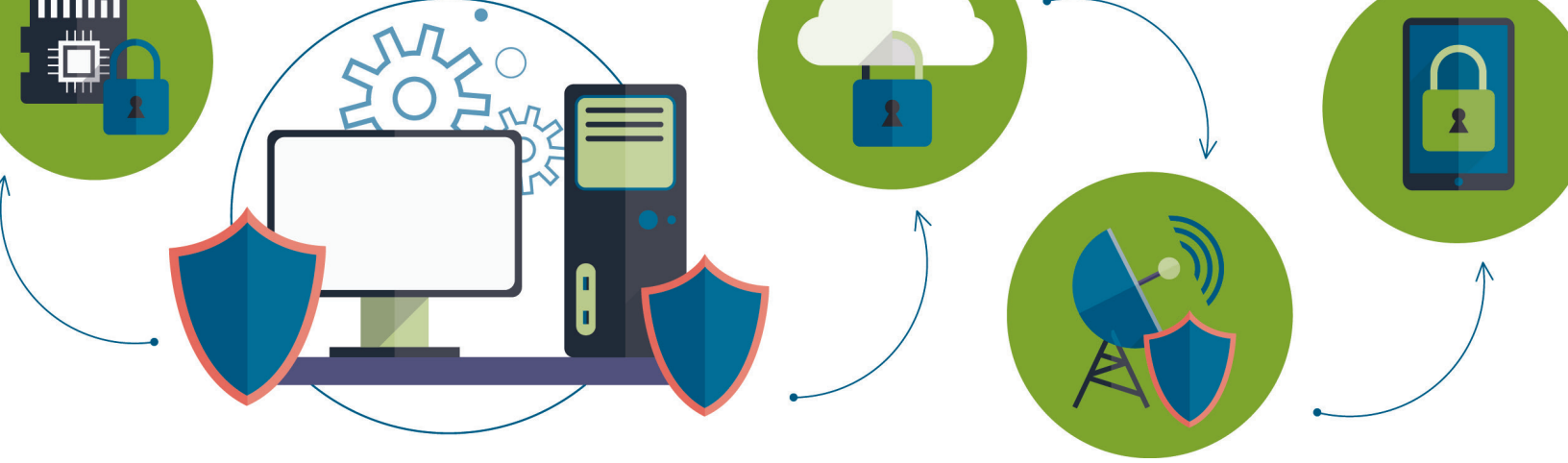
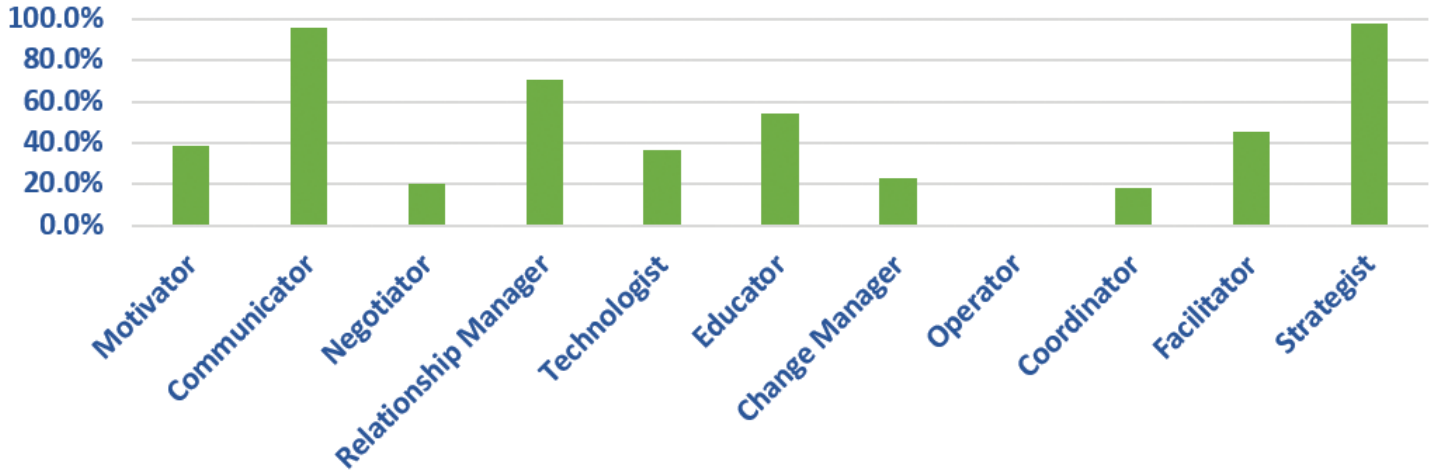


Figure 1

In your experience, what are the most important leadership traits or attributes to the critical success of a State CISO? Please choose your top 5.



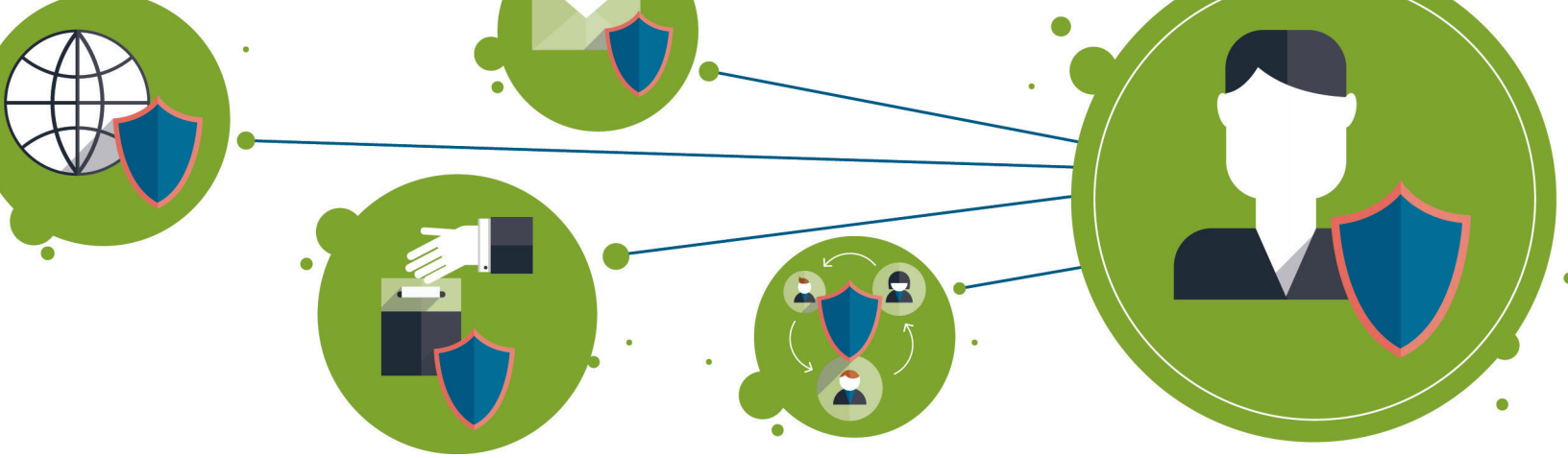
Being a successful CISO not only requires certain attributes, but also the ability to build successful relationships. Next we asked CISOs to rate the importance of each relationship that contributes to the success of the state CISO. Not surprisingly, the relationship with the state CIO was overwhelmingly ranked the most important. Additionally, when we asked CISOs to choose just one relationship instead of ranking a series of relationships, state CIO remained the top answer with 91% of votes.

Considering that all state CISOs report to the state CIO, this is not surprising.

Figure 2

Please rank the importance of each relationship that contributes to the success of the state CISO. Rank the following from least important to most important.

Relationship	Rank
State CIO	1
Agency CISOs	2
Agency CIOs	3
Governor/Chief of Staff/Policy Advisors	4
Executive Agency Heads	5
Homeland Security Advisor (HSA)	6
Budget Director	7
Agency Customers	8
Legislature/Legislators and their staff	9
State Privacy Officer	10
State Police/Law Enforcement	11
Adjunct General/National Guard	12

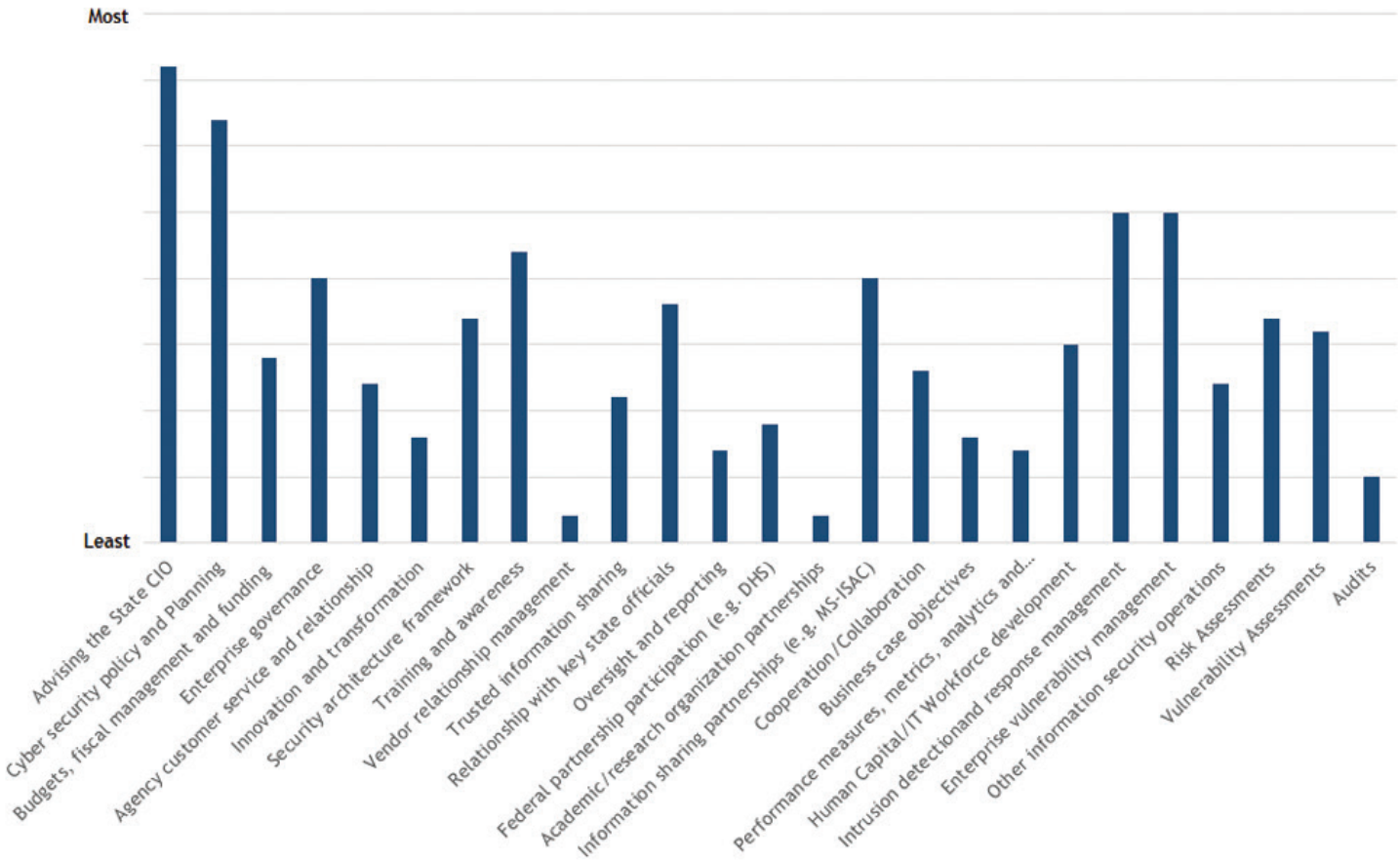


Governor/chief of staff/policy advisors, state budget director and state auditor were next in line of importance when CISOs were asked to rank.

Key attributes and relationships are the foundation for a successful state CISO, but what are the critical actions a state CISO must take? We asked CISOs to rank the most critical factors/dimensions they focus on to advance their agenda and drive results.

Figure 3

Considering your authority and responsibilities as state CISO, what are the most critical factors/dimensions you focus on to advance your agenda and drive results? Rank the following from least important to most important.



The top five most frequent answers were advising the state CIO; cybersecurity policy and planning; intrusion detection and response management; enterprise vulnerability management; and enterprise governance. When asked to choose the *most* important factor, advising the state CIO overwhelmingly came out on top. The importance of a strong relationship between the state CIO and state CISO cannot be overstated. The state CISO will need executive support and "air cover" from the state CIO when things go bad.

Advice from the Trenches

In the 2006 CISO survey, NASCIO asked state CISOs how they spend their time and found that, as to be expected, time was spent on addressing technical issues but a majority of time was spent on strategy, policy & planning activities such as:

- Policy and Strategy
- Maintaining Ongoing IT Security Investment
- Building Relationships
- Enterprise Planning and Strategy Activities
- IT Security Business Case

Likewise in this 2015 study, in addition to the multiple choice and ranking questions, we also asked CISOs a series of open ended questions and the answers revealed that state CISOs still think strategy and policy & planning activities are important.

Policy and Strategy
In the 2006 CISO study, policy and strategy roles for the state CISO are described this way:

> 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.

One of the main goals of the 2015 survey was to answer what makes a public sector or state CISO different than a private sector CISO. The 2014 Deloitte-NASCIO Cybersecurity Study and the 2015 NASCIO Workforce Survey established the difficulty that states have in recruiting qualified cyber security talent. And so, we wanted to know the good, bad and ugly.

Many CISOs expressed that the main difference is the wide range of customers/agencies/ sectors a state CISO supports:

"The breadth of business units is greater in the public sector. Agencies represent a very diverse population with different security needs."
-Rod Davenport, Michigan Interim Chief Security Officer

"The challenge with working within, and complying with, the various regulations of multiple vertical industries (e.g. health care, financial, criminal justice, federal tax, etc.), in lieu of serving as a CISO just for one industry and having the luxury of solely focusing on, and gaining a thorough understanding of, only the specific rules that govern one single organization."

-Art Bakke, North Dakota Enterprise Information Security Administrator/ Security Architect

CISOs are also responsible for protecting a wide range of data and applications—from birth and death certificates to personal health information to criminal and tax records.

"The type of data that we protect. Hackers have their eye on government data, as it is a treasure trove of personally identifiable information."

-Elayne Starkey, Delaware CSO

Not surprisingly, many CISOs mentioned budget constraints and navigating state political environments. Challenges that stem from these constraints range from a lack of control/ authority over the state security landscape and developing baseline security policies.

"State CISOs are faced with the same challenges as private sector CISOs, but typically have far fewer resources at their disposal."

-Joshua Spence, West Virginia CISO

CISOs also discussed citizen service delivery, public trust and image.

"Public trust, perception, and protection of constituent data and critical systems for the safety and well-being of the constituents is more of a driver for a State CISO, whereas a private sector CISO probably operates more as a risk-management offset to the financial well-being of the company."

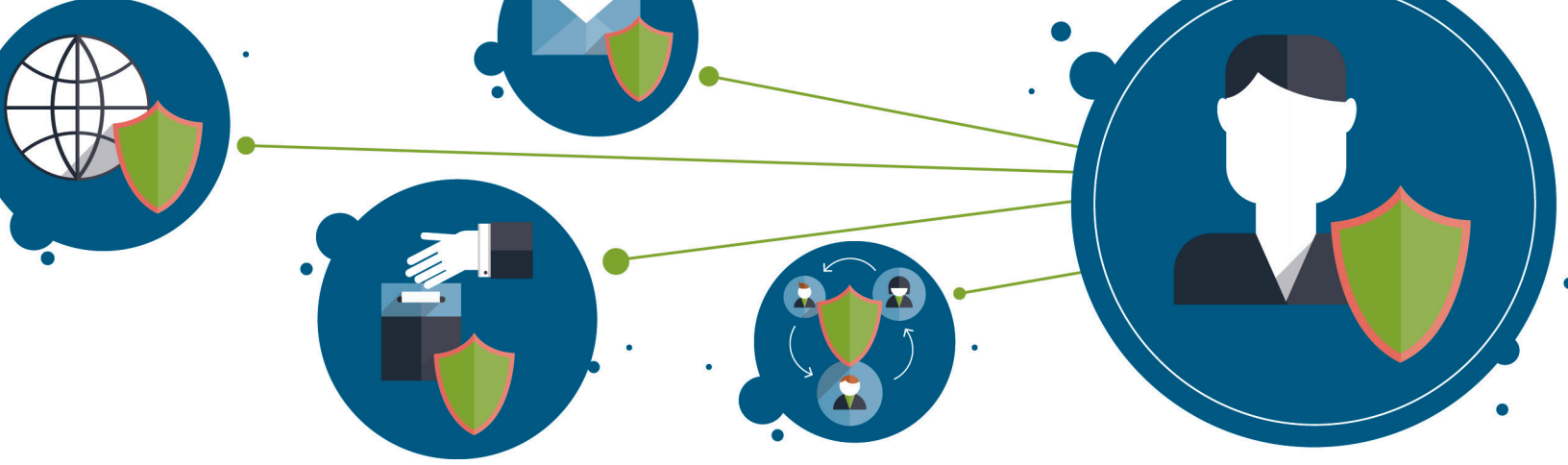
-Darryl Ackley, New Mexico CIO and Acting CISO

"Typically a private sector CISO is focused on the monetary goals and objectives of his or her corporation which is generally tied to their customer base, a Statewide CISO is granted the opportunity to enable operational State Agencies that genuinely improve areas of public service for residents and citizens of the State."

-Dustin Glover, Louisiana CISO

"Florida government is intertwined with citizen service delivery and private sector critical infrastructure, this has a cascading effect on all sectors within the state and has the potential to impact the economy, state and federal. While this is true for a subset of private sector CISOs, this is also true for all state CISOs, across all sectors."

-Danielle Alvarez, Florida CISO



Enterprise Planning and Strategy Activities
The 2006 CISO survey described the breadth and knowledge of a state CISO this way:

> 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.

In the 2015 survey, respondents also mentioned the unique business perspectives offered by a state CISO.

"A state CISO can bring a balanced strategic business and security perspective to the business of state government. They bring the ability to change the conversation from a security conversation to a business conversation."

-Agnes Kirk, Washington CISO

"A state CISO wears multiple hats. A state CISO has to be a great communicator and has to understand and speak the language of the business to build relationships and rapport with key stakeholders. The CISO needs to have strategic vision to understand where the organization is going in order to ensure key security initiatives are in alignment with the organization's strategic plan."

-Erik Avakian, Pennsylvania CISO

It is true that there are many differences and similarities between public and private sector CIOs and, as mentioned in the 2014 Deloitte-NASCIO Cybersecurity Study, that role is constantly evolving.

"The job of the CISO is still being determined across the IT industry."

-Brad Bird, Alabama CISO

But when it comes to risk, *"there really should NOT be any difference. A State CISO needs to have the same mindset as private sector."*

-Kurt Huhn, Rhode Island CISO

Maintaining Ongoing IT Security Investment
Once we established some differences and similarities in the public and private sectors, we wanted to know, once a state CISO is hired, what comes first? We asked, what is the most critical action a state CISO can take in the first 100 days of hiring? Many respondents discussed the importance of getting the lay of the land before doing anything else by reviewing policies and the CISO role.

"Assess the mission business processes and IT related risks affecting the state."

-Mark Reardon, Georgia CISO

"Fully review policies, guidelines, and standards and their adoption/implementation across the state. This process will help the new CISO gain an understanding of his/her jurisdiction and how well the existing policy structure is being adhered to."

-Brad Bird, Alabama CISO

"Get to know what the goals and risk appetite are of the administration. It will help set the strategic direction going forward."

-Michael Watson, Virginia CISO

Building and Maintaining Relationships

After getting a lay of the land, state CISOs were divided on the next step—building relationships with the state CIO and security staff or performing a security assessment. Still, some suggested combining the two. One CISO discussed the importance of conducting an analysis to determine where the gaps are in the security program, developing a roadmap to address them and then communicating and working with others to implement the plan. Still another CISO recommends assessing the security environment and then getting to know the key influencers in the organization.

Many CISOs also stressed the importance of creating and executing a strategic enterprise security plan to improve the state's security posture. One CISO put it simply, "create a strategy and plan."

"Understanding what drives the business of the overall organization and state agencies and then align cyber security governance and risk management initiatives to make those organization and agency driven business outcomes achievable and successful. Build metrics and reporting to align with those business initiatives to show the value of security. Present those metrics to help garner financial support for risk management initiatives to make the organization further secure and successful."

-Erik Avakian, Pennsylvania CISO

Indeed there is a lot for a CISO to first tackle and then proceed and succeed. But, Washington CISO Agnes Kirk cautions, nothing is done overnight, "listening and information gathering takes time."

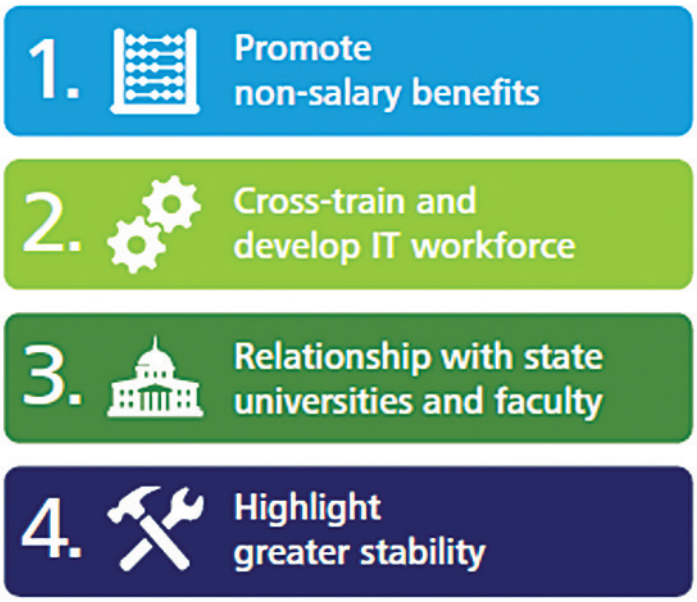
Adequate staffing

It is important to note that in the 2006 CISO survey, the overwhelming majority of respondents said state CISOs need adequate staffing/personnel in order to perform their jobs. Likewise, in the 2015 NASCIO publication State IT Workforce: Facing Innovation with Reality, respondents (49 state CIOs) identified security as the skill that presents the greatest challenge in attracting and retaining IT employees. Further, the Deloitte-NASCIO Cybersecurity study of 2014 identifies the lack of skilled personnel as a talent crisis.

So, what can states do?

The 2014 Deloitte-NASCIO Cybersecurity Study identified four top strategies states are using to retain cybersecurity talent:

Figure 4



The 2015 NASCIO workforce study also contains twenty recommendations for states to recruit and retain a qualified workforce. Two very important recommendations relate to modernizing the state workforce environment by:

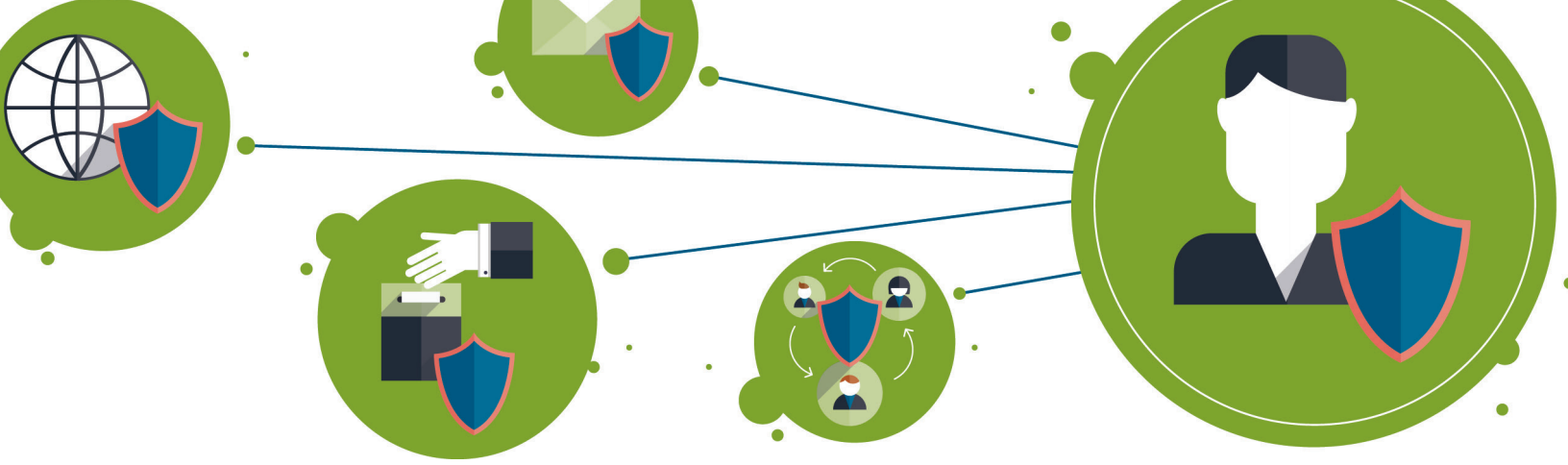
- Creating work environments that are stimulating, fun and attractive to all sectors of the workforce; and
- Providing flexible options for continuing education and skills development

States will never be able to compete with the private sector when it comes to cybersecurity salaries, making intangible benefits that much more important.

CISO Resources

Amid the talent crunch, enterprise planning and management of state cybersecurity efforts, CISOs must stay informed. So where do state CISOs get day to day assistance, ideas and inspiration? In the 2015 state CISO study, many discussed the importance of collaborating with fellow state CISOs at events sponsored by NASCIO and MS-ISAC (Multi State Information Sharing Advisory Center) and also provided specific resources that are helpful.

Figure 5



What I Wish I Knew Then

Finally, we asked a few state CISOs to answer the question, "what do I know now that I wish I knew when I first started as CISO?"

Massachusetts CISO Kevin Burns provided the following:

I wish I knew that…

> *A new state CISO needs to delve into the strategy of the state's IT future and take an inventory of critical systems and data.*
>
> *Cloud is here to stay and CISO's have to be on board, be part of the purchasing process and understand how important the legal process is to ensure protection of the state's digital assets.*
>
> *A new state CISO needs to evaluate her/his workforce and ascertain who will retire in the short and long term, and then set up partnerships with local higher education systems to fill the pipeline with viable candidates.*
>
> *A new state CISO needs to evaluate the training budget and ascertain if there are funds to send her/his personnel to certification training and other interesting training as a way to retain talent.*
>
> *A new state CISO needs to know how code is written, and the security process for review.*

Minnesota CISO Chris Buse observed:

> *"I believe that one of the most important words of wisdom for a new security leader is to take time to plan. Successful security leaders help their organization clearly articulate a long-term strategic vision for cyber security. Along with a clear strategy, security leaders also need a tactical plan to help their organization understand what to prioritize first. Taking time to plan is vital because without written long and short term goals, security leaders can literally use all of the resources at their disposal fighting tactical fires - and never accomplish what needs to be done to move the security bar for the enterprise as a whole."*

From Montana CISO Lynne Pizzini:

> *"It is all about relationships. A CISO must develop and maintain relationships both internally and externally to be successful. A new CISO should start by meeting with individual managers within their organization and then move outward to customers and others. Once relationships are established, you must maintain and develop all of these relationships. I believe over 50% of the*

time can be and should be spent in this area. I practice "management by walking around." I visit all of our internal staff at least once a month through this technique. It provides opportunity for questions, clarification, new information, etc. in both directions."

B. Victor Chakravarty, Maine Enterprise Architect offered the following:

"What I have found most useful is hard metrics. The executive leadership (Governor, Legislators, et al.) cannot devote too much time to understanding cyber security. But when I point out that our State receives every working day 2.2M intrusion attempts, or 30,000 spam emails, or that 15 workstations get infected, producing six person-hours of lost productivity per workstation, then they sit up and take notice. Also, the metrics better add up to a straightforward state-of-the-security picture: Either Gold-Silver-Bronze or Green-Yellow-Red. For this purpose, it is not all that important whether the underlying parameters are based upon NIST or not. Once the security shop gets used to collecting and publishing metrics, the next logical step is to analyze and publish the time-trend. All of this serves two important purposes. One: It serves as internal controls on the effectiveness of the security shop. But two: It also helps justify resources. For an additional $100K, we think we can move this metric from Yellow to Green. Could we give it a shot?"

Delaware Chief Security Officer Elayne Starkey gives this advice:

"Don't underestimate the power of executive level support. Find ways to align your security vision with your CIO's and the Governor's Office. Look for ways to involve both as an active participant and engaged stakeholder."

Continuing to Move Forward

One CISO replied, "The challenges of a CISO are never ending and always changing. The ability to stay calm, factual and methodological yet agile is a requirement for anyone to succeed in this role."

Indeed, key attributes of a successful state CISO are the ability to stay calm and focused, clearly communicate their role and responsibilities, describe threats and vulnerabilities and promote the importance of cyber awareness in clear and concise language to those who are well versed and not versed at all in cyber and technical language.

"As awareness of cyber security keeps growing in the general population, the CISO job keeps evolving. The trick is to build credibility with key decision-makers and influence resource allocation before a major adverse event."

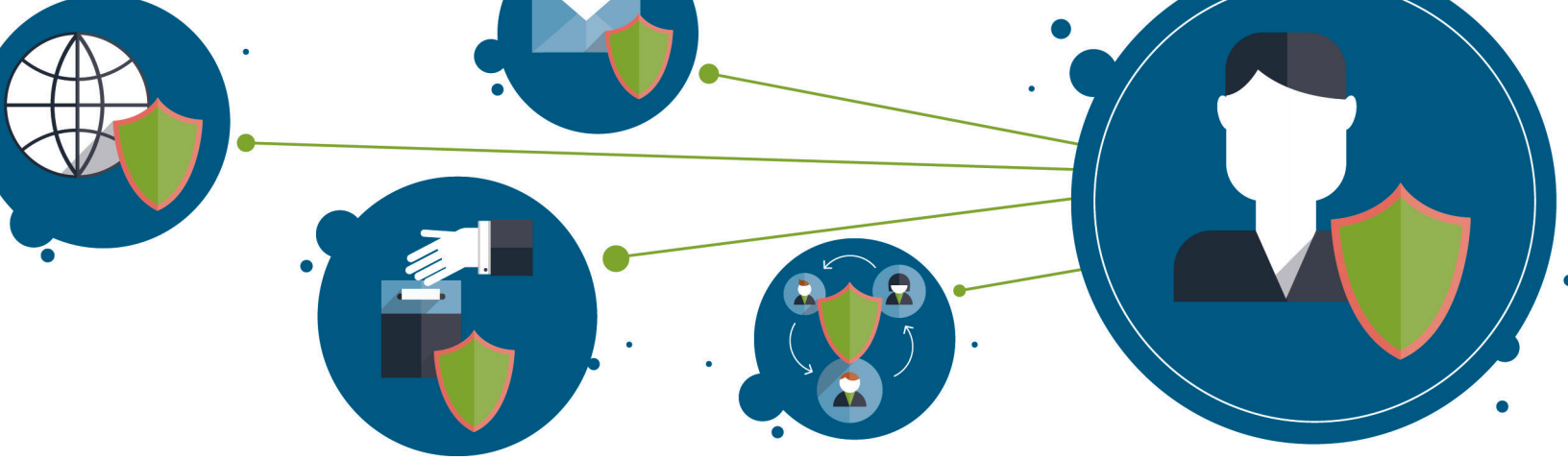
-B. Victor Chakravarty, Maine Enterprise Architect

As the state CISO role does evolve, CISOs must keep up to date on emerging issues—from drones to smart technology and the Internet of Things flood to continuing issues surrounding cloud security.

And like CIOs, state CISOs must constantly expect surprises—from cybersecurity attacks to data breaches, CISOs can count on more than their fair share of disruptions. State CISOs must jump right in to their jobs and can't afford to be unprepared when responding to an incident, especially when communicating to the governor, the CIO, other officials, the public and the media.

In spite of the highs, lows, disruptions and successes, as the 2014 Deloitte-NASCIO Cybersecurity Study highlights, CISOs continue to launch broad-based awareness campaigns, look for qualified talent and homogenize security practices, collaborate with their CIOs and other state and private sector business leaders and, most importantly, change the face of cybersecurity.

As a side note, oftentimes, communicating the importance of these components is an uphill battle to start, so it is critical to communicate effectively and clearly. One resource for state CISOs is the 2014 NASCIO Communications Toolkit for State CIOs, available on the NASCIO Community

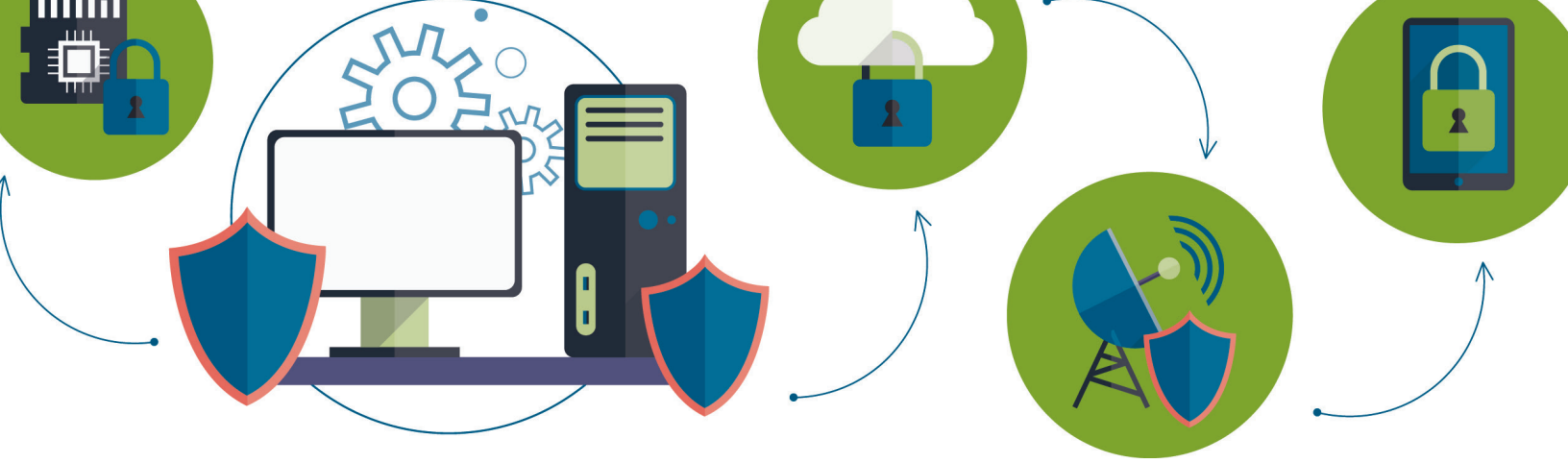


References

Current View of the State CISO: A National Survey Assessment
www.nascio.org/2006CISOSurvey

2014 Deloitte-NASCIO Cybersecurity Study
www.nascio.org/cybersecurity

State IT Workforce: Facing Reality with Innovation
www.nascio.org/workforce



NASCIO staff who contributed to this publication:

Mike Cooke, Web Designer
Sam Hearn, Graphic Designer
Olivia Hook, Research and Digital Communications Coordinator
Amy Hille Glasscock, Senior Policy Analyst
Emily Lane, Program & Brand Coordinator

FOLLOW US