NASCIO Representing Chief Information Officers of the States

Issue Brief

January 2006

NASCIO Staff Contact: Chris Dixon, Issues Coordinator, (859) 514-9148, cdixon@AMRms.com

Findings from NASCIO's Strategic Cyber Security Survey

Introduction

NASCIO has long seen the natural linkage between homeland security and the state and local government chief information officers (CIOs), who oversee information and communications technologies that support key public services. Section 7(c) of Homeland Security Presidential Directive (HSPD)-7 declares that: "It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could...undermine State and local government capacities to maintain order and to deliver minimum essential public services." Section 15 designates "emergency services"—most of which are delivered by state and local authorities—as being among the nation's "critical infrastructure sectors." These directives become all the more urgent when you consider that the nation's information infrastructure is the only part of our national infrastructure that is under attack all the time.

Thus, NASCIO's Information Security Committee, which is led by Denise Moore, CIO of Kansas, recently concluded a survey of strategic cyber security issues that was intended to identify the condition of the states on cyber security and assess the nature of their relationship with U.S. Department of Homeland Security's (DHS) cyber security programs and resources. The survey was conducted from August 16th to the 31st. The chief information officer (CIO) or chief information security officer (CISO)—or the equivalent state-government-wide information security officer—was invited to respond from each state and the District of Columbia. The survey garnered 27 responses from states representing 57% of the nation's population.

The survey was conducted in tandem with the Metropolitan Information Exchange (MIX), the national association of county and municipal CIOs. Both organizations will share the findings from their surveys under separate reports delivered to the U.S. House Committee on Homeland Security, which we hope they will use in guidance for DHS concerning state and local sector coordination. This report contains five high-level, or "strategic," recommendations along with 18 lower-level, or more "tactical," recommendations for action. Quantitative, question-by-question findings can be found in the attached appendix, titled "Detailed Results from NASCIO's Strategic Cyber Security Survey."

Executive Summary

Based on the finding below, NASCIO believes that several constructive recommendations can be made for national action in terms of the cyber security of the state and local sector. Given the ongoing reorganization at DHS, we have an opportunity to make a few key improvements that

Copyright © 2005 NASCIO • All rights reserved

could yield long-term benefits not only for our sector, but for the larger national effort to secure cyber space that has been underway for some time.

Strategic Recommendations:

1. The state CISO's would gladly accept a closer relationship with the DHS, as opposed to the more detached, private-sector based approach that is in place. This is not surprising given the interconnected relationship of federal and state information technology along the vertical lines of business, such as health and law enforcement. Some type of fellowships for state and local CISOs at DHS's National Cyber Security Division (NCSD) would be ideal for broadening NCSD's outreach within the sector and enhancing such efforts as the sector-based government coordinating councils.
2. The best way to ensure that cyber security is adequately addressed for the state and local sector is for a cyber security assessment component to be added to the existing State Homeland Security Assessment and Strategy (SHSAS) process conducted by DHS's Office of Domestic Preparedness (ODP). That doesn't guarantee the cyber security efforts will be funded to the level state CISOs would like, but, ideally, it would ensure that cyber security is adequately considered at the local, state, and federal levels.
3. The existing efforts of InfraGard and the Multi-State ISAC (MS-ISAC) provide an underutilized foundation upon which to promote existing DHS cyber security programs as well as to develop and promulgate best practices, consistent methodologies, and tools for a variety of needs (e.g., Carnegie Mellon's OCTAVE), including risk assessments, continuity of operations planning, training, exercises, and contracting alliances.
4. DHS's role as a direct provider of alerting services seems to be duplicative and their reputation for timeliness seems to be in question. Most state CISOs are confident in their ability to handle automated-external threats, but more emphasis needs to be placed on external-directed attacks as well as internal ineptitude and maliciousness. These are issues requiring specialized analysis, training/awareness, and procedures that could be better addressed by the various private-sector services providers as well as US-CERT, the MS-ISAC, CERT/CC, the Secret Service, the FBI Cybercrime Division, and InfraGard. This may be a question of better coordination and allocation of effort among the multiple entities with a stake in the game, so to speak.
5. State CISOs are unfamiliar with the existing academic programs designed to produce competent workers and practical research in information security. More localized education opportunities as well as a stronger bond between the research community and an organization such as the MS-ISAC and local InfraGard chapters would be beneficial.

Eighteen more specific, recommendations can be found in the text boxes below.

Baseline Information

Familiarity with major federal cyber security agencies and programs

NASCIO found the states were generally familiar with some of the major federal cyber security agencies and programs, including the NCSD, the FBI's "Cybercrime Division," and NIST's

Computer Security Resource Center (CSRC)[1]. The state CISOs were generally unfamiliar with the Center for Education and Research in Information Assurance and Security (CERIAS), U.S. Secret Service Financial Crimes Division's Electronic Crimes unit, and the National Centers of Academic Excellence in Information Assurance Education (NCAEIAE). Even the more familiar entities had as many as 20% of the respondents reporting that they had only "heard of" or "never heard of" these entities.

Recommendation for Action:

1. The federal government needs to increase the "marketing" all of major federal cyber security agencies and programs directly to the state CISOs, including such items as a regularly updated organizational chart of relevant federal entities and a cyber 9-1-1 phone number and portal that makes US-CERT's portal and help desk into a true "one-stop" shop for <u>all</u> federal cybersecurity resources, regardless of whether they are located

Usefulness of various national alerting and analysis resources

In regard to the usefulness of the various national alerting and analysis resources, the state CISOs found most of them to be "somewhat" or (more often) "definitely" useful, including Carnegie Mellon's CERT Coordination Center (CERT/CC), U.S. Computer Emergency Response Team (US-CERT) portal and help desk, US-CERT's National Cyber Alert System (automated e-mail service), SANS Institute/Internet Storm Center, and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The state CISOs were relatively unfamiliar with the services of the U.S. Secret Service Financial Crimes Division's Electronic Crimes unit. The state CISOs were not uniformly enthusiastic with InfraGard.[2]

Recommendations for Action:

2. DHS should better define and promote the role of the Secret Service in terms of state and local cyber security services
3. Given the recently announced "strategic partnership" between DHS and InfraGard, the federal government should seek to ensure the robustness of all the InfraGard chapters.

Familiarity with major cyber security-related documents/strategies

The state CISOs were generally familiar with the major cyber security-related documents/strategies, including the *Federal Information Security Management Act* (FISMA), the *National Strategy to Secure Cyberspace*, National Cyber Security Awareness Month, and *Homeland Security Presidential Directive (HSPD)-7*. However, as many as one-fifth to one-third of the state CISOs still reported being unfamiliar with these documents/strategies. State CISOs

Recommendation for Action:

4. DHS must do a better job of promoting these documents directly to the state CISOs and should seek to ensure that the cyber security elements of each document are aligned and can be "pulled out" to form a coherent, actionable set of goals in terms of preparedness, response, and recovery from cyber incidents.

[1] NOTE: NASCIO has been disappointed by recent cuts in funding for NIST's CSRC. Given that all states are highly interconnected with federal IT, the generalized guidance issued by the CSRC has been invaluable in helping states manage those linkages as well as other aspects of their information security programs and policies.

[2] NOTE: NASCIO has observed (based on comments from various state CISOs) that the robustness of the local InfraGard chapters is relatively inconsistent, with the level of robustness and engagement rising or falling with the level of enthusiasm or expertise of the local, organizing FBI field office.

were less familiar with the newer *Interim National Infrastructure Protection Plan* (NIPP), Carnegie Mellon's *OCTAVE* (Operationally Critical Threat, Asset, and Vulnerability Evaluation), and the older *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.

Recommendations for Action:

5. The sector ISACs should promulgate progressive practices, templates, and assessment tools for developing and benchmarking information security programs.
6. The sector ISACs should assess what the appropriate IT-budget allocation should be to oversee an adequate information security program versus total end users or "seats" or some other generally accepted indicator.
7. The sector ISACs should assess what the appropriate FTE allocation and assignments should be to oversee an adequate information security program versus total end users or "seats" or some other generally accepted indicator.
8. State CISOs need more avenues for hiring qualified information security professionals and for enhancing the skills of those already employed.
9. US-CERT needs to work across the sector ISACs to establish at least a working definition(s) for cyber incidents that will produce meaningful data.

Assessment of enterprise security architecture, policies, budgets, staffing, and incident loads

The state CISOs reported a dichotomy in regard to the state of their enterprise security architecture and policies with 11 (47%) declaring that they have "good" guidelines in place and that the enforcement of these guidelines is "improving." However, ten (37%) reported that they are still "ramping up" guidelines and enforcement efforts. Five states (19%) fell in between these levels and only one state (4%) claimed to have "good" guidelines that are "well enforced."

In regard to the budgets for state CISO offices, only 20 state CISOs offered a number and those amounts ranged from zero dollars to $5.5 million with the average being $1.87 million. Only six states exceeded that average with half the state CISOs reporting less than $1.0 million. Fortunately, all 23 state CISOs were willing to report estimated enterprise-wide security expenditures as a percentage of the state's total IT budget.[3] Five (19%) state CISOs reported dedicating less than 1% of their state's IT budget to information security. Eight (30%) reported spending approximately 1% and five states fell into the approximately 2% and approximately 3% categories. The remaining four state CISOs would not or could not estimate a percentage.

In terms of staffing for enterprise information security offices, the national average from our sample was 6.4 full-time equivalent (FTE) employees. Nine states exceed that average with five state CISOs reporting eight to ten FTEs and four state CISOs reporting 15 to 26 FTEs. Eighteen states fell below the sample average with seven state CISOs reporting one or two FTEs and 11 reporting three to six FTEs.

When it comes to hiring information security personnel, 41% of state CISOs reported a lack of applicants. However, a majority of the state CISOs (64%) reported that applicants displayed a "lack of formal training" as well as a "lack of practical experience", which was cited by 77% of the state CISOs. Fortunately, only 23% of state CISOs reported high turnover as being a problem.

[3] NOTE: A widely promoted benchmark within the information security community is that an enterprise should spend approximately 3% of its total IT budget on information security efforts.

Unfortunately, only 18 state CISOs were willing or able to provide an estimate of the weekly cyber-incident load they are bearing, using US-CERT's very loose definition of an "incident."[4] Eight state CISOs reported between one and five incidents per week. Five state CISOs reported between 20 and 100 incidents per week. Three state CISOs reported between 200 and 500 incidents per week. One state CISO reported 3,000 incidents per week. Another state CISO reported 300,000 incidents per week.

Prevention/Vulnerability Reduction

Actionable alerting information

Twenty state CISOs (77%) reported having "actionable" information for dealing with "external automated" attacks, such as worms, viruses, etc., which have been the national focus for quite some time both in terms of DHS and private-sector service providers (e.g., ISS, Network Associates, Symantec, etc.). However, the remainder said that their information was either "inadequate" (five) or "non-existent" (one). In regard to "external directed" attacks (i.e., hackers/crackers, organized criminals, potential terrorists, etc.), only half the state CISOs reported having adequate information.

Solid majorities (76-84%) of the state CISOs reported having inadequate or no information regarding threats from "internal ineptitude" and "internal maliciousness," which are potentially the most dangerous and which have not received adequate attention within the alerting community to this point**.** For example, detecting and countering external-directed attacks might require a cost-effective national network of intrusion-detection systems (IDS) designed to identify patterns and sort out external-directed attacks aimed at homeland security mission-critical information systems from the cloud of external-automated attacks that pulse all of their IT systems around the clock. Moreover, giving state CISOs the ability to better address potential internal threats might require connecting the state CISO practitioner community with terrorist-watch and background-check information and procedures.

Recommendations for Action:

10. More work remains to be done to ensure that every state has access to actionable information regarding external-automated threats
11. Much more work remains to be done produce actionable information regarding external-directed attacks and procedures for detecting various internal threats

Risk assessments, awareness, continuity plans, and exercises

The vast majority of state CISOs (73%) reported having conducted a risk assessment for information and communications technology systems that are "homeland security mission-critical" assets.

Seventeen state CISOs (63%) reported that *non*-IT government employees undergo training/testing that makes them reasonably well aware of the precautions they should take and ethics they should uphold in using information systems, e-mail, and the Internet in terms of cyber security.

[4] NOTE: US-CERT defines an incident as "…the act of violating an explicit or implied security policy. Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations."

An impressive 81% of state CISOs reported having developed an IT-oriented "continuity of operations" plan intended to help maintain order and to deliver minimum essential public services and emergency services within its jurisdiction in the event of a major cyber/physical attack or disaster. For example, the recent experiences of Louisiana, Mississippi, and Alabama would be gold mines of practical information regarding efforts to maintain IT continuity of business in the face of a major all-hazards-type threat (in this case a hurricane), and serious national resources should be invested to capture and share those experiences in a systematic fashion.

Recommendations for Action:

12. In order to ensure that all of the states are conducting such risk assessments (and doing so consistently), the existing State Homeland Security Assessment and Strategy (SHSAS) process should include a cyber assessment from each state.
13. More work needs to be done within the sector to promulgate progressive practices, templates, and tools for improving and benchmarking employee awareness of cyber security issues.
14. More work needs to be done within the sector to promulgate progressive practices, templates, and tools for consistently developing continuity of operations plans.
15. More work needs to be done within the sector to promulgate progressive practices, scenarios, and tools for conducting exercises as well as the lessons learned from them.[1] Moreover, DHS needs to conduct more frequent and wider ranging cyber- and TOPOFF-type exercises, which will help refine the cyber-exercise methodology and produce information to share with all of the state CISOs soon after the exercise.

Only 44% of state CISOs reported being able to test their continuity of operations plans in an exercise that includes responses to cyber and or physical degradations and disruptions to their information systems.

Dealing with cyber-incidents

When it comes to dealing with an actual cyber-incident, most state CISOs reported that they dealt with internal computer emergency/incident response teams (CERT/CIRT) along with local law enforcement first. Those CERT/CIRT teams are often comprised of specialized staff, who either work for the CISO or are comprised of an aggregation of IT personnel designated to respond from across the state's departments and agencies. Some state CISOs did indicate that they contact external organizations, including contractors, the FBI's Cybercrime Division, and US-CERT, with the Multi-State ISAC (MS-ISAC) being by far the most frequently mentioned.

Only 44% of the state CISOs indicated that they had sought "assistance" from any DHS agency. Several mentioned that they had sought funding and some have received it via the state homeland security grants. None indicated receiving a direct grant-in-aid from DHS. Again, in order to ensure that cyber security issues receive adequate attention at the state and federal levels the existing State Homeland Security Assessment and Strategy (SHSAS) process should include a cyber assessment from each state.

Training opportunities, fellowships, and requests/suggestions

Nearly every responding state (i.e., 26 out of 27) indicated that it would benefit from having local community and technical colleges offer associate degrees in practical cyber security. They also said they would consider hiring graduates of these programs and would consider sending current employees to take courses to broaden their skill sets. Twenty (77%) of state CISOs indicated that they would consider sending employees to *federally funded*, short-term (e.g., 180 day) fellowships in Washington, DC with the National Cyber Security Division (NCSD) where they could learn more about NCSD's mission and capabilities. However, this would not be easy for states with only a handful of information security staff.

The state CISOs were asked what they think DHS's role should be (if any) in providing or funding alerting, analysis, and other emergency/incident response-type services and programs. (Please see individual responses to Q6.3 on pp. 18-20 of the appendix.)

Finally, the state CISOs were asked to suggest one resource or service that would help them improve the cyber security of their government's information systems. (Please see individual responses to Q6.4 on pp. 20-22 of the appendix.)

Recommendations for Action:

16. The federal government should consider implementing this fellowship program in such a way that would allow states with fewer staff to participate.
17. The state CISOs would like to see the following from DHS: more funding for various cyber security needs (7), better leadership and coordination (7), better/more timely alerting services (5) better training/awareness efforts (3), and better/more consistent assessment methodology (2).
18. The state CISOs would like to see the following from DHS: more targeted funding (8), uniform assessment frameworks/templates (3), training courses/materials (3), more national awareness/focused message (2), national contracting vehicle/pooling of resources (2), better coordination/leadership, early alerting, more exercises, and a national public key infrastructure (PKI)

About the Data

Based on the assortment of responding states, NASCIO believes that the data collected for this survey allows for reasonable extrapolation into a national "picture" of the states in regard to strategic cyber security goals that have been promoted by DHS since its formation. As far as non-responding states are concerned, it has been NASCIO's experience that several factors contribute to a state's failure to participate in a survey.

1. As a voluntary membership association, NASCIO relies on goodwill and a strong business case to generate responses, but our surveys still get lost in the shuffle of the workloads of more than few of the officials whom we target to respond.
2. In a few cases the official designated to respond is too new to respond authoritatively or the position is currently unfilled due to turnover.
3. In a few more cases the official designated to either respond cannot respond authoritatively due to organizational constraints or (if he or she could respond authoritatively) is unwilling to "expose" the actual condition of the state.

So, if anything, NASCIO experience leads to the assumption that a 100% response rate would tend to skew the overall picture of the states more toward the scale of uncertainty, a lack of robustness, or unknowingness—but not dramatically so.