Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers

Strengthening Cybersecurity Series

Marilu Goodyear
Chair of the Department of Public Administration
University of Kansas

Holly T. Goerdel
Assistant Professor of Public Administration
University of Kansas

Shannon Portillo
Assistant Professor in the Criminology, Law & Society Department and Deputy Director of the Center for Justice, Law & Society
George Mason University

Linda Williams
Doctoral Student in Public Administration
University of Kansas

IBM Center for
The Business of Government

2010

STRENGTHENING CYBERSECURITY SERIES

Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers

Marilu Goodyear
Chair of the Department of Public Administration
University of Kansas

Holly T. Goerdel
Assistant Professor of Public Administration
University of Kansas

Shannon Portillo
Assistant Professor in the Criminology, Law & Society Department and Deputy Director of the Center for Justice, Law & Society
George Mason University

Linda Williams
Doctoral Student in Public Administration
University of Kansas

IBM Center for
The Business of Government

TABLE OF CONTENTS

Foreword.....5

Introduction.....7
- Federal Concerns about Cybersecurity.....7
- State Concerns about Cybersecurity 9

Results from a Survey of and Interviews with Chief State Cybersecurity Officers.....11
- Titles and Responsibilities of State CISOs 11
- Skills Needed for Successful CISOs 11
- Professionalism and Establishing Credibility 13
- Collaboration and Networks.....14

Case Studies of State Strategies for Cybersecurity.....17
- Five Strategies Used by State Cybersecurity Officers.....17
- Case Studies of State Strategies.....20
  - California 20
  - Colorado.....21
  - Delaware.....23
  - Kansas.....24
  - New York 26
  - Washington.....28

Recommendations.....30

Appendix I: Excerpts from *Essential Body of Knowledge*.....33

Appendix II: Study Methodology and List of Participating States.....34

Endnotes 36

References 37

About the Authors.....39

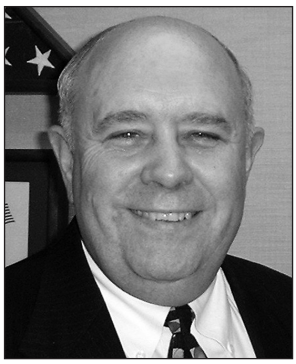
Key Contact Information.....41

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, "Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers," by Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, and Linda Williams.

Jonathan D. Breul

The importance of safeguarding information created and shared on computers and the internet has increased significantly in recent years, as society has become increasingly dependent on information technology in government, business, and in their personal lives. Both corporations and government have responded by creating a new role in their organizations to lead the safeguarding efforts—chief information security officers. The role of these officers is still under development. Do they safeguard best by using law enforcement techniques and technological tools? Or are they more effective if they serve as educators and try to influence the behaviors of technology users?



John Lainhart

This report is a significant contribution to the discussion of the roles and responsibilities of chief information security officers (CISOs) in state governments across the United States. It identifies both strategies and activities used by successful state CISOs, and thereby provides a good roadmap to success for all state CISOs.

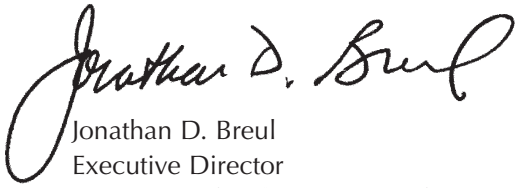
The report cites the Multi-State Information Sharing and Analysis Center (MS-ISAC), which has been championed since its inception by the New York state chief cybersecurity officer as one key cybersecurity collaboration success. The MS-ISAC initiative has yielded measurable results and provided a means of consistent communication across sectors in society.

The report also emphasizes that while a technical education remains important for CISOs, state cybersecurity officials need to be proficient in non-technical skills as well, including collaboration, communication, managerial, organizational, policy alignment, and political skills.

Finally, the report emphasizes the need for state cybersecurity officials to devote increased attention to data management as the defined system/network perimeter has dissolved and the future success of cybersecurity relies on the CISOs, chief information officers, data owners, records managers and archivists to jointly focus on data management to achieve effective business processes.

This report also emphasizes the importance of effective IT governance—as recommended in a report The IBM Center issued in October 2002, *Public-Sector Information Security: A Call to Action for Public Sector CIOs,* by Don Heiman. In the report, IT governance was the first of 10 recommendations that were critical components to a successful response against cybersecurity threats and attacks. That recommendation is just as applicable today as it was in 2002.

We hope that you find this report both timely and informative. We believe its insights and recommendations are relevant to CISOs at all levels of government.



Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
jonathan.d.breul@us.ibm.com

John Lainhart
Partner for Cybersecurity
IBM Global Business Services
john.w.lainhart@us.ibm.com

Introduction

Cybersecurity has been commonly associated with three aspects of information technology "people, process, and technology" (Andress, 2003). People as users and creators of information and technology systems and defined organizational processes clearly affect the ability of any technological environment to be secured. Indeed, some would argue that convincing users to utilize secure processes when handling government information is the key solution to cybersecurity issues. Others argue that technological solutions are most important because they have the ability to define border environments as well as control the behavior of users within those environments.

Increasingly, there is recognition that it may be impossible to control the movement of data and that effective processes and data management are keys to security risk management. Will Pelgrin, director and chief cybersecurity officer of New York's State Office of Cyber Security and Critical Infrastructure Coordination, recently summed up the challenge: "[A] few short years ago we had a well defined perimeter…. [I]t has now dissolved–our job is to protect data that is resident with each and every one of us" (Aul, 2009).

In 2008, a task force coordinated by the Department of Homeland Security defined the profession by publishing a document that defines the essential body of knowledge for cybersecurity (Department of Homeland Security, National Cyber Security Division, 2008). It provides an outline of information security roles and competencies for IT management including the CISO, CIO, and other IT professionals. A list of the 14 essential areas of expertise is presented in Appendix I.

Definition of Cybersecurity

Cybersecurity can simply be defined as security measures being applied to information technology to provide a desired level of protection. The issue of protection can be defined using the acronym CIA for Confidentiality, Integrity, and Availability:

- **Confidentiality** refers to the property that data should only be viewable by authorized parties.
- **Integrity** refers to the principle that only authorized users are allowed to change data, and that these changes will be reflected uniformly across all aspects of the data.
- **Availability** refers to the principle that data and computer resources will always be available to authorized users.

Source: *Conklin, Art and Gregory B. White.* e-Government and Cyber Security: The Role of Cyber Security Exercises. Proceedings of the 39th Hawaii International Conference on System Sciences. *Kauai, Hawaii. January 4–7, 2006.*

Federal Concerns about Cybersecurity

Concerns about the security of computer systems were raised in 1976 by Thomas Rona, who saw the potential threat to information technology (Rona 1976). As the use of technology grew, concern for security of systems and data within increased. Starting with the Clinton Administration in 1998, successive presidents have devoted increased attention to cybersecurity.

Clinton Administration

Federal recognition of the cybersecurity threat came in May 1998, when the Clinton administration issued Presidential Decision Directive 63, instructing

federal agencies to take steps to reduce the vulnerability of computer systems and communications networks. The directive was also intended to implement measures to mitigate threats to the commercial sector. These included:

- Appointment of a National Coordinator for Security, Infrastructure Protection and Counter-terrorism in the National Security Council staff, whose duties included overseeing the development of cybersecurity policy
- Establishment of the National Infrastructure Protection Center (NIPC) in the FBI, with responsibility for coordinating reports of computer crime and attacks
- Establishment of the Critical Infrastructure Assurance Office (CIAO) to coordinate the government's efforts to protect its own vital infrastructure, integrate federal efforts with those of local government, and promote public understanding of threats (Berkowitz and Hahn p. 3)

President Clinton appointed Richard A. Clarke as the National Coordinator for Security, Infrastructure Protection and Counter-terrorism, a Cabinet-level position. Clarke had worked in the State Department during the Reagan Administration, and President George H.W. Bush appointed him as chairman of the Counter-terrorism Security Group and to the United States National Security Council (NSC). During his tenure, the CIAO created and released the *National Plan for Information Systems Protection Version 1.0: An Invitation to a Dialogue,* a report that set forth the Administration's vision for addressing emerging threats.

Bush Administration

The George W. Bush Administration acknowledged the importance of cybersecurity and retained Clarke as a special advisor in the NSC, although his position was no longer at the Cabinet level. The Administration began reviewing cybersecurity policy in January 2001 and in October 2001 issued Executive Order 13231, which was designed to protect critical infrastructure. In February 2003, the administration released its final plan: *The National Strategy to Secure Cyberspace*.

Obama Administration

In 2009, the Obama White House released the report *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (White House, 2009). The report signals the continued importance of cybersecurity, stating clearly. "[T]hreats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies." The report outlines seven key points:

- Cyberspace underpins almost every facet of modern society and provides critical support for the U.S. economy.
- The *status quo* is no longer acceptable.
- A national dialogue on cybersecurity must begin today and government, with industry, should explain the challenge so that the American people appreciate the need for action.
- The United States cannot succeed in securing cyberspace if it works in isolation; public-private partnerships as well as international collaboration are necessary.
- The federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well being of citizens.
- Working with the private sector, performance and security objectives must be defined for next-generation infrastructure.
- The White House must lead the way forward.

The *Cybersecurity Policy Review* conveys a strong signal about the significance of cybersecurity and recognizes its importance to all levels of government and the private sector. Furthermore, it coincides with state level assessments by chief information officers (CIOs), who found that cybersecurity ranked sixth among top ten priorities in a 2010 survey conducted by the National Association of Chief Information Officers.[1]

This renewed interest in cybersecurity by the White House and among top state and local officials comes at a crucial time. All levels of government are challenged by decreases in revenues, and evidence indicates that the current fiscal environment is unprecedented and severe. How will governments improve their cybersecurity profile in these tight fiscal times? Cybersecurity stands at the forefront of these pressures as the scope of security expands and the resources to address security issues do not. The

current condition of the states requires that we continue to work smarter in all areas of information technology.

This report asserts that the professional expertise of information technology employees who focus on security issues is a critical asset for governments at all levels. Making the most of that asset in itself and leveraging it for other fiscal benefits for the state represent important strategies in meeting the current challenge.

Adding to the strain on fiscal and personnel resources, the federal government's Chief Information Officer, Vivek Kundra, has elevated the priority of transparency regarding IT spending of government stimulus funds (Towns, 2009). Recognizing the importance of this initiative to democratic accountability, Kundra will continue asking state and local governments to post data on the web related to stimulus spending. Additionally, in an effort toward further cooperation on transparency issues, the National Association of State Chief Information Officers (NASCIO) is actively working with Kundra. While it challenges resources, this quest for openness provides further reason for cybersecurity professionals to provide more robust approaches to data management and protection.

State Concerns about Cybersecurity

Pressures to elevate cybersecurity as a national priority pose challenges for cybersecurity professionals. Whereas organizing for cybersecurity at the federal level has taken shape within the Department of Homeland Security and the Department of Defense,[2] states have had varied success in establishing links between *cyber* protection and *physical* security, as well as in integrating cybersecurity into overall state infrastructure planning. Their varied success stems from several issues:

- First, many state offices of homeland security have only recently incorporated personnel with expertise in critical infrastructure protection, even less those with expertise in cyber infrastructure.
- Second, to the extent that cyber infrastructure specialists exist, they are mostly situated within IT organizational communities, which may or may not be (in)formally coordinated with the state's homeland security apparatus. As a result, we see more chief information security officers advocating for structural arrangements and policies that can effectively bridge "the chasm between the worlds of critical infrastructure protection and cyber protection."[3]
- Third, states have demonstrated both reluctance and enthusiasm to elevate cybersecurity as a major priority and to engage legislatively or administratively on issues of cybersecurity. For some, a lack of coherent guidance and intergovernmental funding from appropriate federal agencies is a serious hindrance. For others, a bottom-up approach that places state cybersecurity professionals at the forefront of decision making and dialogue is preferable. However, this approach is rife with difficulties. Challenges include overcoming authority and status barriers between federal and state experts on matters of policy (elite-actor bias), and securing two-way communication that reaches beyond symbolism to actual participatory governance (participation-deficit).

In spite of their varying viewpoints on these matters, one conclusion drawn from this research is that state CISOs share common concerns over the role and reach of cybersecurity responsibilities. These concerns include:

- Risks associated with potential violations of privacy and civil liberties of citizens.
- Managing problems that could morph in scope and scale from domestic to international significance.
- Risks associated with taking on additional unfunded security mandates.

Despite these challenges, state CISOs have been on the front-end of cybersecurity dialogue, lending expertise to identifying gaps in policies, testing strategies for remediation, and acting as laboratories of innovation for how best to organize to address threats in an evolving cybersecurity environment (Williams, 2009).

Ultimately, these challenges and opportunities point to the need for collaboration among local, state, federal, and private partners on matters of cybersecurity, as well as on the articulation of values governing collaborations specific to this task. Effective collaboration and planning will establish

links between cyberspace and *physical* attacks, such as those that may compromise electricity grids, water infrastructure, and air traffic control systems. It will also establish links with *informational* attacks, including hacking of e-mail systems of agencies like Department of Defense, computer probes of IT systems at NASA and the Transportation Security Agency, and the loss of billions of dollars in intellectual property from the private sector, which weakens economic resilience (CSIS Commission on Cybersecurity, 2008).

As Lieutenant General Harry D. Raduege, Jr., USAF, Ret., has noted, technology leaders face a "challenging and demanding business," where the "rewards for success are great and dangers for failure are significant" (Aul, 2009). The state-level CISO stands in the middle of these large and complex issues, serving as the partner of the CIO in ensuring the protection of state data and systems. But what do we know about this role?

Building on a 2009 study of the role of the chief information security officer in higher education (Goodyear et al., 2009), this report identifies roles, responsibilities and skill sets of current state chief information security officers. In addition, the report describes the varied strategies used by states to engage their diverse communities on cybersecurity issues. Twenty-nine states were included in the study by participating in an electronic survey, in-person interviews, or phone interviews (Appendix I includes a full description of the research design). This report points to the broad array of concerns for cybersecurity professionals resulting in the need for both technical and leadership skill sets. It is clear that collaboration is a key element in successful implementation of cybersecurity programs in the states.

Results from a Survey of and Interviews with Chief State Cybersecurity Officers

Titles and Responsibilities of State CISOs

Debates about boundaries of the discipline and titles for the top cybersecurity professions in an organization ensued as the profession developed from its beginning in the 1990s. As technology became more complex, all aspects of control and access became potential areas to include within the purview of cybersecurity. Titles changed, but they consistently used combinations of the words "information", "technology", "security" and a word representing an administrative officer (chief, head, director, or officer).

In this report, we found the most common title is that of chief information security officer, often incorporating the word "state" in the title. The majority of CISOs now report directly to the state chief information officer, with a minority reporting to a deputy CIO or an enterprise information systems director. Very few states maintain separate reporting lines for the CISO and the CIO, although it has been argued that separating their roles has the advantage of compartmentalizing operational concerns from security decisions.

Table 1 shows data from 18 state CISOs providing responses on their areas of responsibility. CISOs have primary responsibility for data security, incident management, training and awareness, regulation and standards compliance, risk management, and strategy. Given the small number of respondents, it is not prudent to generalize to the universe of cybersecurity personnel. However, data gathered for this report are consistent with both the essential body of knowledge and data gathered from CISOs in the higher education environment (Goodyear et al., 2009).

Only 38 percent of state CISOs responding to the survey have primary responsibility for digital forensics. Data from interviews indicate that the state CISOs share responsibility for digital forensics with law enforcement agencies; increasingly law enforcement is taking the lead in these types of investigations.

This finding that only 38 percent of state CISOs have responsibility for digital forensics differs from the *Essential Body of Knowledge*, as that report defines the information security officer role as both managing and designing efforts in digital forensics (2008). State-level CISOs report that slightly fewer than half have primary responsibilities in this area.

Skills Needed for Successful CISOs

Responsibilities defined for the position of CISO comprise activities that are technical, managerial and collaborative in nature. Table 2 reports data gathered from 18 CISOs on their review of important skill sets. Survey responses indicate that both CISOs and chief information officers believe a range of skills, beyond those technical in nature, are important to the role.

Non-technical skills include collaboration/conflict management, communication skills, and political skills. Several CIOs noted communication and interpersonal skills as well as relationship capabilities as vital skills for the CISO role. The importance of these skills was also reflected in interviews. As one CISO offered, the ability "to articulate IT security and privacy technical issues in a non-threatening and clear/actionable manner to non-technical leadership" is imperative.[4] Also reported as important are the skill sets that relate to the ability of the CISO to manage and lead security efforts. High on this list

Table 1: State Chief Information Security Officer Areas of Responsibility

	N	Primary	Support	No Responsibility
Most State CISOs Have Primary Responsibility				
Strategic security management	18	94.4%	5.6%	0.0%
IT security training and awareness	18	83.3%	16.7%	0.0%
Security risk management	18	72.2%	27.8%	0.0%
Regulation and standards compliance	18	66.7%	33.3%	0.0%
Data security	18	61.1%	38.9%	0.0%
Incident management	18	61.1%	33.3%	5.6%
Some State CISOs Have Primary Responsibility				
Procurement of technology (review of security aspects)	18	44.4%	55.6%	0.0%
Digital forensics	18	38.9%	55.6%	5.5%
Enterprise continuity	18	33.3%	61.1%	5.6%
Data and information management (classification, retention, destruction)	18	27.8%	72.2%	0.0%
Network and telecommunications security	18	27.8%	72.2%	0.0%
Identity management	18	22.2%	72.2%	5.6%
Few State CISOs Have Primary Responsibility				
Personnel security	18	16.7%	72.2%	11.1%
Physical and environmental security	18	11.1%	83.3%	5.56%
IT systems operations and maintenance	18	5.6%	72.2%	22.2%

Source: 2009 Cybersecurity Management Survey *conducted for this report*

are knowledge of state government processes, planning and strategic management skills, political skills, and policy development and administration. As one CISO stated, "[H]aving an understanding of political relationships between agencies/departments is also helpful. I do not personally get involved in the political arena but there are history and power struggles that impact what I do."[5]

Non-technical skills are used by CISOs as they seek cooperation from across state government in building a secure environment. Another CISO painted a picture of a very demanding role requiring a long list of attributes and skills:

> Determination, drive, ambition, goal orientation, negotiation, listening, retaining, distilling information, writing skills, editorial skills, likability, sense of humor, dedication, honesty, commitment, accountability, success-orientation, positivity, humility, flexibility, patience, deference to others, consensus building, shared authority, letting people excel without being threatened by their prowess, recognize talent, nurture talent, grow talent, bring out the best in others, thick skin.[6]

As table 2 indicates, interpersonal communication and managerial skills are seen as equally important or even more important than technical skills for the success of the CISO. These non-technical skills are viewed as crucial for accomplishing organization objectives related to cybersecurity. However, the standard deviations in this table show that CISOs have a diversity of views about the skills needed to fulfill their jobs; there is a mix of technical, managerial, and policy perspectives. Understanding how skills are valued in various state environments could assist CISOs in determining their professional development priorities.

Table 2: Importance of Skills to State CISO Success

	N	Mean*	Std. Deviation
High to Very High Importance			
Communication and presentation skills	18	4.78	0.428
Policy development and administration	18	4.56	0.705
Political skills	18	4.44	0.616
Knowledge about the state government	18	4.39	0.608
Collaboration and conflict management skills	18	4.33	0.840
Planning and strategic management skills	18	4.33	0.686
Supervisory skills	18	4.28	0.461
Incident management	18	4.22	0.732
Knowledge of regulation and standards compliance	18	4.17	0.618
Risk assessment and management	18	4.17	0.707
Moderate to High Importance			
Budget and fiscal management	18	3.72	0.826
Business process analysis	18	3.89	0.832
Security architecture	18	3.83	0.786
Systems security	18	3.83	0.786
Disaster recovery	18	3.56	0.984
Network security and firewall management	18	3.56	0.856
Identity management	18	3.33	0.840
Data and information management (classification, retention, destruction)	18	3.33	0.686
Application security	18	3.28	0.575
Procurement of systems, software and services	18	3.28	0.752
Database security	18	3.22	0.943
Digital forensics	18	3.11	0.900

**Scale: 1=Very low importance, 2=Low importance, 3=Moderate importance, 4=High importance, 5=Very high importance*
Note: *Whereas skills are ranked in order of their importance according to their reported mean values, those with larger standard deviations (for example, .700 and above) reveal widespread differences of opinion held by CISOs on the importance of such skills.*

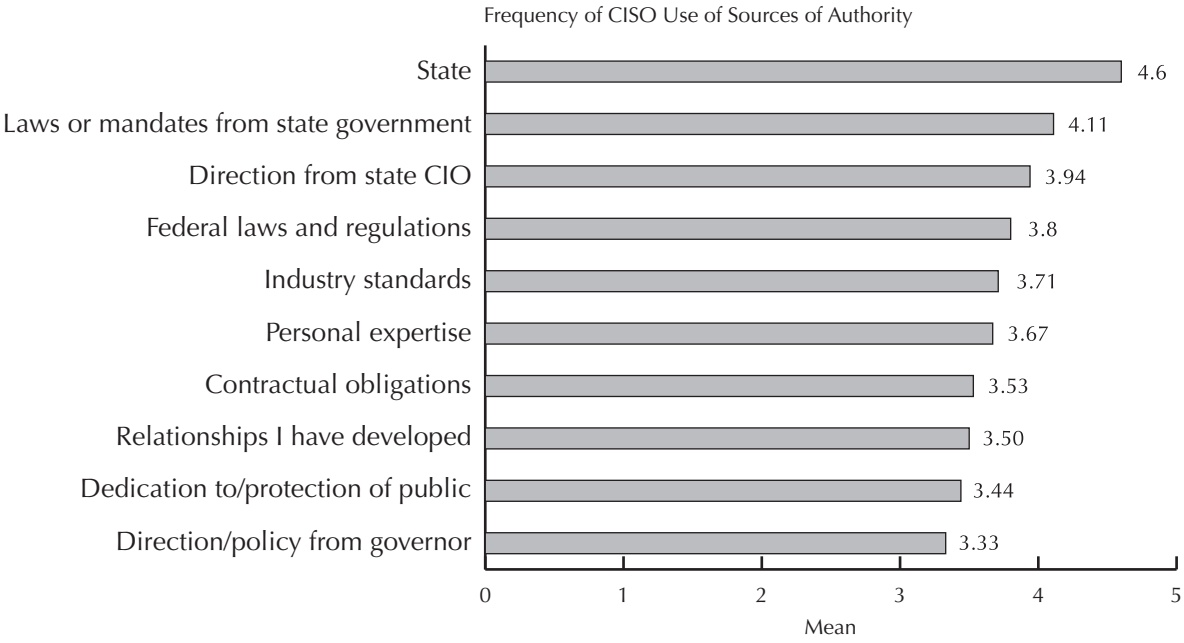
Source: 2009 Cybersecurity Management Survey *conducted for this report*

Professionalism and Establishing Credibility

This emphasis on communication and trust-building is reflected in another piece of feedback received from the CISOs who participated in the survey: the role of professionalism. CISOs identified professionalism as important in building relationships necessary for success. One CISO highlighted it this way: "Conduct the affairs of the CISO's office with professionalism and fairness, and work to establish effective relationships with both upper management and all major state agencies."[7]

The emphasis on professionalism for the role is also addressed by the way in which the CISOs establish their authority. CISOs were asked what types of authority they use to establish credibility. Table 3 summarizes responses from the survey. Reference to laws and state policy are important sources on which CISOs relied, but also important are their personal expertise and relationships they have developed over

Table 3: Types of Authority Used to Establish Credibility*



*Scale: 1=Very rarely or never, 2=Rarely, 3=Occasionally, 4=Frequently, 5=Very frequently or always

Source: 2009 Cybersecurity Management Survey *conducted for this report*

time. These responses demonstrate there is no single path to garnering credibility for the CISO role; rather, complex arrays of expertise (both technical and managerial) and relationships (based on professionalism and trust) are needed to succeed.

Collaboration and Networks

The ability to collaborate across organizational boundaries was also reported as important in the CISO role. CISOs recounted that they frequently or very frequently coordinate with or collaborate with IT staff in other agencies, non-IT staff in other agencies, and with the private sector, including IT vendors.[8] CISOs see communication and conflict management skills as critical to these endeavors, but also highlight the ability to put personal issues aside in the process. One respondent cited "flexibility and patience" as important while another mentioned "humility; understanding you can't do this job alone. Being able to submit your will to that of the group."[9]

CISOs noted the importance of face-to-face meetings in order to build trust and relationships, as well as the benefits of consulting a variety of stakeholders outside of state government. One CISO reported:

> I go to agencies and departments and speak to IT people about their systems, what their needs are, what improvements or help my office can offer, and the key is that I follow up on what we discuss and I do what I promise. I work *with* people and take their input seriously. I may not be able to do as they wish but I am very clear as to reasons why.[10]

Given the complexity of the cybersecurity landscape and the importance of relationship-building in the CISO role, this report places a specific emphasis on collaboration, exploring a major theory in the development and success of networks and how they are relevant to cybersecurity programs.

Provan and Kenis (2007), in their work on the effectiveness of networks, discuss the need for leaders to develop competencies that relate to the management of networks. They postulate that in networks where there is significant interdependence among members, there is a need for coordination skills in addition to task-specific competencies. As this report documents, the work of the CISO is highly collaborative: within

Table 4: Indicators of Competencies Needed to Support Collaborative Work*

Competency		Indicators
Interpersonal Understanding	Demonstrates empathy	+ Listens to understand other perspectives and needs
		+ Develops close relationships with people at all levels
		– Receptiveness to others is dependent on position, rank
		– Unable to understand perspectives outside own expertise
	Understands motivation	+ Understands needs for power, affiliation, and achievement
		+ Adapts own strategies to motivate others effectively
		– Writes off unproductive collaborative members automatically
		– Seeks sanctions for unproductive collaborative members
Teamwork/ cooperation	Inclusive perspective on achievements	+ Inclusive achievement perspective: "We did this"
		+ Identifies outcomes that benefit all involved partners
		+ Reluctant to claim individual credit for collaborative outcomes
		– Individual achievement perspective: "I did this"
	Altruistic perspective on resource sharing	+ Shares resources readily with others: Supports altruistic behavior via personal example
		+ Balances needs of own organization with needs of others
		+ Does not expect return on investment
		– Unwilling to commit resources until others commit first
		– Views resources as organizational property, not public goods: Protects "turf"
	Collaborative conflict resolution	+ Welcomes conflict for the purpose of gaining new perspective
		+ Seeks win-win solutions to problems
		+ Uses boundary-spanning language to find shared meaning
		– Avoids conflict to maintain peace
		– Maintains interest-based positions

**Table is adapted from Getha-Taylor 2008*

states, between states, and among public and private sector organizations. CISOs who participated in the study identified collaboration and networks of both organizations and individuals as critical to their success. How does the IT community understand which skills are necessary to be effective in these collaborative environments?

Getha-Taylor (2008) has studied competencies needed to support collaborative work. She found that federal employees who have been successful at building collaborations place more emphasis on interpersonal understanding, teamwork and cooperation, and team leadership in their collaborative efforts. These competency areas contrast with the U.S. Office of Personnel Management's competencies, which focus on political savvy, negotiating and partnering. Getha-Taylor outlines two aspects of interpersonal understanding that define the competency: demonstrating empathy and understanding motivation.

Three characteristics, as set forth by Getha-Taylor, define competency in teamwork/cooperation:

- Inclusive perspective on achievement
- Altruistic perspective on resource-sharing
- Collaborative conflict resolution

Table 4 provides a detailed look at which indicators would signal effective behavior in these areas.

In our interviews with CISOs, they outline approaches to working with state agencies in ways that reflect many of the behaviors outlined in table 4. In the category of demonstrating empathy, CISOs provided several examples of reaching out to understand others' perspectives, particularly in the area of policy development. They report numerous instances where personal relationships among colleagues enabled them to move their programs forward despite organizational constraints.

A number of CISOs reported focusing on the motivation of those in other agencies to gain their cooperation with and collaboration on cybersecurity programs. It is clear that CISOs attempt to understand agency priorities and seek compliance through a variety of motivational strategies; several examples are described in the case studies in this report. Appealing to a sense of shared responsibility was also reported as a successful strategy to elicit cooperation.

Also related to collaboration, CISOs report a practical approach to cybersecurity incidents; they indicate that they try not to make the investigation about blame, but instead about learning from what went wrong. In a similar vein, credit for successes was shared; CISOs focused on making successful programs into the driving force for change. This inclusive sense of sharing both responsibility and achievement appears to be a critical skill set in gaining cooperation.

Altruistic perspectives on resource sharing are apparent in the broad cybersecurity community. From early in the development of the profession, wide sharing of information about security incidents was common. The state CISOs clearly exemplify this in their approach today, sharing information without an explicit expectation of a return on the investment.

Seeking to "span boundaries" has become second nature to many CISOs given that cybersecurity itself knows no boundaries. CISOs increasingly see including all relevant players as critical to the effort to combat hackers who move seamlessly across organizational boundaries.

CISOs have naturally developed collaborative competencies in response to the needs of their organizations and the evolving challenges of the technological environment. It is clear that such collaborative skills have become essential to the role of the CISO. The next section explores the elements necessary to make those collaborations successful.

Case Studies of State Strategies for Cybersecurity

Cybersecurity clearly fits the definition of a "tangled" problem as discussed by Dawes et al. (2009), an issue far beyond routine and yet not as difficult to approach as "wicked" problems whose solutions are far from apparent. Cybersecurity issues require state governments to engage a broad array of players, across a number of organizational and sector boundaries to achieve common goals that comprise multifaceted (technical, policy, and behavioral) approaches to change. While securing states' data and systems is far from routine, state IT communities have developed well-defined approaches to many basic elements of cybersecurity.

As states explore this "tangled" problem, they have chosen different areas to emphasize. Differences in state culture, resources, political environment, and size have resulted in a variety of strategies aimed toward keeping state data and systems safe. Case studies from five states highlight these different approaches.

Five Strategies Used by State Cybersecurity Officers

Data from the survey and case studies indicate there are five broad strategies utilized by state-level CISOs to advance their security programs. States are engaging in a common set of activities in relation to cybersecurity, but vary in the emphasis placed on each strategy. The strategies are:

- **Strategy One**: Development of policy and legal frameworks
- **Strategy Two:** Increased education of users
- **Strategy Three:** Use of technology and control mechanisms
- **Strategy Four:** Centralization of networks and IT services
- **Strategy Five:** Building collaborations across agencies, levels of government and between sectors

Strategy One: Development of policy and legal frameworks. One of the most common strategies is the development of cybersecurity policies and assessment tools. All the states that responded to the survey have implemented IT governance structures that include a variety of stakeholders as recommended by Heiman (2002). As CISOs have worked within their governance structure to develop policy they have often gained the buy-in of stakeholders as well as developed robust policy.

Many states have implemented standards or procedures which provide more specific guidance for the implementation of the cybersecurity policies that are in place. The use of more specific standards or procedures to implement policies provides the option for adaptation as technology changes without having to change underlying policy. Many states require regular assessments or audits to document compliance (or non-compliance) with cybersecurity policies, procedures, and standards.

CISOs noted the importance of these strong policy environments, since they shift the responsibility for cybersecurity and the responsibility for data protection to other agencies. This allows CISOs and their staff to approach agencies by offering assistance instead approaching them from a dictating compliance stance; security as a "service" then becomes possible. In a few states, these policies have the force of law, providing an even firmer base for the CISO to ensure compliance.

Excerpt from *Public-Sector Information Security: A Call to Action for Public-Sector CIOs*

(By Don Heiman, published in 2002 by the IBM Center for The Business of Government, available at www.businessofgovernment.org)

A Holistic Approach

Security involves more than *just IT.* Holistic security is about physical security, disaster preparedness, emergency response, and critical infrastructure protection. Security requires multi-level cooperation and coordination of military, law enforcement, and subject-matter experts. Security touches auditors, facilities managers, and maintenance workers.

Security management begins with the adoption of security policies that have legitimacy within the enterprise. Security policies come from a process that builds consensus among many key stakeholders. This includes elected officials and other policy makers as well as end users, government employees, and citizens. Security policies should embody standard practices that everyone in the organization must follow. These standard practices include an understanding of specific outcomes or goals the enterprise is committed to achieve. These goals are critical to security planning and critical to assessments about how well the organization protects its assets.

Once security policies and standard practices have been agreed upon, the organization is ready to conduct a security risk assessment. The assessment documents the "as is" and compares the "as is" to the standard practices embodied in policies. The comparison yields a gap. Gaps are important because they point to initiatives. These "gap closing" initiatives are prioritized and become a part of the enterprise's long- as well as short-range security plans. After the initiatives are implemented, audits should be done to make sure the gaps are closed and the standard practices are followed. These audits also help organizations stay compliant to policies and standard practices. In addition, security audits and standard practices are key to creating IT enterprise security architectures. These architectures include design principles for building highly integrated and secure IT infrastructures and applications. Also, standard practices, audits, and security "gap" analyses are critical for establishing IT performance metrics. In fact, the best way to determine if security gaps have been closed and stay closed is through the use of metrics.

Finally, intrusions and vulnerabilities should be closely monitored via automated and manual security technologies. Effective IT security cannot be managed with "guess-timates" or in an environment where responsible parties are too afraid to admit shortcomings. Once standard practices and metrics are in hand, the public-sector CIO is in a position to develop a compelling business case that points from the "as is" to the "to be" state of security, which will assure policy makers and stakeholders that security investments will be effective.

Many government systems provide essential services that touch citizens in a highly direct and personal way. These essential services are part of the nation's critical infrastructure. This makes IT security a key aspect of our nation's homeland security. Therefore, as metric data are gathered, it should be shared confidentially among the states and their federal partners. This will require a forum that fosters open sharing of case studies and lessons learned. We must develop a community of public-sector cyber-emergency responders to work with public safety, health, and emergency-management professionals.

Again, security done well is a way of life. For each of us to be secure, we must radically alter the way we live and the way we conduct our affairs. Radical—that is, fundamental—change is difficult because it challenges our traditional paradigms and our assumptions surrounding the way we live and work. Radical change for the ancient Greeks required a *metanoia*—a deep change of heart. September 11th made apparent the need to change our way of life, and the events of that day call us to a new epistemology—a *metanoia* that redefines what we mean by security and personal responsibility. Government leaders must set aside the "federated" cultures that foster agency autonomy and "my turf" thinking. We must share information, be more watchful, and become more disciplined in how we manage our affairs in community. We must also change our language about security. Security is more than "being safe." It is about justice and self-worth. It is about our dignity. Security is a way of life. This report will serve as a high-level guide for this new way of living.

Strategy Two: Increased education of users. All the states that participated in the study have active cybersecurity user education programs. These programs make full use of content shared nationally through CISO networks but also utilize content developed locally. Efforts to educate users are bolstered by more complex training programs for governmental managers who are would participate in decision-making during cybersecurity-related incidents. States are also engaging in exercises that provide practice with cybersecurity scenarios sponsored by the Department of Homeland Security. Additionally, states test the robustness of their technologies with a variety of means via white-hat processes.

Strategy Three: Use of technology and control mechanisms. The application of technical controls to assist in cybersecurity is common among the states. Initial approaches to network intrusion detection and prevention have been replaced by much more technically detailed ways of watching and identifying network traffic. Virtualization is providing a technical means of controlling data and access. Identity management systems are providing a means of implementing identification, authentication, and authorization schemas. Strong partnerships and outsourcing with private sector companies are assisting the states in improving their technical cybersecurity profiles.

Strategy Four: Centralization of networks and IT services. Centralization and consolidation of information technology services are also strategies utilized by the states. Projects are under way in California and Colorado as well as a number of other states. Centralization of networks and data centers is particularly helpful with cybersecurity efforts aimed at the protection of hardware, systems, and data. Savings from these projects is thought to help states become more cost effective in the delivery of IT services.

Strategy Five: Building collaborations across agencies, levels of government and between sectors. Dawes et al. (2009) write that, in order to successfully approach tangled problems, organizations need to create, lead, and participate in public sector knowledge networks (PSKNs) that are characterized not by a "need to know" information sharing environment but instead a "need to share" environment. Such networks treat the sharing of information and best practices as a primary purpose for existing and focus on sharing processes, practices, software, and other information technologies. Participating networks benefit from more timely, better quality, and more complete information by drawing on collective knowledge.

Within information sharing networks, some "elements of knowledge are explicit, formal, and embodied in easily accessible media or artifacts, and databases," while other elements are embedded in social context and more likely to be conveyed through practice (Dawes et al. 2009, 394). There is a broad array of information being exchanged by CIOs, CISOs, and their staffs within cybersecurity collaborative networks. Much cybersecurity planning information is explicit and is conveyed through policies, best practices, and standards, thus becoming codified. It is this type of information that is being freely exchanged across organizations and sectors. By contrast, a more dynamic environment exists for the exchange of threat information. The exchange of very current information concerning threats illustrates the sophistication of the cybersecurity collaborations. At the initial stages of identifying a security threat, the information that is exchanged is explicit, but has yet to be fully embedded in context. Questions as to the exact nature of the threat, the technical environments that are vulnerable, and the implications for systems and data are addressed as technical investigations yield results. Information begins with sketchy elements of data; then, through quick and dynamic processes of technical investigation and data exchange, threat information develops into explicit, embedded, and contextualized knowledge about the vulnerability, which then becomes relevant to a subset of players who have that particular vulnerability. The capability that the cybersecurity community has developed with data exchange in these systems is quite sophisticated.

Another aspect of knowledge networks is the challenge of bridging not only formal boundaries of organizations but also informal boundaries erected and protected by ideology and professional norms. This study shows the development of a community among CISOs firmly based on common need and practice, thereby demonstrating the value and efficacy of such cross-governmental collaboration. The development of professional norms within the cybersecurity community has created boundary-spanning

networks and capacities within and across the states (and local governments), which are successfully challenging more formal boundaries of government and jurisdiction. It appears the development of formal and informal networks as well as interpersonal relationships are now being deployed to overcome formal organizational boundaries. The development of these relationships is a key element in the successful approach to cybersecurity by the states.

Our study found that the state CISO community has formed and found great value from a number of knowledge networks. CISOs have built these networks both internal to their states (intraorganizational) and across levels of government and sectors (interorganizational). CISOs are spending significant time coordinating groups of IT staff from agencies within their states. In addition, CISOs are participating in a number of regional and national groups focused on the overall improvement of cybersecurity practice that include all levels of government (although Kansas appears to be unique given the heavy involvement of the higher education sector). Groups collaborating across sectors, both formally and informally, are also common.

Case Studies of State Strategies

California

The Person and Position

Mark Weatherford became the chief information security officer (CISO) of California in 2008 in the midst of widespread policy reform directed towards alleviating the state's pending $40 billion budget deficit. Where this fiscal environment would represent a formidable challenge for any top public manager, Weatherford has characterized the timing and urgency of these circumstances, among others, as a unique policy window of opportunity to affect meaningful reform for cybersecurity in his state, across other states, and at the federal level of governance.

In his position as CISO, Weatherford is primarily responsible for developing policy to ensure the security and confidentiality of the state's information assets. Appointed by the governor, Weatherford brings more than 20 years of experience in information security from his time in the U.S. Navy as well as the private sector and most recently his tenure as Colorado's first CISO. These experiences each afforded him the chance to create new policies and effectively adapt to implementation constraints while always keeping an eye towards future needs and strategic planning. These skills made him particularly compatible with California's goal to revolutionize government functions, especially those aimed at how information technology resources improve the relationship between California and its citizens.

The Strategy

To accomplish core organizational objectives, Weatherford engages in a number of policy-focused activities, including creating, vetting, and aligning security policies. Overall, policy development is a rather prescribed collaborative process involving a variety of IT stakeholders from other agencies. For example, Weatherford is developing new statewide enterprise information security policies. Working with a contract partner for the initial development, policy drafts were circulated to approximately 130

California At-A-Glance

Weatherford

Top Cybersecurity Official: Mark Weatherford, Chief Information Security Officer

Strategy: Development of a policy framework through blending entrepreneurship with collaboration

Overview of Strategy: Weatherford focused on policy development through policy entrepreneurship (in that he inventively gathers resources from a variety of sources and in a variety of ways) and collaboration. He works closely with the state CIO as well as with information security professionals at all levels of state and local government and in other jurisdictions to improve the security of California's information assets. He also engages in policy dialogues outside of his own operation, including multi-state and national arenas. His policy activities are varied; they include directly drafting policies as well as indirectly contributing expert opinion and consultation to legislative officials. He also works to align policies of his office with statewide objectives. Finally, he presents an example of how these policy activities are carried out in the context of multiple stakeholder demands, severe budgetary constraints, a polarizing political environment, and volatile cybersecurity threat landscape.

other information security personnel serving within state agencies most likely to be affected by proposed changes. In Weatherford's approach, many workshops are held to help departments understand rationales behind different proposals as well as to collect information on what departments need and expect from the state CISO and CIO. The opportunity to review and give feedback is highly valued by state officials.

Policy alignment is also important for accomplishing broader information security goals of the state. Until recently, there were administrative hurdles that hindered alignment of statewide IT policies and those dealing with information security, including limitations of security personnel in state agencies being in the direct chain of command with chief information officers. However, new legislation helped restructure the Office of Information Security more closely with the CIO. Now Weatherford can focus on how best to help state agencies with security issues in accordance with broader statewide goals of IT standardization for systems such as e-mail, data storage, teleworking, monitoring and detecting vulnerabilities, as well as developing social networking policies. Overall, Weatherford believes a collaborative IT environment is critical for consistency and that compartmentalization, while appropriate and necessary in some circumstances, is often used as an excuse to avoid sharing technologies and information.

Structural changes like these also align well with how Weatherford allocates managerial effort when communicating with the state's IT community. A significant amount of time is spent with the state CIO, agency-level CIOs, or information security officers (ISOs) from state agencies. Regarding the latter, it is important to understand their policy needs and concerns, and establish trust, responsiveness, and a professional community. As Weatherford notes, "My job is to help them do their jobs better, be a resource for them, market myself as an expert for support of what they need when they go before the legislature, and be their backup to help justify their issues and requests."[11]

Several actions support this charge, including regular monthly meetings to communicate security activities with the broader IT community in the state, quarterly meetings of security personnel to report and discuss new policies, and a quarterly CISO lecture series that features both public and private sector experts on a range of salient security-specific topics. Examples include cybersecurity solutions, dealing with hackers and phishers, information risk management, developing security metrics, disaster recovery, consumer protection, open source security tools, and assessing the evolving threat landscape.[12] These meetings and workshops are clearly informational but they also serve the purpose of assessing the status of state policies with a view to the following:

- Whether and how they should be developed, changed, or eliminated
- Advantages and pitfalls
- Feasibility for funding and implementation in the current fiscal and political climate

Policy activities are also directed outward, as Weatherford engages CISOs in local governments and other states and at the federal level. While Weatherford confirms that informal communication among multiple states' CISOs is an important component to information security governance, many interactions are formalized through voluntary organizations, in particular the Multi-State Information Sharing and Analysis Center (MS-ISAC)[13] and the National Association of State Chief Information Officers (NASCIO).[14] Weatherford has served in advisory and leadership capacities within these organizations, often lending expertise to help lay out policy direction and facilitate the diffusion of workable information security policies across state and local boundaries. Weatherford is also able to influence national level discussions on the role of cybersecurity officers, as these voluntary organizations coordinate information and policy with officials at the Department of Homeland Security.

Colorado

The Person and Position

Seth Kulakow, Colorado's chief information security officer since November 2008, is a believer in both technology and centralization in his approach to cybersecurity. The power of that combination has the potential to make a substantial difference to the cyber safety profile of the state of Colorado, moving it to a mature cybersecurity organization. His vision of technology allows easy and cost-effective compliance for agencies and governmental organizations in the state and is on its way toward implementation. He has

Colorado At-A-Glance


Kulakow

Top Cybersecurity Official: Seth Kulakow, Chief Information Security Officer

Strategy: Centralization of networks and IT services

Overview of Strategy: The Colorado focus on centralization and the use of technology to address cybersecurity issues provides an example of a more technology-focused strategy. While a comprehensive program is in place, the emphasis of the Colorado Office of Cyber Security is to provide easy, inexpensive solutions to the entire state along with the ability to gather data to assess environments with a cross-agency statewide capability. While it is clear that not all states are able to achieve the consolidation of IT services that Colorado is implementing, Kulakow points out that the use of technical tools to look across technical environments together with security metrics devised from standards have the potential to move governments to a mature security environment.

plenty of backing from CIO Michael Locatis and from Governor Bill Ritter in his quest to execute his vision.

The CISO position is defined by state law.[15] The statutes also outline a full program for cybersecurity for all three branches of government, leaving out only higher education. A comprehensive set of policies[16] back up the law and provide specific guidance for state agencies and organizations on cybersecurity issues. Kulakow is putting into place a comprehensive vision for security, a plan that utilizes multiple standards to move forward in security issues. The plan is uniquely presented in visual format in a VISIO diagram. It begins at a foundation level, outlining all the requirements which are needed for any program and then builds to a policy and procedure level. Three additional layers of analysis are added: interior, exterior, and repeatable actions. This defense-in-depth process then moves to a spreadsheet format for analysis of priorities and cost. This approach provides a comprehensive view of cybersecurity investments and accomplishments across the state.

The Strategy

This strong policy foundation allows Colorado's Office of Cyber Security (OCS) to focus on assisting the agencies and governmental organizations to comply with the law and policies. An important part of this focus is on removing risk from the local environment. As Kulakow notes, "If you look at it as a threat, when you have determined the risk to the organization, the best way to mitigate that risk is to not hold onto that risk. So if you can put that risk off to someone else who is ready to obtain it and take it and make it work, it makes sense."[17] Thus, his goal for the OCS is creating a pathway to execute a mature security program. That pathway includes consolidation of IT services and offering cost-effective standard solutions.

Strong support from the governor and the CIO on cybersecurity issues has been important in the development of the cybersecurity program in Colorado. The development of a statutory framework and a plan for cybersecurity was complemented by the work of CIO Michael Locatis on the initiative *Colorado Consolidation*. This initiative to consolidate information technology services in the state came first through an Executive Order and was then codified in state law (Centralize IT Management In OIT, Colorado Revised Statutes, 2008, §24-37.5-401-404).

The State of Colorado Consolidation Plan (C2P) called for "centralized information technology management, purchasing, spending, and planning" and its goal, now nearing completion, is to "create a statewide enterprise structure compared with today's department-by-department model" (Governor's Office of Information Technology 2008, 6). The consolidation of services and the implementation of enterprise solutions is a key factor in the Colorado security strategy. Kulakow notes, "[W]hen you have 30 years of inefficient silos of IT—as most states have—and IT staff who have worked in that environment for between 10 and 20 years, there can be a lag in technology. In addition, the involvement of so many contractors with so many pieces of software delivering single solutions, it presents a complex challenge."[18] However, if a security program can provide enterprise solutions delivered over a common network, consolidation can save money. This dual emphasis on consolidation of services and providing cost effective enterprise solutions is bearing fruit in the Colorado environment.

With strong policy infrastructure, a common network, and solid administrative support, Colorado's

leaders are able to move forward to address cybersecurity issues. Kulakow notes, "[A]gencies can see the gains of not having a silo and not having to worry about their data; it streamlines the overall operational functions of the agencies. For a silo department to do the entire security program with so few people, it is really unachievable."[19]

The consolidation strategy leads to cost savings that can be invested in sharing technology across the entire state and with other states. Further, this centralization creates an approach that makes extensive use of technical tools. The Colorado OSC has taken advantage of low cost and free automated tools to provide detailed metrics about the Colorado security environment. Using a combination of NESSUS scanner software[20] and the audit tools[21] of the Center for Internet Security, a nonprofit organization that provides resources for measuring information security, it is possible to gather data on all Colorado systems in the executive branch in a cost-effective way. Kulakow makes the argument that open source and other widely available tools such as these provide the opportunity for all governmental organizations to make a major leap toward "a truly mature security organization."[22]

Delaware

The Person and the Position

Elayne Starkey, chief security officer for the State of Delaware since 2005, is responsible for protecting Delaware's information assets from high consequence events, including cyber and physical terrorism and disasters. A large part of her job is educating her peers and customers about ways to prevent, detect, and respond to these events. Starkey's position was created in response to the growing need in Delaware State Government to provide a governance structure for information security, disaster recovery, and business continuity. She hit the ground running, quickly implementing a number of education and awareness initiatives intended to foster an enterprise-level climate of ownership and accountability for the confidentiality, integrity, and availability of information assets.

While Starkey acknowledges that strong IT skills are a must, she says that basic business and communication skills are also important for chief security officers: "We have to influence decisions and projects that aren't always under our span of control. We need to establish relationships with our peers throughout state organizations and make sure they understand the importance of security." [23]

Delaware At-A-Glance


Starkey

Top Cybersecurity Official: Elayne Starkey, Chief Security Officer (CSO)

Strategy: Increased education of users on the importance of information security

Overview of Strategy: CSO Starkey focused on collaboration and education. Her team uses a number of techniques and tools to point out risks and educate both internal customers and citizens about the risks they face and the cybersecurity techniques they can implement to protect their data. Her office developed a white paper to outline their key targets and metrics.

The Strategy

Starkey uses a number of techniques to remind state employees about the importance of protecting citizen data. Her team publishes a monthly newsletter, hosts training classes, offers policy interpretations, and manages a successful "Latrine Poster Campaign." Every few months, Starkey's office publishes posters that are placed in restrooms throughout the state. The campaign is a lighthearted attempt to get the message about protecting information across in a place where people are likely to stop and pay attention. The campaign, together with other programs, has raised awareness about the importance of information security throughout the organization.

The educational efforts of Starkey's office extend to other citizens of Delaware, as well as state employees. During Cyber Security Awareness Month, her team visits schools and holds assemblies for children to educate them about how to stay safe online. Her office has sponsored travelling billboards on state transit buses, warning citizens about the potential dangers when they go online. Starkey acknowledges that IT staff is not always the best at marketing and business communication, so she taps into the marketing expertise in her department to add a creative flair to the communications.

One of the largest events that Starkey's office hosts each year is an exercise simulating a real world cyber attack on state resources. This year's exercise, nicknamed "Cyber Siege," is the fifth consecutive cybersecurity exercise in Delaware. The exercise planners work closely with the Department of Homeland Security (DHS), and use DHS-endorsed tools and best practices. Delaware participates in regional and national level exercises as well, including "Cyber Storm II" in 2008. This large-scale national exercise simulated a combined cyber and physical attack that escalated to a level requiring a coordinated federal response.

Delaware was also involved in a 2009 exercise, "Defend the Flag," sponsored by DHS and the Multi-State Information Sharing and Analysis Center. Several states participated, attending training on hacker techniques followed by an all-day melee-style competition, where teams split their time between attacker and defender roles. Starkey's team brought some of the ideas back to Delaware and tweaked them to meet the needs of the state. She admits she does not like to focus on fear tactics to get attention on this topic; rather, Starkey helps her customers become aware of the potential implications of a security breach, which in turn facilitates cooperation with her office.

Whenever possible, Starkey taps into resources at the state and national levels. She also pays attention to what other organizations are using as her office has limited resources for developing new material, and she "does not want to reinvent the wheel. A lot of our education materials and ideas depend on what is available and what other states are doing. We borrow ideas and make them unique to Delaware. We share and give credit where we can." [24]

Starkey's educational efforts have been recognized internally, by professional groups, and by the media throughout the state. Both *The Dover Post* and *State Tech Magazine* recently ran stories about her program. And Security Squared covered her contributions on a panel, "Securing the Weakest Link: Cybersecurity Education and Awareness," at the 2009 annual conference of National Association of State Chief Information Officers (NASCIO)[25].

Although Starkey's team spends a lot of time focusing on information security education and awareness, they also take time each year to educate themselves about the current security posture of their customers. They survey all state organizations and deliver back to each a "security scorecard." The scorecard provides a numerical rating for each office, measuring its level of compliance with security policies. It also offers information about how each office is doing relative to its peers. Starkey and her team use the results of the survey to prioritize policy goals for the coming year and communicate with staff in various offices about their own implementation goals.

Kansas

The Person and the Position

Larry Kettlewell, the chief information technology security officer for the State of Kansas since 2001, brings a varied background to the performance of his duties as the lead official responsible for policy and governance oversight for information technology security in all three branches of Kansas state government.

His background in the Army Signal Corps and the Central Intelligence Agency provides him perspective on information technology security as a human intelligence issue. His study of Chinese provides him with a broad international perspective, increasingly relevant to today's cybersecurity landscape. And, having spent time as a staffer in the U.S. Senate, he is well-versed in the political sensitivity and coalition building required to be effective in moving policy forward in new, networked governance structures.

Kettlewell's background illustrates the broad skill sets needed for the successful CISO. Technical, political, policy, and managerial skills combine to provide the CISO the confidence and agility required to respond to each day's issues. In the course of a busy day, the CISO is called upon to move seamlessly from discussing highly technical network protocols with a security staff member, to discussing a citizen phone call with the governor's chief of staff, to reviewing a policy white paper on an emerging security concern, to discussing an important legal issue with the attorney general's office. These activities comprise a typical day for Larry Kettlewell and other CISOs who serve smaller states.

The environment of a smaller state not only results in a broader range of responsibilities for the CISO,

Kansas At-A-Glance


Kettlewell

Top Cybersecurity Official: Larry Kettlewell, Chief Information Technology Security Officer

Strategy: Building collaboration through governance mechanisms

Overview of Strategy: In Kansas, the governance model provides a framework for collaboration across a broad set of stakeholders in the IT environment, and it is the relationships that really pay off for the state. As in Washington State (discussed below), the development of relationships where trust is established through consistent communication is a key factor in dealing with daily cybersecurity issues. In the security field, over time and through working on various problems or incidents, a circle of "trustees" is developed. Once established, these relationships can last years and are invaluable in dealing with the insignificant-to-critical issues that the enterprise faces on a daily basis. Daily communication and coordination with this circle, and indirectly with the trustees' circle of contacts, brings significant expertise to bear on almost any problem.

but also requires finding ways to share expertise and skill sets across the information technology community; with fewer staff in the information technology security office, sharing expertise is vital to success. And, given the importance of sharing skills sets, information technology governance takes on even more importance as it plays a role in promoting collaboration.

The Strategy

Like other states, Kansas has implemented an information technology governance process that attempts to bring together actors from all three branches of government. However, potentially unique to the Kansas model is the broad reach in that it involves all state governmental sectors, including education. This also leads to broad collaboration for cybersecurity. As Kettlewell notes, "[T]echnology is rapidly overrunning our laws and, more importantly, our government structures,"[26] making constant communication and coordination important. The Kansas answer to this challenge is to place a dual focus on technology and policy with the two working together across all governmental sectors.

The foundation of IT governance in Kansas is the Information Technology Executive Council (ITEC). The council "is responsible for approval and maintenance of all information technology policies, IT project management procedures, the statewide technical architecture, and the strategic information management plan," that is, the overall strategic management and planning of the Kansas IT operation (www.da.ks.gov/ITEC/). Seventeen members serve on the council, representing eight areas of government:

- The governor is represented by the secretary of administration.
- Agencies are represented on the council by two cabinet-level agency heads and one non-cabinet agency head, ensuring the perspective of smaller state government agencies.
- Financial issues are represented through the inclusion of the director of the budget.
- The judicial branch is represented by the judicial administrator of the Kansas Supreme Court and the judicial chief information technology officer.
- The Kansas legislative branch is represented by the legislative chief information technology officer.
- Two tiers of education are represented on the council; the commissioner of education represents K-12, and higher education is represented by the president and CEO of the Kansas Board of Regents. Local government is represented by city and county representatives.
- There are representatives from the private sector, in this case three individuals who are either CEOs or CIOs.
- The executive director of a separate organization (the Information Network of Kansas or INK), which advances e-government within the state, is also included in the Council.

The Information Technology Advisory Board (ITAB) supports the work of the broader policy ITEC group. It is empowered by state law to advise the executive branch CITO as well as "adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state agencies." (K.S.A. 2005 Supp. 75-7203 and Kansas Information

Technology Policy 3100) The board comprises senior managers of state information technology organizations (mostly CIOs) along with representatives from private industry and local units of government. The current list of members shows involvement from state agencies, the legislative branch (including legislative post audit), the judicial branch of state government, the state division of information systems and communications, K-12 education, all the state institutions of higher education, local government, and law enforcement (such as the Kansas Bureau of Investigation). The broad array of collaborators provides a forum for the development and refinement of information technology policy, including approaches to cybersecurity.

The governance model in Kansas also utilizes a number of specialized offices that provide support to the ITEC. These areas include enterprise architecture, e-government services, identity management, project management, and GIS. Joining these offices is the Information Technology Security Office (ITSC). An Information Technology Security Council reports directly to the Executive Council and "recommends and reviews policies, guidelines, and best practices for the overall security of information technology systems, infrastructure and data within Kansas state government."[27] Similar to the other governance groups in Kansas, the Security Council has broad participation from the Kansas governmental community. Besides the functional agency involvement, there is strong representation from legal and law enforcement agencies (Attorney General's Office, the U.S. Secret Service, the Kansas Bureau of Investigation, Department of Corrections, the Juvenile Justice Authority, and the Highway Patrol). Also present is the education community, both K through 12 and higher education.

The significant involvement of the higher education community is an important component of the Kansas approach and represents the fulfillment of the strategy of reaching out to build on all IT assets in the state. Higher education IT personnel have been heavily involved in the formation of cybersecurity policy and in security awareness and training programs. The Security Council has successfully constructed policies dealing with security and awareness training and in other far-reaching areas. The council has recommended and ITEC has approved such policies as computer incident response, the companion reporting protocols, and media sanitization.

Perhaps the Security Council's most significant program is the annual security self assessment for agencies and departments in the enterprise. The assessment is based on standards promoted by the National Institute of Standards and Technology. A newly revised enterprise security policy, which meshes with the security self assessment tool, will be finalized this year. In a parallel development, the State of Kansas has recently engaged in preliminary discussions with the Department of Homeland Security, National Cybersecurity Division, to examine the direction of a national assessment framework. The General Accounting Office's Report to the U.S. House of Representatives (October 2009) identifies the need to conduct cybersecurity assessments at all levels of government by June 2011. While the Kansas Department of Emergency Management focuses on more common natural and other disasters, cybersecurity remains an important topic for this agency, and, as such, monthly coordination meetings and informal contacts are the norm. Recently, informal inclusion into the state's Intelligence Fusion Center has begun.

New York

The Person and the Position

William Pelgrin is chief cybersecurity officer for New York State and director of the State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC). He has served in this capacity since 2002. Pelgrin has more than 26 years in government service, during which he has maintained a long-standing belief in the value of building partnerships to accomplish organizational goals: upward with federal officials; outward with other internal agencies, states outside of New York, and the private sector; and downward to local and municipal officials. As chief cybersecurity officer for the state, he is a peer to the CIO. Both serve at the pleasure of the governor, and are structurally located at the cabinet level of administration.

The genesis of Pelgrin's role as a security official predates September 11, 2001. Before the terrorist attacks, Pelgrin was New York's chief technology officer, charged with developing an enterprise view of technology for the state and identifying the need for security measures to support the growing e-commerce environment. During this time he was recognized for his commitment to make "programs the driving force

New York At-A-Glance


Pelgrin

Top Cybersecurity Official: William Pelgrin, Chief Cybersecurity Officer

Strategy: Building collaboration through networking and upward, outward, and downward leadership

Overview of Strategy: New York State's cybersecurity strategy is guided by a philosophy of partnership and networking in all directions: upward towards federal officials; outward with state level agencies, multiple state security officials, and the private sector; and downward towards local and municipal governments. Additionally, the strategy includes leveraging a number of venues and interactions to institutionalize a view of cybersecurity which accounts for core competencies beyond those driven narrowly by technology.

of decisions" rather than being strictly beholden to "technical" aspects of problem solving. Pelgrin recalls the shift in focus after the terrorist attacks: "We all began reflecting on how 9/11 impacted us, and impacted me as a government official; I really wanted then to have a more dedicated focus for cybersecurity."[28] This vision manifested in a new cybersecurity and critical infrastructure organization for the state.

The Strategy

Pelgrin attributes early success in cybersecurity operations to employing a collaboration model from the onset. He notes, "We always had the attitude of partnerships that resonated with people, resulting in a statutory agency dedicated to cybersecurity for the state separate from daily operational activities."[29] Thus, the CIO was able to manage IT operations while Pelgrin addressed highly specialized needs of security and critical infrastructure.

There are five main communities with which Pelgrin engages in partnerships and networking:

- The political and administrative communities within state government
- The private sector
- The multi-state cybersecurity community
- Local and municipal governments
- Entities at the federal level

Snapshots of each demonstrate an overall preference for a proactive versus *ad hoc* approach to building connections and trust, as well as for institutionalizing a view of cybersecurity issues beyond traditional problems of technology.

First, the CSCIC has established credibility with executive and non-executive agencies by offering help in diagnosing compliance with statewide information security policies and laws while also working together with agency-level information security officers to develop remediation plans. This is most evident in the implementation of a compliance reporting system that provides performance information to state agencies on where they stand, a kind of dashboard analysis. Unlike the backlash that frequently accompanies such reporting schemes, Pelgrin and his team have taken great strides to "note the reporting process is not about blame, but rather how we can collectively work together to improve the state's cybersecurity environment."[30] Pelgrin's collaborative approach has made this voluntary reporting effort itself very successful, but more importantly it has led to more effective implementation of information security policies by agencies across the board.

Second, this "collaborative philosophy" has also been a guiding principle when partnering with the private sector. Whereas many information security officials are only now considering whether and how best to collaborate with the private sector, Pelgrin's team, in collaboration with the State Office of Homeland Security, has led a Public/Private Sector Cyber Security Workgroup since 2002. This workgroup takes advantage of the diversified skills and knowledge of its members to "identify and assess vulnerabilities and determine appropriate mitigation strategies."[31] Partners include representatives from the telecommunications, utilities, higher education, public safety, and financial sectors among others. Sector subgroups participate in monthly conference calls to exchange information, and all workgroup participants convene quarterly using webcast technologies.

Third, Pelgrin maintains that a "principled" approach to cybersecurity should reflect a collective mindset as well as recognition of the boundary-free nature of cybersecurity problems. The impetus for reaching out to surrounding states by way of the original Northeast State Homeland Security

Directors' Consortium to create the Multi-State Information Sharing and Analysis Center (MS-ISAC) is one outcome of this mindset and approach. Pelgrin notes, "I believe the collective view is more powerful than the singular view when developing a structure that can protect the whole perimeter," and to do so requires "an understanding with the governor that my responsibilities are broad and my position knows no geographic or political boundaries."[32] With his success working for five governors, as well as leadership and advising of the MS-ISAC, Pelgrin has convincingly merged his understanding of policy demands with the tools of collaboration to respond effectively to his mandate.

Fourth, Pelgrin and his team have been involved in helping other state agencies and local governments understand the dynamic nature of cyber threat environments. They anticipate and respond to requests for help with training, policy direction, and best practices on matters ranging from basic knowledge of cybersecurity solutions to managerial strategies on how to leverage limited personnel, fiscal, and time resources to serve cybersecurity goals. Pelgrin believes these activities serve the statewide mission of achieving cyber readiness and resilience. The work products which help institutionalize cybersecurity as an issue of both management and technology to these various communities include monthly newsletters, a magazine-type guide covering contemporary issues in jargon-free language, regular meetings to receive input on agenda-setting from state and local governments, and working together to define acceptable, workable, and effective "deliverables" to get the job done.

Fifth, in an effort to further institutionalize these values and philosophic approaches to cybersecurity, Pelgrin contributed as a subject expert to the *Comprehensive National Security Strategy for Cyberspace*, a proposal which helped advise the presidential transition team in 2008 (CSIS Commission on Cybersecurity 2008). Similar principles permeate the *White House 60-Day Cyberspace Policy Review*, in which Pelgrin participated directly (White House 2009). The report points to the MS-ISAC as a resource that should be leveraged by the federal government. Additionally, Pelgrin was one of five individuals invited by the White House to participate in a videotaped message discussing cybersecurity and the Administration's approach. The video was made available the day of the President's release of *60-Day Review* and remains online at http://www.whitehouse.gov/CyberReview.

Washington

The Person and the Position

Agnes Kirk has served as the State of Washington's chief information security officer since 2005. The Washington CISO works with a broad range of state agencies to secure the state's IT assets and data. Kirk's responsibilities include:

- The delivery of statewide security services
- Shaping the statewide security strategic direction
- Influencing policy development
- Managing statewide incident response
- Coordinating the state's participation in national cybersecurity efforts
- Representing the state in a variety of professional collaborative groups and meetings

The Strategy

Washington has a robust policy for cybersecurity which is approved by a statewide Information Services Board and implemented through standards and guidelines. Some controls are centrally provided to everyone while others are implemented by agencies according to their needs and risk assessment. Information Technology Security Policy Standard Compliance Audits are required at least once every three years. In addition to this solid policy and compliance foundation, Jim Albert, DIS deputy of operations, cites the single network infrastructure and the development of security architecture for the entire state as important security assets.

Washington matches these policy and technological approaches with educational and collaborative approaches to cybersecurity. A key focus is building relationships both within the state and with regional and national cybersecurity-related personnel and organizations. "It is really about awareness at all levels," Kirk notes, "It is providing visibility of what happens when security is not incorporated into the business processes."[33]

In Washington, the stakeholders within the agencies are regularly engaged with the CISO. The approach is

Washington At-A-Glance


Kirk

Top Cybersecurity Official: Agnes Kirk, Chief Information Security Officer

Strategy: Building collaboration with the private sector by developing relationships to serve business needs.

Overview of strategy: Awareness of cybersecurity issues within state agencies is seen as a key first step in ensuring that the resources of the CISO and staff are productively utilized. Recognizing the expertise each party brings to the table is an important part of the process. Marrying business expertise to cybersecurity expertise allows the state to find the best solutions to the inevitable tension between business and security needs. The consistent communication within the group helps maintain the relationships built through the work on business problems.

The broader collaboration across the Northwest uses these same keys in a looser "participate as your needs dictate" organization. The consistent communication and respect for individual expertise brought to the table provides the basis for the collaboration which can then be called upon during stressful incident times. These approaches to collaboration reflect the principles that have been found to be successful by public sector researchers. The State of Washington is an example of effective cybersecurity collaboration.

for security to be an *enabler* of business processes and to build partnerships between agency stakeholders and the CISO. Rather than just saying "no" to technology requests, relationship-building is used to reach a common goal of providing services to the public while appropriately protecting personal or sensitive information.

To help achieve this, there is a statewide Security Council which involves all state agencies. The council is made up of security leads from all state agencies with representation from local government and higher education. Each security lead is responsible for security and incident response within their agency, for coordinated controls implemented consistently across the state's enterprise, and for working in a collaborative fashion during a statewide incident. The members also participate in statewide cyber exercises; the most recent was held in October 2009. There are also monthly meetings with agenda items ranging from work sessions on specific topics to presentations by both members and vendors on emerging threats and mitigation strategies, to new technology discussions. According to Jim Albert, agencies are motivated to participate in the work of the council because of the value they see in information sharing; he notes, "[M]ost people want to play offense, not defense."[34]

A Council Steering Committee also meets monthly and makes recommendations about security-related projects the council undertakes. Examples include:

- Working with staff from the Information Services Board on developing guideline documents to assist agencies in implementing the newly adopted IT Security Standards
- Participating on evaluation teams for security-related products and services
- Providing speakers at security forums

In addition to working within the state agencies on cybersecurity issues, collaborative relationships have also been built with a broader community of cities, counties, and private sector organizations in the geographic area. The Pacific Northwest CISO group meets on a regular basis, both face-to-face and also via conference calls. This group is made of more than 65 public and private CISOs from a cross section of industries, including health care, insurance, retail, manufacturing, service, telecommunications, and higher education, as well as school districts, cities, counties, and the state. By design, this loosely affiliated organization does not include the vendor community. This venue has been very successful in promoting open communication among the members on issues/challenges, breach information, and requests for assistance during incidents, as well as sharing policies, processes, and recommendations.

The strategy reflected in the Washington approach focuses on relationship building within state government and more broadly with local government and private organizations as a key to cybersecurity. These relationships require: (1) building awareness, (2) respecting the expertise that each party brings to the table, and (3) building trust through interpersonal communication.

Recommendations

This review of the cybersecurity landscape at the state level provides a broad picture of both strategies used to build successful programs and the activities of the CISO. From our research, we draw the following five key recommendations.

Recommendation One: State cybersecurity officials should increase the use of collaboration and networks.
CISOs should manage cybersecurity, in part, by identifying, mobilizing, participating in, and helping maintain public sector knowledge networks relevant to cybersecurity issues. CISOs and CIOs should recognize that the base of these networks is the development and preservation of interpersonal relationships, not a command and control perspective.

Information sharing across boundaries has become the norm for CISOs despite the requirement that sharing information requires spanning a number of state bureaucratic boundaries. By recognizing a shared responsibility, CISOs have created, participated in, and led robust public sector knowledge networks (Dawes et al., 2009). The sharing of technical knowledge is embedded in the professional culture in information technology (through the open source movement) and appears to have been adapted further by the CISO community. While coming from a variety of backgrounds, CISOs have formed a strong professional culture, language, and perspective on the use, exchange, and protection of information.

These networks are both formal and informal and comprise the development of trusted interpersonal relationships between CISOs across states and with IT staff working on cybersecurity issues within states. Chief information officers should focus on the continued development of these networks. Key activities that should be supported include:

- The free exchange of information within CISO networks firmly rooted in values of privacy, appropriateness, and professionalism
- Further definition and institutionalization of approaches that work for different state environments (small versus large jurisdictions, policy-focused, collaboration-oriented, etc.)
- Building and funding cross-state interaction between CISOs through a variety of communication mechanisms
- Investment in building and maintaining these networks as a goal in and of itself, not just for the achievement of specific projects across states

Recommendation Two: State cybersecurity officials should evaluate their formal and informal relationships with federal cybersecurity officials.
In an effort to build on networks as discussed in Recommendation One, CISOs and CIOs should identify authority or status barriers between themselves and federal cybersecurity officials. Managerial efforts should then be directed towards removing, or mitigating, barriers most likely to impair bottom-up participatory governance by states regarding national cybersecurity programs.

CISO collaborations are undertaking important work across sectors (public, private, and nonprofit) and across levels of government (federal, state, and local). An example that is yielding results and providing a means of consistent communication across sectors is the Multi-State Information Sharing and Analysis Centers (MS-ISAC). Importantly, these collaborations focus both on the development of relationships and

the accomplishment of tasks; the literature has shown that both activities are important precursors to the development of successful networks (Dawes et al., 2009). The development and maintenance of expanded networks should include a variety of strategies and modes of communication to ensure that the trusting, information-sharing relationships remain strong.

This report demonstrates that while state approaches vary, there is a common core of responsibilities and strategies for cybersecurity. The CISOs interviewed all expressed the desire for a closer collaborative network with federal actors and for federal leadership based on knowledge gained in the states concerning successful approaches. Some CISOs believe that standards and protocols should comprise the majority of these discussions; others believe that more trusted network approaches are most important. While the authors do not believe that there is consensus within the state-level CISO community as to the approach, there is clear consensus about the need for more and stronger relationships among state CISOs, CIOs, and the various federal agencies working on cybersecurity issues.

Recommendation Three: State cybersecurity officials should devote increased attention to and receive training in multidisciplinary problem solving.
Cybersecurity management requires a practical philosophy of multidisciplinary problem-solving. The development of networks across security disciplines (cybersecurity, emergency management, critical infrastructure, information fusion centers, etc.) is critical for the continued success of cybersecurity efforts. Broadening CISO networks should be a priority for CISOs and CIOs.

The state cybersecurity community is now on the cusp of adapting and making potentially important and unique contributions to homeland security work. The challenge is whether the current professional culture that now exists within the cybersecurity community will mitigate the development of broader collaboration with those involved in homeland security-related functions. Professional cultures create boundaries; in this case information is embedded in the language of information technology and may not be easily extracted and shared with partners from the other disciplines—law enforcement, emergency management, military—involved in homeland security activities. As Dawes et al. (2009) point out:

> For information systems, the knowledge wrapper that holds the logic of data structures, definitions, collection methods, processes, and interpretive schemes is unique to the organizational setting in which it was created. This knowledge may be poorly documented and distributed in ways that make it difficult to aggregate and share (396).

Research indicates that such cultural accommodation among homeland security players will be an important step in making true collaboration possible. Research on network development (Pardo et al., 2009) indicates that the development of specific projects within small but cross-discipline networks has the potential to build trusting relationships and expand the reach of the cybersecurity community out to the broader security community. Ensuring that the diversity of participants' perspectives is recognized will be an important element in the successful cultivation of these networks.

Recommendation Four: State cybersecurity officials should receive training in collaboration competencies and those competencies should be recognized and rewarded.
Education programs for the CISO community should be focused on collaboration skill sets, beyond those technical in nature. Collaboration competencies among CISOs should be incentivized, recognized, and rewarded by CIOs.

While technical education remains important, the CISO role has grown far beyond technical management of cybersecurity tools. States should modernize the philosophical approach to cybersecurity management. At the core of effective CISO skills and competencies is a philosophy that cybersecurity problem solving is more than an exercise in technical proficiency. State CISOs themselves identify non-technical skills as particularly important, including collaboration/conflict management, communication skills, and political skills.

Given that approaches to cybersecurity are generally collaborative in nature, to be successful a CISO must possess and deploy competencies of collaboration

relevant to the task at hand. While CISOs recognize the strong need for non-technical skills, it is important to focus such skill development on those areas which hold the most promise for success at collaboration. As noted earlier, Getha-Taylor's (2008) study of successful collaborators found that interpersonal understanding and teamwork/cooperation were the most important to their success. Yet the development of these skills, which appear to come with experience and maturity, may be less likely to be encouraged than more tangible technical skills. The development of these skills, and the trust within a collaborative network that goes with them, is an important goal in and of itself if long-term collaborations are to be built within the cybersecurity community.

Recommendation Five: State cybersecurity officials should devote increased attention to data management.
CIOs and CISOs should build collaborations with data owners, records managers, and archivists in the development of more robust data management within the states.

The concept of data management did not emerge as a major focus for the state CISOs. This report, however, shows that state governments are now moving beyond a merely technical control approach to security work to a focus on the importance of gaining the cooperation of technology users and the development of effective business processes. As noted earlier in this report, some CISOs believe that the defined network perimeter has dissolved and that the future of cybersecurity is a focus on data management (Aul, 2009). Additionally, the current emphasis on governmental transparency has required that states delineate what data are to be shared and what data are in need of protection.

A focus on the management of data within government organizations is not new; most states have record definition statutes and retention schedules. However, the investment of resources in these programs has varied by state and agency. It appears that the current environment of cybersecurity will provide an opportunity for states to refocus on these efforts as a necessary part of narrowing the zone of protection of state assets.

Appendix I: Excerpts from *Essential Body of Knowledge*

The *Essential Body of Knowledge* includes 14 areas:

- *Data Security*: policies and procedures to ensure confidentiality, integrity, availability, and privacy of data
- *Digital Forensics*: knowledge and techniques of digital investigation
- *Enterprise Continuity*: policies and procedures to ensure enterprise business systems function
- *Incident Management*: processes to prevent, detect, contain, eradicate, and recover from IT security incidents
- *IT Security Training and Awareness*: methods utilized to raise awareness of and educate users about IT security
- *IT Systems Operations and Maintenance*: policies and procedures to maintain, monitor, control and protect IT infrastructure, systems and applications
- *Network and Telecommunications Security*: policies and procedures ensuring security of network and telecommunications devices and software.
- *Personnel Security*: controls to ensure proper personnel selection and the prevention and detection of employee-caused security breaches
- *Physical and Environmental Security*: methods of protecting physical facilities from natural or man-made threats
- *Procurement*: policies and procedures required to plan, apply and evaluate the purchase of IT products and services
- *Regulatory and Standards Compliance*: policies and procedures that enable an organization to meet information security laws, regulations, and standards
- *Security Risk Management*: policies and procedures used to identify and assess risks and balance with costs of mitigating the risk.
- *Strategic Security Management*: practices and methods involved in making managerial decisions in relation to IT security planning
- *Systems and Application Security*: policies and procedures to integrate information security into IT system development

The *Essential Body of Knowledge* assigns the primary responsibility for most of these roles to the chief information security officer and assigns supporting roles for others.

Source: *Department of Homeland Security National Cyber Security Division. 2008.* Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. *Office of Cyber Security and Communications: Washington, DC.*

Appendix II: Study Methodology and List of Participating States

This study relied on a mixed methodology framework. Utilizing semi-structured interviews and an online survey, the researchers mixed qualitative and quantitative approaches to provide in-depth information about chief information security officers (CISOs) at the state level.

Pre-Survey Interviews

The study began with pre-survey interviews conducted in the summer of 2009. These interviews focused on strategies CISOs used to establish their credibility and implement policies as well as information about CISOs' backgrounds and positions. The researchers reached out to a mix of large, medium, and small states for pre-survey interviews. The interviews were semi-structured and conversational in tone. The flexibility of the semi-structured format allowed the CISOs to focus on what they felt was most important for their positions. All interviews were conducted via telephone and all were transcribed and analyzed by members of the research team.

Online Survey

Preliminary findings from the pre-survey interviews were used to complete development of two online surveys: one for CISOs and one for CIOs. The surveys were constructed using information on the CISO role from a previous study two of the authors conducted on CISOs in the higher education community, the Department of Homeland Security *Essential Body of Knowledge*, and outlines of parameters for successful collaboration from public administration literature. The CISO survey focused on the background, credentials, and strategies used to implement policies and collaborations. The CIO survey focused on security planning and strategies used to implement policies and collaborations. The researchers established an informal network of CISOs and practitioners from leading professional organizations to assist with pre-testing the survey. In addition to invaluable feedback concerning the survey's questions and length, these individuals also helped spread the word about the survey in the cyber security community. The assistance of the National Association of State Chief Information Officers (NASCIO) was particularly helpful. Initial e-mails inviting CISOs to complete the online survey went out in late summer 2009. The survey remained active until late fall 2009. Survey data were gathered from 25 states.

Follow-up Interviews

At the conclusion of the survey, CISOs were asked to volunteer to be a part of follow-up interviews. The protocol for these interviews was established from preliminary results of the survey. Like the pre-survey interviews, these were semi-structured and conversational in tone; they took place by phone and included a mix of large, medium, and small states. Additionally, interviews included states that have both long and newly established CISO positions. The follow-up interviews allowed CISOs to expand on responses they provided in surveys, focusing on: strategies they use in establishing their credibility and performing their jobs, and formal and informal collaborations they participate in.

The researchers chose six states to highlight in case studies in the report. All quotes and cases were approved by the CISOs for use in the report.

Table A.1: Participating States

	CIO Survey Participants	CISO Survey Participants	Interviews (all CISO, except as noted)
Alabama	X	X	
Arizona		X	
Arkansas	X		
California		X	X
Colorado			X
Delaware			X
Georgia		X	
Idaho		X	
Indiana		X	X
Iowa	X		X (CIO)
Kansas	X	X	X
Kentucky		X	
Louisiana		X	
Maryland	X		
Minnesota		X	
Montana		X	
Nevada		X	
New Jersey		X	
New York			X
North Carolina		X	
Oregon		X	
Rhode Island		X	
South Carolina		X	
Tennessee	X	X	X
Utah	X		
Vermont		X	
Washington		X (CISO responded to the CIO survey)	X
Washington, D.C.	X		

Endnotes

1. www.nascio.com
2. The Cyber Security Division of DHS coordinates with states by conducting cyber attack exercises, such as "Cyber Storm," as well as by managing a national alert system for monitoring, detecting, analyzing, and sharing cyber vulnerabilities and attacks with state and local partners (see for example the U.S. Computer Emergency Readiness Team, US-CERT, www.us-cert.gov). Cybersecurity management has also taken shape within the Department of Defense, with the recent appointment of Teri Takai, former Chief Information Officer of the State of California. Takai will serve in a new position as IT Consolidator for DOD.
3. Weatherford, Mark. Interview by author. Lawrence, Kansas, 23 July 2009.
4. Goodyear, Marilu. "Chief Information Security Officer Survey." Web. July 30, 2009. www.Qualtrics.com
5. Ibid.
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. Weatherford, Mark. Interview by author. Lawrence, Kansas, 3 August 2009.
12. http://www.cio.ca.gov/OIS/Government/events/prev_event_materials.asp#PrevCISOtg
13. http://www.msisac.org/about/#objectives
14. http://www.nascio.org/aboutNASCIO/
15. Information Security, Colorado Revised Statues 2008 §24-37.5-401-404.
16. http://www.colorado.gov/cs/Satellite/Cyber/CISO/1207647059897
17. Kulakow, Seth. Interview by author. Lawrence, Kansas, 6 November 2009.
18. Ibid.
19. Ibid.
20. NESSUS is a modular software program that performs probabilistic analysis which was originally developed for NASA to do space flight analysis. The software is used as a vulnerability scanner for networks. See www.nessus.org for more information.
21. http://www.cisecurity.org/cistoolmembers.html
22. Kulakow, Seth. Interview by author. Lawrence, Kansas, 6 November 2009.
23. Starkley, Elaine. Interview by author. Washington, DC, 20 November 2009.
24. Starkley, Elaine. Interview by author. Washington, DC, 20 November 2009.
25. http://www.doverpost.com/news/x933814986/Drill-pits-tech-experts-against-digital-foes
    http://www.statetechmag.com/events/updates/spreading-security-awareness.html
    http://www.experteditorial.net/securitysquared/2009/10/rock-your-bosss-world.html
26. Kettlewell, Larry. Interview by author. Lawrence, Kansas, 24 June 2009.
27. www.da.ks.gov/ITEC/
28. Pelgrin, William. Interview by author. Albany, New York, 21 July 2009.
29. Pelgrin, William, Interview by author. Lawrence, Kansas, 25 June 2009.
30. Ibid.
31. Ibid.
32. Ibid.
33. Agnes, Kirk. Interview by author. Lawrence, Kansas, 10 November 2009.
34. Albert, Jim. Interview by author. Austin, Texas, 10 November 2009.

References

Andress, Amanda. 2003. *Surviving Security: How to Integrate People, Process and Technology*. London: CRC Press.

Aul, Sanjog. 2009. "Cyber Security Priorities – The Road Ahead!" Podcast audio program. *CIO Talk Radio*. 28 Oct. 2009. http://www.ciotalkradio.com/archives.html

Aul, Sanjog. 2009. "Cyber Security: Realistically handling the risk of the new." Podcast audio program. *CIO Talk Radio*. 21 Oct. 2009. http://www.ciotalkradio.com/archives.html

Ayoob, Mohammed. 1991. The Security Problematic of the Third World. *World Politics* 43(2): 257-283.

Berkowitz, Bruce and Robert W. Hahn. 2003. Cybersecurity: Who's Watching The Store? *Issues in Science and Technology*. Available at http://www.issues.org/19.3/berkowitz.htm

Critical Infrastructure Assurance Office. 2000. *Defending America's Cyberspace. National Plan for Information Systems Protection Version 1.0 An Invitation to a Dialogue*. Available at www.fas.org/irp/offdocs/pdd/CIP-plan.pdf.

CSIS Commission on Cybersecurity for the 44th Presidency. 2008. *Securing Cyberspace for the 44th Presidency*. Washington, DC. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Dawes, Sharon S., Anthony M. Cresswell, and Theresa A. Pardo. 2009. From 'Need to Know' to 'Need to Share': Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks. *Public Administration Review* 69(3): 392-402.

Department of Homeland Security. 2003. *The National Strategy to Secure Cyberspace*. Available at: www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

Department of Homeland Security National Cyber Security Division. 2008. *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development*. Office of Cyber Security and Communications: Washington, DC.

General Accounting Office. 2009. *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment*. Washington, DC. http://www.gao.gov/products/GAO-09-969.

Getha-Taylor, Heather. 2008. Identifying Collaborative Competencies. *Review of Public Personnel Administration*. 28(2): 103-119.

Goodyear, Marilu, Gail Salaway, Mark Nelson, Rodney Petersen, and Shannon Portillo. 2009. *The Career of the IT Security Officer in Higher Education*._EDUCAUSE Center for Applied Research Occasional Paper: Boulder, CO.

Information Security. *Colorado Revised Statues* 2008 §24-37.5-401-404.

Heiman, Don. 2002, 2nd Ed. *Public-Sector Information Security: A Call to Action for Public-Sector CIOs*. The IBM Center for The Business of Government: Available at www.businessofgovernment.org.

Pardo, Theresa, Brian Burke, Ramon Gilgarcia, and Ahmet Guler. 2009. Clarity of Roles and responsibilities in government cross-boundary information sharing initiatives: Identifying the determinants. *Proceedings of 5th International Conference on e-Government,* ed. Michael Lavin. Boston: Suffolk University.

Provan, Keith G. and Kenis, Patrick. (2008) "Modes of Network Governance: Structure, Management, and Effectiveness," *Journal of Public Administration Research and Theory*. 18(2), 229-252.

Rona, Thomas P. 1976. *Weapons Systems and Information War*. Seattle: Boeing Aerospace Company.

State of Colorado Information Technology Enterprise Architecture, Governance, and Consolidation. 2008: v. 1.05. Accessed at http://www.colorado.gov/cs/Satellite/OIT-New/OITX/1201542356889

Towns, Steve. 2009. *Vivek Kundra Touts Transparency, Accountability and Open Government.* September 1. http://www.govtech.com/gt/articles/717731

White House. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Williams, Matt. (2009). National Cyber-Security Report is a Call to Action. *Government Executive* http://www.govtech.com/gt/691709.

ABOUT THE AUTHORS

Marilu Goodyear
Dr. Goodyear is the Chair of the Department of Public Administration at the University of Kansas. Dr. Goodyear teaches information policy and technology, organizational analysis, and organizational change. Her research focuses in the intersection between technology transitions in organizations and organizational change. Her recent publications focus on the leadership implications of technology transition failure. She recently published in the *Handbook of Public Information Systems* and in *Transforming Public Leadership for the 21st Century*. She co-authored a study of higher education chief information security officers with the EDUCAUSE Center for Applied Research in 2009.

From 1999 to 2005, she served as the vice provost for information services and the chief information officer for the University of Kansas. In this role, she led all campus-wide software, hardware, and networking technology services, printing services, and the KU libraries.

Dr. Goodyear holds master's degrees in library and information science and public administration from the University of Missouri, as well as a doctorate in public administration from the University of Colorado. Dr. Goodyear is an elected Fellow of the National Academy of Public Administration and serves on the Executive Council of the National Association of Schools of Public Affairs and Administration.

Holly T. Goerdel
Dr. Goerdel is Assistant Professor of Public Administration at the University of Kansas. Her research focuses on the contribution of public management to organizational performance, as well as the perceived and actual value of collaboration in interdisciplinary problem solving in the public sector. She has applied both quantitative and qualitative research approaches to confront timely questions of interest to managers, policymakers, and the public in the domains of public education, public health, homeland security governance, and terrorism intelligence and information sharing. Her research has been published in the *Journal of Public Administration, Research & Theory*, *Public Administration Review*, and *Public Performance & Management Review*.

Dr. Goerdel earned a Ph.D. in political science at Texas A&M University, specializing in public policy, public administration, and

comparative politics. She values opportunities to connect her academic efforts to the real world of policy and management, with the hope of serving the public interest in the process.

Shannon Portillo
Dr. Portillo is an Assistant Professor in the Criminology, Law & Society Department and Deputy Director of the Center for Justice, Law & Society at George Mason University.

Her research and teaching interests include law and society as they apply to public bureaucracies. She is particularly interested in the influence of growing racial, ethnic, and gender diversity in public employment and how it affects the meanings of law and rules for public officials. She is a qualitative researcher whose particular proficiency is in narrative and conversational analysis and interviewing. She has recently completed research on the mobilization of rules and laws by public officials, which will appear in *Law & Social Inquiry*, and on gender and organizational rule abidance, which appeared in *Public Administration Review*. Her work primarily focuses on informal (social) and formal (legal) influences on organizational actors' behavior.

Dr. Portillo received her Ph.D. in public administration with a specialization in public law and emphasis field of gender and ethnic studies from the University of Kansas.

Linda Williams
Ms. Williams is a doctoral student in Public Administration at the University of Kansas. Her scholarly research focuses on administrative law, environmental policy, and immigration policy. She is interested in the effects of climate change on the mitigation and adaption policies of local and state governments and comparative immigration and immigrant policies and the process through which immigrant policies are carried out by bureaucratic agencies. Ms. Williams is a National Science Foundation IGERT fellow with the Climate Change, Humans, and Nature in the Global Environment IGERT Fellowship program at KU.

She has a master's degree in public administration from the University of Kansas and a bachelor of arts degree in political science from Truman State University. As a graduate teaching assistant, she has taught courses on project management and public policy analysis. Prior to beginning her doctoral studies, she worked as a project and program manager for private sector information technology companies. She served as the graduate research assistant for Dr. Goodyear during this study.

KEY CONTACT INFORMATION

To contact the authors:

Marilu Goodyear
Chair
Department of Public Administration
University of Kansas
4060 Wescoe Hall
1445 Jayhawk Blvd
Lawrence, KS 66045
(785) 864-3527

e-mail: goodyear@ku.edu

Holly T. Goerdel
Assistant Professor
Department of Public Administration
University of Kansas
4060 Wescoe Hall
Lawrence, KS 66045
(785) 864-9011

e-mail: hgoerdel@ku.edu

Shannon Portillo
Deputy Director
Center for Justice, Law & Society
Assistant Professor
Criminology, Law & Society Department
George Mason University
4400 University Dr. MS 4F4
Fairfax, VA 22030
(703) 993-9896

e-mail: sportill@gmu.edu

Linda M. Williams
Doctoral Student and Graduate Research Assistant
Department of Public Administration
4060 Wescoe Hall, University of Kansas
Lawrence, KS 66045
(785) 864-8297

e-mail: lwilliam@ku.edu

REPORTS from The IBM Center for The Business of Government

For a full listing of IBM Center publications, visit the Center's website at *www.businessofgovernment.org*.

Recent reports available on the website include:

Collaborating Across Boundaries

Designing and Managing Cross-Sector Collaboration: A Case Study in Reducing Traffic Congestions by John M. Bryson, Barbara C. Crosby, Melissa M. Stone, and Emily O. Saunoi-Sandgren

Contracting and Acquisition

The Challenge of Contracting for Large Complex Projects by Trevor L. Brown, Matthew Potoski, and David M. Van Slyke

Fostering Transparency and Democracy

Using Geographic Information Systems to Increase Citizen Engagement by Sukumar Ganapati

Improving Healthcare

The Role and Use of Wireless Technology in the Management and Monitoring of Chronic Diseases by Elie Geisler and Nilmini Wickramasinghe

Creating Telemedicine-Based Medical Networks for Rural and Frontier Areas by Leonard R. Graziplene

Improving Performance

Strategic Use of Analytics in Government by Thomas H. Davenport

Transforming State Government Services Through Process Improvement: A Case Study of Louisiana by Vicki C. Grant

Managing Finances

Strengthening Control and Integrity: A Checklist for Government Managers by James A. Bailey

Managing Risk in Government: An Introduction to Enterprise Risk Management (2nd Edition) by Karen Hardy

Transforming the Workforce

Federated Human Resource Management in the Federal Government by James R. Thompson and Rob Seidner

Using Technology

Moving to the Cloud: An Introduction to Cloud Computing in Government by David C. Wyld

About the IBM Center for The Business of Government

The IBM Center for The Business of Government connects public management research with practice. Since 1998, we have helped public sector executives improve the effectiveness of government with practical ideas and original thinking. We sponsor independent research by top minds in academe and the nonprofit sector, and we create opportunities for dialogue on a broad range of public management topics.

The Center is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Center focuses on the future of the operation and management of the public sector.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line business value. For more information visit www.ibm.com.

For additional information, contact:
Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
1301 K Street, NW
Fourth Floor, West Tower
Washington, DC 20005
(202) 515-4504, fax: (202) 515-4375

e-mail: businessofgovernment@us.ibm.com
website: www.businessofgovernment.org