Meet the Threat: States Confront the Cyber Challenge

2016-17 NGA Chair's Initiative

Memo on State Cybersecurity Governance Bodies

General Overview

This memo identifies commonalities and differences among the 22 states that established governance bodies tasked with identifying the cyber threats facing their state and the avenues to mitigating those threats.[1] These governance bodies are called various names (councils, task forces, advisory councils, working groups, review boards, committees, and teams), and their classifications tend to matter for the state in terms of their lifespan, authorities and public reporting requirements.

The number of members on each body ranged from as many as 18 to as few as two, with a state information technology representative as the only common member across all the bodies. Outside that community, the second-most commonly represented sector was the higher education community, which was present on 12 bodies. Other common agencies included homeland security departments, emergency management agencies, the National Guard and departments of revenue and commerce. Agencies and departments identified as chairs or designated with oversight over the bodies included state's IT departments, departments of homeland security, departments of public safety, emergency management agencies and offices of attorneys general.

These bodies were established through various techniques: 10 were created through executive orders, six were created ad hoc, five were legislatively enacted and one was created through a combination of an executive order and legislation. These bodies' authorities tend to vary, but those with legislative support appear to have more authority than the others. In **West Virginia**, the governor's Executive Information Security Team is responsible for "reviewing any deficient audit findings and rectifying the conditions to a satisfactory status."[2] Likewise, **Maryland**'s Cybersecurity Council is responsible for assisting infrastructure entities in complying with federal cybersecurity guidance and assisting private sector cybersecurity businesses in adopting, adapting and implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[3] The other bodies' roles and responsibilities ranged from broad mandates to specific roles. For example, 13 bodies were tasked with developing policy guidance, goals or recommendations to improve the state's cybersecurity posture, which was the most commonly identified responsibility. In contrast, the **Connecticut** and **Iowa** bodies were specifically tasked with creating a strategic document. Overall, the bodies are tasked with developing recommendations for a host of issues, but they are usually not given any authority to implement their recommendations.

Lastly, there were no clear metrics to measure the effectiveness of the bodies other than the production of a report that contains recommendations. Further, there are a lack of standards to hold the recommendations to, such as assessing a recommendation's ability to fulfill a NIST Cybersecurity Framework standard.

Best Practices

The type of body a governor wishes to create should account for state needs and complement the current IT governance ecosystem. An examination of existing bodies suggests governors could

[1] Texas governance body was set to expire in September 2015.
[2] "Project Charter: Governor's Executive Information Security Team," p, 3. 2008.
[3] "Senate Bill 542: Maryland Cybersecurity Council," p.4, 2015.

take one or a mix of three approaches. Governors could create a governance body tasked with creating a strategic plan that either improves the state's cybersecurity posture generally or addresses specific cybersecurity challenges. Similarly, governors could establish a body with the mission of developing reports with recommendations and continuously advising the governor on cybersecurity issues. Lastly, governors could create a body to assess state agencies' cybersecurity preparedness, identify and detect threats and implement and enforce recommendations.

Equally important to the body's mission are those tasked to carry out that mission. To improve a state's cybersecurity posture, a whole-of-government approach must take place, and therefore a body must have whole-of-government representation. States should consider every aspect of the state IT enterprise and include the education community, homeland security offices, emergency management agencies, National Guard, state police, fusion centers, health and human services, public utilities commissions, departments of transportation, revenue and commerce departments, tax commissioners, locals and others. West Virginia took a unique approach to this by appointing the chief information security officer from each cabinet member's agency onto the body.

Governors should base their governance body's tasks on the needs of the state, and may want to consider conducting a needs and risk assessment to assign its roles. In addition to the state's specific needs, governors should consider assigning their body with:

- Improving critical infrastructure resiliency;
- Identifying sources and methods for accomplishing proposed recommendations;
- Addressing the workforce pipeline challenge;
- Assisting public and private hospitals prepare, respond, and recover from cyber threats;
- Implementing cyber awareness training for state government employees;
- Leveraging business and economic opportunities;
- Implementing cyber assessments for state agencies;
- Evaluating existing statutes for needed updates given cyber risks; and
- Enhancing fusion centers' cybersecurity capabilities.

Lastly, governors, or body members, should consider creating metrics to evaluate the effectiveness of their proposed strategies and recommendations. However, broad metrics, such as prevention of a successful cyber penetration or incident, should be avoided due to their inevitability and, as a result, could distort perceptions of success or failure. Instead, tangible metrics, such as tying recommendations to their ability to further the implementation of the Center for Internet Security's Critical Security Controls or the NIST Framework, would more accurately assess the effectiveness of a governance body.

Below is a table that highlights common characteristics of the 22 bodies. Following the table are the states with a governance body and a brief description of each.

Table 1: Characteristics of State Cybersecurity Bodies

Question	Characteristics	Frequency
How was it established?	Executive Orders	10
	Ad Hoc	6
	Legislation	5
	Executive Order and Legislation	1
What type is it?	Council	7
	Task Force	3
	Advisory Council	3
	Study/Plan	2
	Working Group	2
	Commission	2
	Review Board	1
	Team	1
Where does it reside or who is the chair (if specified)?	IT Department/CIO/CISO	7
	Department of Public Safety	2
	Emergency Management Agency	2
	Department of Homeland Security	2
	Department of Administrative Services	2
	Attorney General's Office	1
Who is involved? (Those listed are only the ones mentioned at least twice).	IT Department	22
	Higher Education	12
	Department of Homeland Security	11
	Emergency Management Agency	8
	Department of Revenue/Commerce	8
	Adjutant General	6
	Department of Administrative Services and Budget	6
	Attorney General's Office/Justice Department	6
	Department of Public Safety	5
	State Police	5
	Health and Human Services	5
	Legislator	4
	Economic Development Department	3
What are the roles and responsibilities? (Those listed are only the ones mentioned at least twice).	Recommend policy guidance, and/or goals on improving the state's cybersecurity posture	13
	Review/create cybersecurity plans of state agencies	7
	Facilitate collaboration	6
	Identify/recommend/implement best practices	6
	Improve the ability to and/or identify and detect threats	6
	Identify sources and methods for	5

	accomplishing recommendations	
	Create a strategic framework	5
	Improve critical infrastructure resiliency	5
	Ensure robust workforce and talent pipeline	5
	Implement cyber awareness training for state employees	5
	Build cyber incident response (IR) capabilities/create IR plan	4
	Leverage business and economic opportunities	4
	Establish data breach reporting and notification requirements	4
	Recommend how to manage cyber risks/data	3
	Recommend best practices on trainings and exercises	3
	Implement cyber assessments	3
	Improve information sharing	2
	Educate the public	2
	Create a governance structure	2
Does the body produce a report?	Yes	11
	No	11

State Cybersecurity Bodies

California

Cybersecurity Task Force

The California Cybersecurity Task Force is responsible for identifying, acquiring and establishing funding mechanisms to enhance cybersecurity efforts; promoting actions to enhance cybersecurity; growing the cybersecurity workforce; developing public education; facilitating economic development by promoting a cyber-safe location for businesses and consumers; enhancing cyber emergency preparedness and response; identifying, understanding and sharing cyber threat information; mitigating the cyber risk; and building a comprehensive digital forensics and cyber investigative capability. The task force serves as an advisory body to senior administration officials in matters related to cybersecurity.

Colorado

Legislation: Cybersecurity Council

The cybersecurity council was created by law and is located within the department of public safety to operate as a steering group to develop cybersecurity policy guidance for the governor; develop comprehensive goals, requirements, initiatives and milestones; and coordinate with the general assembly and the judicial branch regarding cybersecurity. The council consists of several members, including the governor (chair), CIO, CISO, executive director of the department of public safety, National Guard, adjutant general, director of the office of economic development, director of governor's office of state planning and budgeting, attorney general, director of public utilities commission and others.

Connecticut

An Act Concerning a Study of Cybersecurity

This law tasks the department of administrative services and the department of emergency services and public protection to conduct a study to identify cybersecurity issues. They will then make recommendations regarding specific actions the state can implement to promote and coordinate communication among government entities, law enforcement, institutions of higher education, the private sector and the public to improve cybersecurity preparedness.

Delaware

Executive Order: Cyber Security Advisory Council

This executive order created the Cyber Security Advisory Council to facilitate collaboration; develop recommendations for improving the overall cybersecurity posture; develop recommendations for increasing information sharing; recommend sources and methods for accomplishing their recommendations; and provide recommendations to the homeland security advisor on equipment interoperability, technologies and software infrastructure related to the cyber attacks and cybersecurity. The council consists of the CIO, CSO, Delaware's Department of Homeland Security and Emergency Management Agency, the adjutant general and others.

Georgia

Executive Order: State Government Systems Cybersecurity Review Board
This executive order created the State Government Systems Cybersecurity Review Board to review cybersecurity preparedness of the executive branch state agencies and develop recommendations for properly managing cybersecurity risks. The board consists of the state's CIO, the emergency management/homeland security agency, and the adjutant general.

Idaho

Executive Order: Cybersecurity Task Force
This executive order created the Cybersecurity Task Force to identify/detect threats and vulnerabilities in Idaho's IT systems, recommend best practices, educate the public about cybersecurity and implement best practices. The task force consists of the bureau of homeland security, Idaho State Police, department of administration, tax commission, transportation department, department of health and welfare and state colleges and universities.

Indiana

Executive Order: Executive Council on Cybersecurity
This executive order establishes a public-private partnership charged with enhancing Indiana's ability to prevent, respond to and recover from all types of cybersecurity issues, including attacks. The council consists of the homeland security department, CIO, attorney general, adjutant general, state police superintendent, utility regulatory commission chair and others.

Iowa

Executive Order: Cybersecurity Strategic Plan
This executive order requires the homeland security and emergency management department, communications network, National Guard and department of public safety to create a cybersecurity strategy.

Kansas

Information Technology Security Council
A sub-council of and advisory to the Information Technology Executive Council (ITEC), recommends and reviews policies, guidelines and best practices for the overall security of information technology systems, infrastructure and data within Kansas state government. The council consists of the enterprise security office; adjutant general; department of administrative services; attorney general; departments of corrections, transportation and education; and others.

Maine

Executive Order: State of Maine Information Protection Working Group and For Other Purposes
This executive order creates the working group to regularly examine threats and vulnerabilities of state information assets; develop cost-effective defenses, best practices and risk management against threats to state information; develop statewide policies and procedures; and present recommendations to the governor and cabinet as needed. The group consists of the departments of administrative and financial services, defense, veterans, public safety and others.

Maryland

Legislation: Maryland Cybersecurity Council

The council, created in 2015, is responsible for reviewing and conducting risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures; assisting private sector cybersecurity businesses in adopting, adapting and implementing NIST framework; recommending a comprehensive state strategic plan to ensure a coordinated and adaptable response to and recovery from cybersecurity attacks; and other responsibilities. The council is made up of the attorney general (chair), secretary of information technology, secretary of the state police, secretary of business and economic development, adjutant general, executive director of the office of homeland security, the executive director of the development corporation and others.

Legislation: Commission on Maryland Cybersecurity Innovation and Excellence
The commission, created in 2011 and ending in 2014, was responsible for conducting a comprehensive review of state and federal cybersecurity laws, policies and best practices for ensuring the security of computer systems and networks used by educational institutions and state government and other organizations that work with health care records, personally identifiable information, public safety and public service and utilities; conducting a review of the state's role in promoting cyber innovation; and other responsibilities. The commission was composed of one member from the senate, one member from the house of delegates, the information technology and labor secretaries and others.

Montana

Executive Order: Information Security Advisory Council
This executive order created the Information Security Advisory Council to advise the governor with respect to a statewide strategic information security program. The council is comprised of 10 to 15 members, including the chief information officer, homeland security advisor, department of military affairs, justice department, corrections department, public health and human services department, legislators and others.

Nevada

Cyber Security Committee
The committee is within the Nevada Commission on Homeland Security and is responsible for providing advice and recommendations on the state's cybersecurity risk; cyber threat preparedness posture; statewide cybersecurity plans; cyber-related training; and exercises and enhancement of security awareness through education, public awareness and engagement with public and private sector partners.

New York

Cybersecurity Advisory Board (Potential Law)
Created in 2013 by the governor, the Cybersecurity Advisory Board is tasked with investigating and making recommendations concerning cybersecurity issues involving the public and private sectors, plus steps that can be taken to protect critical cyber infrastructure, financial systems, telecommunications networks, electrical grids, security systems, first responder systems and infrastructure, physical infrastructure systems, transportation systems and any other sector the board deems prudent. The board consists of the division of military and naval affairs, state police and department of homeland and emergency services.

North Dakota

Cybersecurity Task Force

The governor created the Cybersecurity Task Force to review the state's current cybersecurity policies and practices and make policy and resource recommendations needed to ensure the security of state networks and systems. The task force will expand the governance structure for cybersecurity among the state's executive branch of government to share best practices and recommend new policies for mitigating future cyber attacks. The team will also identify ways to enhance the use of network defense and monitoring tools, implement training and awareness programs for state employees and develop a cyber incident response strategy. The task force consists of the chief information officer, bureau of criminal investigation, department of emergency services, division of homeland security, department of transportation, state tax commissioner and others.

Rhode Island

Executive Order: Cybersecurity Commission

This executive order created the Rhode Island Cybersecurity Commission to establish a process to regularly assess cybersecurity infrastructure and activities within state agencies, identify cybersecurity awareness training needs and establish a framework for coordinated responses. The commission consists of the emergency management agency, National Guard, department of public safety, department of business regulation, office of digital excellence and executive office of commerce.

Tennessee

Information Systems Council

Chaired by the commissioner of the Tennessee Department of Finance and Administration, the council is charged with overseeing information technology for the entire state and for developing policies for managing information technology overall. The council is made up of the office of legislative information services, department of general services, comptroller of the treasury, legislators, supreme court, department of health and private sector partners.

Texas

Cybersecurity, Education and Economic Development Council (2012)

The Texas Cybersecurity, Education and Economic Development Council was created to leverage public-private partnerships to examine the infrastructure of the state's cybersecurity operations with the intent to produce strategies to accelerate the growth of cybersecurity as an industry within Texas, and to encourage industry members to call Texas "home." The council is made up of the chief information security officer, Army National Guard, academia members and private sector partners.

Utah

Legislation: Data Security Management Council

This law created the Data Security Management Council to review existing state government data security policies, assess ongoing risks to state government, create a method to notify state and local government entities of new risks, coordinate data breach simulation exercises and conduct other cybersecurity related activities. The council consists of the chief information officer, an individual appointed by the governor, an individual appointed by the speaker of the House of Representatives and the highest-ranking IT official from the judicial council, the board of regents, the office of education, the Utah College of Applied Technology, the state tax commission and the office of the attorney general.

Virginia

Executive Order: Virginia Cyber Security Commission

This executive order established the Virginia Cybersecurity Commission to identify high-risk cybersecurity issues, provide suggestions for more secure network plans and procedures, offer response strategies and best practices for the state, promote cyber hygiene, help facilitate the development of cutting-edge science and technology in the cybersecurity realm, implement state cyber assessments and contribute to the overall cyber safety of Virginia stakeholders. The commission consists of the secretaries of technology, commerce and trade, public safety, education, health and human resources and veteran affairs and homeland security.

West Virginia

Governor's Executive Information Security Team (GEIST) Charter (Executive Order, Legislation)

Established by a bill in 2006 and through an executive order, the mission of the GEIST is to reduce overall security-related risk to state IT systems, and all data, through the application of appropriate procedures, processes and controls, with an emphasis on administrative controls. The GEIST is chaired by the chief information security officer and composed of the information security administrators of each cabinet secretary. The GEIST is steered by the office of information security and controls.