Act and Adjust: A Call to Action for Governors for Cybersecurity

Cybersecurity remains one of the most significant challenges facing the nation. Although implementing policies and practices that will make state systems and data more secure will be an iterative and lengthy process, governors can take a number of actions immediately that will help detect and defend against cyber attacks occurring today and help deter future attacks.

Those actions include:

- Establishing a governance and authority structure for cybersecurity;
- Conducting risk assessments and allocating resources accordingly;
- Implementing continuous vulnerability assessments and threat mitigation practices;
- Ensuring that the state complies with current security methodologies and business disciplines in cybersecurity; and
- Creating a culture of risk awareness.

By implementing those recommendations immediately, governors can greatly enhance states' cybersecurity posture.

Guiding Principles

This *Call to Action,* as well as the work of the NGA Resource Center for State Cybersecurity (Resource Center), is guided by a set of core principles:

- **Support Governors.** The work of the Resource Center is singular in its focus on supporting governors' efforts to improve cybersecurity. The Resource Center marks the first large-scale effort exclusively focused on the role of governors in improving cybersecurity.

- **Be Actionable.** The goal of the Resource Center is to provide to governors recommendations and resources that promote actions that reduce risk.

- **Reduce Complexity.** Cybersecurity policy is designed and implemented in a complex environment. The Resource Center aims to reduce that complexity by looking for common principles and practices that are effective in that environment.

- **Protect Privacy.** The recommendations made through the Resource Center aim to both improve cybersecurity and protect the privacy, civil rights, and civil liberties of citizens.

- **Employ Technologically Neutral Solutions.** The recommendations made through the Resource Center emphasize nonproprietary, open standards.

- **Focus on the State as Enterprise.** The work of the Resource Center aims to improve governors' understanding of the state as an enterprise including the interdependencies among state agencies; between the public and private sector; and regionally across state boundaries.

- **Promote Flexible Federalism.** To the extent possible,the Resource Center emphasizes the benefits of and opportunities for flexibility within federal programs to allow for tailored state solutions.

- **Rely on Evidence-Based Practices.** The Resource Center makes recommendations that build on evidence-based practices.

- **Use and Generate Metrics.** The Resource Center promotes recommendations that use dynamic performance metrics to manage and improve state processes and practices.

- **Promote the Use of Incentives.** The Resource Center makes recommendations that promote the use of incentives to improve cybersecurity practices in a state.

Immediate Actions to Protect States

Domestic and international actors are launching a significant number of cyber attacks against states. Although many of the actions necessary to reduce the nation's vulnerabilities to cyberattacks require long-term structural improvements and business redesign, governors can take actions now that can immediately improve their state's cybersecurity posture. Implementation of the actions described below will help to ensure strong governance and oversight, a baseline of cybersecurity capabilities, and quicker identification of attacks and threats; it also will help to improve basic cybersecurity practices.

Establish a governance structure for cybersecurity. Because state systems and networks are interconnected, developing a robust cybersecurity posture will require an enterprise-wide approach. To that end, governors need to ensure that they have a strong statewide governance structure with some degree of central authority that provides a framework to prepare for, respond to, and prevent cyber attacks. Several recent attacks reveal that states which fail to put in place a strong governance structure are at a distinct disadvantage.

For many states, chief information security officers (CISOs), who are responsible for developing and carrying out information technology (IT) security policies, have only limited responsibility and authority over statewide cyber networks. CISOs can operate in federated or decentralized environments where technology and security resources are dispersed across various agencies and departments. In addition, the sharing of cyber threat information with the private sector and local governments is handled by state homeland security agencies, further complicating the overall cybersecurity governance structure.

According to a survey conducted by Deloitte for the National Association of State Chief Information Officers (NASCIO), 56 percent of state CISOs indicate that they have authority over only their executive branch agencies, departments, and offices.[1] Although most states have a CISO, if they do not have a visible agency-level security posture, they can encounter obstacles to implementing an effective cybersecurity program. Among the elements of an effective program are enforcement mechanisms to ensure compliance with security policies and audit findings. States without governance structures to build and operate effective programs will be limited in their ability to identify an ongoing cyber attacks and respond in a coordinated way.

Governors can grant their chief information officers (CIOs) or CISOs the authority to develop and steer a coordinated governance structure (for example, a task force, commission, or advisory body) that can greatly improve coordination and awareness across agencies that operate statewide cyber networks. Such an approach also helps enable the CIO or CISO to take actions to prevent or mitigate damage in the event of a cyber breach.

Michigan has created a centralized security department run by a chief security officer (CSO) that brings together both physical security and cybersecurity. Directors, managers, and employees within each agency

[1] "State Governments at Risk: A Call for Collaboration and Compliance," Deloitte and the National Association of State Chief Information Officers, October 26, 2012, accessed March 10, 2013, http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_nascio%20Cybersecurity%20Study_10192012.pdf, 10.

coordinate through the centralized governance structure to focus on each agency's need for both physical security and cybersecurity. Governance of that type is especially important during an incident or a disaster. The approach allows the CSO and CIO to work closely to manage the state's cyber networks and infrastructure and to ensure that effective governance practices are in place.

Although a central authority is essential, it does not obviate the importance of collaboration among local governments, nongovernmental organizations, and the private sector. Those relationships are essential to understanding the culture, operations, and business practices of various agencies and organizations with cyber assets within the state. In Michigan, for example, in addition to dedicated and full-time state employees in the Office of Cybersecurity, a risk management team leverages many resources around the state to gather information and resolve an incident efficiently and effectively.

Minnesota is another example of a state that adopted a governance framework that stresses teamwork and communication between a centralized information technology organization and stakeholders. The state CIO works collaboratively with the governor, the Technology Advisory Committee, and other agency leaders. Minnesota also has several governing bodies that have an agency CIO, providing a direct link to the state CIO and operational decisions made at the different agency team levels.[2]

Recognizing the need to foster collaboration at all levels of government and with the private sector, **California** recently created the California Cybersecurity Task Force. The task force focuses on sharing information to improve the security of government and private-sector IT assets.[3]

Conduct risk assessments and allocate resources accordingly. Governors and other key state actors need a comprehensive understanding of the risk and threat landscape to make accurate and timely decisions when allocating scarce resources. Without a comprehensive understanding of the risks, including the interdependencies among critical assets, states are vulnerable to interruptions in business operations as well as financial and data losses. To gain this awareness, states must develop security strategies and business practices by conducting risk assessments that identify information assets, model different threats to those assets, and allow for planning to protect against those threats.[4]

In addition to establishing sound business practices and using existing resources, states also must conduct hands-on activities and exercises as a part of their assessments. Those practices include regular penetration testing and vulnerability scanning and should be referenced in security policies. States can take advantage of resources from federal and private entities to conduct those activities. Once an independent statewide assessment has been conducted, governors can make necessary decisions on where scarce resources should be allocated to prevent the loss of essential information and resources and to protect critical infrastructure and assets. The initial assessment also will help determine the frequency of such assessments in the future, based on the risk profile of agencies. As an example, agencies with sensitive citizen data might require annual assessments and quarterly follow-up in their corrective action plan.

Additionally, governors and their senior staff who have appropriate security clearances should receive regular classified cybersecurity threat briefings. The Department of Homeland Security (DHS) can assist states in planning these briefings.

---

[2] "State of Minnesota IT Governance Framework," http://mn.gov/oet/images/StateofMinnesotaITGovernanceFramework.pdf (June 2012)
[3] "California Launches Cybersecurity Task Force," http://www.govtech.com/security/California-Launches-Cybersecurity-Task-Force.html (May 17, 2013)
[4] "5 Steps to Cybersecurity Risk Assessment" http://www.govtech.com/security/5-Steps-to-Cyber-Security.html?page=1 (June 24, 2010)

Implement continuous vulnerability assessments and threat mitigation practices. Consistently monitoring threats and vulnerabilities will help governors proactively defend cyber networks. Every day, states are exposed to phishing scams, malware, denial-of-service attacks, and other common tactics employed by cyber attackers. Governors must ensure that mission-critical systems are equipped with technologies and have implemented business practices that will identify potential threats, track all stages of cyber attacks in real time, and offer mitigation techniques and options for any resulting loss or damage.

Maryland leverages the cybersecurity capabilities of the Maryland Air National Guard 175th Network Warfare Squadron to support its cybersecurity assessments. State agencies participate in collaborative Web penetration training exercises with the Maryland Air Guard Squadron. The exercises that feature simulated attacks from malicious outsiders or insidious insiders are useful in evaluating the security of selected state websites and portals. Security issues uncovered through the penetration tests lead to technical and procedural countermeasures to reduce risks. The Guard also provides network vulnerability assessment services to various state agencies while, in return, it receives beneficial training for the squadron's members. A number of other states have similar practices in place.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) has been designated by DHS as a key resource for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal governments. Through its state-of-the-art Security Operations Center, available 24 hours a day, seven days a week, the MS-ISAC serves as a central resource for situational awareness and incident response. The MS-ISAC also provides state, local, tribal, and territorial governments with managed security services, which are outsourced security operations that include ongoing monitoring of networks and firewalls for intrusions.

Another related resource available to state and local governments is DHS's newly launched Continuous Diagnostics and Mitigation (CDM) program. The CDM program at the federal level works by expanding deployment of automated network sensors that feed data about an agency's cybersecurity vulnerabilities into a continuously updated dashboard. To support states in improving their capabilities to prevent and detect intrusions, the CDM has a blanket purchasing agreement that reduces the cost to states of purchasing tools and services that enhance their cybersecurity. It is important to note that such purchases are most effective when coordinated with MS-ISAC's managed security services so as to maintain collective situational awareness across state and local governments.

Ensure that your state complies with current security methodologies and business disciplines in cybersecurity. States can turn to two industry standards for a baseline of effective cybersecurity practices. First, the Council on CyberSecurity's *Critical Controls for Effective Cyber Defense* is an industry standard that provides states with a security framework that can strengthen their cyber defenses and ultimately protect information, infrastructure, and critical assets. Compliance with that standard will provide a baseline of defense, deter a significant number of attacks, and help minimize compromises, recovery, and costs. The controls are based upon five guiding principles: using evidence-based practices to build effective defenses, assigning priorities risk reduction and protection actions, establishing a common language that measures the effectiveness of security, continuous monitoring, and automating defenses.[5] The controls also identify key network components and how to secure them.

The second standard is the Information Technology Infrastructure Library (ITIL). An ITIL is a set of practices for information technology service management (ITSM) that are designed to align information technol-

[5] "CSIS: 20 Critical Security Controls," http://www.sans.org/critical-security-controls/guidelines.php

ogy (IT) with core business requirements. The latest editions of ITIL, which were published in July 2011, form the core guidance of best management practices and can greatly strengthen states' IT practices. The ITIL has been adopted by companies in many private-sector industries, including banking, retail services, technology, and entertainment. For states, an ITIL will help ensure that states' IT assets correlate with their critical assets.[6]

Create a culture of risk awareness. The best firewalls and most advanced antivirus software cannot deter a cyber attack if the individuals using a network are either careless or inattentive to basic security practices. The strongest door and most secure lock will not keep a burglar out if the door is left open or unlocked.

Governors have the opportunity to promote a culture of cybersecurity awareness that will help to minimize the likelihood of a successful cyber attack. Building a strong cybersecurity culture means making individuals aware of the many risks and ongoing threats facing their networks. Those individuals must understand the potential negative implications of their activities or inattentiveness. To develop a strong cybersecurity culture, focus should be put on increasing awareness, setting appropriate expectations, and influencing day-to-day security practices of end users. Awareness can be created by including relevant training and content in the orientation process of new staff as well as annual review of current staff. Expectations about users' behaviors can also be set by adding cybersecurity components to job responsibilities.

However, creating a culture of awareness will be an ongoing process that will require constant attention and ongoing training. Governors have the opportunity to use the bully pulpit to make cybersecurity the responsibility of all, including ordinary citizens. In **Delaware**, state employees conduct cybersecurity presentations for elementary school students to reinforce the importance of Internet safety practices. The state also hosts video and poster contests that encourage the public to create materials that promote cybersecurity awareness.[7]

Effective awareness training and education for end-users is recognized as the single most effective factor in preventing security breaches and data losses. States such as **Michigan** have launched security awareness training for all state employees and have posted online guides that are available to the public with the goal of reducing risk.[8] More than 50,000 users and partners are currently enrolled in Michigan's training program, an online interactive program consisting of a dozen 10-minute lessons. Other organizations, such as the MS-ISAC, also offer training resources that are readily available online.

Michigan also has recently launched a research, test, training, and evaluation facility for cybersecurity and cyberdefense. In partnership with state universities, the private sector, and state and local governments, Merit Network Inc., a 501(c)(3) nonprofit organization, built and developed the state-of-the-art center to further advance cybersecurity training in Michigan. A wide variety of course offerings includes certifications in incident handling, disaster recovery, forensics, and wireless security. Dozens of technical staff have already completed training and received certifications.

In addition to offering training, states like **Maryland** conduct tabletop exercises to raise the awareness and response capabilities of key state actors. Maryland, through the state's Emergency Management Administration (MEMA), facilitated an initial cabinet-level tabletop exercise in which cybersecurity and continuity of operations awareness and readiness were assessed. In addition to MEMA, DHS and the National Security Agency Cyber Command assisted in hosting this exercise.

[6] "ITIL: The Basics, "http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf
[7] See http://www.dti.delaware.gov/information/cybersecurity.shtml
[8] See State of Michigan Security Office website

The Path Forward

The actions described above are a first step for governors to improve cybersecurity for state-owned and operated systems. However, a secure cybersecurity fabric will require an enterprise-wide approach that includes coordination and partnerships with critical infrastructure owners and operators, private industry, and the public.

Over the course of the next year, the NGA Resource Center for State Cybersecurity will issue a series of reports focusing on critical areas for mid- to long-term actions governors can take to strengthen their states' cyber posture. Those areas include improving coordination between state and federal governments, leveraging state fusion centers to respond to cyber threats, enhancing the cybersecurity of critical energy systems and infrastructure, and developing a skilled cybersecurity workforce.

In addition to the work of the Resource Center, NGA also is leading efforts through the Council of Governors to collaborate with the Departments of Defense and Homeland Security on how the National Guard could be used to better protect both state and federal networks. The National Guard's unique role serving governors and the President, combined with its ability to attract and retain individuals who have full-time employment in IT and related fields, make it an ideal solution to help address the shortage of highly skilled personnel necessary to protect critical networks and systems.

Across the country, several states have established National Guard cyber capabilities that are closely aligned with civilian agencies and coordinate regularly with public utility commissions, owners and operators of critical infrastructure, and other public and private sector partners.

Thomas MacLellan
Division Director
Homeland Security & Public Safety Division
NGA Center for Best Practices
202-624-5427

September 2013

The NGA Resource Center for State Cybersecurity is made possible through the generous support from our grant makers, including the American Gas Association, Citi, Deloitte, Edison Electric Institute, Good Technology, Hewlett-Packard, IBM, Northrop Grumman, Nuclear Energy Institute, Symantec, and VMware.