State Trends in Cybersecurity
Written Testimony
December 12, 2016

Timothy Blute
Program Director
Center for Best Practices
National Governors Association

Introduction

Good afternoon. My name is Timothy Blute, and I am the Program Director for cybersecurity and communications at the National Governors Association (NGA) Center for Best Practices (Center), Homeland Security and Public Safety Division (HSPS). Thank you for inviting me to speak to you about our work on state cybersecurity, an issue of central importance to the nation's governors.

Through NGA, governors share innovative policy solutions, voice collective positions on national priorities, and work together to improve the lives of all Americans. I am here today to discuss the trends in state cybersecurity that I have observed in my work with states. These trends exemplify a growing awareness of cybersecurity threats and a corresponding increase in policy development to meet this threat.

NGA's Cybersecurity Focus

Each year, the Chair of NGA chooses a policy initiative to focus much of the organization's time and energy on during his or her term. The current chair, Virginia Governor Terry McAuliffe, selected cybersecurity as his initiative. Titled *Meet the Threat: States Confront the Cyber Challenge*, this nationwide project places states at the center of defining solutions to the growing cyber threats facing our country. Governors recognizes that cybersecurity is a core business concern of state government. In the new digital economy, both public and private sectors rely on computer systems to deliver timely and effective results. Through regional summits, roundtables, webinars, podcasts, and written products, NGA is convening state, federal, local, and private partners together. We foster collaboration to identify cybersecurity best practices in health care, workforce development, critical infrastructure, public safety, and education.

In addition to the initiative, Governor McAuliffe and Michigan Governor Rick Snyder co-chair the NGA Resource Center for State Cybersecurity (Resource Center). Established in 2012, the Resource Center supports governors, their staff, and state agencies. In 2015, the Resource Center sponsored the first-of-its-kind National Summit on State Cybersecurity. The summit gathered officials from across state government—chief information officers (CIOs), homeland security advisers (HSAs), Adjutants General, and public safety officials—to explore cross-cutting challenges, obstacles to coordination, and potential solutions.

Drawing from lessons learned during the summit, NGA launched the Policy Academy on Enhancing State Cybersecurity. NGA issued a nationwide request for applications and selected the five states, including Oregon, through a competitive process. Through the academy, we convened the five state teams and other cybersecurity experts to identify best practices. These officials also worked to create a roadmap based upon the specific goals identified in their initial application. At the conclusion of this effort, each state will have developed custom cybersecurity solutions based on their individual risk.

The policy academy began in June and we are now holding workshops in each state to either reaffirm or revise the state's goals. For the next several months, we will assist each team as they implement their individual initiatives. Each state team will have the opportunity to share their accomplishments with the nation in June 2017 at a second National Summit.

Throughout the project, NGA has been thoroughly impressed with Oregon's commitment and creativity in the face of this growing threat. The application, which required an accompanying letter from the applicant state's governor, showed Governor Brown's deep commitment to this complex challenge. I am here today to assist the team she appointed and describe how its efforts correspond with the cybersecurity trends we see across the states.

Ecosystem

Although NGA's main constituents—governors, their staff, and state agencies—lie within the executive branch, cybersecurity requires a "whole of government" approach. The term has become a cliché, but it may be an understatement in this context. In fact, addressing the cybersecurity challenge in states requires more: a "whole society" approach. Governors and legislators are charged with protecting state networks and the sensitive data they store. Their first priority is the safety and security of constituents, businesses, and critical services—many of which suffer from frequent cyber attacks. Moreover, these threats often hop seamlessly between private computer systems and public networks. Consequently, cybersecurity is a cross-sector challenge that demands a collaborative ecosystem of state, local, federal, tribal, and private partners. All stakeholders must work together and share information and resources.

Each state has a unique cybersecurity ecosystem. Although no two states are the same, states often engage with certain stakeholders working within their borders. Those players include localities, legislators, the courts, vendors, federal agencies, educational institutions, and owners and operators of critical infrastructure. It is vital that Oregon identifies who among these stakeholders are missing in its cybersecurity ecosystem. The state must also identify how it can best work with these stakeholders.

Throughout this project, Oregon has stood out because of its "whole of state" approach to cybersecurity. In its application and subsequent meetings, the state's team has articulated a strategic framework that envisions collaboration with state government, localities, the private sector, and higher education to improve the cybersecurity of the entire state.

Trends

I wanted to discuss the state's cybersecurity ecosystem first because the state's choice of stakeholders determines how the state tackles cybersecurity. Although each state is unique, I have seen states embrace five overall trends:

- Governance;
- Risk management;
- Strategic planning;
- Incident response planning; and
- Policy integration and coordination centers.

Governance

The first and most important element of state cybersecurity is governance. The driving questions in the field are no longer focused on computer security techniques. Experts know how to foil almost all attackers. Today, the primary challenge in large organizations, such as state government, is three-fold: (1) formulating rules, procedures, and incentives to ensure that human beings implement best practices; (2) shaping these policies to account for business needs; and (3) securing and sustaining necessary resources to accomplish the first two goals. Good governance aims to achieve all three needs.

A state's cybersecurity governance determines how its ecosystem work together, create policies, and overcome internal challenges. Perhaps due to the number of stakeholders involved, I often see a desire among states to centralize and consolidate authority. Often, states see centralization as necessary to improve effectiveness and efficiency. It is vital that everyone understands their roles and responsibilities before, during, and after a cyber incident occurs. The time to delineate roles and responsibilities is not during a crisis. Identifying roles beforehand improves the government's response to cyberattacks and maximizes resources during steady-state, day-to-day security operations.

Centralization provides leaders with mechanisms to coordinate the state's entire cybersecurity ecosystem by consolidating duplicative efforts, quickly elevating calls for assistance, and generating the best return on investments. A recent published study supports this argument as it found that the centralization of IT functions in the state CIO's office—particularly those related to strategy and IT personnel management—led to higher IT performance.[1]

Risk Management

The second emerging trend is an increasing application of risk management approaches in cyber policies. For the past few years, I have seen a slow transition from a compliance-based approach to cybersecurity to a risk-based approach. A risk-based model is more effective because, as mentioned earlier, every state is different and risks may vary from state to state. Also, risk-based assessments allow the state to evaluate what resides on their state networks, who has access to those networks, the threats to those networks, and the consequences should those networks become compromised. Thus, the risk assessment reveals the "crown jewels" of the states and helps determine the amount of resources needed to protect them. It enables the legislature, as appropriators, to allocate resources commensurate with the threat levels facing the state.

Moreover, a risk-based approach informs a state cybersecurity strategy by acknowledging not every asset can be protected to the same degree. The risk assessment identifies resources that reside within the entire state's ecosystem, such as national laboratories and higher educational institutions, that can be utilized to achieve strategic objectives.

Strategy Development

Strategy development is the third national trend that I have seen become a priority among states. A strategy is critical because it scopes and defines the cybersecurity challenge to the state, and thereby personalizes the strategy to the state, which facilitates the creation of specific objectives that leverages the state strengths. In fact, a recent survey by Deloitte, a multinational professional services firm, and National Association of State Chief Information Officers (NASCIO) found that more funds were allocated to cybersecurity in states that had a dedicated cybersecurity strategy.[2] The strategic planning process identifies state resources, which further narrows what the state can feasibly accomplish. On a national scale, I see states focus on protecting state networks, growing the cyber workforce, developing cyber response plans, improving employee cyber hygiene, enhancing partnerships, and creating a governance structure with metrics.

This last point is important. Strategy development and establishing a governance structure has a chicken or egg problem. States must decide whether to create a strategy that identifies a process for establishing a governance structure or whether to create a governance structure that identifies the strategic priorities for the state. Iowa, for example, took the former approach and the governor signed an executive order that identified the stakeholders to develop a strategy. These stakeholders delivered their product to him at the end of the year. Illinois embraced the latter approach by simultaneously creating a governance structure and developing a strategy. There is no right answer, each state must choose the path that makes the most sense for them.

Response Planning

The fourth trend I see in states across the country is a concerted focus on developing and exercising cyber response plans. A cyber response plan is as important as an earthquake or terrorism response plan. Like terrorism, cyber is just one attack vector that malicious actors will use to cause physical

---

[1] Denford, James; Dawson, Gregory; and Desouza Kevin. "An Argument for Centralization of IT Governance in the Public Sector."

[2] "2016 Deloitte-NASCIO Cybersecurity Study: State Governments at Risk: Turning Strategy and Awareness into Progress," National Association of State Chief Information Officers and Deloitte.

or economic damage. A cyber response plan ensures that a cybersecurity ecosystem can effectively prepare, respond, and recover from a cyber event. Response planning includes an examination of the state's emergency operations plan, ensuring there are hard copies of key documents, and guaranteeing that state law enforcement have the resources and legal authority to prosecute perpetrators. Ensuring that these policies are reviewed, revised, and exercised will inevitably translate into economic savings and mitigate the impacts of a cyber event.

Integration Centers

Lastly, many states are looking to establish cybersecurity integration and coordination centers. The timely sharing of information is an indispensable component of any effective cybersecurity program. Quickly sharing the tactics, techniques, and procedures employed by attackers to trick human defenders, subvert automated defenses, and conceal intrusions enables potential targets to take preventive steps. The financial sector's relatively strong cybersecurity posture comes from robust information sharing arrangements centered in the Financial Services Information Sharing and Analysis Center (FS-ISAC). A host of other integration centers, including the Multi-State Information Sharing and Analysis Centers (MS-ISAC), are modeled on this approach.

Recently, states have established their own integration and coordination centers. Michigan established the Cyber Command Center (MC3). New Jersey founded the New Jersey Cybersecurity and Communications Integration Center (NJCCIC). California established the California Cyber Security Integration Center (Cal-CSIC). Indiana hosts the Indiana ISAC (IN-ISAC). Colorado just inaugurated the National Cybersecurity Center. These organizations represent only a sampling of integration centers nationwide.

These institutions share similar names but exercise different functions. Some focus on cyber disruption response while others act as clearinghouses for public or private sector entities seeking information on best practices. All of them, however, are relatively independent bodies staffed with subject-matter experts, and tasked with organizing, integrating, and coordinating disparate cybersecurity initiatives across state government.

Each one of these centers exemplifies the growing ecosystem of cybersecurity actors and the need for coordinated and timely sharing of best practices throughout and among states. Reflecting this trend, several of our policy academy states, including Oregon, are pursuing their own cyber centers.

Conclusion

I would like to conclude by, once again, reaffirming NGA's commitment to promoting cybersecurity and ensuring that states are in the best position to meet cyber threats. As technology advances, the state and, more importantly, the citizens, will become increasingly vulnerable to cyber threats. Shunning innovation is not the answer. Rather, states should meet the cybersecurity threat today, allowing them to embrace the benefits of technology more fully.