NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

The Cybersecurity Task Force held its second in-person meeting in Chicago, IL on Sunday Aug. 7, 2016. Task Force members recommended two topics for discussion at the meeting: data analytics with risk management and workforce development and education.

Speakers for the first session, "Two Tools for Cybersecurity: Risk Assessment and Data Analytics," included Commissioner and Chief Information Officer in Minnesota, Tom Baden; Stu Bradley, Vice President of Cybersecurity Solutions at SAS; and Angela Gleason with the American Insurance Association.

Tom Baden talked about how Minnesota consolidated its IT services five years ago and is now establishing security policies and standards and guidelines across the state. Lack of spending continues to be an issue for the state—the state is well below comparable federal and private corporate spending on IT and cybersecurity. Minnesota spends two percent on general IT and only two percent of that IT spending is on cybersecurity. In comparison, federal IT expenditures are around eight percent and corporate IT is around 18 percent. The CIO is leveraging analytics to improve efficiency in their systems' security even though IT consumption has doubled while the budget remains flat.

One best practice that came out of the conversation was the need for legislators to talk to their Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) outside of public hearings where sensitive information on vulnerabilities cannot be shared. It is imperative to develop trust, especially since the average tenure of CISOs is roughly 18 months. Also, Commissioner Baden highlighted the work of state and federal support systems such as federal Department of Homeland Security resources around data analytics, NASCIO reports and statistics and the Multi-State information sharing center--MS-ISAC.

Stu Bradley from SAS highlighted that the average time for states to detect a hacker is 80 days. Half the time the company is not the one to detect the hack. In order to overcome operational challenges, it is important to break down silos among different agencies and departments. Information sharing is key. Insider threats to systems can be reduced by employee training and education, and levels of security clearances can be required for access to sensitive data. A common requisite for both companies and government are standards and implementation goals as a means to benchmark progress in securing their networks.

Angela Gleason offered an interesting perspective on cyber insurance. This is a new area with little actuarial data upon which to base insurance rates. However, questions posed by insurance companies can be a way to assess an organization's risk posture. Some of the questions to address can include: What is the risk culture in the agency? How do you approach training for employees? Are there guidelines for third party relationships? Is there a cyber playbook or remediation response plan in case of a breach? How often (if at all) is the plan updated?

Do you do self-audits? If you had a breach, how long did it take to recover and how much money did it cost? What standards are used to assess your system? Do you follow NIST? What protocols do you have in place such as virus software, firewalls, etc.? Does anyone use table top exercises as a means to find out key vulnerabilities?

Sen. Westerfield from Kentucky asked about whether state systems should focus on stronger password policies given recent trends towards multifactor authentication or biometric authentication. Angela responded that although industry is moving towards more secure methods of protection (and away from normal passwords and a culture of renewing passwords every couple of weeks/months), stronger password guidelines are still appropriate. Co-Chair Assemblywoman Jacqui Irwin mentioned that California tests state employees, and any that click on phishing links sent by the IT department must undergo training, and the employee's machine is locked until they complete it.

The second half of the afternoon focused on the "Cybersecurity Education and Workforce Development" session with Senator Susan Lee from Maryland; Rodney Petersen with the National Initiative for Cybersecurity Education at the U.S. Department of Commerce in MD; Seth Robinson, Senior Director of Technology Analysis at CompTIA; and Captain Paul J. Tortora at the Center for Cyber Security Studies with the U.S. Naval Academy.

Senator Susan Lee, a member of the NCSL Cybersecurity Task Force, gave a presentation about the innovative ways Maryland is addressing cybersecurity. The state established a cyber commission for a three-year term (2011-2014) to promote jobs and innovation. A 2015 cyber council was established through the University of Maryland (at no cost to taxpayers) to develop comprehensive strategies and recommendations to protect the state's critical infrastructure and move Maryland forward as a hub of cybersecurity innovation and jobs. The council released an interim report in July. Senator Lee noted that cyber education starts in middle school to get kids interested in the subject area including through summer camps. Students are encouraged to go into computer and cybersecurity fields through tuition incentives and employment in state government as part of a tuition for service program. Senator Lee also noted that state agency personnel have to take a class each month to get access to networks, which is done through the Maryland Department of Innovation and Technology.

Rodney Petersen talked about workforce inclusion, especially reaching out to those who are underemployed. With minimal education and training some can easily enter the cyber field. As for recruitment and retention of the cyber workforce, federal and state governments are challenged to get people excited about public service in IT. Captain Tortorra talked about the Naval Academy's cyber operations major. They offer a 16-week freshman course that looks at how computers operate, how to hack, and how to defend against an attack. A mock cyber war is held between students at the end of the semester.

Speakers and members of the task force also had a larger conversation about how to engage women, minorities and veterans in this field. Workplace culture, balancing work and family life, as well as hiring processes, are some of the ways to encourage diversity. Also, states can actively recruit outside normal military and science fields, for example, recruiting potential employees in political science and law as well. Sen. Hudgins from Washington mentioned that the cyber workforce is lacking in the U.S., so people pull talent internationally, but it is hard to hire foreign nationals for security jobs.

Rep. Garofalo from Minnesota asked if any statewide policy academies have been developed at the K-12 level. Sen. Lee mentioned that Maryland recommended but did not mandate K-12 academies. North Dakota has coding schools that also are available online so anyone can go online and take the courses. Coding competitions are growing in popularity, especially with girls, who may be more engaged when working in teams or working on practical applications and coding for real life problems.

Upcoming meetings for the task force will include a joint webinar with NASCIO to discuss the upcoming survey called the “State of the States,” in October. On December 6th, the task force will meet in person again as a preconference to the NCSL Capitol Forum. Our topics of discussion will include digital crime and critical infrastructure, and we will also meet with federal counterparts and the House Cyber Security Caucus.