NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
July 2018

Happy early 4th of July! In light of the fact that our next newsletter is scheduled to come out at the beginning of the 4th of July holiday weekend, the task force is sending out this month's newsletter early. Don't forget! For all task force members who can attend NCSL's Legislative Summit, registration is now live for our next Cybersecurity Task Force Meeting on **Monday, July 30, in Los Angeles, Calif**.

Also in Cyber Task Force news:

Task Force Highlights

NCSL Staff Met with National Association of Counties and National League of Cities on State-Local Cyber Coordination

NCSL staff discussed the work of the Cyber Task Force and the recently approved proposal for a work product on state-local coordination at a recent meeting in Washington, D.C. The discussion included information on upcoming Task Force roundtable discussion to be held at the 2018 NCSL Legislative Summit to further discuss the work product. We have reached out to both the National League of Cities and the National Association of Counties for key points and high-level priorities in cybersecurity for local governments and we hope to present this feedback at our upcoming meeting.

Cyber Task Force Meeting in Los Angeles is Monday, July 30!

We hope to see you all at our future meeting in Los Angeles on July 30. Registration is now open, and we look forward to providing you with programming on Cybersecurity and Disaster Response, National Guard Cybersecurity Training and Resources for States, Data Breach and the Entertainment Industry, and Cybersecurity Maturity. We are also programming concurrent sessions in the afternoon on "Cybersecurity for Elections," joint with NCSL's Redistricting and Elections Committee; and "Responding to New Security Threats in Legislatures," joint with NCSL's legislative information technology staff section.
If Task Force members have a session idea that they would like to see programming on at a future meeting, please let us know!

Partner Highlight

IBM Study: Responding to Cybersecurity Incidents Still a Major Challenge for Businesses
IBM Security in March announced the results of a global cybersecurity study conducted by Ponemon Institute and sponsored by IBM Resilient. The study found that 77 percent of businesses that responded to the survey admit they do not have a formal cyber security incident response plan applied consistently across their organization. Nearly half of the 2800 respondents reported that their incident response plan is either informal/ad hoc or completely non-existent, and 69 percent reported that their funding for cyber resiliency is insufficient.

Learn more about the full results of the study here.

Security Tip of the Month

Cell Phone Account Fraud
Consumer Reports cautions about a new threat: cell-phone account fraud. "Crooks open up a phony cell-phone account in your name and use it to access your bank account, sign up for credit cards, or sell the phone number for other criminals to use." Steps to take to protect yourself from this scam include getting a PIN/passcode for your account from your cell phone provider and freezing your credit information. AT&T offers more tips to prevent porting of your cell phone number.

Articles We Are Reading

An Idaho Case Study on Cybersecurity Awareness and Training of State Employees:
In May, Idaho state government underwent two cyber-attacks in three days. One of the targets was a state employee in the state's tax commission who clicked on a phishing email and entered his government credentials into the site he was directed to. The state's chief information officer (CIO) caught the vulnerability and acted quickly to mitigate the damage, isolating it to only the one employee's computer. Even with the limited damage, the state had to inform 36 tax payers that their personal information was on the employee's inbox and that the employee had been compromised. The phishing email was forwarded to 103 additional contacts before the attack was contained. The state has also informed those who received the forwarded phishing email of the cybersecurity threat. Two days later, both the state legislature's website and iCourt website, which provides a portal for status updates and payments on Idaho trials, were vandalized. The state will continue providing cybersecurity training to its employees in the wake of the attack, following a call from Republican Gov. "Butch" Otter in January to create a more regimented approach to cybersecurity awareness and training throughout the state.

The full article can be read here.

Indiana CIO Offers Best Practices on the State's Cybersecurity Operations Center
StateTech summarized Indiana CIO Dewand Neely's presentation at the end of May, highlighting Indiana's successful consolidation of its IT operations of more than 100 state agencies, including six or seven data centers into one while also combining more than 10 email systems and 13 domains. However, the state found new challenges in defending the unified enterprise. Where individual agencies previously held responsibility for their own cyber defense, now the state had to establish a

cybersecurity operations center (CSOC) to defend the unified enterprise. In 2014, the state published "Ten Strategies of a World-Class Cybersecurity Operations Center," highlighting best practices and lessons learned on how to defend the entire network under a consolidated centralized CSOC. Of the 10, the CIO determined the state failed at three:

- First, staff: sometimes less is more. Originally, leadership decided to move people from operations to security and retrain existing staff. CIO Neely states in the article: "We had more hands, but we had no way to prioritize or even identify what work they should be doing."
- Second, don't bite off more than you can chew. The state's initial approach was to buy a whole suite of tools and throw them against the challenge. Later, IT leaders took a more strategic approach, adopted the National Institute of Standards and Technology Cybersecurity Framework and carefully focused on implanting one piece of it before doing something else.
- Third, understand and have reasonable expectations for data analytics and what it can do for the enterprise. Indiana used Security Information and Event Management (SIEM) and found it was trying to do too much with it, and therefore got less done. (what is SIEM?)

The full article can be read here.

State-Local Coordination a Priority in the Wake of High-Profile Attacks

Statescoop interviewed Jeff McLeod, director of the Homeland Security & Public Safety Division at the National Governors Association and CEO Alan Shark of the Public Technology Institute and a consultant for the National Association of Counties. The take-away? State and local governments are more aware of the risks and vulnerabilities in their networks and are prioritizing coordination across all levels of government. The article notes, "Coordination and cooperation between different jurisdictions and levels of government, both Shark and McLeod agreed, will be one of the key factors in improving government cybersecurity as a whole across counties of all sizes. Thankfully, Shark said, cybersecurity is on an "upward trend" among the officials he's spoken to within the last year."

You can read the full article here.

New America Foundation's Report on State Cybersecurity Efforts

In May, the New America Foundation published its report, Cybersecurity for the States: Lessons from Across America, examining state actions to advance cybersecurity efforts, with an in-depth focus on three case studies of states that have seen demonstrable successes. The three case studies include Arizona and the Arizona Cyber Threat Response Alliance, New Jersey and the New Jersey Cybersecurity and Communications Integration Cell, and Washington state's multidisciplinary approach. The report includes recommendations for the federal government's role in helping states develop their cybersecurity programs.

National Governors Association Continues Cybersecurity Policy Academy

The National Governors Association (NGA) will work with four states through their Policy Academy on Implementing State Cybersecurity. Indiana, North Carolina, West Virginia and

Wisconsin were chosen for the policy academy and have dedicated resources and support from their governor to work on strengthening cybersecurity in their state. NGA looked for states that "already have some planning in place—they have maybe some response plan or some governance plan, and they're at the point now where they want to implement that successfully or maybe just receive support for ongoing efforts to do that," McLeod is quoted in the Statescoop article.

You can read the article here, and find more information about the NGA Cybersecurity Policy Academy here.

StateTech Lists its Top Four Threats Against State and Local Governments

1. Malware. Although not a new threat, the evolution of more sophisticated attacks such as ransomware continue to pose a significant threat to state networks.
2. Talented attackers and well-funded attacks known as advanced persistent threats target government agencies. These attackers, typically sponsored by nation-states, are quite patient and focus on very specific targets. Once they gain access, they operate with stealthy techniques, placing a high priority on avoiding detection.
3. IoT devices have critical deficiencies in security measures—including an increased reliance on cellular networks.
4. Legacy systems lack up-to-date cybersecurity controls that can protect against attacks.

You can read the article here.

Federal Activity

Federal Agency Re-org?

The Hill reported a recent announcement from the Office of Management and Budget saying the agency will begin a reorganization effort to streamline hiring cybersecurity professionals as one of its top priorities. As with all levels of government, the federal government struggles to retain and hire qualified cyber professionals. The Department of Homeland Security and the Office of Management and Budget, working in coordination with all federal departments and agencies, will unify their cyber workforce efforts as one way to address the talent shortage and the growing demand across the private and public sector for cybersecurity professionals. The report states that "this Administration will work towards a standardized approach to federal cybersecurity personnel, ensuring Government-wide visibility into talent gaps, as well as unified solutions to fill those gaps in a timely and prioritized manner."

Read the full article here.

President Nominates the Assistant Secretary of Energy for Cybersecurity

Earlier this month, the president nominated Karen Evans as the assistant secretary of energy for Cybersecurity, Energy Security and Emergency Response. The assistant secretary will be a key figure in a new office at the Department of Energy, who is responsible for addressing cyber and security in the energy sector. Evans is currently the national director for the U.S. Cyber Challenge and a former

Bush administration IT official. She also served as the Energy Department's chief information officer and later the administrator for E-Government and Information Technology under Bush.

Senate Confirms Department of Homeland Security Cyber Unit Secretary
The Hill reported earlier this month of the recent Senate confirmation of Christopher Krebs to serve as the lead on the Homeland Security's National Protection and Programs Directorate (NPPD) in the Homeland Security Cyber Unit. Formerly the acting undersecretary, Krebs will now be responsible for overseeing the security of federal civilian networks and spearheading the federal government's efforts to protect critical infrastructure from cyber and physical threats. NPPD is also newly responsible for helping states secure their digital voting systems.

Learn more about the confirmation here.

State Activity

New State Data Security Laws
New laws in Idaho, Kansas and Virginia this year impose security requirements on state agencies.

Idaho passed legislation that establishes the Office of Information Technology Services to oversee coordination and implementation of the state's cybersecurity policies. The office is required to communicate with state agencies concerning information security needs, coordinate with them to test the vulnerability of technology systems and mitigate risks, and ensure that state agencies implement mandatory education of state employees. The law requires the office to create a statewide cybersecurity website, publish cybersecurity best practices, and develop statewide public outreach efforts for the protection of sensitive data.

Kansas established a new Information Security Office. The office, directed by the chief information security officer (CISO), must implement information security risk-management programs, assist in the development of recovery procedures in the event of cyberattacks, and ensure that cybersecurity training programs are provided to executive branch agencies. The law also requires that executive agency heads ensure the existence of information security programs, participate in statewide cybersecurity programs, implement policies that ensure all data and information and technology resources are properly maintained, develop safeguards to protect against and recover from cybersecurity threats, and submit cybersecurity assessment reports to the CISO.

Virginia now requires the state CIO to conduct an annual cybersecurity policy review of each executive branch agency and submit a report to the chairman of the House Committee on Appropriations and the Senate Committee on Finance.

Additional information about other state data security laws is available here, and 2018 cybersecurity legislation is listed here.

NCSL Cybersecurity Staff: Susan Parnas Frederick (susan.frederick@ncsl.org), Danielle Dean (danielle.dean@ncsl.org), Pam Greenberg (pam.greenberg@ncsl.org.

Denver: 303-364-7700
Washington, D.C.: 202-624-5400