NATIONAL CONFERENCE OF STATE LEGISLATURES

NCSL Executive Task Force on Cybersecurity
Jan. - Feb. 2019

Task Force Highlights

We had a terrific meeting last month in New Orleans. Thanks to all who attended. The agenda for the meeting and presentation materials are now posted on the task force website. Our next meeting will be at NCSL's Legislative Summit in Nashville, Tenn., on Sunday, Aug. 4. Details to follow.

Task Force Cited in Government Technology Article

NCSL's Cybersecurity Task Force was cited in a recent article in Government Technology for answering the call to address cybersecurity issues in the states. The article noted that as governments increasingly move to digital platforms, IT professionals have identified security and risk management as a top priority

in the National Association of Chief Information Officer's new report. Many state legislatures will take up IT budgets this year and may have to deal with how best to budget for cybersecurity.

NCSL is lauded for working to educate state officials on cybersecurity issues such as filling the talent gap and providing adequate funding for security are listed as top priorities for Chief Information Officer's. Read more here.

Federal Activity

Bipartisan Support for Cybersecurity Workforce Development

A bill from Senators Amy Klobuchar (D-Minn.) and John Thune (R-S.D.) would create an exchange program between the federal government and private industry to boost the public cybersecurity workforce. Federal workers would be able to develop expertise in private firms while industry or academic experts would have the opportunity to work for federal agencies for up to two years.

Further, the Senate Homeland Security Committee is taking up several bills on cybersecurity, including legislation that would allow federal cybersecurity workers to move to other agencies more easily. Read more here.

New GAO Report Calls for Federal Legislation on Internet Privacy

In the wake of last year's Facebook admission that up to 87 million users' personal data may have been improperly disclosed, the U.S. Government Accountability Office (GAO) has recommended that Congress "consider developing comprehensive internet privacy legislation to better protect consumers." Currently, the U.S. does not have a comprehensive law governing internet privacy. The Federal Trade Commission (FTC) has issued internet privacy regulations that protect children and the financial privacy of adults. Stakeholders who were interviewed for the GAO's report stated that there needs to be an overarching federal internet privacy statute, that the FTC should engage in further rulemaking on internet privacy to provide clarity on the subject, and that the FTC should have civil penalty authority for first time violations of the FTC Act, which protects consumers from unfair and deceptive trade practices.

Read the highlights and full report here.

House Committee on Homeland Security Holds Election Security Hearing

On Feb. 13, the U.S. House Homeland Security Committee held a hearing on election security. The hearing addressed the election administration provisions of H.R. 1, the "For the People Act." This bill is a comprehensive look at election integrity, access, and security. It requires mandatory online voter registration, auditable paper trails, and authorized funding for election infrastructure research and development funding. Listen to the hearing here.

Security Tip of the Month

Can You Spot a Phishing Email?

Jigsaw, a unit at Google's parent company, Alphabet, just released an online quiz based on the latest techniques used by attackers. Phishing messages often appear to be from well-known or seemingly trustworthy entities, but instead collect information for fraudulent purposes. Twenty-three states and Guam have laws specifically aimed at phishing schemes.

Try taking Jigsaw's phishing quiz—it's harder than you might think. Then read Forbes' Four Phishing Attack Trends To Look Out For In 2019.

State Activity

Data Security Laws

At least 24 states have laws that address data security practices of private sector entities. Most of these data security laws require businesses that own, license, or maintain personal information about a state resident to implement and maintain reasonable security procedures and practices, and to protect personal information from unauthorized access or disclosure.

NCSL regularly tracks cybersecurity legislation, and determined that the number of states with these data security laws doubled just since 2016, reflecting growing concerns about computer crimes and breaches of personal information. We will soon post tracking web pages for 2019 cybersecurity and security breach legislation.

NCSL Resources on State Digital Privacy and Security Issues

A new NCSL web page on Digital Privacy and Security Resources brings together NCSL resources on data privacy, cybersecurity and data security and computer crime issues. The web page is designed to make it easier to find web pages and links to NCSL publications in these topic areas. The web page is an extensive, but not exhaustive list of resources available, so if you don't see what you need, please ask if we have additional information.

What We're Reading

Survey: Execs Worldwide Back IoT Security Rules

Tech executives and business decision-makers want stronger regulation and guidelines for internet-of-things (IoT) devices, according to a recent survey, an FCW article reports. The survey of 950 IT and business decision makers globally, including 200 in the United States, found that nine in 10 respondents supported some IoT cybersecurity regulations.

Among those that are seeking more regulations, 59 percent said that rules should include identifying who is responsible for securing data in different parts of the ecosystem, and 53 percent said there should be consequences for lapses. Read more here.

Cyber Drill Demonstrates Need for More Coordination

A drill called Jack Voltaic 2.0 with the City of Houston, regional emergency management officials, and the Army Cyber Institute shed light on gaps in cyber-attack response and coordination. Cities, states, and regional authorities are working with the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security to improve response, but a report on the drill provides several state and federal recommendations to further prepare for attacks. Read more here.

NCSL Cybersecurity Staff: Susan Parnas Frederick, Pam Greenberg, Abbie Gruwell and Heather Morton.

Denver: 303-364-7700

Washington, D.C.: 202-624-5400