NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
March 2018

Good Afternoon Task Force Members. Please save the date for the next meeting of the NCSL Executive Task Force on Cybersecurity will be in **Denver, Colorado on Friday, May 11th** at the J.W. Marriott, in conjunction with the NCSL Executive Committee Meeting.

The task force will host a dinner Thursday evening, May 10th and all the details as well as the proposed session topics can be found on the attached agenda. The registration link will be live soon and more information about hotel, flight and stipend will be sent out to the task force listserv.

Also in Cyber Task Force News:

Task Force Highlight: Oregon

The Oregon Joint Legislative Committee on Information Management and Technology held a meeting on Friday, February 9, 2018 to receive an update on the implementation of Senate Bill 90. The meeting included a recently completed assessment report that is designed to support the development plan for Oregon's Cyber Security Center of Excellence. Interestingly, the first chapter of the report outlines a comparative policy analysis with California, Colorado, Florida, Illinois, Maryland, Michigan, New Jersey, New York, Texas, Virginia, and Washington.

Also included are recommendations for Oregon's Cyber Center of Excellence in three major policy areas: Workforce Development Initiatives; Cyber Hygiene Training, and Multi-Sector Engagement. The final chapter of the report prescribes next steps including continued learning from other states, workforce development and engaging funding experts.

The full report can be read here.

Center for Internet Security Releases Handbook on Elections Security

The Center for Internet Security released a set of best practices on how to protect elections infrastructure. The publication, *A Handbook for Elections Infrastructure Security*, focuses on assisting organizations involved in elections to better understand what to focus on, know how to prioritize and parse through the enormous amount of guidance available on protecting IT-related systems and address common threats.
The handbook is available here.

Articles We Are Reading

Apple and Cisco to Introduce Cyber Insurance

Apple and Cisco announced a new partnership with insurers Aon and Allianz to offer cyber insurance policies for organizations that meet best security practices and use products from the technology companies. The policies may cover data breach response, a potentially expensive undertaking that can involve forensic investigators, public outreach, managing inquiries from regulators and lawsuits.
Found in Apple Newsroom

SANS Institute Pilots Cyber Training for High School Girls

Eighteen states and one territory will release a new online cybersecurity training pilot program for high school girls this year. Originally, SANS piloted CyberStart in 7 states, only to find out that of the participants they received, only 5 percent were women. Now that its scaled up to 18 states, SANS released Girls Go CyberStart, specifically targeting high school girls. The first-place winner in each state will receive a trip to the Women in Cybersecurity conference in Chicago March 23-24.
Govtech's full article is here States Partner to Get Girls Interested in Cyber, IT.

Department of Justice Charges 36 Cyber Criminals

The DOJ charged 36 individuals in a cybercrime ring bust that trafficked in peoples stolen online personal and financial information. The accused all participated in an international operation called "Infraud" that sold stolen identities, credit card data, financial information, social security numbers and other personally identifiable information. They also sold and used malware. So far, 13 of the individuals have been arrested and 5 are Americans. The total operation gained about $530 million from financial institutions and other victims throughout the world.
The entire article can be read in the Hill.

Unreported Cyber Crime

In what was described as an 'iceberg' of unseen crimes, this article dives into one state law enforcement's journey into the under reporting of cybercrimes. The story begins with the Utah chief of law enforcement tracking on the opioid crisis, which led to the observation that underreporting of online sales of fentanyl were hindering his investigation. The nature of the internet has allowed criminals to perpetrate crimes anonymously and remotely, with criminals capable of committing crimes while outside of the state. Crimes such as: identity theft; sexual exploitation; ransomware attacks; fentanyl purchases on the dark web; human trafficking for sex or labor; revenge porn; credit card fraud; and a host of other crimes committed are not only vastly underreported, but open other jurisdictional issues such as what state 'owns' their crimes? Who must investigate them? What are the specific violations? Who are the victims?
Read the full article in the New York Times

Federal Activity

U.S. House Introduces Bill for Funding State Elections Infrastructure

Representative Thompson (D-Miss.) introduced H.R. 5011, the Elections Security Act, on Feb. 14th. The legislation would include more than $1 billion in federal grants to assist states secure voting infrastructure including updating voting machines, providing cybersecurity training and hiring new technology staff. Another aspect of the bill would be to authorize a $20 million grant program for states to perform post-election audits or "risk-limiting" audits.

The proposal does come with some limitations, as states would be prohibited from spending federal funds unless voting system sellers agree to report cyberattacks and observe certain guidelines set by the Elections Assistance Commission and Department of Homeland Security.

Read the full article in the hill

Data Breach Notification Laws a Hot Topic Again

House Financial services subcommittee discussed state and federal data breach notification and cybersecurity laws. Panelists testified that Congress should consider a national data breach notification bill to preempt the 'myriad' of state standards companies currently adhere to. Generally NCSL does not oppose baseline federal data security breach notification standards, provided that the requirements do not preempt state authority to adopt standards that provide additional protection and notification. NCSLs full data security breach notification policy is located here. The full hearing can be seen here.

Legislation to Help Fight Cyber Crime

Sen. Hatch (R-Utah) introduced a bill on Monday Feb. 5th that would establish a framework for law enforcement to gain access to cloud-stored data. The "Clarifying Lawful Overseas Use of Data" (CLOUD) Act would apply to data located inside or outside of the United States and establish standards for U.S. officials to create international data sharing agreements. The CLOUD Act would likely impact Microsoft's pending Supreme Court case on whether the U.S. can obtain Microsoft emails which are stored in a data center in Ireland. The lower court ruled that Microsoft did not have to release the data overseas, after denying the Department of Justice's request.

To read the full article in The Hill, click here.

State Activity

State Legislatures Amend Data Breach Legislation

Although forty-eight states have security breach notification laws, other state legislators are still working to protect consumers in the face of continuing data breaches. At least 30 states, Puerto Rico and D.C. in 2018 are considering security breach notification bills or resolutions. Of the two states without a breach law, South Dakota passed legislation this year and the bill has been sent to the governor. Alabama has bills pending.

Legislation in most other states would amend existing security breach laws. For example, since the Equifax data breach in 2017, a number of states introduced legislation that would provide for free

credit freezes for victims of data breaches or that are otherwise directed at credit bureaus or financial institutions. Other bills would amend breach laws to expand the definition of "personal information," to set specific timeframes within which a breach must be reported, or require reporting to the state's attorney general. In addition, several bills would require notification in the case of breaches of student information.
Additional information is available here.

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