NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News | November 29, 2017

As states turn their eyes toward the 2018 legislative session, legislators already are beginning to think about budgeting and how cybersecurity will fit into their state plans. This month's cybersecurity newsletter discusses the cybersecurity topics states might consider in the upcoming year as well as providing a few highlights on activity across the U.S.

But first:

Task Force Highlight: Rhode Island Cyber Hygiene Event

Senator Louis P. DiPalma (D) and U.S. Representative James R. Langevin (D) hosted a cyber hygiene event for Rhode Island constituents on Oct. 18. The event was aimed at providing a public forum to bring awareness to the various current cyberthreats and provide practical steps to protect one's self, family, identity and data from cyberattacks. The full press release can be found here and on our task force website.

NCSL Staff, Heather Morton, Discusses Blockchain

Did You Know?

- The World Economic Forum estimates that taxes will be collected for the first time by a government via blockchain by 2023.
- Blockchain is a shared ledger database that records and shares every transaction that occurs in the network of users.
- Five states—Arizona, Delaware, Illinois, Nevada and Vermont—have enacted or adopted blockchain legislation.

Digital currencies are only one way to use blockchain. Other evolving applications can include online voting, medical records, insurance policies, property and real estate records, distribution of copyrights and licenses, supply chain tracking and smart contracts where payouts between the contracted parties are embedded in the blockchain and automatically execute when contractual conditions have been met. As these other applications evolve, developers will need to address the issues of setting blockchain technological standards and the danger that the lack of standards could impede interoperability.

In 2017, four states—Arizona, Delaware, Illinois and Nevada—enacted or adopted blockchain legislation. Arizona enacted two bills. The first bill, H.B. 2417, established guidelines for electronic signatures and records using blockchain technology. In the second bill, H.B. 2216, the Legislature made it unlawful to require a person to use or be subject to electronic firearm tracking technology and included blockchain and distributed ledger systems in the definition of electronic firearm tracking technology.

Read the full LegisBrief.

The Task Force will be hosting a session on Blockchain at our next meeting on December 12 in Coronado, CA. Be sure to REGISTER HERE and attend the meeting!

Sponsor Highlight: AT&T Discusses Cyber Budgeting

Developing a budget to limit the cyber risk to an organization can be a stressful experience. Balancing maintenance with development, adding in a dash of compliance or legal requirements, and something to cover unforeseen expenses helps to establish your anticipated costs. Then there are unexpected expenses that could be the result of a technology change, a cyberattack, or simply a change in the regulatory environment. Splitting security out from the overall IT budget, however, may better protect against funding cuts for security. In many organizations, the IT security budget is a part of the overall IT budget and therefore can be a place to save when budgets start to get tight.

Read the full AT&T article.

NCSL Staff, Pam Greenberg, Discusses Cybersecurity

Did You Know?

- Financial, health care and public sector organizations accounted for more than half of the breaches in a 2017 Verizon report on data breaches.

- The No. 1 leading cause of data breaches worldwide is employee error, according to the Privacy Rights Clearinghouse.

- Most cyberattacks begin with a user clicking on a phishing (fraudulent) email, says threat management company PhishMe, and an average of 4,000 ransomware attacks occurred per day in 2016, according to the FBI.

A little more than a decade ago, a security breach that released the personal information of almost 145,000 people to a criminal enterprise created a rush in state legislatures to enact security breach disclosure laws. That early breach seems almost insignificant when compared to the recent Equifax data breach, which exposed the Social Security numbers and other sensitive personal information of nearly 146 million Americans.

Forty-eight states, Washington, D.C., and the territories now have laws requiring that security breaches be disclosed to consumers. Many state lawmakers, however, continue to ask what they can do to protect citizens from security breaches.

Read the full LegisBrief.

Federal Activity

Cyber Advisory Board Approves Report to Trump on Internet Security Challenges

An advisory committee under NSTAC unanimously approved and released the report Thursday Nov. 16, recommending baseline cybersecurity standards in internet of things (IoT) devices as well as Department of Justice (DOJ) enforcement against botnets and those that operate them. This report will contribute to a larger report mandated by the president under the cyber executive order.

Possible State Pre-emption?

The report addresses private sector concern about state and federal overlap on regulatory requirements. NSTAC states that if the government wants to be a partner with the private sector in addressing cyber threats, government activity must not come in the form of regulation and punitive enforcement. The report further suggests that the Federal Government should discourage state activity regulating data security and enforcement. This is not the end however, where NSTAC does recommend "that the Federal Government should encourage states first to adopt and implement available consistent cybersecurity best practices and recommendations for the states' own administrative organizations…States should be encouraged to participate in national venues with key stakeholders to attain consistent approaches toward cybersecurity. These should include the National Governors Association, the National Association of State Chief Information Officers; the National Conference of State Legislatures, and the DHS State, Local, Tribal and Territorial Government Coordinating Council".

Read the full report.

SAVE THE DATE: Tuesday Dec. 5th , MS-ISAC Webinar on Smart Cities, Cybersecurity and the Intersection of IoT

IoT and smart cities technologies are affecting—and improving—the business of government at all levels. Powering performance by accelerating processes, agencies are growing increasingly reliant on IoT devices and the data they produce. The security implications of these emerging technologies, however, are an ongoing challenge, particularly as IoT devices present new entry points into networks for malicious attacks.

What you'll learn:

- How state and local cyber professionals are coordinating efforts to bolster data security in today's age of connectivity and smart technology.
- How IoT is changing today's cyber landscape—from emerging threat vectors to new security considerations and more.
- How to securely leverage IoT and smart cities technology to improve your organization's processes and strengthen your cyber posture.

Moderator
Roisin Suver, senior liaison to the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC)
Panelist:
Robert O'Connor, chief information security officer, Maricopa County, Ariz.

Additional Panelists TBD
You can register for the event up through Tuesday, Dec. 5, 2017, at Noon EST.

Register Now

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)

Denver: 303-364-7700
Washington: 202-624-5400