NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
Aug. 2018

Thank you to all who were able to attend the Cybersecurity Task Force meeting during NCSL's 2018 Legislative Summit. We hope that you enjoyed the sessions. If you have any topics you'd like us to program for our next meeting, please let any of our NCSL staff on the task force know. Here is the reimbursement form. Please include all receipts with the form and submit the documents to ap@ncsl.org. After accounting receives the information, it should take about two weeks for processing and reimbursement.

Also in Cyber Task Force news:

Task Force Highlights

NCSL 2018 Legislative Summit Highlights

NCSL now has the live-streamed Summit sessions available on our website. You can find the sessions here, including Cybersecurity for Elections: State Policy Options and Cryptocurrency: Currency of the Future or Just a Fad?

The NCSL Blog covered the Cybersecurity for Elections: State Policy Options session in two blog posts—one on July 31 and another on Aug. 10.

Also, presentations and handouts from the task force sessions are available here, including presentations by speakers for the Responding to Cybersecurity Threats in Legislatures session: Adam Kleiner of Microsoft, Paul Hoffman of MS-ISAC, and Jeff Ford of the Indiana General Assembly.

Another task force member, Sean McFaden of Oregon, spoke at the Evaluating the Cost of IT Projects session. His presentation is available here.

Partner Highlights

Microsoft Blog: From Policy to Practice: Strengthening Cybersecurity in State Governments

Cyberattacks continue to threaten our everyday lives, effecting the way we shop, the way we communicate and the way we do business. State governments play a significant role in society, administering and delivering services, and providing the backbone of governance in the United States. It is, therefore, important that they implement a robust and multi-faceted cyber policy. Microsoft's new white paper, From Policy to Practice: Strengthening Cybersecurity in State Governments provides support and key policy recommendations for state governments as they look to strengthen their existing state practices.

Read the Blog.

IBM Report: Managing Cybersecurity Risk in Government

IBM's Center for the Business of Government released a report that addresses how government can find and tailor a risk assessment and management model to fit agency needs and vulnerabilities while taking into consideration existing law and policy. The model outlines five steps to improve security outcomes: Prioritize, Resource, Implement, Standardize, and Monitor—or the PRISM model.

Read the report.

Security Tip of the Month

The Center for Internet Security: Sun, Sand and Cybersecurity

Thomas Duffy, MS-ISAC chair and senior vice president of operations and services at the Center for Internet Security, has a few suggestions about good cyber practices during the summer season. As a previous speaker at NCSL's cyber task force meetings, he provides eleven tips to "avoid mayhem and make magical family memories by taking a few simple cyber safety steps before you head out of town. The goal here is to prepare your devices for travel and to keep them from being used against you."

Read the tips and the full article.

Articles We Are Reading

Cyber Insurance: Georgia's Perspective

July marks the first-year anniversary of the Georgia's cybersecurity insurance policy. Is the insurance plan worth it? It is to Georgia CTO Steve Nichols and CISO Stanton Gatewood, according to this recent GCN article. About 38 percent of states had cyber insurance in 2017, according to the National Association of State Chief Information Officers' October 2017 survey. South Carolina is the most recent state to issue a request for proposals on cyber insurance, but other states bought in several years ago. For instance, West Virginia has had a policy since 2014 and Utah since 2015.

As for Georgia, the insurance policy has been particularly helpful when a cyber incident occurs, and the provider can deliver incident response services, including legal, public relations and notification services. This allows the agency to focus on security management and updates. The article notes that "Georgia's policy covers all executive branch agencies except for the Georgia Department of Defense (which serves as the state's National Guard and is run like a federal agency), the state Department of Education and all higher-education institutions. Because insurers rank personally identifiable information high on the risk list, the broker said that including education data on minors would distort the pricing."

Read the full article.

ICMA Report: Protecting Local Government Digital Resources

The International City/County Management Association released a report, with the support of Microsoft, on local government cybersecurity efforts across the country. The report begins with a survey that looks at major challenges local governments face in implementing a strong cybersecurity strategy. Chief information officers in 411 local governments with populations of 25,000 and greater responded to the survey, identifying the top cyber challenges local governments are facing.

The most important problem: the constant threat of cyberattack. Of the respondents, about 44 percent reported that they are under attack hourly or daily. Another problematic finding was that 27.6 percent did not know how often they were attacked, 29.7 percent did not know how often they've experienced a cyber incident and 41.0 percent did not know how many breaches have occurred. One of top barriers to cybersecurity, according to 58.3 percent of total respondents, is not being able to pay competitive salaries for cybersecurity personnel.

The report also discusses planning and leveraging resources for cybersecurity effectively. It includes three case studies: DeKalb County, Georgia; Jefferson County, Alabama; and the City of Roseville, California. The report includes an annotated list of online cybersecurity resources.

Read the report.

NACo 2018: 5 Ways Counties Can Stay Secure If They Use Foreign Hardware and Software

County IT leaders and technology experts, speaking on a panel at the National Association of Counties 83rd Annual Conference and Exposition in Nashville, Tenn., said that county governments must always be vigilant around IT security, no matter where they get their hardware and software. State Tech magazine summarizes the session and five key take-aways:

1. Ensure IT Solutions Comply with Cybersecurity Requirements.
2. Follow the Advice of Cybersecurity Frameworks.
3. Hold Technology Vendor Partners Accountable.
4. Bake Cybersecurity into All IT Devices and Services.
5. Create (and Practice) a Cybersecurity Incident Response Plan.

Read the full article.

Arizona: Election Security Highlight

"As a state, we get attacked about 8.5 million times a month," said Mike Lettman, co-chair of the Arizona cybersecurity team. The computers at the Secretary of State's office, which houses the elections division, gets hit tens of thousands of times. "It's not uncommon to get over 50,000 unwarranted attempts or intrusions a month," said Secretary of State Michele Reagan. So how is the state keeping hackers out of its databases?

Some key take aways: First, your vote is not online. Ballots are also paper, so they can be recounted. Voter information, however, is online. That means it is vulnerable to hacking. Additionally, Arizona's team communicates with federal cybersecurity officials to ensure they're up to date on the latest threats and methods.

Read the full article.

Federal Activity

U.S. Chamber of Commerce Coalition Letter in Support of H.R. 3359

The U.S. Chamber of Commerce sent a coalition letter to Senate Majority Leader McConnell and Senate Minority Leader Schumer in support of H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act. The House passed the bill in December 2017. Other coalition members include the American Bankers Association, American Gas Association, CTIA and USTelecom-The Broadband Association.

According to the letter, H.R. 3359 would modernize the Department of Homeland Security National Protection and Programs Directorate (NPPD)—which provides key leadership to strengthen the security and resilience of our country's cyber and physical infrastructure in two important ways. First, it would restructure the directorate to optimize the ways in which NPPD carries out its authorities, including engaging with businesses before, during, and after cyber incidents. Second, the bill would rename NPPD the Cybersecurity and Infrastructure Security Agency to more clearly communicate the agency's cybersecurity mission.

State Activity

Colorado and Vermont Enact New Data Security Laws

Colorado's governor, in late May, signed H.B. 18-1128, putting into effect new security procedures for government and businesses.

Businesses that maintain, own, or license personally identifying information or that use a third party as a service provider must implement and maintain reasonable security procedures and practices that are appropriate to the information stored and size, and nature of the entity.

Governmental entities must also maintain reasonable security measures to protect personal identifying information from unauthorized access, use, modification, disclosure or destruction. Those that use third-party service providers must require the providers to implement reasonable security measures.

The act also amends the state's security breach notification law by adding new definitions of personal information, requiring reporting of a breach no later than 30 days from the date of the breach and specifying what information must be included in a breach notification.

Vermont became the first state in the country to enact legislation (H.B. 764) to regulate data brokers by requiring registration and security standards. The legislation, enacted in May, defines a "data broker" as "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship."

The act sets forth detailed elements of a required data security program. In addition to requiring annual registration by data brokers, it provides that companies must disclose to consumers data that is collected and provide clear instructions about how to opt out of having their data collected.

The act also requires the attorney general and secretary of state to prepare a report about the implementation of the act to the House Committee on Commerce and Economic Development and the Senate Committee on Economic Development, Housing and General Affairs by March 1, 2019.

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