NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
June 2018

Good afternoon Task Force members. 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

Georgia Governor Vetoes Controversial Cybersecurity Bill

During our Spring Executive Committee Task Force meeting, Georgia Representative Don Parsons discussed a cybersecurity bill that was debated, approved and eventually vetoed in his state. Senate Bill 315, would have amended Georgia's law governing computer crimes to create an exception under the definition of "unauthorized computer access." It would allow individuals to engage in "active defense measures that are designed to prevent or detect unauthorized computer access." Opposition to the bill, including Google and Microsoft, warned that the provision "broadly authorizes the hacking of other networks and systems under the undefined guise of cybersecurity."

"Network operators should indeed have the right and permission to defend themselves from attack, but, before Georgia endorses 'hack back' authority in 'defense' or even anticipation of a potential attack with no statutory criteria, it should have a much more thorough understanding of the ramifications of such a policy," the tech groups wrote to the governor.

For more on the legislation and the broader debate around 'active cyber defense,' click here.

NCSL Staff Present to NASCIO D.C. Fly-In Delegation

Susan Frederick and Danielle Dean discussed the work of the Cyber Task Force before a meeting of state Chief Information Security Officers (CISOs) in Washington, D.C. last month. The discussion included information on upcoming Task Force programming as well as highlighting our most recent work product "Budgeting for Cybersecurity."

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

Although we saw many of you at our meeting in Denver, we also hope to see you at our future meeting in L.A. 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 (NALIT).
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

AT&T Public Sector Page on LinkedIn

AT&T is promoting the NCSL Cybersecurity Task Force "Budgeting for Cybersecurity Guide" on their public-sector page on LinkedIn. The introduction states: "budgeting for state cybersecurity efforts is a challenging process." Check out the NCSL discussion guide for legislators, chief information security officers and chief information officers. *You can follow on LinkedIn here.*

Security Tip of the Month

Securing Your Web Browser

According to the U.S. Computer Emergency Readiness Team (US-CERT), there is an increasing threat from software attacks that take advantage of vulnerable web browsers. These attacks can cause problems such as spyware being installed without your knowledge or intruders taking control of your computer. Information from US-CERT discusses why you need to secure your web browser, outlines web browser features and risks, and explains how to secure different browsers, including Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome and other browsers.

Articles We Are Reading

Tennessee County Election Website Taken Offline During Voting

A DDoS (distributed denial of service) attack took several servers offline during an April Knox County, Tenn. election. The attack focused on the election commission website that displayed results of the county mayoral primary, and the county had to distribute printed results during the outage. Knox county confirmed that election results were not affected and the election machines are never connected to the internet. A security firm has been hired to analyze the attack and report on what occurred during the outage.

The full article can be read here.

Webinar: Best Practices for State and Local Government Disaster Recover Planning

Government Technology hosted a webinar on May 24 exploring state and local disaster recovery planning. The U.S. Department of Justice estimates more than 4,000 ransomware attacks have occurred every day since the beginning of 2016, and government is a prime target. Given such risks, a robust disaster recovery and data protection plan is critical for any state or local government organization. Speakers included: Herminio Rodriguez, Director of Information Technology, City of Sarasota, Fla; Salim Ruffin, Senior Systems Engineer, Veeam Software; Moderator: Morgan Wright, Senior Fellow, Center for Digital Government.

The webinar explored:

- How government agencies can meet growing employee and citizen expectations for access to online services while ensuring data is well-protected.
- How to maintain control, visibility and access to data.
- How to confirm strong data recovery capabilities are in place should the unexpected occur.
- How the city of Sarasota, Fla., fought back after a virus encrypted 160,000 files and cyber criminals demanded $33 million in Bitcoin as ransom.

Watch the full webinar here.

Six States Hit Harder by Cyberattacks Than Previously Known, New Report Reveals

National Public Radio reported on a recently released Senate Intelligence Committee report detailing initial findings on Russian interference in U.S. elections systems. The committee report confirms that they uncovered no evidence that any vote tallies were manipulated or that any voter registration data was deleted or changed. But six states were targets for hacking into public-facing websites to gain access and either read or manipulate data. The article goes on to explain how manipulating voting results on a website, when not actually changing ballots, can sow doubt in the election process.

The full article can be read on their website.

How Connected Devices Can Be Used to Mine Cryptocurrency

Steve McGregory, director of the Application and Threat Intelligence Program at Ixia, talks with Greg Otto, Editor-in-chief of CyberScoop News, on how criminals are using people's connected devices to mine cryptocurrency.

You can watch the full video here.

Cybercrime Costs Americans Billions

According to the FBI's Internet Crime Complaint Center report released earlier this month, cybercriminals cost Americans $1.42 billion in 2017. Last year the FBI received nearly 300,000 complaints, with the largest exploits derived from payment scams, data breaches, phishing attacks, identity theft and business email compromises. The latter led to the heaviest losses, with $676 million in costs for businesses attacked under email compromise schemes. States with the most reported victims and highest losses: California, Texas, Florida, New York and Pennsylvania.

Federal Activity

House Energy and Commerce Committee Clears Electric Grid Cybersecurity Bills

Four bills cleared the House Economic and Commerce Committee earlier this month, all by voice vote. The bills—H.R. 5174, H.R. 5175, H.R. 5239, and H.R. 5240—would strengthen the Department of Energy's emergency response efforts; coordinate federal, state and business responses to physical and cyber threats; establish a voluntary program housed in the Department of Energy to test cyber products to be used in power systems; and encourage public-private partnerships.

Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts

The U.S. Department of Homeland Security (DHS) released a strategy outlining the Department's approach to identifying and managing national cybersecurity risk. The DHS strategy details a department-wide approach to address the evolving threats to our nation's cyber and critical infrastructure security. The department's strategy sets forth a five-part approach to manage national cyber risk aimed at ensuring the availability of critical national functions and fostering efficiency, innovation, trustworthy communication, and economic prosperity in ways consistent with our national values and that protect privacy and civil liberties.

- **Risk Identification:** Assess the evolving national cybersecurity risk posture to inform and prioritize risk management activities.
- **Vulnerability Reduction:** Protect federal government information systems by reducing the vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity.
- **Threat Reduction**: Reduce national cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.
- **Consequence Mitigation**: Respond effectively to cyber incidents to thereby minimize consequences from potentially significant cyber incidents through coordinated community-wide response efforts.
- **Enable Cybersecurity Outcomes**: Strengthen the security and reliability of the cyber ecosystem by supporting policies and activities that enable improved global cybersecurity risk management and execute departmental cybersecurity efforts in an integrated and prioritized way.

Learn more about the strategy here.

State Activity

The Michigan Cyber Civilian Corps (MiC3) is a group of trained cybersecurity experts who volunteer expert assistance to enhance the state's ability to rapidly resolve cyber incidents when activated under a governor-declared state of emergency.

Michigan H.B. 4508 was signed by the governor in late 2017, solidifying the program in statute. A House Fiscal Agency analysis summarizes the legislation and outlines arguments for and against the bill.

The law requires volunteers to enter into a contract with the Department of Technology, Management, and Budget (DTMB). Volunteers must agree to protect from disclosure any confidential information acquired through participation in the program, may not have any conflicts of interest, and must consent to a criminal history check and criminal records check.

The law also provides that the DTMB and the state are immune from tort liability for acts or omissions by a volunteer. In addition, volunteers are immune from tort liability for an injury to a person or damage to property that occurs while he or she is deployed and acting on behalf of the DTMB.

Bills in Indiana and the District of Columbia were introduced this year to create similar programs.

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