NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
February 2018

It is a productive start to 2018. Bills are being filed at the state and federal level to secure internal networks and to protect against cyber criminals. There are several events to look for, AT&T has some words of wisdom for states as they continue with sessions, and the task force released their cyber budgeting guide book. This newsletter will focus on all the upcoming events and what states should keep in mind while discussing cyber policy in their 2018 legislative sessions.

But first:

Task Force Highlight: Budgeting for Cybersecurity

NCSL staff is excited to announce the release of the NCSL Cybersecurity Task Force Budgeting for Cybersecurity Guide, now available on our website. Thank you to all task force members and sponsors for your contributions to the guide. A very special thank you to **Sean McSpaden** and **Monique Appeaning** for your time, knowledge, and considerable contributions in writing the guide. Also, thank you to the National Association of State Chief Information Officers and the U.S. General Services Administration for your expertise. This guide is meant to be a starting point for task force members as you discuss and respond to cybersecurity related budget requests, and we hope it will help you evaluate budgeting priorities for cybersecurity expenditures in your states.
Is your state looking at specific cybersecurity issues that you would like to feature in our newsletter? Are you working on cybersecurity legislation that you would like to highlight? Send us your cyber news and we will share it with the task force.

Sponsor Highlight: AT&T

AT&T Blog Post: Healthy Living, Healthy Agency: AT&T spotlights healthy cyber secure lifestyle habits for agencies:

2018 is here! The inevitable "New Year's Resolution" (NYR) is done, but probably not in effect. As with many, the NYR is often dead on arrival the moment it meets a "real" test, like chocolate, hamburgers, or the dreaded 5:00 a.m. workout. As humans, we're remarkably predictable. That's why gym memberships rise in January. It's why almost every magazine focuses on health. And, it's

what cyber criminals rely on. Human predictability. The elite cyber criminals know human behavior better than most, and exploit those behaviors very effectively.

That led me to think about NYR's and a new class of NYR – the healthy cyber secure lifestyle. Most particularly, a **healthy cyber lifestyle** for agencies and organizations. The parallels between a healthy human lifestyle and a healthy cyber secure lifestyle are uncanny:

To read the full AT&T blog go to the task force website.

Webinar: Cybersecurity and the Grid, Feb. 15th 3:00 P.M. EST

What: Please join the National Governors Association for a webinar examining states' best practices on creating partnerships and policies to enhance the cybersecurity of our nation's electric grid. (This is the first of a series of NGA webinars on cybersecurity.)

Who:

- Arthur House, Connecticut's chief cybersecurity risk officer, will discuss his initiatives in Connecticut and his prior experience as chairman of Connecticut's Public Utility Authority.
- Richard Ward, director of national security policy at the Edison Electric Institute, will talk about the Cyber Mutual Assistance Program and other EEI initiatives.

When: Feb. 15th, 3:00-4:00 P.M. EST.

How:

- For audio, you must dial 888-858-6021, and enter the code 202-624-5356.
- For visual, please click on the "Join Skype Meeting" in the attached calendar, or use this link: Join Skype Meeting

If you have any questions, please contact Michael Garcia at mgarcia@nga.org or David Forscey at dforscey@nga.org.

How to Secure your Next Campaign: Harvard Belfer Center Releases Cybersecurity Campaign Playbook

The Belfer Center for Science and International Affairs at Harvard Kennedy School released their cybersecurity campaign playbook report, a bipartisan effort to secure campaign information ahead of November elections. The full report explains that the information is for any campaign in any party. It was designed to give simple, actionable information that will make campaign's information more secure while allowing legislators to spend more time on campaigning.

See also NCSL Site: Cybersecurity Recommendations (For When You're Wearing Your Campaigner's Hat)

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.*

Biggest Take-Away: Update your Software!

The Online Trust Alliance released a report showing cyber threats doubled against businesses in 2017 as compared to 2016. The biggest threat? Ransomware. The report also highlighted that "93 percent of all breaches could've been prevented with easy steps such as updating software."

Cyber Incidents are on the Rise

Another survey summarizes cyber incidents in 2017, finding that 36 percent of organizations suffered a data breach in 2017 alone. What do organization's find to be the top tool in securing data? Forty-four percent said encryption for increased usage of the cloud; 35 percent said encryption for adoption of big data; and 48 percent said encryption for securing internet-connected devices.

2017 Cybersecurity Legislation Wrap-Up with a 50 - State Map

In 2017, at least 42 states introduced more than 240 bills or resolutions related to cybersecurity. Included in the state map, about half the states enacted cybersecurity legislation in 2017. Some of the key areas of legislative activity included:

- Improving government security practices.
- Establishing commissions, task forces and studies.
- Funding for cybersecurity programs and initiatives.
- Targeting computer crimes.
- Restricting public disclosure of sensitive security information, and
- Promoting workforce, training, economic development.

For more information, Contact Pam Greenberg

Federal Activity

U.S. House Passes the Cyber Diplomacy Act

The House passed the Cyber Diplomacy Act on Jan. 17th by voice vote. The bill would restore the cyber office within the State Department, and is charged with leading diplomatic efforts on

international cyber policy with other nations. The leader of the office would be appointed by the president and confirmed by the Senate, and have the same status and privileges as a U.S. ambassador. The secretary of state will be required to provide classified and unclassified versions of international cyberspace norms.

Read the full article in the FCW

Elections Hacking Bill Aimed at Russia

The House and Senate have introduced the Defending Elections from Threats by Establishing Redlines (DETER) Act that would impose penalties on foreign powers, including Russia, that interfere in U.S. elections. Reps. Ileana Ros-Lehtinen (R-Fla.) and Brad Schneider (D-Ill.) have introduced the House version and Sens. Marco Rubio (R-Fla.) and Chris Van Hollen (D-Md.) introduced the original bill in the Senate.

Read the full article in the Hill

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)