NCSL Staff Notes from Jan. 27 NGA/NCSL Webinar

On Jan. 27th NCSL lead staff Susan Frederick, along with the legislator co-chairs of NCSL's executive committee task force on cybersecurity, presented on a webinar with the National Governors Association as part of their year-long *Policy Academy on Enhancing State Cybersecurity.* Along with the private sector perspective provided by law partner a David Wheeler, the webinar consisted of engaging state lawmakers on developing strong cybersecurity postures by encouraging close coordination between the executive and legislative branches. It is critical for state cybersecurity officials to build relationships with the legislators who fund and oversee their security initiatives, and the webinar provided an opportunity to hear directly from state lawmakers on methods for engaging the legislative branch on this key issue.

Susan Frederick – Senior Federal Affairs Counsel, NCSL – Introduced NCSL's Executive Task Force on Cybersecurity - http://www.ncsl.org/ncsl-in-dc/task-forces/task-force-on-cybersecurity.aspx and identified its core mission:

1. To produce guidance on best practices for state legislators on cyber issues through massive education campaign;
2. Partnering with organizations like NGA and NASCIO that represent the executive branch will hopefully help bridge the gap in communication between the executive and legislative branches of state government.

NCSL's priority issues in cybersecurity include state budgeting for cyber, identifying the biggest cyber threats to state systems, cyber education and workforce issues, and communication between executive and legislative branches of government so that each knows the scope of the cyber issues facing their state. NCSL's Cybersecurity Task Force has partnered with executive branch officials at every meeting – we had the MN CISO at our kickoff meeting last May and most recently at our December meeting, we heard from NGA staff and Karen Jackson, Virginia's Secretary of Technology. Based on these presentations, webinars like this one, and the input of our task force members we are in the process of compiling questions for legislators to ask their CISO's, CIO's and executive branch cyber officials which we hope can be used in the legislative sessions currently underway.

Assemblymember Jacqui Irwin (CA) – Communication between the Executive Branch and Legislative Branch is fundamental to ensuring strong cybersecurity policies and procedures. California has learned two key lessons from the communications between the two branches. First, transparency is very important. . In CA, this idea was met with resistance because a lot of information was categorized as "classified." Further, Assemblymember Irwin discovered that not all agencies were complying with cyber readiness protocols so she introduced legislation in CA that was passed requiring assessments in all agencies.

Second, the sharing of threat information between the branches of government needs to occur more frequently. Upfront communications is also important part of that sharing of information. The legislature should have regular briefings and there should be more collaborative work. There is a need to make cyber a priority in the legislature. These briefings should be occurring on a regular basis and can be formal or informal with the option to reserve confidential information to private conversations. It is also important to note that realization is key in order to make it "real" for even the legislators not regularly involved with cyber issues. For example, sharing the number of attacks or other real data may help considerably.

It is hard for a legislator to vote for cyber legislation, like expanded funding, without being able to explain to constituents why.

Senator Thomas Alexander (SC) – It took a crisis to get the attention paid to cybersecurity in South Carolina. Unfortunately, the SC legislature first learned of the breach via the media. From this crisis, we were able to identify areas in which we could take action and focus on cybersecurity. For example, joint meetings between key legislators and key executive branch staff is incredibly beneficial. In some cases, it is helpful to bring in 3rd party witnesses to hearings, like academics, etc.(impartial testimony) in order to make the case and lay out the facts. Cyber is a tough issue because it cannot be visualized. When CISOs and/or CIOs explain cyber issues to legislators, it may helpful to use analogies that people can relate to – non-technology speak. Some members of the legislature predate computers and technology advances and need to be "brought along." It may be best to reach out to younger members of the legislature because they are probably more tech savvy. At a minimum, state legislative leadership must be briefed on cyber issues.

After the breach, SC had to re-appropriate the following amounts:

1. $10 million for consumer ID protection;
2. $250,000 for consumer affairs (notification);
3. $200,000 for a reimbursement fund;
4. $10 million for new safeguards;
5. $20 million for repayment of the Dept. of Revenue loan

These appropriations are not indicative of any future sums that may be appropriated for cyber in SC. It is much better to appropriate for cyber on the front end rather than on the back end.

There should be a mention of cyber in the state of the state address. SC had a special committee that met 12 times after the breach and was able to hire a CIO. This helped us to discover that many of the agencies are "silo-ed," and don't do cyber the same. Bridging the silos is an important and having the joint committee meetings will help in that regard.

David Wheeler –
David wheeler, Partner at Chapman Spingola law firm in Chicago, counsels companies regarding data security and privacy. He has a background as a software developer and serves on the American Bar Association Cybersecurity Legal Task Force for the state and local government law section. In the private sector, the average cost for a cyber breach response is between $158-168 per record. This is an incredibly high amount when one considers the numbers involved. For

example, if an agencies holds 25 million records and is breached, the cost for response may be close to $4B. Cyber has to be a priority and must be continually reviewed. It must be in the forefront of executive and legislative branch leadership.

<u>Q&A-</u>

1. How do you quantify the return on investment for cyber budgets? And how do you quantify the threat? This is not easily done, if at all. What you prevent from occurring, you can't quantify.

Senator Alexander – 76 million in recurring and on-recurring cyber in subsequent years after our breach. A unit was put in place in the Consumer Affairs Dept. to help people restore their identity. Cyber is a non-partisan issue - "it's like your home is being broken into" – A good analogy to use in cyber context.

David Wheeler – It is important to conduct risk assessments and there needs to be an inventory of information assets. By doing an inventory of information held you can quantify the threat in a way. The question to be asked is, "how sensitive is this information?" It is also important to remember that plaintiffs' class action groups exist who will sue when there is a breach. This will drive up costs.

2. What about cyber as a legacy issue? Wouldn't a legislator want to champion cyber legislation to leave his/her mark on the legislature?

Senator Alexander – It could be a legacy issue. Maybe look for someone in law enforcement who serves in the legislature to champion a cyber bill. Be aware that self-imposed term limits in some states may hamper this effort.

3. What about cyber insurance?

David Wheeler – It's becoming more popular. Companies are looking into it.

4. Any other comments or remarks?

Oregon CISO – A good cyber culture needs to be built and accountability needs to be in the right place. Agency directors need to have skin in the game and there needs to be independent audits. A European model in which there are Data Protection Officers who cannot lose their jobs (by law) for delivering bad news may be instructive.