# Legislating Cybersecurity: Lawmakers Recognize Their Responsibility with Cyberthreats

David Raths | October 11, 2016

*Editor's note: This story is part one is a two-part series on the important role legislators play in tackling cybersecurity.*

In March 2016, just a few weeks after a contentious legislative oversight hearing, Michele Robinson, California's chief information security officer (CISO), stepped down. The Feb. 24 hearing's focus was a 2015 audit that questioned the state government's cybersecurity preparedness.

One of the legislators holding the state's feet to the fire is Assemblymember Jacqui Irwin, D-Thousand Oaks, who chairs the Assembly Select Committee on Cybersecurity. Recalling that hearing, Irwin said legislators asked how much departments spend on cybersecurity and Robinson didn't have an answer. "That hearing did not go well for the Department of Technology. The state's approach was pretty decentralized and nobody was being held accountable for the decisions being made about how we manage the risk," she explained.

California has 160 departments required to do security assessments, Irwin added. “But when we looked more deeply into it, only 20 departments had actually done the security assessments. And the Department of Technology was not holding these departments accountable.”

Irwin authored a bill signed into law and now being implemented that requires the state to perform a minimum of 35 network security assessments per year on state agencies, departments and offices. The assessments are to be performed based upon a defined risk index that prioritizes the amount of valuable personal information, financial information or health records held by that entity.

Unfortunately legislators like Irwin, who take the time to study cybersecurity issues and ask tough questions of CIOs and CISOs, are still the exception rather than the rule. But that may be changing. High-profile government data breaches and recent ransomware incidents in health care have put the topic on the front burner in legislative committees.

“Five years ago cybersecurity was seen as an IT issue. But with threats so much in the news now, it is not something anyone can ignore anymore,” said Agnes Kirk, CISO of Washington state. She has spent time working to raise awareness and education in the Legislature. In the 2013-15 budget cycle, the Legislature provided funding to increase the security posture of the state. “Since then I have reached out to legislators to create awareness opportunities, culminating in the governor’s first cybersecurity and privacy summit,” she added.

*Agnes Kirk, chief information security officer for Washington state, has spent time working to raise cybersecurity awareness and education in the Legislature. Photo by David Kidd.*

Privacy and security are the main IT issues that rise to the policy level, Kirk noted. People are trying to make appropriate laws, but it is such a complex issue and only one of the many that legislators need to address, so it is difficult to make good laws, she said. After the cybersecurity and privacy summit, she met with legislators, and in the most recent legislative session they created a state data privacy office and a cybersecurity jobs act. " They had a better understanding of the issues and they worked with us on those. It was an opportunity to collaborate on getting good policy into law."

One way Kirk reaches out is to hold tours of the Security Operations Center for legislators. "They can see in real time what is happening," she said. "They can see all these attacks coming in. I can talk more specifically about the types of attacks we are seeing right then, and what would happen if we weren't protecting our network the way we are. That gives them a real-life view."

Legislators who focus on cybersecurity tend to be people who have some technology or legal background. For instance, Irwin's training was in systems engineering, and she worked at the Johns Hopkins University Applied Physics Lab and Teledyne Technologies. "I think that gives me a little more comfort with the issue, because cybersecurity has evolved very quickly," Irwin said.

Karen Jackson, secretary of technology for Virginia, headed up a state cybersecurity commission over the last two years and turned to the Legislature to pass seven bills related to cybersecurity and cybercrime. In the last session the Virginia legislature also invested more than $20 million in cybersecurity for training, hiring and shared services for state agencies.

Jackson said that when it comes to cybercrime legislation, there are legislators who are prosecutors and defense attorneys who grasp the concepts quickly because they are in the legal system every day. "Cyber as a technology is a little more difficult," she admitted. "Unless you have somebody who spends a lot of time in the environment, it is difficult to keep up with. We don't have one constant cyberchampion in either party who is always the go-to person. It is more spread out based on committee."

## NCSL Task Force Allows Legislators to Share Best Practices

Besides leading the charge on cybersecurity in the California Legislature, Rep. Irwin is co-chairing a cybersecurity task force recently created by the National Conference of State Legislatures (NCSL). "We just had a conference call on the new federal data-sharing legislation," she said. "My hope is to produce a working product that would be a list of recommendations or best practices for states. We all know the important thing is to get the word out and tell legislators about their responsibility for oversight. It can't just be the executive branch that is worried about this, so we want to come up with a list of questions legislators should be asking."

Jeff McLeod, director of the Homeland Security and Public Safety Division of the National Governors Association Center for Best Practices, said there is a crucial role for legislators to play in terms of investing in workforce training and oversight. “The biggest thing is at the policy level, making sure the state is organized effectively in terms of governance, and making sure the state is taking a risk management approach and using resources where they can have the biggest impact in addressing or reducing the threat.”

Susan Parnas Frederick, NCSL’s senior federal affairs counsel, said her organization had been tracking cybersecurity activity at the state level for several years, and it seemed like a good time to form a formal body to create a work product to inform legislators who may sit on technology and appropriations committees. “This task force gives those people with expertise an opportunity to work with colleagues in other parts of the country to share information on what they have done in their state,” she said. The task force, which also includes Rhode Island’s state Sen. Louis DiPalma and state Rep. Stephen Ucci as members, has a two-year time limit, but Frederick said it could be extended. “What we found was that as soon as it was announced to the membership, we got lots of requests to join. There is a lot of interest out there.”

http://www.govtech.com/security/Legislating-Cybersecurity-Lawmakers-Recognize-Their-Responsibility-with-Cyberthreats.html