The Our American States podcast—produced by the National Conference of State Legislatures—is where you hear compelling conversations that tell the story of America's state legislatures, the people in them, the politics that compel them, and the important work of democracy.

You can subscribe through iTunes or Google Play.

Cybersecurity Task Force | OAS Episode 16 | Aug. 24, 2017

Welcome to Our American States, a podcast of meaningful conversations that tell the story of America's state legislatures, the people in them, the politics that compel them, and the important work of democracy. For the National Conference of State Legislatures, I'm your host, Gene Rose.

Joining us on Our American States is California Assembly Member Jacqui Irwin, co-chair of the National Conference of State Legislatures Cybersecurity Taskforce. Welcome to the program.

Jacqui: It's an honor to be here.

Gene: Thank you. You know, cybersecurity is a word that is tossed around a lot and especially in connection to elections in this country. So why don't you tell us in your own words what cybersecurity means to you? Is it more than just being concerned about elections?

Jacqui: It's certainly much more than being concerned about elections. We started focusing on cybersecurity a few years ago, right around the time of the Sony breach and the OPM breach. So cybersecurity affects every single American and it's about data protection and just basically public safety.

But what we've seen over the last year, it's also about free and democratic elections, trying to make sure that you don't have interference in them, trying to make sure that the population is not manipulated.

So it's a broad range of very crucial issues. And one of the things that we focused on at NCSL this year was IOT. So whether you're talking about elections, personal information, public safety or Internet-of-things devices, every American should be concerned that their information is being protected.

Gene: The IOT – can you describe for our listeners what that's an acronym for?

Jacqui: Well, IOT is the "Internet of Things" and they're all the really fancy devices, whether you're talking about ALEXA or RING or NEST – these are devices that make our lives much easier. So if I come home I have ALEXA or the DOT and I tell ALEXA to change the temperature in the house, or when I walk in the door the RING doorbell in my home sends a picture over to my phone and to my husband's phone. So these are the multitude of devices that make our lives easier and streamline our lives, but they also open us up to a lot of issues relating to privacy and personal safety.

Gene: So, why don't you walk us through the goals of the Cybersecurity Taskforce? Tell us why it was formed and what its mission is.

Jacqui: This was an issue that really wasn't being focused on, and once you started to hear in the news about all these big breaches, I was very happy that NCSL decided to form this taskforce. So the taskforce has been working since May of 2016 to bring together legislators, legislative staff and cybersecurity policy experts to understand how states can work on this growing threat.

And we've already held meetings in Minneapolis, Chicago, D.C., Santa Fe and Boston and at each of these meetings we brought speakers to help talk about what is cyber and what the role of state government is. The taskforce has also gone to Microsoft headquarters in Washington State, and when we were in Boston, we toured IBM's Cyber Range, which was really fascinating. We've also had FBI and Homeland Security come and speak to us.

As a result of all these conversations, we published a Cybersecurity Conversation Guide and this is basically trying to educate legislators about what their role is as far as cybersecurity is concerned. This education guide had an executive section, which focused on helping legislators find the maturity of their own state's cybersecurity; a legislative section that helps legislators engage with leadership to know if their own branch is cyber-secure; and then a higher education section. And even though that doesn't seem as relevant, that's probably the place that state government can make the biggest impact, is making sure that we are training young people to fill our pipeline.

So basically we're all working together looking at best practices, looking at legislation that's going on in other states. We don't want to keep reinventing the wheel, but we need to make sure that our legislators are basically fulfilling the role they have, which is oversight of the executive branch and making sure that the executive branch is doing everything they need to, to keep the information of the state secure.

Gene: You mentioned the Sony hack a little while ago. There have been various reports of other major security issues. For the most part, it seems like government has been fairly well protected. Would you agree with that, or do you think that there's a pretty big danger out there?

Jacqui: We have not seen a big news story except probably the OPM breach, which was quite disturbing, and I don't think that we really have the end results of what the effects of that were. OPM had fingerprints of people who were employed by the government and had security clearances.

But I think that states… certainly we heard many stories about states being hacked. What we found is that we were probably not as prepared as we should have been. You look at California –

we're home to Silicon Valley – you would think that the state would be really prepared when you are talking about departments protecting their own information. But when we started to research it, we found that even though the administrative manual required that every department do a security assessment, most of our 160-or-so departments were not doing that.

So I passed a bill two years ago which mandated independent security assessments for every agency, and most of these have been performed by the California Guard. We're starting to see the results coming in and we're starting to really see departments look at what they should be doing. So it's first looking at the assessments, seeing what your vulnerabilities are, patching them, then making sure that you do full audits, and that includes also training your employees to make sure that employees are not clicking on links.

As we know, with most of these breaches, our people are the weakest link. So I don't think states are where they should be, but I look at least in California and with our new CTO and our new CIO, we have made tremendous progress at bringing these issues of cybersecurity forward.

Gene: So, as this cybersecurity taskforce keeps meeting, what are the major things that you are… if you could tell legislators to do one or two things right away, what would you advise them to do?

Jacqui: Well, I think that legislatures need to make sure that they're educated on this issue. My background is in engineering, so this subject does not scare me. I know the questions to ask. My I think legislatures need to realize that they have a very important role in providing adequate oversight, and they need to have ongoing conversations with the executive branch and be willing to provide the tools and the funding needed to implement best practices.

I think we need to look at every state, making sure that they have legislators who are focusing on this issue of cybersecurity, and working with their executive branch.

Gene: You mentioned earlier about going to various sites around the country and hearing from experts. Is there any particular testimony or presentation that you heard that really stood out for you as something you wish everybody knew and understood?

Jacqui: I think each of them has been really interesting. When you look at what IBM is doing, in general trying to stop big viruses from attacking systems of their customers, and then making sure to pass that information out, I think that was really interesting information.

But looking also at… most recently the Cyber Range in Boston – we went through a simulation of a breach at a company and one of the valuable lessons we learned there was that you have to have open lines of communication when an organization is responding to a cyberattack. And you have to make sure that all departments, ahead of time, understand what their role is going to be when there is a cyberattack. So you have to look at IT and legal and communications and make sure that they're all working together to fix the problem as quickly as possible and make sure the public is confident that you're working as quickly as possible to get the problem fixed.

But it was a very interesting exercise; it lasted about an hour. I think most of the time when they run these simulations, they go almost five hours. Almost everybody walked out saying: Oh, I wish I could have stayed longer, because it really gave you a very good insight as to what these small companies are facing and how basically you can ruin the reputation of your company and

allow a lot of personal information out into the public if you are not prepared, if you do not have resilient systems, and if you're not very direct in the way that you deal with an attack.

Gene: And the work that you're doing here, you're placing as much emphasis on the business sector as you are the private sector, would you say?

Jacqui: With the Cybersecurity Taskforce, of course, I think we look at business too. But our main focus, I have to be really clear, our main focus over the last couple of years is making sure that government is doing everything it can so that the public can feel confident that we're protecting information.

I think it's not that easy to go in and start telling business how to protect their information if you're not setting a good example yourself. Certainly as we go forward we need to look at: Are there more areas that the state should be weighing in on? And one of the issues that I think is really important is: What is the state's role in making sure that infrastructure is properly protected, whether you're talking about the electric grid or the water systems or communications? A lot of those sectors are very advanced in how they're protecting their information. But we're trying to determine what the state role should be and certainly there's already a federal role. There could be some role for the state also.

And then when you look at things like the Internet of Things, should we be looking at regulations to make sure that every product that is put out there has at least some minimal security standards. We understand when listening at the taskforce presentation that some of the IOT items don't even require you to put in a password, which makes them very vulnerable to being used in DDOS attack.

So we are kind of wading through that, but our first responsibility is, again, making sure that the state, which holds a great deal of personal information, keeps all that information secure. So that's our biggest focus right now. And again, the other focus is making sure that we're training the taskforce.

In California we have a world-class education system between our public system and our private system, and we're training a lot of people in computer science and cybersecurity. But we're not nearly meeting the demand. The great thing about California is we are the home to Silicon Valley and they're picking up those graduates as quickly as they can. But we need some of those people to be interested in working for state or local government where there is a great need.

Gene: You mentioned a DDOS attack and I'm going to have to ask you what that means.

Jacqui: Distributed Denial of Service. You take all these different devices that you have in your home, whether it's your refrigerator or your net, and they can be taken over and basically be used to attack and overwhelm companies' communication. So we saw something passed, and I think it was about six month ago, with a company that provided services for I think Twitter and a couple of other communications companies where things went down or were really slow for a number of hours.

So we just need to make sure that all these devices, that there should be protections in there from hackers.

Gene: Assembly Member Irwin, when your report, your guide, first came out, there were reports of two states that were hacked by Russians during the election and subsequently there have been reports that as many as 30 plus states were targeted. Has that changed your approach or the taskforce's approach to how they're addressing the issue of cybersecurity?

Jacqui: I think it is going to be very important to look at how we protect the integrity of our elections, and when you see the attempted attacks, I certainly think we have a big concern with that. In California, all our different counties' systems are basically protected where the election, the computer that is tallying the ballots for the election, is not connected to the Internet.

So we certainly have security in that way and our Secretary of State came and spoke to NCSL on the security of elections. People are going to keep trying to attack our systems and it is critical to our democracy that people have confidence in the outcomes of elections. So this is something that we will definitely be focusing on going forward.

We want to continue to look at what happens as we start to connect devices to the Internet and what type of danger that could present. Obviously there's a lot of ease in that, but when you're taking something that's controlling a water system and it used to be you had to go in and physically push a button and now it's on the Internet, it does create vulnerabilities that have to be designed for. So we'll continue to look at that, again, as part of infrastructure.

One of the other things that we were looking at, as I mentioned, I think the biggest role of the state is to make sure that we are doing everything we can to fill the pipeline. So we had a bill this year which would be to start a pilot program at the community colleges and make it a four-year IT degree. So it would be a bachelor of applied sciences. That got stuck in committee, but we are really interested in continuing that conversation because we need a wide range of people that are talented in these areas, and having a four-year technical degree or vocational degree in IT I think would be very beneficial for a lot of our companies and for the public sector as well.

So we have a couple of bills that are still trying to push the department of technology. One of them is AB1022, which would require state departments to submit inventories of their critical infrastructure controls, and this would help the CIOs to warn and assist departments with vulnerabilities in their network.

And basically looking at what type of information does every department hold and making sure that you have properly ranked the sensitivity of that information and you're starting to design policies to figure out what information has to be encrypted.

So work is continually expanding. When we started this cybersecurity wasn't in much of the public dialogue but, again, with what's happened with elections and some of these other issues with Russia, many people are much more interested in cybersecurity.

And then just for me personally, what I've tried to do is… individuals are the weakest link; your employees are the weakest link. And so every time I have a chance to address a group of people, I tell them to pull out their IPhones, I ask them if they have two-step authentication with their Gmail, make sure that they keep their phone completely up-to-date because IPhones or the

droids, every time they issue updates, you can be pretty sure that the security patch is really important for you to download. I do regular security tips via Twitter and on my Facebook, making sure that people are very wary when they're going on public wifis, and then looking at all your applications and figuring out which ones are following you that don't necessarily need to.

So I think that's the best way to start to have people kind of take their heads out of the sand and realize that they have some responsibility in this also.

Gene: So what was it about this issue that really got you personally connected to it?

Jacqui: We have so many issues that we look at in the state government and education to me is really important and a lot of our social services issues. But there has been so much work done in those areas already and what I liked about the cybersecurity part was that nobody was really addressing it in the legislature and you could see when we got started that it was going to be an exploding issue.

One of our first speakers said he sleeps like a baby every night, you know, wakes up every two hours and cries because of all the things that could potentially happen. And I think that was somebody from Homeland Security. When you start to hear stories like that, you realize this is really an issue that has to be focused on. And as government, even though it's difficult to get the type of resources that you need, you need to really push the issue, try to get as much talent into government as possible. We need to focus on what we can do to protect ourselves.

Gene: We'll let you get out on this. Any final words or thoughts that you'd like to share with your colleagues around the country?

Jacqui: I just would encourage all of my fellow state legislators to make sure that you have a number of people in your body who are focusing on this issue. Every single state needs to address it. We are doing some work with the Governors Association. I think they have a big focus this year on cybersecurity and I think that the legislatures need to maintain that same focus. We need to make sure that we are providing the oversight that we need to of the executive branch.

And I would also tell my fellow legislators that we have the Cybersecurity Conversation Guide, that NCSL has copies of that. Everybody should take a look at that for tips on how to get started in this area.

Gene: So we've been talking with California Assembly Member Jacqui Irwin. Thank you, Jacqui, for being a guest on Our American States.

Jacqui: I enjoyed it. Thank you very much.

Music and Gene:

And that concludes this edition of Our American States. We invite you to subscribe to this podcast on ITunes and Google play. Until our next episode, this is Gene Rose for the National Conference of State Legislatures. Thanks for listening.