Our American States | An NCSL Podcast

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 | Episode 7 | April 13, 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.

On this episode of "Our American States," we dive into the complex world of cybersecurity. For most Americans it's not something we give a lot of thought to until a news story breaks regarding a breach of a major company's data center. If it's a company that we have shared data with, we anxiously try to find out the level of the breach and what, if any, data was compromised.

What many of us don't realize is that nearly all of us have data stored on a state website. If you've filed a tax return, applied for a driver's license, started a business, or qualified for social services, your state has important information about you that you would not want in the hands of criminals or hackers.

Joining us on this podcast is the head of an organization that works on behalf of state information officers, and a state senator from a state that suffered a serious cyberattack. We're going to learn how many times a state system is attacked every day, what steps policymakers need to consider to protect their data and how an NCSL Task Force on Cybersecurity is helping state legislatures. We'll have those interviews right after this break.

Break

Gene: To help us understand the cybersecurity threats for state governments, we are joined by Doug Robinson who is the executive director of the National Association of State Chief Information Officers. Thanks for joining us today, Doug.

Doug: My pleasure, Gene. An important topic for us to discuss.

Gene: Well first, Doug, tell us what NASCIO does and what its mission is.

Doug: Well, NASCIO represents the state chief information officers. Each state has an information technology executive appointed by their governor or even the territories in the District of Columbia. And our mission is to really foster government excellence through information management technology policy and represent the interests of the state CIOs and other state IT executives with research and products, services, conferences, webinars, and other events that advance both the knowledge of these issues as well as advocate for their interests. So we advocate as well as provide some policy analysis and research.

Gene: And you personally, Doug, how long have you been involved with this issue?

Doug: I had a career in state government information technology in the CIO office for a number of years, about a dozen years, and we were talking about cybersecurity and security then. I've been in NASCIO since 2004 and cybersecurity has been on our list of topics and issues and priorities for state CIOs certainly since that time.

I believe NASCIO's first formal publication on security was issued as a call to action in 2002. So this is not new to the state CIO community and state IT officials, and it's been on our top-ten list. Each year we do a top-ten priority list which is essentially a vote, a ballot by our state CIOs, and we did our first one in 2006, and security has been on that list since 2006 and in the number-one position for the last four years. So it's been the top priority of our state CIO members.

Gene: What are the top two or three cybersecurity threats to states today?

Doug: Surprisingly I think the major threat to states is the fact that they are not organized for success, and by that I mean in terms of their governance and decision making. We know we've heard certainly in headline news and we've seen the reports from the FBI and from the Department of Homeland Security and many others about the external threats, and those are numerous and multiplying and becoming more aggressive.

But I think the major challenge is that the states still have a long way to go in terms of mitigating the risk and being more resilient. And so I think a major challenge for them is really getting organized and getting this in front of the chief policymakers, the governors and lawmakers, and so those are the things that we look at. We've seen some progress there and so we're pleased to see that. Cybersecurity, at least in the public sector, has not risen to the same what I'll call board-level priority as it has in the private sector. We're continually working on that.

The second part of that, as you'd probably expect, is the external threats that we're seeing – those external threats are certainly increasing, becoming more sophisticated, and those are certainly one of the challenges that we see in terms of attacks, using social engineering. We've

heard headline news about ransom-ware, the ability to lock up computers in the public and private sector and hold the data for ransom.

We've seen a significant increase in the last couple of years in hacktivism, basically social activism/civil unrest using technology. And so we have elements, both domestic and foreign, that are coming after state governments.

And then, of course, there's the increasing sophistication and proliferation of all these other threats that we've seen particularly from foreign nation states where they are on a constant attack mode, looking for vulnerabilities in all public sector organizations, but particularly state and local government.

Gene: There's certainly been a lot in the news lately about Russian attacks on security systems today. Do you think that's kind of raised the awareness level perhaps of policymakers?

Doug: I think it has and, even though at the state level we haven't had what I'll call a very high success rate for those types of attacks, the attacks at state systems and networks are literally in the millions every month, you know, tens of millions for some states. It's easy to have what I call the department of big scary numbers; people have heard me say that those are things you can talk about.

But I think the most important thing is recognizing that those represent dramatic risks that states have vulnerabilities in their environment, and those external threats represent risk. And they are doing this 24 hours a day, seven days a week. So they only have to get it right once and states, particularly our state government members, have to spend an inordinate amount of resources and effort and personnel in order to thwart those attempts, which become more and more sophisticated it seems like each week.

Gene: So you mentioned earlier about the importance of having policymakers, state legislators, governors be more aware of this issue. What kind of steps is your group taking to make that happen?

Doug: Well, we obviously try to distribute reports and educate the lawmakers, recognizing that that may not always be the most effective way. So we've been partnering with external organizations, the National Conference of State Legislatures, the Council of State Governments and other groups that certainly have state legislator representatives.

And also, of course, we partner with the National Governors Association and other state associations that are counterparts in the various offices of state government: budget directors, procurement officials – we try to bring them into the fold through a series of either educational workshops, which we've done a number of, conference sessions – I speak at a number of conferences each year on this topic, and certainly our annual conferences and webinars that we produce. I can't think of the last time we didn't have an event where cybersecurity was not on the agenda in some form or fashion, whether a panel session or a presentation.

So we do the traditional things, Gene. I think most importantly is I'm an advocate of making sure that we have data-driven strategies, meaning that we're speaking from a standpoint of evidence and not from anecdote. So since 2010 we have partnered with Deloitte, one of our corporate

members, so produce a biennial national study, a survey of the chief information security officers, and then a study of the states – that is called State Governments at Risk. So we've produced that a number of times and, of course, the most recently in 2016.

So we now have data… in this case it was from 49 respondents, so a remarkable response from our states. This study examines all of those issues, but has the data behind it to talk about what's going on in terms of the risks, the growing number of risks, and then, of course, the mitigations: What are states doing? Are states spending more money? Are they communicating it better?

Those are the things we focused on. So rather than focusing on all of the threat levels in a lot of detail, we focus on what I'll call kind of the policy landscape and decision-making landscape on that. So those are important things to do and we've certainly been speaking to both appointed, elected officials about the results of this survey and we advocate for more understanding using this data with a set of recommendations.

Gene: And it appears to me, Doug, that to address this issue, it requires a special type of workforce. Are there enough qualified people for states to have the workforce that they need?

Doug: Gene, there is not. That is one area I think which is fairly… maybe I would call it a universal truth among the states, and certainly the challenges of recruiting and retaining cybersecurity professionals. But it's not just state government; it's across the board in all sectors of the economy. There is virtually no unemployment and cybersecurity professionals are what the Bureau of Labor Statistics would call information security professionals; there's a whole series. But if you look at those across the board, it is a challenge having dedicated cybersecurity professionals in state government; it's really a challenge.

And it's, again, the response even in looking at the questions around the state's ability… again, a very, very high consensus, I think 96 percent said that the salary rates and the pay rate structures… 96 percent of our respondents said that's a tremendous barrier. More than half expressed concerns about the lack of qualified candidates, and that's because of, again, the compensation levels are dramatically different in the private sector than in the public sector. And so they have a number of key cybersecurity thresholds, including the state chief information security officers in the last couple of years, we've had many of them leave for higher-paying, private sector positions.

So the states are working on innovative strategies around contributing to perhaps serving the public, trying to kind of pull up their public sector interests and kind of facing big challenges and working in a challenging working environment like state governments. That still is not going to solve the whole issue. There are a number of things states have done including use of interns, targeting veterans for hiring and trying to train them up. But I think it's going to be a continuing challenge.

I'm not totally pessimistic about the future, but I can't be totally optimistic either given the dramatic compensation differences, and it continues to rise in the private sector because of the demand. So states are at a real disadvantage. And I think generally the perception from the outside is that the state government might not be an attractive place to have a career when, in

fact, I think most that get in find it's very challenging and they're working on major public sector problems.

This is in our own surveys and our own studies. When we asked about the most difficult position to fill in state governments, security was number one across the board, and I think other organizations would probably say the same thing.

Gene: I noticed on your website that you started a State CIOs Make a Difference campaign. Is this kind of relationship to this to try to promote awareness of state jobs?

Doug: Some do. In fact, a number of states have really done some interesting things including hiring chief recruiters within the CIO office, or hiring a point person to actually actively cultivate a network of recruits. As I heard one CIO office HR person say: The post-and-prey approach does not work anymore. So that was the common practice. They now are actively using social media; they have networking events.

I think one of the more interesting examples is an initiative in the state of California under the CIO office; it's WaTech, is the CIO office. They've branded themselves. They have begun to reform their culture. They've gone to a very modern, open-office concept with kind of teaming arrangements. They redid their job classifications and titles to streamline those and align those more with the marketplace.

And in the Seattle area out in Olympia, they're competing with some of the top tech giants in the world. So they had to do things to differentiate themselves. So what they've done actually to change the culture, the environment to, again, make sure they're a much more attractive place for candidates, was to go through a really deliberate process including introducing holacracy, which a number of private sector firms have looked at, which is basically eliminating supervisors. So everybody works in teams. So they've done that in part of that organization.

So they've done some very fascinating, innovative things. They were the recipient of our 2016 State CIO Recognition Award for what they're doing to be what they call the "IT employer of choice." I think it's going to take that in many states to attract the kind of candidates. So the CIOs can make a difference by, again, being really innovative and coming up with solutions that would attract perhaps individuals who would not be seeking employment in state government. You really have to go out and cultivate them. You can't just expect that they're going to show up on your website.

Gene: Well, as we close out here, Doug, what final thoughts would you have for state legislators across the country as they consider cybersecurity issues?

Doug: I think that as I talk to many state legislators across the country and even do briefings with them, I think what I find is that perhaps they don't perceive cybersecurity as a business risk. It's a complex area, complex policy area. It's one that is not funded at the level that's commensurate with the risk. And so I think they're always confronted with: we need more money for cyber, which is fairly common.

But I think they'd be best served by understanding that this is not about information technology. It's fairly common for me to hear that: well, I'm not well-versed in information technology. I

think for them to understand this better they need to think of cyber as a business risk. Just like they think of other natural and manmade risks that confront state governments: You have to be prepared, you have to be resilient, you have to have a plan, you have to be organized. So, as they think about perhaps natural disasters and the emergency response to those things, that's something they're more familiar with.

I think they really need to look at cybersecurity not as an IT issue, but as a business issue, and that's the common thread I use is: treat this as a business risk. It's not a project. It's not an initiative. It's life – life in the digital age. And I think that's something they have to become more and more comfortable with. It does take probably a greater degree of perhaps understanding than some of the other areas. But I don't think they should be deterred from really understanding this by treating it in kind of a different light rather than simply as information technology.

Gene: Because there's probably a certain expectation by the public that all their information is being protected, correct?

Doug: There is. There is I think a high expectation from the public that the data that the state holds they're holding in trust. But other national surveys have shown that, for the most part, citizens are not very confident in state and local government, that they're doing the right thing in protecting their data. I think in many cases the evidence might warrant that concern when you look at the lack of overall risk protection.

So I think our advocacy stance from NASCIO is that this is an enterprise challenge for all three branches of government, for elected officials. It is not just one of the executive branch which is what we really represent; that it's a much broader issue and should be treated as an enterprise risk. I think that's certainly what the private sector firms that have experienced massive data breaches and the consequences of financial challenges because of that, states need to see it the same way.

If they're holding taxpayer information, then they need to invest in the protection of that information commensurate to the value of the asset that they are protecting. That has not happened broadly across all states yet. It's still a maturity process. But we're hoping through all of our efforts that we can kind of push that along.

Gene: We've been talking with Doug Robinson who is the Executive Director of the National Association of State Chief Information Officers. Doug, we really appreciate you sharing your expertise with us today.

Doug: Gene, it's been a pleasure and, again, I hope to talk to you again soon.

Gene: After this break we'll talk to South Carolina Senator Thomas Alexander who will walk us through an attack on his state's system and what steps he recommends for legislators in other states to protect their systems.

Break

Gene: So we have with us today Senator Thomas Alexander who serves on the NCSL task force on cybersecurity. Senator, thanks for being with us today.

Thom: It's a pleasure to be with you, Gene. Thank you so much.

Gene: Senator, the general public is well aware of attacks on giant retailers or the large email companies like Yahoo being attacked by outsiders. What's at stake for state security systems these days?

Thom: Well, certainly cybersecurity is very important to the states. We have a lot of very personal and private information on the citizens of our states, and I think there certainly is very much the importance that we protect that information and that it's treated as the type of information that it is, very personal and very private information.

So I think there's a lot at stake as far as the credibility and the integrity of the state and its system to make sure that we have the public's trust and that information is being provided and protected in the most secure way as possible.

Gene: Okay. So your state, South Carolina, was the target of an attack. Can you tell us what happened there and what your response has been?

Thom: Yes, unfortunately several years ago our Department of Revenue was the target of a cybersecurity attack. That system was breached. And so we went in to making sure first and foremost that we could do everything we could to assist our citizens. Fortunately it appears that no information has been back out, but we've done a lot to make sure that we've put best practices into place. It was a very painful experience to go through. It was very unfortunate.

So I would encourage states to make sure you're doing all that you can before a cybersecurity breach becomes an issue. One of the things that I remember very much from one of the reports and briefings that we had was that, you know there are two types: those that have been breached and those that will be breached. And you're only as good as the system you have in place to protect that information.

And it's critically important, I believe, that we continue to be vigilant at updating that information, because I can assure the hackers are using the most modern technology, the most modern tools that they have available to them, and it's up to the states to do the same thing. We obviously have done a lot since then with our chief information officer trying to bring about all of the different systems into line, putting proper protections into place. It continues to be at the forefront for us to make sure that we're giving the type of support that is necessary for the systems to be protected from that standpoint.

So it certainly has highlighted the vulnerability or the potential vulnerability, but also, more importantly, the amount of necessary resources that are needed to make sure that we're providing the tools to not only the chief information officer, but to the agencies that are protecting that information.

So we will continue to work to that end and it's one of those projects now that is never done; it is a continuing, ongoing issue quarter by quarter, year by year from that standpoint, and I don't see that changing in the foreseeable future.

Gene: Senator, that kind of brings up a couple of points here. I mean, this all sounds very expensive, as you alluded to, that states have to dedicate some resources to this. But it probably also means you have to have a certain type of workforce available to work on this problem.

Thom: No question. The IT workforce is very critical to the success and certainly it's a challenge to make sure that we in state government are competitive with salaries and benefits to the private sector. So that is certainly a challenge and something I think that all states need to be aware of, that you need to make sure that it is being addressed so that you're not always having a revolving door of folks leaving your state government for the private sector, because it can certainly have an impact on your ability to address the situation.

Gene: The country has kind of been mesmerized by this Russian attack during our last elections. This kind of brings up communications between the branches of government itself, like you're being in the legislative branch, but there is probably communication that goes on between your branch and the government, the judicial branch. Are those types of things a concern right now or not?

Thom: Well, I think we're very fortunate in South Carolina to have good dialogue and good communication between not only the legislative branch, but the judicial branch and the executive branch. I think that it brought about a reality that we're all in this together, there are not winners and losers from agency to agency, that we have to do this as a team approach, and that we're better served as a government, but more importantly our citizens our better served by us working together and addressing this and trying to consolidate the resources and bring those to bear in a unified way.

So certainly if we continue to be aware of that… and we don't want any agency or branch of our state government to fail when it comes to any program, but especially cybersecurity when you're dealing with, again, the most private, personal information that a citizen has. I think it's a duty and responsibility that we have to the citizens to do everything that we can to make sure we're providing the tools to the IT community to address those needs in the State of South Carolina. We've had good broad-based and unified support from that standpoint and, as you say, dialogue is a central part of that.

Gene: As you're working with the NCSL task force, what's your sense of how states are treating this issue these days? Do you think it's going to take attacks on them in order for them to react, or do you see states being more progressive in trying to prevent an attack?

Thom: I really think the task force has been a very key component of elevating the awareness and the potential of what can happen, and as we hear from meeting to meeting about the work that's being done, cooperation that's being done, I sense that states understand the importance of this and that the NCSL task force is a tremendous tool where we can bring together ideas, we can bring together a learning opportunity from the experts and the professionals across the country from the private sector as well as experience from the public sector.

And certainly from a personal standpoint, I want to be a resource to folks in other states to let them know to go ahead and put forth that emphasis, go ahead and be proactive in addressing this issue so that you don't find yourself after a breach saying: Why didn't we do more?

So my sense in talking to task force members and listening to their comments, I think it's to reengage folks, that is provide the opportunity to have the understanding that we need to have that coordinated effort with the executive branch and the judicial branch, all branches of government working together from that standpoint. And the main thing is having some folks that are raising that awareness in the various states as well.

Gene: And as the work of the task force continues, what kinds of things do you think the task force is going to be focusing on? What areas of cybersecurity do you think really need attention these days?

Thom: Well, I think it's just being a resource to the states, but also providing the best practices and making sure that we understand the threats are just as real in the public sector as they are in the private sector, and making sure that we're providing the tools to the members of the task force and to the other states, and to be a resource for them.

I think it's important that we continue to look at trends, look at opportunities that legislators need to be educated on and not only best practices, but the latest that we're seeing out there from those that are trying to provide these insights on attacks so that we're being proactive as much as we can be and understand it from that point.

So I think to me the task force is a critical tool for us to continue to utilize to make sure that the states are prepared before it's too late.

Gene: Okay, so we're covered a lot of ground here, Senator. Is there something that I haven't asked you that you feel is important for other state legislators across the country to know about?

Thom: Well, it's not that you haven't asked, but I think I want to re-emphasize that states be on guard, they be prepared, and that they be proactive, because you can be assured there are those that are seeking to get that information from their systems. They're only as strong as that weakest link; the old saying goes from that standpoint.

So they need to make sure that these systems are being updated. It's a financial commitment; there's no question about that. But that technology changes so much that we can't sit back and say well, we've invested in that and that's an issue that we've dealt with and we can get onto something else. It's one of those issues that you will continue to deal with.

In the legislative branch so many times once you deal with reform or once you deal with an issue from a budgetary standpoint, you feel like you can take a breather for a while. Cybersecurity is not one of those areas that you can take a breather from because be assured that those folks that are trying to attack the system are out there day in and day out trying to breach that system. They're not taking a break, so we need to make sure that we in state government aren't either because, again, it gets back to once you have that breach and you've lost the confidence of the citizens of the state, you can't put a price on the loss of that confidence that the people

have and that information that they have to continue to provide to state agencies to be able to do the work more and more, and we depend on it more and more in electronic form as well.

So this is something that is not going to be going away and I would just encourage states to make sure that it is the priority that it should be and not one that they'll regret that they did not make a priority.

Gene: Okay, we've been talking with Senator Thomas Alexander from South Carolina. Senator, we appreciate you sharing your expertise with state legislators across the country today.

Thom: It was a pleasure to be a part of it. Thank you so much for providing the opportunity.

Gene:

And that concludes this episode of "Our American States." A reminder that more information on this issue and NCSL's Task Force on Cybersecurity force are available at www.ncsl.org. NCSL staff also provides customized assistance for state legislatures including briefings on state policy trends, in-depth research and meeting facilitation. We encourage you to subscribe to this podcast on iTunes, Google Play or on the NCSL website, www.ncsl.org/podcast. Until our next episode, this is Gene Rose. Thanks for listening.