FEDERAL TECH PODCAST

Ep. 61Understanding the National Cybersecurity Strategy

00:04
Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. In the studio today. We have world famous BILL Right. He's the Global Head of Government Affairs at elastic, he L A s ti c.co. And we're going to talk about a topic that's been bouncing around town here for the last few weeks, we're gonna talk about the National Cybersecurity strategy. And Bill's got a wonderful background. And he's got a background in the law. He's got a background in technology. So he'll better explain a lot of aspects of this report and maybe see how it affects your agency. And maybe at the end, talking about elastic and how maybe elastic can help you achieve some of these, these laudable goals, I'd say. But first, I'd be remiss, I mentioned your law background and your tech background. Bill, perhaps you can fill us in.

00:47
Yeah, thank you, John. First off, very, very happy to be here. Again, I'm the head of global government affairs here at elastic. I've been on board just for about six months, really loving it so far. But of course, I started my career with public service on Capitol Hill, went off to law school, as you mentioned, graduated and worked for a Chicago law firm. Once 911 happened, of course, like many of us in DC, I was drawn back to DC where I was at the Department of State and National Counterterrorism Center, then moved back to Capitol Hill and was subcommittee staff director on Senate Homeland Security Committee Affairs Committee, where I worked on the very first cybersecurity bill, the Lieberman Collins bill. Of course, it was ill fated. But it really brought about my focus on to tech. And in cyber, so I've been with elastic about six months, it's perfect spot data is continuing to grow, necessarily, and that value of data is continuing to increase. And as you know, John better than most, as I've heard, many of your guests say, data is really growing exponentially as our as our digital lives are expanding the value of that data data is also growing. It's at this point where elastic sits, we have a unified scalable data platform really allows your agencies and those listening to transform these massive amounts of data into the actionable mission critical insights that they need. So whether that's through our search capabilities, observability, or security, it's this security capability that really got me most excited about being it elastic. This data powered approach really bolsters the resiliency. And that's something you'll hear me discuss today. And that is, throughout the strategy, bolsters that resiliency from endpoint to cloud, by enabling these agencies to identify anomalies, detect these threats and address vulnerabilities in real time.

02:51
While spring training has gone down on Florida, I'm looking at you I'm thinking of spring training, who they caught. Where are they at? Now, usually, when I play baseball, there's always coaches that could watch a pitcher and they could see things that I couldn't see you move your foot on that, and they would help the pitcher and I have an eye for that. And I think you have an eye for what's going on on Capitol Hill and going on in the agencies here. I think that's why I want to get your observations on this big fancy pants National

Cybersecurity strategy. And, and let's let me state the obvious. I think when I read it, first thing that pops up is, yeah, cyber, you know, nation states are attacking the United States government. I mean, like stating the obvious here. I mean, how much more obvious can that be?

03:33

Yeah, no, absolutely. You know, this isn't isn't new. We've faced similar challenges from nation states to script kiddies to your run of the mill cybercriminals for a long time now, and I think we have as a nation, maybe we have resisted some of the changes that really need to occur in the in the data ecosystem in order to remain resilient. And that's what I think, in part with this National Cybersecurity strategy is attempting to do, you know, really builds on the Trump administration cybersecurity strategy, thankfully, may come as a surprise, but thankfully cyber remains one of the last bastions, I think of bipartisan core cooperation. The strategy itself ally outlined some really important priorities that that industry can collaborate on, including one you know how to defend us critical infrastructure, this is becoming increasingly more important. Second, you know, how do we dismantle how do we disrupt those threat actors? Third, how do we shape market forces? How does the government help to shape market forces that are going to drive security and resilience there's been a bit of a failure in the market someone argue forth, how we're investing into that reserve. salient future? And lastly, how do we forge those international partnerships to pursue these the shared goals. And all of these are important, obviously. But there are two big moves that I wanted to highlight in this strategy for you, John, that I think are probably fundamentally different than what we had been used to in the past. So first, the strategy calls for increased regulation on Cybersecurity and Critical infrastructure. Unlike many countries in the world, about 80% of our critical infrastructure is privately owned and privately run. A second area that strategy takes on is to shift security liability to software and service providers. So this, again, is a fundamental shift. And all the areas laid out in the strategy, this could get the most sort of pushback from industry. And I can discuss a little bit of that later. But first, let me just dive a little bit into the the first part protecting critical infrastructure section. I think the key takeaway from this area and for your, for your readers, or for your listeners to understand is that some areas critical infrastructure, we really have seen a bit of a market failure. So today's marketplace doesn't necessarily reward or incentivize these owners and these operators of critical infrastructure, who invest in proactive measures to try to mitigate these cyber threats. So the thought is coming out of the administration, is that where that market fails, the government needs to step in, and potentially regulate, of course, some critical infrastructure areas are already regulated. So it's not not a huge leap in logic, agencies with those authorities that exist already, we'll need to be more assertive and expected to sort of set these necessary cyber requirements for those agencies that don't have the legal authority right now to regulate, Congress is going to step in and try to close those gaps. I think it's important to keep in mind that not all critical infrastructure sectors are created equal. As you know, there's a wide disparity in the maturity of the different sectors, you know, you take financial, the financial sector is far more mature from a cybersecurity standpoint than, say, our water or utilities. So to the administration's great credit, the strategy calls for these regulations to be modern, nimble frameworks, and they're going to be tailored toward each sectors unique risk profile. That's another central theme, you will see throughout the strategy is how industry and government are best going to work together.

07:52

You know, if I assigned to the task of writing a history of, you know, this decade, you may come up with this early part and go Well, why now? So this is why I mean, why now, why did they pop this right now? Is it Was there an incident that no one's talking about is something happened? That yeah, so why now?

08:08

Yeah, you know, obviously, the cybersecurity landscape is evolving. It's evolving quickly. But there's one truism that that remains, and that is, you know, technology is always going to outpace policy. So, you know, we find ourselves in kind of a constant catch up mode. You know, that said, I think the buying administration and Congress has done a decent job. You know, we look back just over the last two years in particular, cybersecurity leadership has been in place then, Jenny's surely at CES and Newburger at NSC. Chris Inglis is the National Cyber director who recently left now of course, Director Kemba Walden. Anyway, they've all worked well together to keep cybersecurity as a top national priority. If you think about it, just two years ago, the NCD was just an idea. It's now filled with AD professionals that are driving these things. So I think the since since we last talked and what you ask why now, the administration issued a very comprehensive cybersecurity executive order back in May of 2021. This was primarily if you'll remember correctly, as a reaction to the solar winds breach and the Colonial Pipeline breach, the EO really focused on using the federal government's purchasing power to kind of help shape the broader ecosystem. I think it was a very comprehensive plan, agencies are still implementing large portions of that executive order. So think, you know, they're still trying to modernize those log management systems are still trying to implement the zero trust architecture. And of course, this was all sort of built to the National Cybersecurity strategy which is was issued just earlier this month. It's a strategy that's going to have, I think, broad implications on our on our industry and on our government and on your listeners for a very long time. So I'm really happy to kind of, kind of discuss this. So no, it wasn't based on a particular moment. But I think it was recognition, perhaps, John, that, that we really needed to put some, you know, what was prior into pen and to ideas, but actually putting it into action. And I think that's what this strategy really starts to try to do.

10:34

Now, if you think it's a 39 page report, and if you read it carefully, sit down, have a cup of coffee and get a notepad and take notes. You may run out of ink. I mean, there's a lot of stuff going on here. So the question is, the question is, is, okay, Arabel springtime weekend, and on this weekend, I want you to clean up that tree in their backyard and plant this and do that and paint the deck. And and when you're done wash the car and collect the garage. Oh, boy. I mean, at what point? Is it too ambitious knows eight hours in a day. And there's certain limitations here. And so what areas of the strategy think will work? And what do you think, made me some nudging?

11:11

Yeah, great. Great question, John. You know, it is, as you mentioned, it is chock full of, of good ideas. It is definitely ambitious. Now, many sections are just restatements of you know, of prior policies that they're trying to sort of underscore. But I think broadly speaking, implementation of a plan is always more difficult than actually developing the strategy. And I think that's probably the case here, too. There are a few areas in particular that I think are going to present a challenge. You know, for instance, take pillar three calls for five federal privacy legislation. Well, you and I have been doing this a long enough time, John, you know, I think

getting federal privacy legislation done, especially in a divided Congress is going to be really, really difficult. I think any online privacy legislation that does get passed in the next two years, it's probably going to deal in sort of these niche or edge cases, but not a holistic how private entities collect, protect, and use your sensitive data, that's just too, too ambitious of a task IVIG. So I'm a little bit dubious about areas of the strategy that are going to really depend on congressional action. We're losing some of our biggest cyber leaders in Congress, as you probably know, we last saw Senator Rob Portman, Representative John Katko, both retired, by the way, also Congressman land Jabin, perhaps the biggest cyber leader, most knowledgeable cyber leader on the hill, also announcing that he won't be seeking reelection. So I think we're going to have a real dearth of back cybersecurity background on the hill as it is anyway. You know, I think the strategy is also going to face some strong headwinds with with pillar one, which I mentioned a little bit earlier, this is defending our critical infrastructure, you know, where gaps exist for agencies to try to regulate, they're going to need to go to Congress, that's going to be very difficult in this environment. Another challenge is going to be around Sissa, which, you know, interesting, I think, over the last couple of years has done such a good job at partnering with industry. So partnering in a public private partnership and voluntary ways. And they're now going to be asked to move to a more regulatory more enforcement role in the future. And so seeing how director easterly and CIS is able to sort of harmonize regulations, I think it's going to be, it's going to be really, really interesting how they sort of how they go forward. And I would say, just one last, one last piece here is the strategy is a fairly controversial strategy, but I think an important one, and that is to shift the security liability on to software makers. So the administration is trying to incentivize security and resilience by design, instead of having people try to bolt on security after the fact. So how does the government impose these kinds of obligations on private sector? First, there'll be a legal stick. The strategy calls for imposing legal liability on stakeholders who are capable of building more secure software, those with the map market power to kind of move the needle so we're thinking, better protection at scale. And users have tried for decades, as you know, to try to bolt on security and resilience after the fact. And I think we've reached the point where there's just not a lot of success there. Everyone seems to agree that security and resilience really needs to be really needs to be baked in to the products themselves. So that's another area that I think will will be quite controversial. But we'll also get a lot of, if we can, if we can make it to the other end of that, I think it'll have broad scale protections.

15:17
Well, Bill, I'm gonna ask you to put on your DoD hat. Now, there was an initiative over the DOD, and we know about cmmc. And as soon as that came out, there are a lot of industry groups. They chimed in on what they thought. I mean, it's like, I don't think you'd do anything this time with five industry. You know, you could go get a hamburger for lunch, and they'll chime in on what's ahead. I mean, these industries are everywhere. So where do they stand on how they come in with this, if they, you know, started marching in the streets, or they agreed with it, or what's happened with these really powerful industry groups?

15:47
Yeah. So I mean, I think that what you would find is that maybe different industry groups have different different priorities. Well, that's a fair statement,

15:55
isn't it? That's a lawyer's statement.

16:00
You know, if you if you take, for instance, John, if you take I think there's going to be significant in pushback from industry groups around cybersecurity requirements for critical critical infrastructure sectors. So opponents from these industry groups are likely going to point to recent efforts, one by the Transportation Security Agency, TSA, another by the EPA, Environmental Protection Agency, they came out directly, you know, within a day of the cybersecurity strategy and released earlier and tried to issue cybersecurity mandates, at least in the case of EPA released cybersecurity mandates, no water system. So, you know, the administration for good reason exists expressed a lot of concern around cybersecurity risks. However, the pushback began almost immediately, cyber experts have noted that EPA doesn't necessarily have the right cyber knowledge to adequately assess such a complex subject as protecting industrial systems from cyber threats. Also, I think there was a general feeling that these kinds of mandates really weren't developed in collaboration with the water, water industry groups, which is goes completely against the spirit of the strategy to collaborate with, with industry in every way. So I think each sector is going to push back on regulation in their own way and make this pillar pretty difficult to implement. But again, my view is that if industry is fully engaged, I believe that the government industry can can get together and get where they need to be.

17:44
If I get into my little SpaceX rocket and look at this from space, I looked down. And if you look at what is infrastructure, you know, water, obviously, is infrastructure power, because infrastructure, data centers, and technology, it's all of a sudden, it's like, hey, there's new kid coming in. Hey, can build play second base would come on in here? Yeah, it's the new kid. The block is in the infrastructure world. I'm, I'm sure if you pulled her a book from 1960, the list infrastructure and maybe, maybe 1970, maybe 1980. But this is a new kid. I mean, all of a sudden data centers. That's part of the infrastructure United States is part of our part of our blood.

18:18
Yeah, absolutely. And, you know, critical infrastructure sectors really refer to those systems, those networks, those assets that have become essential to the functioning of our society and our economy. And as more of our life goes digital, I suppose the more sectors ultimately will be, quote, critical. And we'll need, you know, increased cyber protections going into the future. So let's talk more

18:49
about this public private partnership. And we know that term is bandied about all over the place, that could be anything and but it seems like the the Eye of Sauron the eye is focused, okay, let's talk about these and how can a company like elastic helping this transition? And they're looking right at you? And well, how can you help us with this transition? I'm See, that's, that's what I read between the lines here. I mean, they're, they're looking at say we'd have all the answers and looking at you. Yeah, there's a direct question.

19:18
Yeah, I mean, basically, John, I think that a lot of this, what we saw on the cyber executive order in May, a lot of what we see from the strategy now is an invitation to private sector to help. So, you know, I think you have your sector specific expertise. For instance, you know, we would never profess to the government would likely

never profess to understand the intricacies of how to protect water infrastructure. But those private sector companies that are running those for many years, they have a much better understanding of that. You know, we at elastic Of course, we understand data, we understand site for security, so those areas where public private partnerships are offered Take, for instance, the joint cyber defense collaborative that Jen easterly has. And those abscissa have started, this has shown tremendous success in, in mitigating, mitigating threats through sharing and through public private partnership. And you're right, it has been a little amorphous through the years. But it has definitely stayed consistent. And I think it's the government really recognizing that they don't have all the answers, and that they need the private sector expertise to contribute in a number of different areas.

20:37
I want to finish up this interview with talking about reporting. And this has been the nemesis of many CIOs and many agencies, we can write them down, you can probably have a list right now in front of you. And so do you think this is going to step up to the plate here at the baseball reference step up to the plate and maybe harmonized these reporting requirements across all these infrastructure sectors is a lot to juggle?

21:00
Yeah, I think it's gonna be a huge challenge. versus, you know, like I mentioned, they traditionally have played a role of close partner and close friend to, to industry, they're going to have to put on a slightly different hat. I think, going forward. You know, I think that the system or the government would readily admit there's so many challenges around the patchwork of cyber incident reporting requirements that are imposed on industry. Today, for instance, there are two dozen or so 24 federal agencies that have their own unique, proposed or codified cyber incident reporting requirements. So in addition, what could possibly go wrong? You got it exactly. So you know, and that's in addition to new proposals that keep surfacing at the federal level. While most states have individual breach report reporting requirements overall. So huge challenge to CES a harmonizing the cyber incident notification requirements, it's going to be a complex task. And again, it's going to require close collaboration between the government and the industry. Fortunately, CIS has managed to build up a ton of trust. And I think goodwill with industry over the years through this close public private partnerships, such as JC DC, so while they have their workout ahead of them, I think that I think they're up to the task.

22:23
Now, if you're listening to this, and there's snow on the ground, and you want to get more information, the company that deals with is elastic, e la sgic.co, for more information, and if you want to pursue this topic further, and learn more, go to elastic.co/industries/public-sector and a slash at the unless slashes and dashes here, but I think it's, it's really, it's good to get this perspective from you, Bill, because you can see things that and I'm sure every agency is unique and different. They want to have their own little plan. But there's got to be outsiders, views and maybe giving opinions on how this could work because it's so it's too complicated. And the threats to the first part of the report, you know, cyber threat. It's a real threat. It's there. Well, unfortunately, we're running out of time here, Bill, you have been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest BILL Right. Global Head of Government Affairs at elastic. Thanks, Bill. Thank you, John. Have a good day.