FEDERAL TECH PODCAST

# EP91 Insights on the National Cyber Security Strategy



00:28
Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator in the virtual studio today. We have Jim Richburg. He's a public sector field, Cisco and Vice President of Information Security at a company called Fortinet f o r t i n e t, kind of a well known company people kind of know what Fortinet has been around a while very well established reputation in the area. Now I've done a bunch of podcasts and the last couple of podcasts I've done, maybe I've gotten into the weeds a little bit. I mean, I did a deep dive on, you know, data at rest versus data in use security and encryption in data in transit that may have got a little boring. And so sometimes African may pull up to 40,000 feet and get a bigger perspective. So Jim's a perfect guy for that. I went to his LinkedIn profile, and it took me a half hour to read it. He's been ever done. He's kind of like Forrest Gump. Yeah, I've been there to this to that Stanford, here there, MIT CIA. And so I'm not even gonna give you his background. We're gonna do this. Okay, you've got his great background, Jim, give me the 40,000 foot perspective on what's going on the federal government today. And, and what I see people talking about is a National Cybersecurity strategy. Now, this is a guy who's on tactics and strategy, but inside the government outside the government. So Jim, is this just something at every single, you know, the president ministration? Does? Is this something new? Is this like, you know, whistling against the wind? Is this something that's going to actually come to fruition? So give me your two cents and 40,000 feet?

01:59
So do John, I thought we're gonna go talk about data in motion at 40,000. Oh, right.

02:04
I've done that so many times. I guess we'll,

02:06
we'll talk about the national strategy instead. Well, yeah. The reality is, virtually every administration does put out a national security strategy. And then they put out other strategies that support that, but that's their vision for how do they protect the United States, you know, so they'll put out a national security strategy, and then the Defense Department will put out a defense strategy, my former community will put out an intelligent strategy, I then had to put out a cyber intelligence strategy. So they all nest together. And for the last several administrations, we have had separate National Cybersecurity strategies, which ideally map to that national security strategy. And of course, this national security strategy was talking about, it's a scary world, we now have a change. And you know, what was going on great power competition, different visions of the internet, things like that are in the national security strategy. And then they fold into the National Cybersecurity strategy that President Biden released in March as well. Now, if you look at that national, that National Cybersecurity

strategy, it's an admittedly complicated document. It's organized around six thematic pillars, and it contains nearly 70 specific initiatives. And it's easy to get overwhelmed by all those details shown. But the reality is, if you read it, the bulk of the documents, actions are actually directed at the executive branch of the US government, which actually makes a ton of sense, as somebody who's been involved in creating or implementing a dozen aren't strategies, because what's the one audience who really has to pay attention to the president is the chief executive, that's the executive branch. So if you're doing a strategy, ideally, you want to have a lot of that strategy be directed at people who have to pay attention to what you're saying. And most of those government focused initiatives are not, in fact, new, which again, makes a lot of sense, John, because in my experience, having again been part of a lot of strategies in my 30 plus years in government, two factors distinguished a strategy that was likely to be successfully implemented from something that was going to become shelfware, where people would look at it later and say, oh, yeah, we wrote one of those, didn't we? And the two things are number one, that much of that strategy is evolutionary, not revolutionary. I mean, it. It's okay once in a while to have a strategy that says, hey, brainstorm, instead of going north, we need to go south, but you don't do that too often. I mean, once in a while, those are paradigm shifts. Normally, a strategy is a way of organizing and orchestrating what you're doing, putting a more strategic ship hoe around what otherwise looks like a bunch of disparate stovepipes. And the second thing for a government strategy in particular is it's more likely to be implemented, if most of the activities it describes don't require new funding to accomplish if you have a strategy that has A whole bunch of things that would be considered new starts in budgetary terms. Number one, you have to get them through Congress. Number two, if you have a continuing resolution, you can't do a new start. So who wants a strategy where you say yes, and if Congress would fund it, we could start it. So rather, this strategy builds on is a thematic way of wrapping together a lot of things government is doing and adding some other content as well.



05:25

So jump out about 1/10 as smart as you are, and maybe 150 for your experience. But when I when I read this and try to, you know, maybe highlight something, or back in the day with paper and highlighters, you'd highlight something. Yeah, it's called shift liability. It's like, oh, okay, guess what? Old Jim's got to step up to the plate now, because he's responsible for Jim software to is that evolution? Or is that new? I mean, that seems like something radically different.

05:54

As I said, there are parts of this strategy. It is mostly evolutionary, but has some things that are a departure. And this strategy was predicated on the idea that we have had a market failure when it comes to cybersecurity, doing cybersecurity has been something that some companies did, because they felt it was the right thing to do, or they've been attacked, and other companies did. Now, if you're just, you know, Acme Company, producing your little widgets, and you get, and you fail to do it securely, and that affects you and your customers. The other hand, if you're a utility that provides power to the East Coast, your failure is collective failure. That's what makes you part of critical infrastructure. And this strategy said, it's time to level the playing field, it's time to mainstream cybersecurity, it's time to not make it optional for the organizations that are in cybersecurity. And this strategy is really about trying to build systemic resilience to say, nobody has got perfect cyber security. People make mistakes, adversaries are adaptive and nimble, sometimes they get lucky. So let's, rather than try to have cyber perfection, find ways of building building down the risk. And the strategy

does seek to do a fundamental shift, John, in the sense that it says, We want to move the risk in the ecosystem, from the end user, which can be small and medium business as well to those who are systemically more able to absorb it. And that would be the big companies that produce it and communication solutions. So people often throw around the metaphor of automotive safety. And they say, you know, we used to just say the way to have fewer auto fatalities is people just have to drive safely. It's all about the drivers responsibility, and I'm talking about their 1950s. And then you had the book, Unsafe at Any Speed that showed there were actually cars that were designed, was known they had flaws that made them unstable. We didn't have seatbelts. So we started doing a lot of things. You know, we had Driver's Ed, come on in school, we had, you know, drug anti drunk driving campaigns, including stepped up law enforcement, we started literally building roads safer and polluting, you know, devices that if you crash into them will give rather than impel you on a guardrail. But what really moved the needle more than anything else was when the manufacturers started making cars that were inherently more safe, and when they got sued to your point of liability for failing to make them safe. So yes, there's lots of moving parts to this. But arguably, if you really want to move the needle, you make the people who should be in a position to best understand it, the people making the products and services responsible for it. And John too often with with cybersecurity, we have had this Let's rush in IT product to market because first of market is going to capture the market share its innovative, etc. And then security was almost an afterthought, we'll bolt that on will take care of that in the first patch. And this was an attempt by this administration to say no, we need to move the needle security needs to be part of this things need to be secure by design, and delivered to the users in configurations that are secure by default. Now you can go in and turn off all those options. But let's give it to you most people are I won't say lazy, but we're creatures of habit, we will take a software product we'll install it will count ourselves lucky when we get it to run, we then don't go in and start tweaking all the security settings. So if you give it to people with all the security options turned on, that's probably the way they're getting long winded answer to what that really is one of the fundamental departures of this strategy. John,



09:34

years ago when we were in grade school, I'm sure you took a health class and said, you know, eat a balanced diet. Okay. And I'm sure maybe read articles where here's the pyramid and here's the balanced diet. And you know, I can I can say that you could say that and, and I'm sure if you're at an event people Yeah, you work out I work out too. And, and when I hear this phrase public private partnership, it's you know, 10 people I mean, send it from thanks for some people means Oh, yeah. That means something other people see. And so that is another aspect I think of this this strategy. And they are using, they are pointing their finger at CES or going Hey, Sis, you're up to bat here, you got to take an approach some this public private partnership in order to maybe to do it. And so is this something that's just a palabora? Is this something that's written in the wall somewhere? Is this actually thing because it's going to be a change? Because it doesn't cost anything. So maybe it's Ontraport, too?

10:25

Well, public private partnership is going to be absolutely integral to this strategy I talked about most of the initiatives were focused on the US government, but that means they have action on moving forward. That doesn't mean success is entirely contingent on how well the government does. So for instance, secure by design secure by default, I've said is one of the big departures of this. And yes, Sissa has the pin on this, this is

something that applies to all 16 critical infrastructures, they all need to make cybersecurity Intune. But what's the one that delivers the products that they all live on in this digital world, the ITN communications people? So Sissa is pointing the finger directly at us. And I'm actually one of the leaders, co leaders of the industry effort on saying, Okay, how do we take this high sounding good phrase, like eat a healthy diet, deliver secure products? How do we operationalize that in a fashion that we can do that isn't going to drive us to, you know, to bankruptcy, that's going to make a difference. So we're actively working on that very intensely with Cisco right now. So they're, they're putting effort where were the words are right now, but on the broader issue of public private partnership, you know, the reality is, most of the technology innovation comes from the private sector. And we remember the Cold War where yes, things like, you know, transistor and all that we're really coming out of government funded effort. We're now in an era where other than little niches in my former world of national security and intelligence where we succeed because we could do Mission Impossible I have IT sector is driving thing, they have more money, they have on balance, more smart people the government does. So the the innovation tends to come from the private sector. On the other hand, things like the frameworks for cybersecurity tend to come from government. I was one of the people who helped put together the the NIST National Institute of Standards and Technology cybersecurity framework in 2014. If you had ever told me that, cybersecurity professionals around the world would think of the functions identify, detect, protect, respond, recover, that we were putting together for government, I would have said you're crazy. But the reality is government does a good job putting together conceptual frameworks that are technology and threat in vendor agnostic, they did the same thing I was very trust, they really came up with the concepts that became zero, the private sector and marketing firms stuck what frankly, is an unhelpful label on this, but government, what I'm saying, John, is there's a good partnership here. A lot of the smart thinking on actual solutions will come from the private sector, but a way to get beyond any one company's reach and say, here's a broader perspective on this that often comes from governments organizations like NIST, or even CIS, as you said, another element in cyber John, that site where public private partnership is integral, and I've heard government increasingly recognize it is on sharing information about threats that the private sector a company like Fortinet sees way more threat information even than the big three letter agency comm organizations in the world I come from. They're in different places, they're in there with people's consent. They're their customers, now, they're not spying on them, as we would say government could be doing. But the reality is, both sides public and private sector see something about cyber threats, and you need to find a way to share it. And you've got you've got constructs that have been put together like the JC DC, which is not a you know, a throwback 70s Rock Band, it's the joint cyber defense collaborative. You know, we've talked in when we were at war in Sandy places about the need to get to the left of boom, you know, that nation of the ID if you wanted to defeat it, it was not by having a harder vehicle, it was snowing where it was going to be disrupting the planners. We tried to do the same thing now on cyber JCTC as a way of saying rather than bring the private sector in for cleanup on Aisle Five, there has been a major cyber breach that affects them as well as us. Let's do smarter planning, let's systemically solve some of these things. Let's say Hey, I see part of the juicy part of that we put it together, it's a threat and here's how we can solve it. Whether government doing law enforcement, whether the private sector say well, you know, I can make that vulnerability go away by designing it out of the news. So yeah, John, public private sector partnership is absolutely critical to solving this problem.



14:54

We began this interview with me being kind of jovial and talking about 40,000 feet. Let's go down the grid. Let's go down to my backyard. My backyard. I have a pond and a waterfall and the pump failed. Well, I went online just like Jim would do. And I got a replacement pump that's gonna come in tomorrow. And I've never put a pump in upon before I have no I have no idea. I know there's TriCity involved in fitting. And so it was pretty easy for me to find it online. I found it like, I don't know, five, five seconds it was bank, putting the gallons per hour bank, it's right there and it's delivered the next day. That's easy. So coming up with a strategy. That's pretty cool. My strategy is to put on a pond pump. But you know, I may have to call you up on Saturday morning, or Hey, Big Jim, come on down and help me I cannot implement the installation of this. So so there's the implementation question that I love strategies, Hey, eat a good breakfast workout every day run 10 miles a day, but then it comes down to the reality It's six o'clock in the morning and you don't want to go to bed, you're not gonna run 10 miles, you can run two miles. So what about implementation of all this? Is this something a fairy tale? Is this actually going to happen? I mean, they have some measurement here involved in it. So So what about implementation?



16:05
First off, John, you know, you're gonna get banner ads pumps for the next year. So my life will have died and you'll still be getting Nero

16:13
banner again, Jim rich Bruce pump company on my front door. Hi, I'm Jim, do you want to buy a pump? Yeah, I bought one.

16:20
So as I said, this strategy has an advantage in that a lot of the activities that describes are things that are already ongoing by government. It's a way of putting this a way of saying, Oh, I see what department a department B department see we're doing and they all look like separate things. And they are, but they all fit together under one of these pillars, whether it was defending critical infrastructure, whether you know, whether it was changed the ecosystem. So the implementation plan was just released by the administration, not two weeks ago from when we're actually taping this. And it talked about which agency has the lead on which initiative and where they're supposed to do it. And you look at it and said, Wow, there was for instance, and initiative here on the governor record, they reserve the right to do more regulation, the R word, the thing that scares people in the private sector. But that's sort of the tool of last resort. They want to use incentives to do it. So boom, last week, because the other part of the R word was said we recognize we hear the private sector say we have too many cybersecurity regulations from the federal government. We know we don't want to respond to 12 separate things, when a bad thing happens, sometimes even tell us to do contradictory things. So what was one of the activities, regulatory harmonization and deconfliction? That's already come out as a request for information for the private sector government says we know it's a problem. Tell us how. So John, my point is some parts of the strategy are already being implemented. There was something there that said, you know, one of the things people have said in cybersecurity is if I'm looking if I'm looking for that pond pump, John, I have no idea which of them are cybersecurity, which of them aren't, you might actually make this be an Internet of Things device that can report into your phone and say, Hey, John, I'm overheating and I'm gonna fail, you might like that. You wouldn't like the fact that it might be able to go into your phone, it's still your

banking information. So you would like to know, if I'm buying an internet of things connected pump? Is it upgradable? Is it secure? And the reality is right now, it's really hard to look for that, to know that even if you go to the manufacturers website and try to do it. So we were looking for the equivalent of something that would provide the something like the Energy Star rating, but security for IoT devices, the Federal Communications Commission already started to release something on this last week. So you know, this strategy is not just shelfware, you've actually got very demonstrable steps that will be impactful, that are already being taken by some of the departments and agencies. If you look at the implementation plan that was released, it literally gives you a roadmap, who's got the pen, and what their timeline is, for 65 of the initiatives in the strategy. It's actually a very comprehensive roadmap. And it even says, oh, NCD let's throw another four letter within the Office of the National Cyber during which was the author, principal author of this strategy, has got responsibility for overseeing implementation to for reporting to the President on how it's doing for incorporating lessons learned. Well, this one seemed like a good idea hasn't worked. Let's fold that in. And for working with the Office of Management and Budget on budgetary guidance, and having been one of the overseers of a previous whole government, cyber camp, cyber activity under Presidents Bush and Obama. This is a lesson learned. They're benefiting from some of the things we were unable to do. So yeah, I look at the strategy and go, they really are doing things on implementation that I think will make this a more achievable strategy. Okay, Jen, let's



19:59

say we find I remember the whiteboard, and and I write out all 65 actions. And then I hand you a red marker and I go, Okay, Jim, you have written standards, you've implemented standards, you've been frustrated with standards. You've seen standards successful. Sanford's fail. And so just as a final question here, you know, what do you think will be the most consequential in the near term and implementation here, I'll have all these actions to take all they're all important. Well, you know, Jim, Jim seen, so what are maybe one or two that maybe maybe move up on the list.

20:30

So you know, it's an old triad of you know, you have cheap, quick and effective, pick two, consequential versus near term, I think are going to be are going to be different. Now, if you want to talk about who's going to be most affected, the IT sector is arguably in the short term going to be one of the most affected this whole idea of secure by design secure by default, which nests with other things, this whole idea of you may have heard the phrase, s bomb software bill of materials, the idea that for code, we don't have the equivalent of an ingredient, we don't know what goes into a piece of to a software program. And yet a lot of those are software modules that are being recycled. So there's a lot that will affect the IT sector voluntary standards, but the thing is, if it starts creating expectations, by your customers by the other critical infrastructures, then that becomes something that I think is very impactful. Shifting liability for software security is one that they have in there. And I joke that if you want to make quick progress on an issue, John sick, the lawyers are gonna make long term progress on it, let the engineers boy, you want to move the needle in the short term, you make a liability, we want changed corporate behavior, on liability with something like Sarbanes Oxley about saying, Hey, you guys individually may have civil and criminal liability for so Oh, that change corporate behavior very quickly. So there are multiple ways I think that they'll try to shift liability for software. But it's a way of saying it shouldn't be dependent, the user shouldn't be the one who has to put everything together, make it work, and then make it secure as well. Shame on you. It's like saying here, John, here's a car, you go put the safety features on it and

make it over that one, I think is going to be very impact. And I'll throw a final one, John, which is asleep. Because towards the end of the strategy, there's something that says support for cyber informed engineering principles. And, you know, the, the National Cyber director was Chris ankles, he, you know, he left shortly after the draft right around the time the strategy was released. And I think this was one of Chris's personal touches in the strategy, because he used to talk about he was an engineer, when he was trained as an engineer. It didn't your engineering training didn't include things like environmental impact and safety. I mean, it wasn't your responsibility of what you made turned out to be a polluting device or an unsafe, that was somebody else's you designed to specification. Now, environmental impact and safety are taught in all engineering disciplines. It's part of your fundamental job. And he's hoping I think, with this cyber informed engineering principles to do the same thing to say, Everybody who's designing something now should have should have had cybersecurity as a part of their engineering training. So again, it shouldn't just be a matter of saying, this is the CISOs job in the company or this is you know, that part of the product team. No, it should be something where if you're thinking about how to solve a problem, cybersecurity should be one of the criteria you're trying to address.



23:30
I want to end this interview with a reference made to s bomb. I spent 25 years on doing live radio on NPR, and I did everything humanly possible to avoid any F bombs. And yes, I did because the FCC didn't come down on me for any s bomb at all.

23:45
At least we tried to we tried to define them, but we s AC DC, and we were here with the best but we do define our acronyms.

23:54
You have been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Jim Richards, public sector field Cisco, and VP of information security for Fortinet. Thank you, Jim.

24:05
My pleasure. This has been a great conversation.

24:10
Thanks for listening to the federal tech podcast. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcasts.