FEDERAL TECH PODCAST

The Supply Chain and Federal Security

SUMMARY KEYWORDS
vulnerabilities, software, company, fortress, automate, security, people, dod, john, critical infrastructure, supply chain, patched, satellites, automation, organizations, bad, folks, francesco, buyer, business

Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Our guest today is John Co. Francesco, Vice President of Business Development at fortress information security. John, how are you today?

02:28
I'm doing well. Thank you for having me back.

02:30
I've known John for many years. And he's kind of like a surfer. He kind of he somehow I don't know how I used to be a football player, not a surfer. He kind of surfs the technology when it comes to information security, the federal government, and he's very good at knowing what's going on, I thought we'd bring him in. And we talk about his company, and some of the concepts he's talking about, as far as supply side security for the federal government. And, and if we just say the word, you know, supply side security or software bill of materials or something like that, it opens up a whole world of discussion here. But John, I'll let you introduce yourself, your company and and come up with a couple different topics we're gonna focus on today, because it's such a big topic.

03:07
Well, John, as you know, I've been working in and around the federal government, my entire career, I tried to stay just ahead of the wave, follow the surfer analogy, in terms of really what's most innovative, what's the most important new space. And typically, what I'm doing is I'm bringing really high end commercial technologies or practices into the federal space. That's really where my expertise lies. As a company, what fortress does, is focuses on cyber supply chain security. So we're really, really focused on making sure that the assets, the hardware, the software, the firmware, that you're putting on your networks, into weapons systems, serving the taxpayer, that those are secure and coming from secure sources. And I can tell you right off the bat, that they are not secure, and they're not coming from secure sources. So we've had a very busy two years.

03:56
And if you're listening to this, I just want to say the website for the company is fortress info sec.com. Last year, I was in LA twice. And one of my visits, I went out to Long Beach and did a boat ride and saw the ships out there, you know, I mean, they're stacked up, they're like mountains. And I think this is what most people think

about supply chain problems. It's it's a it's a router, it's a it's a physical product that's sitting on a ship trying to get in and there's issues and everything else. But But I think this whole idea of supply. So it goes way beyond just hardware, doesn't it software, and it includes hardware has to doesn't it?

04:31
Yeah, actually you will component by component basis software typically has a much broader supply chain than hardware. It's a it's a more ephemeral to think about, but the reality is, is that there are probably 10,000 individual people who contribute to a big piece of software, many of whom are completely anonymous.

04:53
That's unsettling for some people. There's companies like cyanotype and you know, these folks is cyanotype. They, they do surveys and everything else And, in fact, last year, they did a survey. And they saw 12,000 vulnerabilities and different pieces of software they've seen. I mean, this is 1000s. This isn't one or two. So this is almost a standard operating procedure, these vulnerabilities and software, isn't it?

05:14
Yeah, it's a really big deal. And you have to understand why what's driving that is, you're a software developer, you have somebody over the top of you probably a manager who's never developed a piece of software telling you, you got to make this thing right now, we're two weeks behind, and it was due yesterday, everybody yelling and screaming to get stuff done. So what people do is they, they pull open source software, from community sources, primarily GitHub and other places that have open source contributors, so anonymous contributors. And when you keep doing that, you keep building dependencies into your software. Ultimately, what you do is you create a really great aperture for creating vulnerability. So Sona type, and companies like mine, we're continuously finding major pieces of software from important companies, that just has really vulnerable components.

06:04
You know, I did some research before this interview, and my my, my, we could go for about 20 hours on this topic. You know, if you look at the DOD, they have a bounty out for finding vulnerabilities. And just last year, they have report this out that in the defense industrial base that much Avanta Dib. These bounty hunters, they found 400 vulnerabilities. These are people who supply software to the DOD. This is not software to John Gilroy, is doughnut shop. I mean, this seems like a big issue here, isn't it?

06:38
Yeah, it's a really big issue, because you have to think about there's 300,000 companies that serve the defense industrial base, each one of those companies has an opportunity to accidentally or through sort of laziness introduce a vulnerability or multiple vulnerabilities. And it isn't just that they're building network systems for the DOD. I mean, these people are building aircraft and missiles and all the other things that you really want to have some good controls around. The other part. And this makes it super hard for the DoD buyer, the Federal buyer, is that they don't have insight into what is going into this product, you would think and certainly I used to think that the DoD buyer sort of had a map of everything they were buying write a list. But in

reality, about 2030 years ago, some of the regulations changed. They move away from God's G OTS government off the shelf, and milspec designed equipment over to cots, C OTs, consumer off the shelf equipment. And it really makes this a black box. So you have major weapon systems, major major network systems, that the DoD user, the DoD buyer just really doesn't know what's in it.

07:44
Speaking of what's in it, I was I keep track with this log for je vulnerability. And I mean, I saw this the study this morning, and this is just incredible to believe, is that there's there's 90,000 servers that have not been patched, they know it's a vulnerability, they know how to fix it, and they did a scan, and there's 90,000 servers that aren't patched, this would lead to the whole question of automating some of this. I mean, I think we're almost getting forced to automate some of this, because there are obviously systems managers, administrators that are ignoring the obvious, aren't they?

08:19
Well, you know, you got to think about it from a resource management perspective, that so you're you're one system manager, maybe you're a small company, maybe you're at a big company, and you have 10,000 vulnerabilities, you're gonna choose the ones that are affecting your users now. And that's why log for J and other vulnerabilities like that, which are prolific hang around, sometimes for years. And in fact, when luck for Jay first happened, and it really was getting the press, you know, we predicted that it would take something on two years to really close that gap. We're still months into that discussion, right? We're not years into that discussion yet. I think we've got a long way to go on that one another still,

08:58
I wanted to bring up the topic of automation. That was my obscure way of bringing it up. But it would seem that in a an environment, with distributed software coming in all over the place, there's got to be some way to automate or some kind of a way to take and scan the code. So it's not vulnerable. I think that's where your company sits, is that right?

09:18
Yeah. So we manage a lot of that business really taking on vast quantities of, you know, vulnerability and bringing to bear to our clients. First, the ability to identify, hey, you know, you've got poison in the Punchbowl. And then second, giving them away to automate the the, you know, solution to that issue. I will say the government itself is taking on a lot of this. So we're seeing the FBI and Cisco and other agencies trying to assist but at the end of the day, the organization that owns that software that the company that bought it, if they're not playing ball, if they're not going out and doing some of this work, it'll never get done automation or not. Because somebody has to approve it. Somebody has to hit the go button.

10:01
There is a foundation in DC called the Sunlight Foundation. And they talk about being transparent being visible. And and in this whole discussion of software security, some people say, Well, really, it's if you have

free and open source software, this is one way to eliminate some vulnerabilities. Is that just too, too much of a glib answer? Is that's just not even worth discussing, or was that fit in this discussion?

10:24

You know, I think that was an answer that people were giving pre pandemic, the practical reality is, is that a lot of these vulnerabilities are coming from open source organizations. So and let's kind of walk through the story there, right, that's, uh, you have programmer Joe sitting in his office, he's got told, Hey, you got to whip out this software here in two, three weeks, he knows he doesn't have two or three weeks, really to get it done, he's gonna get pressured to get it done quickly. And he's probably got two months of work to do. So what he does is he goes to open source sites that already have pre built components, really valuable components, pulls them down without having checked or reviewed them, because he's short on time, right, and then introduces them into his software. Now, here's the thing, even if all the immediate components that Joe downloaded and is now using a new software are good, those pieces of software themselves have components. And often it's that second or third or fourth layer, where you find these vulnerabilities look for J is a great example. It's not immediately apparent to most of the people programming most of the people introducing, you know, the software into their code, you sometimes you have to find a ended up bedded or dependent library. And this is what's going on. And so it's actually this open source libraries that induce a lot of the problems that we have today.

11:41

Wow, that's a that's kind of scary going to take a look different topics we're talking about today. Automation, good, bad. I mean, when I think of automation, I think of unmanned unmanned systems. And I do a podcast involved in satellite in space world, and there's gonna be 30,000 satellites out there. I look those as unmanned systems out there. And, and are there vulnerabilities with automating some of this process?

12:05

Well, yeah, let's vote, the vulnerabilities tend to pop up and things that have been automated. So let me give you kind of a description why we'll talk about satellites, right? If you're Russia, it's going to be pretty difficult for you to shut down all of America's satellites. And if you do it, even if you shoot down one, right, that's going to cause a lot of hubbub. But if you hack a satellite, or two, or three or 10, or 100, right, gonna be very difficult for the United States to respond to that first event to prove it was Russia. Second, right, they're gonna have to have some kinetic response that could escalate things. So if you're the bad guy, you have a lot of interest in using vulnerabilities in critical infrastructure satellites, a great example. Right? And there's a lot of aperture to do that, that. So when a system is manned with a human, right, you have a person sitting there turning the wrench, you really can't hack the human, right? I mean, you might be able to bribe them, but you can't hack them. But when you automate a system, say a pipeline, right, or satellite, well, that's a great opportunity, which what you've just done, as you said, have removed the human. But I've introduced a machine and that machine is hackable. So, automation is really good for resolving these types of issues. But automation also creates some of these issues. It's what that is actually what makes America uniquely vulnerable, more than any other economy on Earth. We have automated, much of our critical infrastructure. And that's why the bad guys like to use this angle to get after us. You saw that in the Colonial Pipeline hack. And you're seeing that now quietly amongst America and her allies, as Russia does some outward attacks.

13:35
But if I were a system administrator working 6070 hours a week, and I see an automated solution, well, I could put my feet up and smoke cigar. Well, why not? I mean, I think there are companies out there that would say, Well, yeah, automate it, right. I mean, we're How do you guys handle differentiation automation?

13:58
Well, you know, absolutely. We're not saying no automation, we're huge fan of automation. In fact, we introduce and sell automations ourselves, but rather, what we're saying is that you have to have the appropriate, you know, sec ops program. So when you're building your software, or you're buying software, you need to make sure that the people from whom you've bought it or yourself, are taking the appropriate actions to make sure that software is secure and being maintained. And, you know, I think the best way to equate it is, is to sort of walk it back to food safety. You know, if you went back the clock, 100 years, you know, food wasn't as safe in this country as it is today. Today, you can go to any gas station, the United States, and you can be reasonably certain that the Slim Jim, you pulled off the counter there isn't gonna kill you. Right. And that's because between that Slim Jim, you know, hit the counter at the 711. Right, and it being produced. There's five or six federal and state agencies who are reviewing it. And there's a lot of regulations there that really put controls in place as to what happens so you can be reasonably assured that what you're eating is not going to make you sick, that doesn't exist. In software and in hardware, so that $5 widget that's going into nuclear power plant, the $5,000 piece of software that you just put put into a government network, the $500,000 piece of software that just went into a military piece of equipment. In practice, that is only reviewed between the buyer and the seller, there really isn't a regulatory body looking at that. And that means it's a little bit of the Wild West, and a lot of silliness can happen. That's really what fortress does. So fortress is coming in as a third party saying, Hey, we're going to fill that role, because nobody else is.

15:35
Earlier, I quoted these folks from resilient, they talked about 90,000 servers, that they're not patched. This morning, I was reading about Cisco, we all know CIS in town here, they have something called the vulnerability exploitability exchange, the VX, which lets vulnerabilities, is this just an exercise in frustration? Of Oh, John, your back doors open? Okay. Oh, by the way, your back door? is are these lists even usable? Or what's the purpose of lists like this?

16:05
But you know, John, I think that's the best question. You know, that may be the most pertinent question. It depends on who you are. So, you know, we have had the opportunity to talk to somebody, even the most sophisticated companies, and let me tell you, even they don't have a lot of the expertise required to take on this new level of challenge. And part of that's a Manning issue, right? There just aren't enough Americans around, or, you know, people in the free world around to take on some of these challenges really trained in cybersecurity, right. And part of that is, is really just how quickly the field is growing. Every day, the good guys come up with something the bad guys are coming up with two new something. So I think this is done a really great job of LaTorre job of bringing new new techniques, new capabilities to bear, the Vex is a great example

of vulnerability exchange data. But we're really in a place as a market, where the average company, even the big company is struggling to meet these requirements very, very difficult. And really, that has to be focused on the small businesses, there's 300,000 small businesses that serve as the defense industrial base and broader federal government. And you're asking a construction company of 5060 people who are really experts in laying down concrete, okay, now I need you to be experts in cyber, that's a tall order. That's a tall order, when even your multibillion dollar companies are struggling to do this.

17:24
Earlier in the interview, you use these phrase kinetic response. And imagine when you're a young man on the football field, you had a lot of kinetic response at the 50 yard line. And, and then when I think of kinetic response, and today, there are parts of the world in Ukraine where there's a lot of kinetic response, and actually the rubber hits the road in some of these areas. And so why don't we take and broaden our discussion to you know, the whole world here? Are there organizations like a Global Security Alliance are coming together to talk about these threats or so I would imagine fortress is involved in many, many aspects, not just the federal government.

17:55
Yeah, well, we have great relations with a number of organizations. The GBA Global Business Alliance represents the 200 largest foreign owned domestic manufacturers, that are great partners of ours, we're working with various icepacks, the Chamber of Commerce and others, both to work on policy, but also to help the companies themselves. But there is a practical reality here that, you know, the bad guys who are out there doing these things, they're not going to stop until somebody physically stops them. You know, there's that old adage, right, everybody has a plan until they get punched in the face. America hasn't been throwing that many punches in cyber, and I'm a big fan of starting to do that.

18:35
Everyone has a plan until there's a kinetic response. That's the way to phrase it. I went to your website, I mentioned it earlier. Fortress infosec.com and keyword there is critical infrastructure. John, did I lose? Yeah. Yeah, I think he froze up. Yeah, he froze up. To your company, website, fortress infosec.com. And the key word phrase is critical infrastructure. It would seem that the emphasis here is on critical infrastructure only. But fortress is much more than that, isn't it?

19:26
Well, yeah, but so when people think traditional critical infrastructure, right, what they're thinking about his roads, bridges and things of that nature. And it's true that those now have embedded in them a great deal of software. But if you follow the, the cysa designation, there, you're talking about hospitals, large ITSM companies, you're talking about organizations from the military all the way down into food supply that so when when you think about fortress and what we're doing it's really if you're working in an industry where if that industry fails or falters, it changes the the everyday life of the American. That's where we are. And we really, really started The business in the energy sector. Obviously, if lights go off, things change immediately for everybody. But but since then we have expanded out and really have engaged across the infrastructure space.

20:11
So from infrastructure or even talks about lessons learned, what are the lessons learned? I mean, the fact that you said no training friendliest OT and it so operational technology in it. So it is, is a lesson learned, secure ahead of time patch, or is it? Is it the main vulnerability for this is email and phishing? I mean, I hear all kinds of different sources of information on tax is it phishing? Is it is people actually trolling infrastructure sites like oil pipelines?

20:39
You know, what if I if I had one piece of advice to give to folks, it would really be look at the devices look at the software that if it fails, it's going to have an impact on the actual function of your business or organization. And what I mean by that is, if you're at a nuclear power plant, and you have 1000 printers that have vulnerabilities, that's not great. But it isn't that big a deal compared to one $10 servo that has a vulnerability if that servos controlling the nuclear rods, right, the cooling rods, so you have to look at vulnerability in context of outcome. I think a lot of times when we talk about IT security, or OT, operational technology security, folks are looking at it in numbers, right? So they're saying, hey, the the 10 vulnerabilities on the printer is 10 times more than the one vulnerability on the servo. The reality is, is that servos worth far, far more. So think about outcome first, when you're deciding where to invest your time and effort.

21:35
On the top of your website, there's a banner ad saying that fortress InfoSec receives $125 million in investments from so why are they Betting on you guys? I mean, there's just 1000 security companies just in DC, why they better than you?

21:51
Well, you know, Goldman Sachs really takes a very thorough view of the market. Ultimately, and this is sort of reiterating what they told us when they elected to invest was that they looked across the market. And they decided, hey, this is the company that can really touch the most important parts of a company's network itno T, and help them to secure it. So loads of other companies doing lots of interesting stuff. But if you're really concerned with no kidding, security, not security theater, if you really care about security, then where your guys, there are definitely folks who are better dancers and actors. And I'll leave those firms to that.

22:27
Oh, I liked security, kabuki theater, theater, that's a it's a good perspective on this whole idea. My listeners are gummies and 60%. Typically, so many times they are charged with putting together reports on incidents, and I can't even listen to reports have to have. So how can your company help my listeners in generating reports for compliance purposes?

22:51
Good. So that's the place where automation takes takes place, right? So if you think about what fortress does, right, we're really bringing no kidding security to it ot networks, helping you to understand who who's made it

into your supply chain. That takes thinking that takes work. But the reporting on it shouldn't. That's where you can automate. That's where we have automated, okay, give me an idea around this, that's a your average government employee has something between, you know, 20 and 500 500. It related policies that they have to comply with, depending on their seniority and what position they are in, in the organization. We're taking all those policies, putting them into our system, so the system just spits out that report that so instead of spending 80% of your time generating this, this PDF, or, or PowerPoint that needs to go to the boss, you're spending 80% of your time, really addressing the security issues, and then you're doing that last 20% is hitting the go button, the report being printed, and then you're discussing it with your teammates.

23:49
I think we're stumbling on something here. That's important. There's something called the better cybercrime metrics act. And it talks about what's happened and and then there's this event she talked about. I mean, there's there's a lot of Yak here, John, I mean, there's a lot of people saying this is, and I think maybe this is why Goldman Sachs is investing in you. I think reading between the lines here is that there's some kind of action involved here where you do some analysis and and maybe maybe, for some kind of a patch management system, I think, is that by reading between the lines here that there's a little bit of punch behind this company?

24:27
We absolutely right, that so we have really close relationships with folks on Capitol Hill. We work closely with representatives from the White House and others, that we've been helping to guide sort of the next steps here and America's cyber defense policy. Certainly not the only ones have been really forward thinkers, folks in the solarium commission, Senator Scott's office, but others along those lines and what we're seeing is there is a coalescing around this idea that we need to implement some base level standards. This is no different than what happened in food security. How Two years ago, right, the book, The Jungle comes out. People start getting smart on maybe I want to know a little bit too what's in the sausage. same is happening here. And it's bipartisan. So you have the White House on one hand. I mean, you have one of the leading Republican senators and Senator Scott, on the other hand, all working together to put together some legislation, some regulations around this. It is one of the few things left in Washington that is truly bipartisan. Nobody wants to have their constituents without power or water or food. Cybersecurity is a meaningful vulnerability in those spaces. And really, things are starting to change. They're

25:35
enjoying the reference to Upton Sinclair, I'm an old history buff. That's interesting. One of my heroes is guy named Brigadier General Greg touhill. And he runs this place called cert over and Pittsburgh does a lot of other things too. And on your website, you talk about a Security Exchange collaborative Cybersecurity Information Exchange, do you work with folks like serve their preferred organizations you tend to work with

25:57
you know, that's a we run a network called the acid to vendor network, it really is the first of its kind, in in, you know, the power generation and critical infrastructure industries. And what that's designed to do. So if your

power company one, and then you look at a vendor, you determine that they're good, bad or otherwise, it gives you a mechanism of sharing that information anonymously, and non competitively with the other power companies. And this way, those power companies can work together to ensure mutual security, while not creating a loss of, of intellectual property for themselves. So it's a great opportunity to sort of raise the bar. And it also allows the power industry and other industries that have now gotten into the DOD, specifically, to pressure vendors. So let me tell you, a lot of what happens is that a vendor comes out with an asset that becomes prolifically used, and it's weak, it's vulnerable, it's vulnerable, it's weak. And then one of the the customers will go back to that vendor and say, hey, I want you to make this stronger, I want you to patch it. And basically, the vendor will say pound sand. Because an individual consumer, even if that consumers, the Navy, or the Air Force, isn't buying enough of that asset to change the economics for the company. But if you have a network of companies are a network of buyers, in this case, power and the DOD and healthcare coming together and saying, Hey, we're going to stop buying this asset. If you don't make it more secure. The company is a little bit more reticent to tell them the pound sand, they're much more willing to play ball. And so we built this first and energy we have since now rolled it out to really all of the critical infrastructure spaces. And it has been a game changer in changing behaviors of vendors and asset producers.

27:34
Well, there's a headline for this interview, change of behavior. We can list vulnerabilities all day long. We can talk about sharing vulnerabilities. But you know, if there's not action there, we're going to be in trouble in the future. Well, unfortunately, John, we're running out of time here. You've been listening to federal tech podcast with John Gilroy, like thank my guest, John Co. Francesco, Vice President of Business Development, fortress information security. Thanks, John.

28:00
Well, thank you so much, John. It's always a pleasure to be with you.