HPN – Cybersecurity with John Cofrancesco - Fortress Information Security

Jim Murtha: Host
John Cofrancesco: Guest

Jim Murtha: *The following podcast is sponsored by fortress information security. Fortress offers the only comprehensive cybersecurity solution for your entire supply chain. That strength combined with fortresses operational vulnerability solutions, and your organization is protected from a full spectrum of cybersecurity risks. This program is a production of Macallan Communications publishers of Homeland Preparedness News. The mission of HPN is to inform and educate the American public about the efforts undertaken by its government and private sector to protect them from the ever-evolving threats to the homeland. HPN can be found at WWW dot homeland prep news.com.*

And welcome to the Homeland Preparedness News podcast. I'm your host Jim Murtha. The trillions of dollars spent in the intervening decades since the end of the Second World War by the US and its allies have created a defensive shield as well as an overwhelming offensive force toward off any potential entity conspiring to do us harm. The military might have Western Allied forces is massive, complex and lethal. But many people have wondered if what we have created can address the 21st century threats that look nothing like a missile, a tank, a battalion of soldiers or a nuclear weapon. Cybersecurity has been the newest front in the defense of the homeland.

When it comes to cybersecurity, we often hear nothing but bad news, threats that could cripple a nation's power grid, its air traffic control system, its water supply, and even its massive military could come from a relatively small group of computer literate individuals. But in fact, there are reasons to feel encouraged by the level of innovation going on in the cybersecurity space. For starters, the US is stronger in its offensive capabilities than many people give us credit for. Yet there are soldiers located around the world armed with only bad intentions in minds of computer code trying to hack into our most sensitive systems and bring the US to its knees without firing a single shot. But the good news is, we do have companies and our own tech champions prepared to protect critical infrastructure vital to each and every American.

Joining us today to talk about how America has strengthened and developed its cyber defense capabilities is John Cofrancesco, who currently serves as vice president for Fortress Information Security, a firm headquartered in Orlando, Florida, and specializing in cyber defense.

John Cofrancesco, welcome to the Homeland Preparedness News podcast.

John Cofrancesco: *Hey, Jim, thank you so much for having me. I'm really looking forward to the conversation today.*

Jim Murtha: *You're welcome. Before we get started on the substance of our conversation, John, how about explaining your background in information security and your role at Fortress?*

John Cofrancesco: *Yeah, well, I started my career with the United States Navy, as a civilian, I worked for what I think is one of the coolest parts of the Navy, Military Sealift Command that so those are the not the US's ships, but the US NS ships, the ones that are manned by the civilians, they do all the really exciting stuff, like replenishing, replenishing the carriers, refueling, you know, various weapon systems. So that's where I started my career, I worked my way through a number of well-known companies in the defense industry before getting an entrepreneurship. But my focus has always been on regulated spaces. So spaces that are really at the edge of where policies and technology meet. So, I've spent a good deal on really my whole career doing that. Here at Fortress, I'm responsible for developing our business, but also the technologies overseeing how we deploy technologies to the federal and then defense industrial base spaces around cyber supply chain security. So, I enjoy both the business development side and the actual delivery side of our business there.*

Jim Murtha: *In my preamble, I tried to paint kind of a grim picture of the vulnerabilities facing our country from cyber threats. You recently wrote about some of the dangers facing the country just before the I believe it's called the log4J happened.*

John Cofrancesco: *You can call it log4J, you also call it log jam. That's the next log jam.*

Jim Murtha: *Let's call it log jam then, apparently you knew about that was going to happen and it's going to happen again, what should we be doing industry and as a country to prevent those things from happening again?*

John Cofrancesco: *You know, that's all I couldn't say that log4J was going to be the vulnerability but certainly, I knew that some type of vulnerability like that was going to come to fruition. And I knew that because the incentive structure behind software development today is so incompatible with security that it was it was just easy to see it didn't have to be a fortune teller to do that. I can put some detail around that Jim. So, your average company is trying to put out software as fast as they can. Because they got to beat the market, right? They want to they want their competitors. They want it to be really good. They also need to keep costs down, and sure is where we get into trouble. So, you can have fast, and you can have good but you can't have secure at the same time. So, we have a situation where the most important pieces of software that are going into things like our weapon systems that are going into grandma's, you know, heart monitor, that are going into our food supply systems, they are pulling components from public sources. And those public sources really aren't checked and reviewed.*

So, our adversaries, folks that really hate the American way of life, they're able to just put all sorts of poisons, or because they are diligent, they accidentally create vulnerabilities that are then introduced to all the things that we depend on.

Jim Murtha: *For our some of our listeners aren't familiar with log jam. What exactly happened there?*

John Cofrancesco: *Yeah, so this is one of these times where a vulnerability wasn't nefarious. So, everybody's using software for everything right from your phone, to your medicine, everything in between. Yep. And one of the things that becomes really important is the human machine interface. Right. So how the human interacts with the software. So log4Jis a really common component. Think about it, like the salt in the cookies that you made, but also the salt in the cold cuts on your sandwich, and also the salt on your table. So, this is a really common component that goes into just about every piece of software that has a human wish.*

Jim Murtha: *Would you see it on in your phone?*

John Cofrancesco: *Yeah, absolutely. You can see it on your phone, you see it on websites, it definitely web-based applications are going to have it more frequently that so it was just a very ubiquitous component, a very ubiquitous ingredient, if you will, and that ingredient happened to have a really, really big weakness, a weakness that you didn't have to be very sophisticated to take advantage of. And if you did, it would give you tons of exposure to somebody network.*

Jim Murtha: *Wow. Did it wreak a lot of havoc?*

John Cofrancesco: *You know, so this is one of the tricky things in cybersecurity, I can tell you candidly, it has wreaked a lot of havoc, but you know, nobody wants embarrassment, right? Nobody wants to, you know, raise their hand and say, Oh, I was the one that they got hacked. Right. That's so although we know that a number of companies, some big companies were breached through this vulnerability. We also know that there were a lot more vulnerabilities that folks didn't disclose. And some very public sources have talked about the number of attempted hacks that, you know, organizations from China and Russia and other adversarial countries have been using that, basically taking advantage of this vulnerability.*

Jim Murtha: *Okay, well, let's move on to defense, then. I think for the average person, you think, well, our government is our first line of defense in the cyber-attacks. If that, so how well is it equipped to handle the job?*

John Cofrancesco: *Well, you know, I think I think, Jim, that's a little bit of a misnomer. And you know, the government isn't the first line of defense. And this is where things get tricky. The first line of defense is the company with whom you're working yourself being smart about having good passwords and things like that. If it gets to the point where the government's doing it, it's really gotten to the point where you're, you've probably already lost the game. And unfortunately, in the defense arena, where government is, is, in fact, the first line of defense, right? In a lot of respects, we're just behind. We are far more exposed than our near peer nations the China's and Russia's the world. And we have not for the economic reasons I mentioned earlier, invested the appropriate amount of money and regulations to ensure security. So, we're in a tough spot, and we're working to fix it.*

Jim Murtha: *Well, I don't know if that makes me feel any better to be honest with you. I guess. I think most people think that government can be somewhat omnipotent in these spaces, and you're telling me*

that it is not. So, let's suppose that you were given carte blanche to implement any safeguards against a major cyber-attack. With budget being no restriction whatsoever, what would you do?

John Cofrancesco: *You know, if I lived in that world, I would take measures that matched the economic outcomes of failure that so if you actually look at the energy production field, right, so there's big power plants that make our electricity? Sure, they have a pretty stringent I would argue, perhaps the most stringent regulatory environment for cybersecurity. You know, electricity is really important. I don't want Russia turning off the lights. But you know,what's every bit as important as lights? Water. I really like to have fresh water in my house. I love turning on the tap and washing my hands. It feels great when I take a shower. I'm sure you like that, too. I do. The water industry doesn't have anything near the level of sophistication when it comes to cyber regulations as power does that. So that's an area where I'd say hey, you're gonna adopt the electric standard, and there are some other industries like oil and gas, healthcare, that I would probably move the bar up I would raise the bar. Now you can never get rid of all the all the risk, you can never get rid of all the vulnerability.*

But you know, cyber-attacks are really economic game. That's the cyber attackers, they like cyber weapons, because they're inexpensive. So, we can make it more expensive for them to have successful attacks, we'll have fewer cyber-attacks. So, I picked those industries where the economic outcomes were just too important, I'd raised the bar. And then for the rest of the country, you know, I encourage the regulations to make sure that asset providers to those folks that are making your software making your hardware that they're building in more securities, you know, there is no, no-risk world, but we can be measured, and we can absolutely raise the bar, would it be fair to say that a lot of industries are just sitting back and waiting for the worst to happen? They're doing the minimum, to protect themselves? And they're, they're saying, Wow, my industry is not that high profile. We don't think it's all that important. They're not doing enough to protect themselves.

You know, I had a lot of industries fall in that category. But you know, that I do, but for a really specific reason. Actually, this is a conversation I was having with a really, really smart young man who's joining our company. And he has an economics background. And I asked him, I said, you know, who is in charge of cyber security to company. And, you know, like most college grads doing well, it's probably the CIO or the CTO or and then he went and did some research and said, Well, what about this CIS Oh, guy, right? This chief information security officer, surely, that person is in charge of security? And I laughed at him? Because the answer is no. Right? The person who's really responsible for security companies, the CFO, it's a financial question, right. And so you have really, really smart and talented security professionals in just about every major industry in this country. And they are tax limited by what they're allowed to spend. Now, that isn't to say that you should spend infinite on security.

But Jim, I think you're on the money here. Most industries are ducking this because they don't want to absorb the cost. And that's sort of what I think needs to change at a regulatory level.

Jim Murtha: *We were speaking earlier, I'd remarked that, you know, almost all the stuff that's involved in this in cyber war warfare. The software, the hardware was all created here in the United States, with some exceptions, but it all began here. It was created here with the Bill Gates's, the Steve Jobs and all those people created all this stuff. Now, knowing that I think the average American is asking to*

themselves, well, if they're doing it to us, can we do it to them? So the question to you is, Can we? And are we?

John Cofrancesco: *Well, it is definitely the case that we have in the United States, the most advanced offensive cyber capabilities of any country on Earth. And there are a handful of other countries, China, Russia, Iran, Israel, you know, other partner countries like Germany that have some pretty sophisticated capabilities, but we are also the most exposed country on earth. You see, if we turn the lights off in Moscow, Vladimir Putin doesn't care. Because his people, they don't get to vote. They're not really citizens. But here in the United States, if the power goes out, it's a huge deal. This is a democracy. We're an open society. So that wonderful, that powerful offensive capability does something for us. But it's an asymmetrical vulnerability. We're way more exposed. And it's actually our lack of defense. That is the bigger issue. So yes, Jim, we absolutely do things. But that's not really where the heart of the value the heart of the issue is. So I guess then we are doing things overseas. But because we're probably doing to them to autocratic societies that are run by a relatively small group of people. We just don't hear about it. Yeah, absolutely. I mean, and even when we do hear about it, it just doesn't change what's going on in that country. Right. They just continue on the path. I mean, Iran is a great example. Nobody officially knows who released the Stuxnet attack on the Iranian centrifuges that were building their nuclear weapons.*

Almost certainly, it was us, maybe with the help of the Israelis and the Germans, but we certainly had a hand in it. But did the average Iranian know about that? No. Even now, does the average Iranian know about it? No. And are they still on track to build nuclear weapons or fissile material? Absolutely. Because in those types of societies, cyber-attacks just don't have the same bearing, as as they do here. Because, again, those people may legally be citizens in the international sense, but in the sort of moral sense, they're not citizens, they don't vote they don't have to say, and that's the only open societies that these cyber-attacks really land heavy, heavy punch.

Jim Murtha*: Your company Fortress Information Security is currently doing some cutting-edge protection of the DoD. In as much as you can tell me what you're doing. What are you doing?*

John Cofrancesco: *So Jim, you made a really interesting comment earlier about, you know, we created all this stuff, and then maybe it's coming back to haunt us a little bit. It's true, we did create the stuff but actually the majority of the things that are being created today, manufactured today, are not being manufactured the United States, even our weapon systems. Now we're permeated with components, think of microchips and pieces of software that come from China and Russia and other countries that we don't want them to come from. So, what we're doing is working to DOD to help them to identify where that has happened. So, they can throw out the junk so they can remove the poison out of the systems. And it's worked, we're really proud of that.*

Jim Murtha*: And we put a lot of effort into in advance in doing prep work for this podcast, I did some reading. And I just assumed that we were getting attacked. And I use that term very broadly, you know, every day. And I found out that that is not only true, but it's happening like 10s of 1000s of times a day, is that really true?*

John Cofrancesco: *Even 10s of 1000s might be a low number. We're under continuous and ongoing attack. Now, let's remember, we talked about that, you know, if you think about international relations, right? If you invade a country, like Russia is preparing to do in the Ukraine, that is a very kinetic thing. It's a physical thing, right? And we can get it I can watch the Russian tanks come across the border, right? That Jim, cyber is different in that in that you can't always attribute who's doing the things. But second to that, you know, if somebody blows up a Russian tank, well, that's one less tank they have, if we managed to defeat a cyber-attack, they can just release an unlimited number of cyber-attacks, right? They just have another server and another server and another server because there isn't a kinetic defense, there's no physical way to stop them, really. So, we're under constant attack. But there's, it's really important to sort of separate out the attacks that are going to change America's way of life, versus the attacks that are sort of more criminal in nature.*

Jim Murtha: *I did a podcast earlier in the year on ransomware. I assume that that kind of falls into the same category that we've been discussing on this podcast, correct?*

John Cofrancesco: *Yeah, absolutely. And ransomware, you know, it's one of those economic attacks. Now, to be clear, state actors sometimes hide their attacks through ransomware. Right, that's they want to make you think it was criminal when really was a state actor. But primarily, that's a money generating operation. So, it's a very sort of different thing than the sort of nightmare scenario of somebody attacking a water system or a power plant. But it's fairly sophisticated, though, in its execution. It isn't, it isn't that so and maybe it's, maybe it's worth detailing this and hopefully, your listeners will appreciate this. So you, when was the last time you downloaded a patch or an update for your phone, Jim?*

Jim Murtha*: It does it automatically, periodically, I get a notice because I have an Apple phone, I get a notice from Apple, that they're going to upgrade the software while I'm sleeping. And then it does it. And then I'm done.*

John Cofrancesco: *Now I am, I am afraid to say I'm not an Apple user, maybe I should be. But for those of us who are on the other side live in the Windows world, you actually have to hit the go button on those patches or those updates. Now, what the bad guys love to do is they love to go through what's called patch notes. So, they actually go through the notes of the new patch. And they see here all the things that that patch just fixed. And then they turn around to all the people, all the companies that didn't hit the patch button, for whatever reason, maybe laziness, and they attack them using known vulnerabilities. So, there are absolutely times for the bad guy sort of create something new. But Jim, most of the time, the attacks are unsophisticated, they find somebody who had a weak password or click the stupid email or didn't patch something when they should and they take advantage of that. That's a that actually makes up the preponderance of what we're seeing here. And then once they're in, well, then they get this great opportunity to take your stuff and then charge you get it back. So, it's a it's definitely a situation that can be remedied in large measure, if people just took pretty standard steps.*

Jim Murtha: *I realize that a lot of our discussion here is theoretical, for a lot of people that might be listening to it. Like, you know, they're sitting here listening. Well, I don't I just can't think of anything. That bad ever happened to me that I know about. Can you think of an example where or an attack*

occurred that an average person would understand or remember that something untoward occurred with a phone or a desktop or, or a public utility or anything like that?

John Cofrancesco: *Yeah, absolutely. I think I think the most famous one that was recent was the Colonial Pipeline. And you know, people were waiting in long gas lines all over the East Coast. It was terrible.*

Jim Murtha: *You know, what was that was ransomware was it?*

John Cofrancesco: *It was, and that was a really interesting attack. And then I can share with you a couple details on it.*

Jim Murtha: *Sure.*

John Cofrancesco: *Most of the time when you think about or what I think about sort of a pipeline attack or a power plant attack. I'm thinking about them attacking the software or the hardware that is physically operating systems. And I think some people mistakenly believe that's what happened there. But in fact, that's not what happened. What really happened is the hackers attacked some of the systems that controlled payment. Think about like when you go to the gas station, right? You see the meter there that so they're able to charge you well write effectively, what the hackers did is they turned off the ability of the pipeline to charge the people taking the fuel out. So, the company had to stop the flow of fuel. They didn't know who was taking what out.*

Jim Murtha: *Really? Oh, yeah, that's because I thought all along, they somehow hacked into the system shut some valves down and prevented the flow of crude from, you know, word originated to where it was gonna go.*

John Cofrancesco: *No, there was definitely concerns about that. I think like, like every like you, most people thought that but in fact, the OT network, the operational network had had remained pretty safe. It was actually the IT network that overlay basically the payment system that they were that they were effective in attacking. And that is the tricky thing here. Because the bad guys, they don't have to win every time, they only have to win occasionally, to have a really, really impactful result. Now obviously, that's sort of the great fear of everybody who works in our industry.*

Jim Murtha: *It's been my experience over the years that the regulated are always two step steps ahead of the regulators, for example, and you're probably intimately familiar with this, because you testified in Congress, Congress is working on a bipartisan bill that will attempt to shore up our defenses against cyber-attacks. My question is, given the length of the legislative process, and how things can get watered down, will the bills currently under consideration be obsolete by the time and if they are signed into law by the President?*

John Cofrancesco: *Well, that depends largely on what they pass. Right? So if they pass us, if they if they pass a static bill that says, hey, you're going to do XY and Z, yeah, the adversaries will overcome that quickly. But if they pass a bill, and this is what we're angling for, that continually raises the bar, it'll*

give us a real opportunity to change the economics of cyber-attacks, right, it'll give us an opportunity to just continually stay one step ahead. And there have been some really great leaders on both parties, both sides that have stepped up to do this, you know freshmen congressmen like Scott Franklin, have been stepping up. Stephanie Murphy, also from Florida, has really gone to bat on this issue. So, there's a number of folks both sides of the aisle that have worked really hard to see this come to fruition.

***Jim Murtha**: Okay, I'm gonna get you out here on this, I always like to ask my guests to look ahead. And you're I'm sure that there are there is probably tons of things that you can't tell me. But I'm asking you in the nights that you can't sleep and you're worried about work. What are those kinds of things that keep you up at night?*

***John Cofrancesco:** You know, I think the big thing that that keeps me up, you know, with regards to my field, is that, for silly reasons, we're gonna pass up an opportunity to stay out in front America, we really have something special. We're not perfect, but we really do have something special here. And if we let the political bickering get in the way of us defending ourselves, we're gonna find ourselves with less freedom. Right? And you see this on Facebook, you see this in our systems that the bad guys are taking advantage of us. That doesn't have to be the case. today. It is the case. And I'm hopeful that we'll overcome it, but it is definitely my fear that that will let sort of silly domestic politics get in the way of doing it.*

***Jim Murtha:** Okay. Well, that's all the time we have for today's program, John Cofrancesco of Fortress Information Security. Thank you for a really interesting and somewhat sobering discussion.*

***John Cofrancesco:** My pleasure, Jim, and I'm grateful for the opportunity, cheers.*

***Jim Murtha:** The previous podcast was sponsored by Fortress Information Security. Fortress offers the only comprehensive cybersecurity solution for your entire supply chain. That strength combined with fortresses operation vulnerability solutions, and your organization is protected from a full spectrum of cybersecurity risks. To learn more, just go to www dot fortress infosec.com. The preceding podcast was a production of Macallan Communications publishers of Homeland Preparedness News. If you have a topic for a future program, just go to www dot homeland prep news.com. Look for the podcast section on the front page.*

Until next time, I'm your host Jim Murtha. Be well be safe, and be prosperous.

#