DEI - Fortress Information Security - NAESAD - SBOM – https://www.fortressinfosec.com/home

FINAL *Transcript

April 12, 2023

Murtha: *The following podcast is sponsored by Fortress Information Security. Fortress secures North America's power and defense supply chains from cyber-attacks on operational and critical enterprise technologies.*

The program is produced by Macallan Communications publishers of the Daily Energy Insider. DEI is your source for the latest on US policy and regulation news that is helping to shape an evolving energy sector. DEI can be found on the web at WWW dot daily energy insider.com

And welcome to the Daily Energy Insider podcast. I am your host, Jim Murtha. America's public utilities are an essential part of the nation's economic backbone. They supply the power that underwrites a $22 trillion economy. We take them for granted because for the most part, they operate almost anonymously. We don't notice them until well, the lights go out. But just because most of us pay them no heed doesn't mean they aren't attracting attention. Each day, maybe hundreds of times. The computer systems that run power plants are under attack, not physically. Although vandalism of power plant infrastructure is on the rise, but by a kind of cyber terrorism whose purpose is to damage or even shut down a public utility. And along with it the homes and businesses that rely on the power they generate.

This insidious practice is known as hacking among computer professionals. And the practitioners known as hackers come in a variety of backgrounds. From the lonely soul type who was looking for a personal thrill to foreign state sponsored teams, some from China and Russia, looking to inflict serious damage on an adversary. But no matter where the attacks come from, they keep coming, relentlessly.

While the defensive challenges are considerable, the nation's utilities are not standing idly by. Many of them have partnered with Fortress Information Security to protect their systems. Fortress, based in Orlando, Florida are the creators of the Asset to Vendor Network, which helps utilities protect their IT systems from threats that might arise from the network of subcontractors, who helped keep the utilities online and running efficiently.

In February, Fortress launched the North American energy Software Assurance database. NAYSAD, as it's called, is in the embryonic stages of forming a consortium of public utilities who will share information about software they use. This collective sharing is known as the Software Bills of Materials. Under this program, utilities can identify and triage the most troublesome risks to their IT systems and deal with them before major impactful damage can occur.

To help us understand how all this works. We've invited the CEO of Fortress Information Security, Alex Santos, to explain how his company maintains a post at the front in the battle against hackers, malware and ransomware.

Alex Santos welcome to the Daily Energy Insider podcast.

Santos: Thank you, Jim. It's great to be here.

Murtha: *Before we get into the heart of our discussion, tell our audience a bit about your company, Fortress Information Security, what you do, and how you interact with the nation's electric utilities.*

Santos: Jim fortress is a cyber supply chain, risk management company. So, what we do is we vet your supply chain. And we vet your vendors, we vet the products and services that they provide. And we really help the business use the vetting that we do to increase the resilience of the grid. 90% of our customers come from the power industry. And Fortress is a company that is an expert and specializes in the particular facts, circumstances, vendors and products that our industry uses.

Murtha: *Okay, since cyber terrorism, cyber-attacks are in your wheelhouse. I want to talk about that a little bit, for the most part, and I'm a civilian, obviously, in this particular industry. I know a little bit about it, but not a lot. But it's my impression that most of the cyber-attacks are anonymous, you don't hear about them. But occasionally occasionally, you hear about a few. And I'm speaking of the Solar Winds hack, in which more than 30,000 public and private organizations, including all levels of government, had their data and networks and systems compromised. And then probably more famously, was the Colonial Pipeline ransomware hack that basically shut down fuel deliveries to the east coast of the United States. And both of these hacks were extremely damaging. But the public rarely hears about all the other so it from where you sit as an expert in this industry. Just how bad is it out there?*

Santos: Let me start with the positive side. Though the positive is that the power industry, I think it's not just my opinion, but an opinion shared by many other smarter people than me is that the two leading industries in America with respect to cybersecurity are finance and power. Particularly, the publicly traded larger investor-owned utilities have large, talented, hard-working teams that are doing a great job of preventing and detecting cyber-attacks.
So let's talk about the bad news. Now, the bad news is, is that our society, but let's double click on power, our industry is experiencing technological change never seen before.
In terms of its pace, its depth, its consequences. All these technologies, improve our life, improve our industry, they improve our revenue, and they reduce our costs.

But all these fancy technologies come with a cost, which is cyber risk. And human nature is that whether it's an opportunistic, organized criminal, or a nation state adversary, is going to use whatever they can to perpetrate their crime or their mission. And it's so just so happens that in our rush to get some of these technologies deployed, we haven't hardened the technologies to the extent to keep out the organized criminals in the nation states, which is a great example of, you know, I think you brought up Solar Winds and Colonial right, but I did a good example of an organized crime type of situation. And Solar Winds is a good example of a nation state. I think our country is attributing Solar Winds to Russia.

And so those attacks, they both alerted the public as to the danger. But they're also dramatically, they have dramatically different sophistication levels, which really reflects who perpetrated those crimes. And I can go into that if you think your audience would be interested. But those are two crimes that I think highlight the risk going forward. And I think some of the difficulty people have in truly understanding the scope of the problem is that when we talk about this, you know, we're talking, you know, the whole American public utility industry, the banking system and whatnot.

***Murtha**: Let's boil it down to I'm in suburban Philadelphia, my electric provider is PECO. Now, it's an average utility. I mean, it's a big utility, but it's nothing too dissimilar than you could find any other place in the country. What would a utility like PECO face on a daily basis in a way of hacks or, or whatever to try to upset its IT system?*

Santos: So let's talk about organized crime first, okay. So you're trying to make money, organized crime is trying to make money. And the most, the most common way they try to make money is ransomware. And ransomware, is think of it as a product that they buy, like the criminal will actually buy a product from another criminal. So, the criminal let's say, the criminal has 30 people working for them. They used to, this is Philadelphia, you said.

***Murtha:** Right.*

Santos: So yes, probably a great work is crime thing, right? So, in the old days, they would, they would do gambling, but now they're doing cyber-crimes. So, the same 30 guys that used to kind of, you know, do loan sharking are now doing cyber-crimes. But those guys aren't software developers, right? So, they're buying the software to do the ransomware from, you know, some it developer that came up with the software, and then they're deploying it to try to make money, right. So, it's almost that's why they call it ransomware as a service, And that's, that's an example of what happened to Colonial and most commonly, they're trying to take advantage of a human clicking on something that they shouldn't click. And then from there, the software that the that the ransomware game developed and sold to the organized criminal. Well then, on an automated basis, we'll try to jump from one come either to next, and do as much damage as possible.

Typically, it's encrypting computers. And that will lead to lead to a ransom. And if they get the right computers, the reason you don't hear about it very often is if they get like, Mike, let's say, they get our computer, right. And we're the, we're the CEO, or maybe we're working in the accounting department, right, it's not going to disrupt day to day, our delivery operations, we don't hear about it. But every once in a while, they get lucky. And they fish the right person, and it ends up shutting down the billing system, or it gets in, it gets into a SIP environment. And once it gets into a SIP environment, then you're gonna see the security department shutting everything down, disconnecting everything, think of it, they're gonna, like, disconnect everything, and then ask questions later, right? Because they don't want it to spread, right?

So, you know, I once was told by utility, because I was talking to a utility about some vulnerabilities that their server had, right, so they had the server that had vulnerabilities and vulnerabilities can be hard to, to address, right, because you have to patch them. And in order to patch a vulnerability, you got to bring that server down. And power companies don't like doing that sometimes, because that may affect power delivery.

So the common workaround, or a common solution to that is to install a firewall around that server. And that will keep the bad guys from using that vulnerability. So, I asked the question, I said, Well, what if you what if you ask, What if you unplug the firewall? And, and you forget to plug it back in? Or let's say you reboot the firewall, and it's down for three minutes? Their answer was astonishing. But it really is educational. They found that it takes less than three minutes for the adversary to exploit a vulnerability that isn't protected by a firewall. Wow. Think about that.

Murtha: *That's pretty fast.*

Santos: So I think what that Yeah, and I think what that really if you kind of think about that, you know, you always hear in the news about, you know, you'll hear JP Morgan, say our company is attacked 10 billion times per day, you sort of scratch your head, and you're like, how

does that even possible? Well, what's happening really is you have these organized criminals, it could be it could also be nation states. But you have all these people using the cloud to automate these attacks. And as soon as companies leave something like a window open, the firewall unplugged. It's it's software that's doing the hacking, it's not a human. So that's why it takes a couple minutes, because all your servers are constantly being surveilled and examined by bad guys.
Now what, what how that comes out in the media, as you'll hear our company is attacked and daily, millions of times per day. That's what that's kind of like taking that media story and bringing it out.

Murtha: *You said millions.*

Santos: If you Google that, right, you'll see different companies that will say we're being attacked millions of times per day, billions of times per day, because it's kind of misleading, right? It's software that the bad guys have deployed, that is automatically scanning companies looking for a way in. So, in a sense, it's correct. But in a sense, it's also misleading. It's not like you have a human doing a million attacks. Yeah.

Murtha: *But I guess technically a hack is a hack, no matter the source, whether it's a human or software.*

Santos: That's my point, right, that's how good they are. I guess that's how effective they are at their jobs is that they, they've made it automated, like if we, if you and I were going to go rob cars in a parking lot, we'd have to go car by car to see which one is open. Right? That would take us more than three minutes to do a mall. Right. But the bad guys can do that. In you know, they can do the whole world in three minutes, I guess is my point. Right? And that's, that's kind of what we're up against. And that I would say it's kind of the organized crime way of doing things. The nation states are a little bit more sophisticated, although they could also try to get a foothold in, in a way like that as well.

Murtha: *All right, well, let's um, I think we have a handle on the scope of the problem. Let's let's talk about now about what we're going to do about it. Recently, the White House released a National Cybersecurity strategy that lays out goals to help private industry and government combat these cyber-attacks. Inside the strategy, there's five pillars of interests that will guide our efforts to keep our IT systems safe. The goals broadly encompass investment, counter attacks and international partnerships to fight off these assaults.*

Now, however, laudatory the White House effort may be, government inertia and bureaucratic speed bumps can sap the energy even out of even the most promising initiatives? Given that our

system of government makes it really hard to implement change? How confident are you that the White House plan can be put in place in time to make a difference?

Santos: Jim, I couldn't have said it better myself. And I'm on the record of saying just that. It's a great strategy. It's been a long time coming. But the implementation approach involving over 30 agencies is going to take 10 years or longer, and we have we don't have that kind of time.
So I think they need to need to find a faster way of implementing these things. Maybe less consensus and more centralization. In order to get some of these things done quicker. While speaking you that in in owing to what we just agreed on that government is really slow to change.

Murtha: *Does the country really need the federal government to steer the effort? Or is a private sector best position to do things that matter?*

Santos: Ah, this is the tricky question, correct?

Murtha: *It is. Yes, sir.*

Santos: Yes. So, let me give you some background. I am an entrepreneur for 20 years, I am a staunch capitalist brought my kids up that way. In my last entrepreneurial endeavor, my partner and I started a company that recovered $90 billion for the taxpayer, because of subprime mortgages, right. And, and, and the reason they're mean, now with SVB, right, we all kind of remember 2008, especially, guys, my age, Jim.

But in 2008, if you remember, we all learned about mortgage-backed securities and how, you know, we'd learned about stated income loans and stated asset loans. Remember those terms?

Murtha: *Sure. CDOs.*

Santos: CTOs, CDO squared, we could go on and on right bops swaps. So what happened there is even the a capitalist would say that capitalism was unbridled, and got out of control. And so I think history shows us that there is a place for regulation to keep, you know, capitalism on some guardrails. And I'm not saying that what the regulation we got was perfect. We got the Dodd Frank, and that certainly has affected the mortgage market, positively and negatively. So, no regulation is perfect. But absent that regulation, we could have easily seen a repeat of the financial crisis right. Now, if we look at if we look at the President's cyber strategy, you know, I think I think the President is correct, that, you know, cyber is a cost center. And I can tell you, as a CEO of a cybersecurity vendor, it's difficult. It's not impossible, but it's very difficult to demonstrate the return on investment of security investments, you have to connect the

investment to an increase in resilience, a decrease in downtime. And you have to sort of convince people at in Philadelphia, that are PECO subscribers, how does this affect me, and that's not always easy.

We do work for the DOD. And so we have to convince F 35 pilots, why we need to secure the F 35. Right, because what they're concerned about is when they push the button, the missile goes off. And so given that it's a cost center, given that the ROI is difficult, but given the consequences of inaction, I think some regulations are in order. And that's why I think the President's cyber strategy is sound, I think it strikes a good balance. I will say, however, that not all sectors are created equal. I think finance and power are clear leaders in cybersecurity. I don't think it's a point. I don't think it's a coincidence that those sectors are regulated from a cybersecurity perspective through narc and through various financial regulators, including the OCC.
So, you know, with all that being said, I, you know, I think I have credibility in the matter because I'm a capitalist and entrepreneur and a successful business-person. But I think in this case, additional regulatory scrutiny is required because capitalism is not going to directly encourage some of these investments that need to be made.

Murtha: *We have heard a lot about supply chains recently in the last year and a half or so just getting goods from ports to where they're distributed, and then ultimately to retailers. But there's also a cybersecurity supply chain. Can you talk a little bit about what those are and how that fits into work that your company does?*

Santos: Great question, Jim. So, it used to be that a developer, software developer, a programmer, they would program, they would code, they would write on a keyboard, the software that they were that they were building, that doesn't happen anymore, software now is assembled. It's more like a Lego set than it is something you do from scratch, right? Something that you built from scratch. And we refer to those in the cyber supply chain, there's individual Lego pieces as components, you know, so imagine you're building a sock, you're building a piece of software, let's say you're building a website for your podcast. And you want your listeners to register and create an account.

You know, that feature that allows your visitors to register and create an account that's been that's code has been written 1000s, maybe even a million times? And so why would you spend your time writing that again, in fact, you'll learn that that's readily available as an open-source component that you just like, click on it and drag it into your software. It's like click and drag. So you see, it's not as it's not programmed, it's more like, click and drag, click and drag. That's how you build software now, and you're dragging software components, many of which are open source. And, you know, in case your listeners don't know what open source is, that means that it's a publicly available piece of software that anyone in the public can contribute to.

Right, so you and I could go to an open-source repository, apply to be applied to make a change to the code, and going through a process, we can make a change to that code. And now that's part of a publicly available piece of software. And there's minimal if no, minimal if any vetting of your main gem, right we could write, and nothing stops us from being Chinese or Russian agents, by the way.

Okay. So, we took, a look at some of the software that our power grid is using. And we found that, on average, there are over 500 components in the software. So, we just went over one example you and I Jim, right, which is the account creation and login, we found over 500 components. Of those 500, we found that roughly a third were open-source components. And of the open-source components, we found that Russian and Chinese citizens contributed software on over 75% of those components. So, it goes to show you how software development has changed. And in the opportunity that our adversaries have almost unfettered to affect our software supply chain.

What our company does is we do the hard work, the detailed work, of deconstructing the software and examining each individual component to understand where it came from and in whether or not it's vulnerable.

Murtha: *Okay, well, speaking of software, the National Cybersecurity strategy specifically outlined the need for Software Bills of Material for every critical infrastructure vendor and product. Can you explain what that is? What is an SBOM? And how does it work?*

Santos: Sure, as SBOM is software, build materials, just a list of what's in the software. You know, if you if the power industry, or let's say the buyer of software, they call it consumer, but the consumer of software, I like to use the word buyer it sounds makes more sense to me at least, that when if the buyer of software has to hire Fortress to deconstruct the software, it's cost prohibitive for us to you know, even using automated methods. It's very expensive for us to sit there and deconstruct the software, identify vulnerabilities and then and then even figure out if the vulnerabilities meaning mean anything just because they're a vulnerability doesn't mean that the bad guys can use them.

That would add tremendous cost and friction to the to the transaction of buying software to the purchase of software. So SBOM are a way to exchange that information, much easier, much more easily, much more inexpensively, quicker. So, it's a list of software components that a manufacturer can provide to a buyer or a seller to a buyer. That sort of warns warranties probably the wrong word but communicates to the buyer.

What is in the software, a lot of people use the metaphor of it's a, a nutrition label, right? Because when you buy a Twinkie, it tells you what is the card was the protein, what is the fat? What are the ingredients, let people make that that metaphor, and then allows the consumer to sort of determine for themselves, if they should buy that software, how they should deploy that software, they should eat the Twinkie, etc, that's, that's essentially an SBOM. Well, when you put it that way, it makes it a heck of a lot easier to understand.

Murtha: *Your company is putting SBOMs to use innovatively launching with several large energy companies. And you can mention those in your answer. You're launching the North American Energy Software Assurance database or NAYSAD. Explain what that is and how it makes our energy producing industries better able to ward off cyber threats.*

Santos: NAYSAD is a collaboration between Fortress, American Electric Power, NYSOURCE, and in several other utilities to produce a central repository, a central clearinghouse for SBOMs. So, let's imagine if we don't do this, okay, and then they settle make more sense. So, if every supplier needs to evaluate the software, they're buying vis a vis the SBOM that means that, you know, we have roughly by my count, roughly 2000 utilities in our country, that's 2000 utility. And let's say they're each buying, you know, 100 pieces of critical software.

What is that 2 million requests across maybe 1000 vendors, so there's so much duplication, you have all these utilities, making the same exact request to the same exact vendors, it's a lot of duplication of effort, it's a lot of wasted effort wasted by both the utility and the manufacturer responses requests. And you're always gonna get inconsistent results, some utilities will do more with the information than others, some consumers of the information will have a higher quality interpretation than others. And so, you get a lot of inconsistencies.

Also, a waste is also a waste, because you'll have irrational economic behavior happening, for example, you know, those that are uninformed by software, they shouldn't. And, and similarly, those that are uninformed may or may decline to buy software that they should. And so, what we're trying to do is centralize all of that, right. So instead of each individual utility going to each individual vendor, and asking for the information, both parties will, the manufacturer will supply SBOMs to NAYSAD. And then the utility companies will subscribe to the NAYSAD database to get the information pulled from them. And what's really important is we're not just going to pass along the SBOM, we're going to enrich it, we're through our analysis, okay, in our analysis is super important. And if we do the analysis once, it's also going to save a tremendous amount of time and money.

Let me give you a sense of that. So our work thus far has, has shown that there are a significant number of vulnerabilities that we didn't know about. Once we look at the SBOMs

so many vulnerabilities that I'm not sure that our clients can do much. There's so many vulnerabilities. And I'm not sure that the manufacturers know where to start, because there's so many. So one of the things we do as part of our analysis is we identify which vulnerabilities are the most critical, and which ones are exploitable.

And so, we try to prioritize the work and then we collaborate with the manufacturer and the asset owner to make sure our analysis is sound. But imagine if every, every utility, every consumer of the software, recreated that analysis. We already have a shortage of cybersecurity talent. But imagine the costs complexity and delay that that would cause and so NAYSAD does that once and then shares that best practice with its members but also adds a tremendous value to the manufacturers because they can then prioritize the quality enhancing initiatives that they have for their software. So, I expect it to be a huge benefit for the industry.

Murtha: *Okay, let's stay on SBOMs for a second. In doing the research for our conversation, I noticed that the SBOMs are open source. And to me, that's as well anybody can get good at these things, is that causing some concern amongst the people and organizations that you work with or would like to work with.*

Santos: So let's break it down. So some what I would call forward thinking manufacturers have said that they're going to provide their SBOMS, publicly, let's call those open source.
Others had others, the other way to look at SBOMs is that its intellectual property, it's sensitive information, and I'm only going to share it with those that have a need to know.
In either case, an SBOM in of itself is not extremely valuable or useful to the consumer, it requires interpretation and analysis.

Okay, so to answer your question, that has very little effect on our on our set project, because it's the analysis, the aggregation is, is part of the value, but the bigger part of the value is the analysis of how do we make an SBOM actionable? And what do we do with this as well? So let's see that your value added, that's your value, right?

Murtha: *Correct.*

Santos: Okay, so I'll give you a couple examples. So, if you are, let's say you pointed out to Colonial and Solar Winds, you didn't say anything about law enforcement. But you, probably your listeners are probably heard about that. So, let's look at it this way. So, most security teams came into work that morning. And their goal that day was to keep working on their day jobs. And their day jobs have, you know, have an element to a routine amount of tasks. And then there's this element of projects, the projects are what we have to get done this year. So, I can so our department can reach its goals, right? And so, I can get my bonus, everything changed that

day, because LOG4J they spent the next four months working on LOG4J and not on anything else.

And what they were, what they were looking for, is to figure out where in the 1000s of pieces of software that their enterprises that their enterprise utilizes, where's the log for? And is it in? Is it exploitable. So, without sponsors, we can reduce that from four months to one month. Since then, of them losing an entire quarter, you're only going to lose a month. So, that's shows you how you know that's what two thirds reduction in time.

And I think we can do better than a month, by the way. So, I'm just giving you a kind of conservative numbers. But that's one practical, real tangible benefit of SBOMs. Another tangible benefit is let's say you have a piece of grid software that's installed. And you have a bone, you know, under the CIP standards, you have to manage vulnerabilities of those assets. And specifically, you have to patch you have to apply any patches within 75 days they become available, we may learn of vulnerable vulnerabilities that those assets have through the SBOM process.
And that's a good thing, because it's better that we learned about it before Russia and China do. And once we learn about the vulnerability, we can then go and ask the manufacturer to patch it, which we can then apply and prevent a cyber-attack. Those are two like real world applications of SBOMS.

Murtha: *My impression over the years as a consumer of the public utilities product, I always thought that they kind of just existed in their own little franchises that the state regulatory agencies give them. And it seems to me like you're putting together an effort to get them to band together. What happens if they don't?*

Santos: If they don't band together? I think that you know, our slogan is better, faster, cheaper. So, I think it'll be slower, not as good and more expensive. And that's going to get passed along to ratepayers. And eventually, someone will notice that because I know that there's bigger expenses flowing through rape cases. But eventually someone noticed it I think speed is probably potentially one of the key areas. Because they may experience a cyber-attack that maybe their colleagues or their neighboring utility did not.

To give an example of speed is, you know, what NAYSAD will do is, if you think about the speed at which software is published, that's the speed of which we need to analyze the SBOM and prescribe any, any kind of fixes or remediations, that the President cyber strategy refers to real time, cyber protection. So, imagine, you know, you have companies like, I realize, I understand completely, that Facebook is not really relevant. But I'm bringing them up because they publish changes to their software multiple times per day, okay. And every time they publish new software, that's a new one that has to be analyzed, that has to be triaged. And so if that's not

fully automated, you're not going to be acting in real time. Remember, we talked about how the bad guys, it takes them three minutes to find the hole?

So, if you're not moving at real time, speed, you're at a disadvantage. And that's why the President mentioned that. Right. Okay. But that's, that's Facebook, but there's other technologies that are getting published. I use that to make a point, right, you know, grid technologies are not getting patched every, you know, maybe once a month that, you know, for certain systems, like maybe the operating systems and things like that.
But you can see where I'm going with that, that the speed at which this information is collected, processed, and then actioned is a competitive difference. It's a defense against an adversary who's trying to leverage the information arbitrage the information, think of its vulnerabilities are an information arbitrage. You know because vulnerabilities are public. They're public because we want everyone to know about them so they can patch them. The side effect of that is that a bad guys know about them, too. So it's a race, it's a race to see, can you patch it before they can use it against you? And so I think that's probably the main consequence of someone not collaborating on this is speed, because I think cost and quality is harder for the ratepayer to detach, because it's not as expensive as buying solar panels and, and other types of capital equipment.

Another question, Jim would be why wouldn't they? Right? Like, what is it? What is it? There's nothing proprietary about this? You know, utilities don't, don't compete based on who's got the best cybersecurity. It's actually one of the most collaborative industries I've ever been part of. So maybe, maybe that's a you know, I'll just leave it at that as a rhetorical question is, why wouldn't it?

Murtha: *I was gonna finish up with that question. But another one occurred to me during our conversation. And that's artificial intelligence, AI. And everybody has heard about ChatGPT. And I've used it myself, just to see what it was like. And I have to admit, I was impressed. Not completely, I wasn't blown away by it. But it was definitely an impressive item that people can use.*
How do you look at AI? And in how you do business and how you service your customers is making things that much more difficult?

Santos: What's, what's it like out there knowing that AI is right around the corner?
So early in our chat? I think it bears repeating. Because it's important point early in our call. I said all these technologies are making our life better. But they also come with a cyber risk. In ChatGBT is no different.

Like you, Jim, I'm pretty impressed with what they've been able to do fastest growing websites since Tick Tok. Rumor is they're spending $5 million a day in Azure, because their cloud bill is

so expensive. Investors tripping over themselves to invest in this technology, competitors think Facebook said, you know, the hell with the meta thing or whatever, you know, let's focus on AI. They've changed priorities. Right? So, huge, huge impact. But then there's always a cyber risk, right?

You know, like, for example, AI is, you know, at the end of the day, right, at the end of the day, it's garbage in garbage out. And you know, you can see this in chapter 15. Now, go look at you know, whatever your political leaning is go query on politics, and then show it to your who your friend who disagrees with you and you'll see how it's garbage in, garbage out.
or let me use a different term, whatever, it's a font, the outputs are a function of the inputs. And so remember what I said earlier today, earlier as well, the bad people that want to do us harm are going to game the system. So, are there any controls in place to make sure that the information being fed into AI engines is accurate? What controls do we have in place as a society to make sure that the data that the AI is using to do its work is sound accurate?

So that's, that's one of the risks, but I think there's a lot of good that can come out of it. So, you know, for example, we have a lot of data about vendors and products and services that they sell. And we, we spend enormous amounts of money, designing and developing user interfaces that our clients can use to quickly get their arms around a vendor or a product they sell. And we have all sorts of information. It's like, who owns the vendor? What country are they from? Are they controlled, or influenced by one of our adversaries? What are the vulnerabilities what security controls they have in place? The data that we have on vendors and suppliers, who's on
a great application would be you query an AI engine and say, tell me about G's solar panel management system, what do we know about that? And it writes you a paragraph. And you probably did this for charging me to write you a paragraph with everything you needed.
And that's it. That's an example of something good.

But if we ever did that queries rely on the accuracy of that information. It's got to be right, right. So, I think that's the main thing with ChatGBT is just another. It's not just another technology is a great technology. But like all great technologies, it has a little side effect as little cyber risk associated with it.

Murtha: *Okay, well, that's all the time we have for our program. Alex Santos, CEO of Fortress Information Security. Thank you so much for a very interesting discussion.*

Santos: Thank you, Jim. It was a pleasure. I hope you have a great rest of your day.

Murtha: *The preceding podcast was sponsored by Fortress Information Security. Fortress is a company on the frontlines and defending our energy companies against the constant threat to*

their IP systems, and ultimately, power they produce to keep America humming. The program was produced by Macallan Communications publishers of the Daily Energy Insider. You can find DEI on the web at WWW dot daily energy insider.com.

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

- *Transcript was created from a speech-to-text platform. Great effort is placed in identifying and correcting errors that naturally result from the platform's inability to distinguish nuanced pronunciations in a multitude of spoken words. Inevitably, some errors are not caught and corrected but we believe this transcript captures the essence of the conversation.*

DEI