Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Deneen DeFiore. Welcome to the podcast, Deneen.

Deneen DeFiore: Thanks, Brian. I'm glad to be here.

Brian Contos: Deneen, before we get started could you give our listeners a little bit of background about yourself and kind of the path you took in cybersecurity to end up where you are today?

Deneen DeFiore: Sure, so I'm currently the Senior Vice President, Chief Information and Product Security Officer for GE Aviation. In my role, I serve as the technical expert and advisor to a lot of GE senior leaders on all cyber risks related to products, technology, services, and ongoing operations. I have a pretty varied background in technical project management, digital technology, infrastructure technologies, but really focused on cybersecurity for the past eight or nine years.

Deneen DeFiore: I guess I would say I got started in cybersecurity by accident, really. I didn't actually have a plan to be the next CSO for GE aviation. And I really look back at my career path and the way I got here was really just finding kind of the next big opportunity and challenge. And it was during my time as a CIO, actually, in a business unit in GE Energy, that I was really truly exposed to cybersecurity. I experienced several cybersecurity incidents at that time in my role as a CIO. And working through those issues and incidents really opened my eyes to an entire new and emerging aspect of technology that was cybersecurity. And I loved it. It was dynamic. It was fast. You had to make decisions on limited data, and I was hooked. So, I got through that incident and then I decided that this was where my passion was, and I've been in cyber and a CSO ever since.

Deneen DeFiore: Well, I think my work in cybersecurity forces me to continuously evolve. There's of course standards and best practices that we all share within our domain and industry, but there's really no blueprint to follow. Every day is new, and I can
learn and continuously stay challenged. And I think cybersecurity really touches every aspect of technology and every aspect of our business operations, and it's evolving every day. It started out as a very technical IT technology risk, and now it's a business risk. And I love being connected to the business. You know, every time I board a flight, I'm reminded that the work I do really makes real world impact. I protect the purpose of GE Aviation to invent the future of flight, lift people up, and bring them home safely.

Brian Contos: Well, I've got to tell you, for somebody that flies a couple of hundred thousand miles a year like I do, I really thank you for that. And only once have I ever seen the pilot walk to the back with a roll of duct tape, and that kind of made me a little bit nervous.

Deneen DeFiore: Yeah, yeah, yeah.

Brian Contos: So, let's talk a little bit about the aviation sector. And every sector is a little bit different. We've had people on here from military and government, universities, financial, retail, healthcare, et cetera. But aviation's a little bit of a different beast. What are some of the biggest challenges and maybe some of the cyber threats within the aviation sector that you've been dealing with or are somewhat unique to your sector?

Deneen DeFiore: Sure. I think there's of course some common, I say, key risk drivers in aviation that every business is going through. But there's also, like you mentioned, some specific ones as well too. You know, I think the first one is really around digital technologies that are truly reshaping the aviation industries. We're relying more and more on data and software to run the aviation ecosystem. There are solutions that airlines use to use big data that predict maintenance of the aircraft to optimizing how passenger's experience be. So, increasing this dependency on digital operations is really, really driving some more risk within the cyber arena.

Deneen DeFiore: I think there's also expectations from pilot crew and maintenance personnel that they expect data and connections to the aircraft and ancillary systems in different ways than they did before. You know, you think about an electronic flight bag, which is an iPad that the pilot uses to optimize his approach to flying the aircraft. They want data from weather sources, from air traffic control, from their airline operation center at their fingertips. So, they want to be able to have data at their fingertips while operating the aircraft.

Deneen DeFiore: And you think about, too, some of the challenges that we're facing just from an expectation on the passenger side. We're bringing more and more capable devices with stronger computing power onto the aircraft, and people are expecting the same experience that they have around connectivity and being
connected to everything that they would expect on the ground as they do in the air.

Deneen DeFiore: And then when you talked about all those drivers, right? That pace of technology keeps changing rapidly, and the aviation industry isn't used to that. So, to give you some context, when we talk about onboard systems, it can take years just to have one change in one line of code. That's years, right?

Brian Contos: Wow.

Deneen DeFiore: Yeah. So, that results in adversaries having a real asymmetric advantage. It's unfortunate, but it's a reality, and we're working to be able to keep up with that pace of change. But it's a really a different animal that the aviation industry is experiencing right now.

Brian Contos: You mentioned a term earlier, the passenger experience. And I liken it to when I talk to healthcare professionals, especially the health care provider side hospitals and the like, about the patient experience. And every dollar that they spend on cyber is a dollar they're not spending on nurses and doctors and MRI machines and other things to make the patient experience better. Whether it's how long are they having to wait in the lobby, what's the follow-up care, and things like that. How much of a role does that passenger experience play on decisions you're trying to make from a cybersecurity perspective? I'm assuming it's of the highest priority, but I mean, is there a very strict process to make sure that everything we're doing to make us more secure is not having, yeah, a negative impact on our passenger experience.

Deneen DeFiore: Right. So, I think in my world it's really around, I'll say, cyber assurance as it relates to kind of safety and operability, right?

Brian Contos: Sure.

Deneen DeFiore: So, we make jet engines and avionics systems and things like that, so making sure that there's no risk associated with safety critical systems is expected, right? It's part of the airworthiness of the aircraft, right? And I think the airlines and operators are getting to that point where they have that expectation of cyber assurance, just as they would continued airworthiness based on safety. So again, it's a paradigm shift in our industry, but I think it's an expectation and we're treating it just like we would safety. Which is a good thing.

Brian Contos: Yeah. Yeah. I think you're right. And I think it talks to the maturation, not just in our space, but of general non-security people that are assuming that these controls are going to be in place and they're going to be safe, right? They're going to be safe and they're going to be secure.
Deneen DeFiore:  Yep.

Brian Contos:  Yeah.

Deneen DeFiore:  You bet.

Brian Contos:  So, let's drill down a little bit more into GE Aviation itself and some of the top risks that your organization faces. But you know, more importantly, GE Aviation is definitely known for innovation, and maybe some of the innovative strategies that you're using to mitigate those risks.

Deneen DeFiore:  Sure. So, like any other organization, I think some of the top risks are around loss of intellectual property. You know, we still have challenges with asset vulnerability as technology ages and changes and new exploits are found. Keeping up with the pace of technology, emerging technology, right? Our business partners are consuming technology faster than we can secure it in a lot of cases. We have a lot of pressure from legal and regulatory compliance aspects as well, too. Our regulators are responding to what's happening in the world and we are expected to be compliant with their new rules and regulations.

Deneen DeFiore:  But one of the things that I'll take a little bit of a deeper dive in, and I think this is applicable to a lot of organizations, but particularly within GE Aviation, is we're really looking at the risk across the total ecosystem, and that includes our supply chain. And in the aviation industry, it's an ecosystem, right? Our assets are big. They fly, they're mobile, they fly from place to place that have different levels of security. Different components that are manufactured across the different parts of the globe. Maintenance and repair facilities that are across the globe as well, too. So, a very collaborative and inclusive environment, but we all share that risk. So, one of the things that we're trying to do is really look at, "How do we secure that supply chain and ecosystem a little bit differently?"

Deneen DeFiore:  So, we're taking a lot of approaches, right? Not only from assurance of cybersecurity, like everyone does around assessments and risk assignment to suppliers, but we're also looking at cyber assurance as part of the product they deliver to us. So, we're looking at technologies across the board that can really, if we're buying software or chips or some other hardware, right? Looking at technologies that can provide assurance that those products were designed to our specifications from a cyber quality perspective. So that's a little bit different than what I'm seeing some of the organizations take approach to cybersecurity, but it's something that I think will allow us to get ahead of the threat and make sure that we are detecting any presence of compromised software or counterfeited hardware, things like that.

Deneen DeFiore:  So, that's one thing we're doing that I think is a little bit innovative.
Brian Contos: Yeah, no. That's awesome. And, certainly, we've seen some headlines of that counterfeit and nefarious hardware being put in places that it shouldn't be. So, the fact that you're taking those very forward-thinking steps to mitigate that, it shows that the organization has really stepped up and taken the charge of this. That's great to hear. It's really, really fantastic when you hear an organization that large is that forward-thinking. Especially when you compare that to what you said earlier. Sometimes a line of code might take a year to change.

Deneen DeFiore: Yes.

Brian Contos: But you know, you get it, because there's just so many other variables to consider.

Brian Contos: So, let's talk about other CSOs, and whatever their title is, an IT security leader. What are some of the most important things that you'd want to share with them from your perspectives and your lessons learned from being in the trenches?

Deneen DeFiore: Sure. So, I think there's two things that I'll kind of address here, right? One is that we're all fighting the same fight. So, the continued collaboration and sharing of threat information and best practices and what's going on in your environment compared to mine is key. So, I think as we all approach cybersecurity collectively, we can make a better advancement to combating the threat.

Deneen DeFiore: The other thing, too, is thinking about where cybersecurity is in its evolution as a business risk, right? You know, typically the business relationships and business trust was abstracted from technology. But I talked about earlier that today's businesses, particularly in aviation, were being transformed by all these digital technologies. You know, for example, in GE's case, where our customers are relying on us to manage really high value assets like jet engines for optimal performance based on data and digital technologies, so a data breach or a service outage caused by cyber, or maybe even not cyber, really breaks that trust with the customer.

Deneen DeFiore: And when you think about it, the customer's not going to be mad at the firewall rule that failed or the CIS admin that misconfigured a VPC that allowed that that issue to happen, they lose trust in our business, right? So, as a CSO, you need to start thinking about protecting those customer relationships. That means managing cyber risk and technology risk. So, it's really imperative as a CSO that we start acting on that premise versus thinking of it as a technical issue.

Brian Contos: Now, do you feel that senior leaders, and outside of security, outside of IT, senior business leaders, they understand the risks and the impact to the organization, and you're given the resources, and they have the visibility they
need? Is it treated strategically like operations and finance and other key strategic business units within the organization?

Deneen DeFiore: Yeah, absolutely. In GE Aviation particularly, I have complete, I think, support and understanding of cyber security as a risk. It's actually rated in the top business risks. So, I'm integrated into all of our risk management and enterprise risk management processes, and I'm in front of our CEO and senior leaders more often than I probably would like to be.

Deneen DeFiore: But the education around what cyber risks are and the impact to business operations, and really translating those particular issues. Like say, for instance, vulnerability and asset management, right? Translating that to “Okay, if there is an issue on the manufacturing floor that is caused by a vulnerability, there's impact on product quality and on time delivery,” right? Translating those cyber risks into business metrics that they hear every day and they’re accustomed to has really made a difference. So, I've had a lot of support over the years, and we're really strategically managing cybersecurity risk at GE Aviation, which is a good thing.

Brian Contos: That's awesome. It sounds like you're doing what's supposed to be done at this point. And I'm happy to say a lot of organizations, I hear, they might not quite be where you are today, but it sounds like everyone's moving that direction. And maybe a little bit too much time in front of the board, a little bit too much time in front of the rest of the executives, but better than not enough.

Deneen DeFiore: Yeah, yeah.

Deneen DeFiore: I like to have a light glow on me, not a big spotlight.

Brian Contos: That's right. That's right. So, last question as we wrap up here, Deneen. Who is your favorite superhero or super villain, and why?

Deneen DeFiore: You know, what probably resonates with me the most would be Captain Marvel, Carol Danvers. Yeah, she really was, from my perspective, a strong leader, right. And she put her team and mentored other people there to make her impact as a hero. So, I think she has a real strong sense of people and empowerment, not for herself, but for the others around her, and really measures success as a team effort. So that really resonated with me.

Brian Contos: Yeah. Yeah. Well said. And no spoilers here, but if you saw Avengers Endgame, plays a pretty critical role in that. So...

Deneen DeFiore: I did not. Did not.
Brian Contos: Awesome. Well, Deneen, thanks so much for jumping on the podcast, and thanks to all our listeners for joining. And be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.