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 Dave Ockwell-Jenner. Welcome to the Cybersecurity Effectiveness Podcast, Dave.

Dave O-Jenner: Well thanks, Brian. It's great to be here.

Brian Contos: Dave, before we get going, could you give everybody a little bit of background about you and what you do?

Dave O-Jenner: Absolutely, clarify that International Man of Mystery moniker that I seem to have picked up.

Brian Contos: Sure.

Dave O-Jenner: [I'm] Dave Ockwell-Jenner. I manage a team called Storm for a company called SITA. I have about 25 years in the IT industry overall. Probably about the last 12 or so I've been focused really in the information security realm. For my part, I lead a team of security professionals that are dedicated to defending against cyber threats in the air transport industry.

Brian Contos: Well, that sounds like a big job. Let's give everybody kind of an overview of that, because the aviation industry as a whole, that's not something that you hear people talk a lot about in cybersecurity and other areas. We talk a lot about financial services, and health care, and other flavors of critical infrastructure, but we rarely dive into the aviation industry. Maybe you could give us a little background on the aviation industry as a whole and how it's changing.

Dave O-Jenner: Yeah, certainly. For my part, it actually came as quite a shock. I spent a good chunk of my career in the telecommunications and high tech sector. So, coming into the aviation world was quite an eye-opener for me. Certainly, in the time I've spent here -- I've been about 11 years or so within this industry -- it's changed quite a lot. I would say the pace of change is actually fairly incredible for an industry that I think a lot of people would see as being somewhat static or maybe slow. At least from my perspective, I would say that what we see changing is really the nature of the business, just the scale of things.
Dave O-Jenner: The number of passengers is increasing year on year. Somehow we need to move more people more efficiently to more points in the world. I think technology is certainly being seen as the savior, almost, of figuring out: How do we get to that point? How do we move people more efficiently? How do we make the most of what we can with what we have? because we obviously just cannot continue to build more and more and bigger and bigger airports and larger and larger aircrafts. The business model just does not support that. So, how do we leverage technology to make those journeys smarter and more efficient?

Brian Contos: Dave, from my perspective, I travel probably at least 150,000-200,000 miles a year all over the country and all over the world, and oftentimes not just to industrialized countries, but to emerging markets. I've got to tell you -- knock on wood -- very rarely do I have a major, major issue. Sometimes there's delays because of weather, or maintenance, or the flight crew's late, or things like that, or maybe there's a baggage issue here and there, although I rarely ever check baggage. But I've got to tell you, it's been pretty efficient and pretty effective over the last a couple of years.

Brian Contos: There's things I'd love to change. I would love the security lines to be shorter and things like that, but I have to tell you, overall efficiency and effectiveness over the years for somebody like myself that travels a ton, [it's] pretty darn good, pretty impressive for the amount of people and the amount of metal that's moving around up there.

Dave O-Jenner: Yeah. Again, as I said, coming into this industry fresh, I don't think I had any kind of appreciation for just the scale of the mechanism that is moving people around the globe. It truly is, I think, the most global business I can think of outside of the traditional financial services.

Brian Contos: Sure, sure. Tell you what, let's switch gears to cybersecurity now. What are some of the unique security challenges specific to aviation?

Dave O-Jenner: Well, I'm actually going to pick up with the point I just made. It's that global nature. I mean, in most organizations that are dealing with understanding cybersecurity risk and figuring out how to deal with that, you usually have some sort of set of constraints. Maybe you operate in a particular country or a small number of countries. You maybe have one or just a handful of laws and regulations that you need to comply with.

Dave O-Jenner: If you think about the aviation industry, you need to comply with all of them in every country all of the time. That, really, I think is trickling down into the security realm. Somehow you need to provide and understand what kind of capability is required to manage that risk, but doing so on a truly global scale. That involves partnerships both with the airlines themselves, the airports and
the authorities that run those facilities, but also even at the governmental level to make sure that those programs, and those policies, and those capabilities can be effective. I think that’s pretty unique for us.

Brian Contos: Yeah. A lot of people have regulatory mandates and various compliance items that they have to address, but certainly in aviation I can see how that could have a large multiplier because of what you’re doing.

Brian Contos: Let’s dive into the executive side of that. Given the cybersecurity landscape, given what you’re doing, the regulatory landscape, et cetera, how are executives dealing with this today?

Dave O-Jenner: Well, I think executives have had a little bit of a tough time, because the industry has changed quite radically. If we think back to even maybe just 15 or 20 years ago, a lot of the aviation infrastructure was very exotic, I’ll say, so somewhat custom or proprietary. In that time that industry has moved forward to adopt a lot more commodity technologies. Yes, that comes with all the benefits that we know and love from commodity technology, but also all the risks as well.

Dave O-Jenner: So, I think from the executives’ point of view they’ve done a fairly tremendous job of getting up to speed very quickly. I think a lot of other industries have had a lot longer lead time to get there. We’re certainly seeing the executive levels within the aviation space really grasping that cybersecurity is a real, tangible thing that they need to look at beyond the sort of traditional view of security, which was largely safety-based. So, I think that’s probably where they’re really doing a fantastic job, is taking some of those lessons that they’ve maybe learned from the safety world, now applying them to the cybersecurity realm.

Brian Contos: Dave, do people like you and folks on your team, do they get the time, do they get the cycles with the executive leadership to really help them understand some of these threats, at least to the point where they can actually start making business decisions predicated on your expertise and your background as you’re providing them metrics, and measurements, and other types of information to make their jobs easier? Are you getting that audience? Are you able to get that voice with the executive team?

Dave O-Jenner: Yeah. I obviously can’t speak for everyone in the industry, but at least from SITA’s perspective, I would say it’s an overwhelming positive yes to that answer. We certainly do have quite a good air time with our executives, even with our management board as well and really use that time fairly effectively to talk about the types of threats that we see, the types of threats that we think we’re going to see, and what we can do as an organization to take that risk and reduce that to a level that we’re all comfortable with. So, yes, I think, at least in our case, the answer is certainly yes.
Brian Contos: I'll give a little shout-out to SITA. SITA is so involved in the cybersecurity side, from relationships with Airbus and building up a sort of aviation SOCs and threat intelligence around this space. I think it's a very forward-thinking company. It's great to see organizations like SITA being so engaged in the cybersecurity side and bringing this sort of legacy and modern approach to safety and security together in this way. That's something that I don't think we see across the board in every vertical, so it's very nice to see SITA doing that.

Brian Contos: From a security analyst's perspective -- let's get off the notion of boards, and executives, and things like that, but actual folks with hands on keyboard -- how are they adapting to this landscape today? There must be just a number of challenges. To your point, you've got a lot of specialized systems that were maybe a bit more proprietary in legacy working along with very modern, cutting-edge solutions. That must be challenging.

Dave O-Jenner: Yeah. I think the work of a security analyst is... It's funny. People say, "Hey, Dave, I want to get into the security industry. What advice do you have?" I always tell people the exact same thing: "If you fancy a job where you are guaranteed to fail, and it's always your fault, dive right in, because that's exactly the industry that we're in."


Dave O-Jenner: Yeah, run away. For sure.

Dave O-Jenner: I think the security analysts, the folks that are really at the coal face of this, they've got really a couple of different challenges, but also some great opportunities. On the challenge front, it's keeping current. I don't think this is unique in the aviation industry. I think it's just a challenge that all security analysts have the world over, understanding what these threats are, how they're evolving. What are the tools, tactics, and procedures that our threat actor friends are using? How are they doing what they're doing, and what do we need to do to combat or counteract that?

Dave O-Jenner: I think that's the great challenge, is just staying current. It's very easy, I think, on the analyst side to just fall into being busy, just doing work, because there is a lot to do. We need to be very mindful that we have to take a little bit of time out to maintain that currency. So that, on the challenge side, I would say is it.

Dave O-Jenner: On the opportunity side, though, I think we have some good little balances to try and bring this pendulum back a little bit in our favor. Certainly in terms of some of the things that our team is looking at, one is around leveraging automation so that we can scale more effectively. If you think about trying to defend against cyber threats in a company that's maybe three offices in one country, that's one problem that you need to solve. Scale that up to every
airport in the world. That suddenly becomes a much more difficult and different problem to solve. So, we certainly are seeing [that] our practitioners are looking for opportunities to automated some of the tasks that they do.

Dave O-Jenner: Then, lastly, I think it's about pulling intelligence out of the data that we have. Quite oftentimes it's not necessarily needing to invest in new capability. Perhaps the capability is already there. We're maybe just not making the most of it. So, certainly, our analysts are looking fairly frequently in terms of, what data does the organization have? What might we be able to conclude from the data we already have, without necessarily seeking out more?

Brian Contos: I love that final statement there. Really, it's about getting value from our security goals and our people and processes, but making sure that not only are the tools functioning, and optimized, and doing what we want, but we're able to actually communicate that and generate data to show: Hey, are we getting better? Are we getting worse? Show our bosses that are giving us these checks to invest that, "Look, it actually is providing value," or showing auditors that, "Yes, we really do need this solution, because here are the problems."

Brian Contos: I think that's really a growing issues with a lot of organizations today. It's really hard to show that your security tools are doing what they're supposed to do, empirically at least.

Dave O-Jenner: Yeah. I mean, it's one thing to look on the box, and it says, "I do A, B, and C." But until you actually use that in a real world environment and put it in, you really don't know. To your point, and I think it's a very strong one, a lot of organizations I think bring in technical solutions looking to solve one problem, but they maybe don't fully capitalize on the fact that it might actually help you in two or three other problems that you hadn't even considered.

Brian Contos: Absolutely. Absolutely. Getting value out of what you've got is, I think, becoming a mainstay now of everybody in security.

Brian Contos: Dave, I know one of the things that you're very passionate about is threat intelligence. Maybe you could dive into a little bit about how threat intelligence, and maybe some other security capabilities, is being leveraged.

Dave O-Jenner: Yeah. I've mentioned this in a couple of talks I've given over the years. I think threat intelligence is our great opportunity to swing the balance back to the good guys. What do I mean by that? Well, if you think about the threat landscape, you have a bunch of threat actors here, there, and everywhere. They are collaborating. They have been collaborating for a number of years. They're not necessarily working in isolation.
Dave O-Jenner: But, when it comes to us on sort of that defensive side, we're still very coy. It's a little bit like the high school dance. We're all sort of sat around the outside. We really want to dance with someone, but nobody's really going to make that first move. I think there's a little bit of that within the defensive side.

Dave O-Jenner: What we've seen and at SITA what we're trying to promote is, "Just get out there. Just take that first step. Walk into the middle of the room. Grab someone. Invite them for a dance." We're certainly seeing that within our industry, [as] much as we've seen in some of the others, like financial services, for example, the setting up of facilities where organizations like ours, and our customers, and our suppliers can actually have candid conversations about: "What are we seeing? What are we doing? How are we combatting this threat? What did we try that worked really well? What did we try that was a terrible failure, and what did we learn from that?"

Dave O-Jenner: So, certainly within our industry, there's a couple of things that I would mention that really have helped this. One is a homegrown capability from SITA, which is something called our Community Cyber Threat Center. This is a threat intelligence and otherwise information-sharing exchange between ourselves and our member airlines, airports, and other SITA members. That's a facility that we have to directly reach out to our customers, share what we know, and get their sense.

Dave O-Jenner: I think the other one I would mention, too, is the Aviation ISAC, which is really a global attempt to bring everyone in the aviation ecosystem together and give them that ability to share and exchange any kind of information within that security space. So, as defenders, we are most definitely leveraging this newfound ability to talk to each other.

Brian Contos: Now, I love that notion, just because there are so many moving parts when you think about the aviation industry, and some of them are behemoths, and some of the them are extremely small. To be able to have some type of centralized intelligence sharing, some way to take what others are learning and make that available to some of the smaller players as well, I think is so critical, because they are all interconnected. It's part of one big ecosystem, so it behooves them to do that. I think that's a fantastic notion.

Brian Contos: By the way, I love your analogy of the school dance. As soon as you said that, I was thinking back to 7th grade, and I've got my Members Only jacket. I'm on the boys' side of the gymnasium. Stacy Kettle's over there. Like, "Should I talk to her? I don't know." My jacket's really cool, though.

Dave O-Jenner: The aviation industry, working together and collaborating, it's kind of what we do. It's in our DNA. So, if any industry is going to exchange information and
make the most of this facility, I think it's going to be ours. I'm just super excited that this is something that we can do.

Brian Contos: Well, that's great. It sounds like it's a very exciting time to be working in cybersecurity within the aviation industry, for sure, with all these changes.

Dave O-Jenner: Mm-hmm.

Brian Contos: Dave, as we wrap up here, a question I like to ask all of our guests: Who is your favorite superhero or supervillain, and why?

Dave O-Jenner: Oh, wow. What a great question. I think I'm going to give consideration to three, because I can't pick one. I'm terrible at deciding things, as my wife will tell me. I'm going to go with three. My first favorite is possibly one of the worst superheroes ever. It's a superhero called Barrier Man.

Dave O-Jenner: I've got to tell a quick story as to the genesis of Barrier Man. This actually came by way of a photo that was tweeted to me probably about three or four years ago now. If you imagine you're going to a music concert, they have those long rows of metal barriers that are put up so that you can form a nice, orderly queue and get into the venue, right?

Brian Contos: Yeah. Sure, sure.

Dave O-Jenner: There's a guy putting out these barriers, and on the back of his high-visibility jacket, on the back it says Barrier Man, because he's a man who puts barriers up. So, I thought, "Wouldn't that be just the best superhero ever?" His only ability is putting barriers up.

Brian Contos: That's awesome.

Dave O-Jenner: I like that one. That's my tongue-in-cheek one. Slightly sort of in the same vein, I'm a massive fan of a cartoon series called "Savage Chickens" drawn by a Canadian cartoonist from the British Columbia area. He has a series of cartoons called Useless Mutant. One of these is a mutant called Flashback Man. He has the ability to predict the past, which again I think is one of these useless ideas. I don't know why. I think I'm drawn to the idea of superheroes with not actually incredible powers --

Brian Contos: That's right.

Dave O-Jenner: -- just slightly average powers.

Brian Contos: "I can see through wooden doors."
Dave O-Jenner: Yeah, something like that. Exactly that.

Dave O-Jenner: On a more serious note, I think my all-time favorite superheroes are -- and this is going to sound super-cheesy -- it's all the men and women that are in the profession that we're in, working tirelessly doing what we do, most oftentimes without the fame, the fortune, and the credit -- certainly without the fame and fortune -- just sat there day in, day out, doing what they do, trying to keep things safe. Those would be my superheroes.

Brian Contos: Awesome, awesome. Very nice sentiment, for sure. Well, thanks so much, Dave. It was great having you as part of this podcast today.

Brian Contos: Thanks to our listeners for joining. Be sure to check out other Cybersecurity Effectiveness Podcasts sponsored by Verodin.