VIDEO TRANSCRIPT

INTERVIEW WITH DEBBIE WHEELER, CISO, DELTA AIRLINES, JAN. 16, 2019, ATLANTA, GEORGIA

Filmed and edited by Cybersecurity Ventures

Cybersecurity Ventures filmed an interview with Debbie Wheeler, CISO of Delta Airlines, on Jan. 16, 2019, in Atlanta, Ga. A video of the entire interview can be seen on YouTube at https://www.youtube.com/watch?v=us62A08YgMw

A full transcript of the interview is provided here.

GR: Hi, everybody. It's Georgia Reid from Cybercrime Magazine. I'm here doing another Ask the CISO interview. Ask the CISO is sponsored by Fortinet. I'm here today, January 16, 2019, with Debbie Wheeler. Welcome, Debbie.

DW: Thank you, Georgia.

GR: Thanks so much for coming down here today. We're in Atlanta today for the FutureCon event. You are the CISO for one of the biggest companies in America, let alone Atlanta, Delta Airlines. How long have you been there?

DW: Almost two years.

GR: In February?

DW: Yes.

GR: I just wanted to hear a little bit about yourself to start us off, your background as a woman in cyber, and now the CISO at Delta. How did you get interested in and involved in this area of work as cybersecurity expert?

DW: I've been in technology all my career. I started in telecommunications. I was a network engineer for a company called MCI. One day my boss came to me and under that "other duties as assigned" clause of my job description, asked me if I'd be interested in taking on a project to tackle viruses. At that time, viruses were something that dumped all your words in your Word document to the bottom of the screen or caused your spreadsheet to not calculate properly, so very different than what we're dealing with today. I did that project and soon any type of a security-related project was coming to my doorstep. That's how I wound up in the field.

GR: So, you really enjoyed that?

DW: I did. I really did.

GR: What aspects of it interested you the most?

DW: I think a couple of things. First, the mentality or the psychology of why people want to do bad things.

GR: That is interesting. The crime aspect.

DW: Absolutely. And then the problem-solving aspect of it.

GR: You said you went from telecommunications. Where did you go from there? Did cybersecurity take you next?

DW: From telecommunications, I did a two-year stint in the healthcare industry. Then, from there, I entered banking and spent 20 years of my career in financial services working in cybersecurity.

GR: When you're at an airline such as Delta, how different or similar is it to working in healthcare and finance? What are some of the similar challenges versus different challenges that you face as a CISO?

DW: I think there's probably more similarities than differences. I think regardless of the industry, if you're working in technology, we all experience the same challenges and problems. It's certainly true in the security space. There is no shortage of bad guys trying to do bad things with technology. While the attacks might differ by industry, the outcomes are usually the same. There are financial gain aspects, espionage aspects, and just pure chaos.

GR: How much data is under your purview? You're protecting not just the corporation but also the customers. Is that correct?

DW: That's correct.

GR: How do you go about finding the best people and the best workforce to help you with that task?

DW: I'm fortunate to work for a great company. The Delta brand brings a lot of people to our door that might not otherwise show up. We've got a phenomenal culture at Delta. People that want to experience that culture — it's a very employee centric culture — will put their resume into our hands. We find a lot of folks that are just really, really wanting to work in that environment coming forward.

Having been in the industry for as long as I have, I've had the opportunity to work for a lot of great companies and see a lot of great talent. As I've moved to various positions, I've brought people with me. I've been able to build a team by bringing people with me who I've worked with in the past.

Then I think, too, as a result of our environment and Delta being 80,000 strong, it's very much a family environment. We get a lot of internal referrals, so a lot of people that have passion for Delta and are very dedicated to the company and serving our customers connect with and know other people that share a similar passion and will refer them to us. We've made some great higher as a result of that.

GR: So, there are 80,000 employees at Delta?

DW: Yes, there are.

GR: Do you know how many are on the cybersecurity team?

DW: We've got about 60 FTE and then we're supported by a great group of contractors and a couple of manu-service contracts.

GR: That's huge.

DW: It is, but we also have the advantage of 80,000 family members who are as dedicated to protecting our customers as we are.

GR: So, you train them meticulously on inside threat and phishing scams and things like that. How do you go about doing that? Do you have creative ways that you could share with other CISOs?

DW: I'm sure we do a lot of the same things other security organizations do. We do the phishing campaigns, but we also bring in guest speakers on a quarterly basis, so we have a lot of folks who have come in and have talked about various topics in information security. We've had the FBI come in and make everybody a hacker for the day, teach them how to conduct phishing campaigns, and what the value and the benefit is for the threat actor. It gives them a different perspective and it helps them understand not just how to protect themselves, which we want them to walk away with, but how to protect the company, and it gives them a view into the mindset of why some threat actors do what they do.

GR: I want to just get you on the record giving someone advice about going into this career. If they're looking for advice, what would Debbie Wheeler say about this career?

DW: Go for it! Absolutely go for it. It's fascinating. There are challenges every day, opportunities every day, and you get to do good.

GR: Yes, that's true. We do need more cybersecurity workers. Speaking of cybersecurity risks and threat actors, what is one area that you can speak to that you're particularly concerned about in general at work but also outside of work for the general consumer?

DW: I think what I worry about in my personal life is the Internet of Things and how many things we're building technology and Wi-Fi capability into. I don't think that we have a full appreciation yet for the risks that we are introducing. A lot of people don't have the advantage of having someone in their family or knowing somebody that is in the cybersecurity field that can help guide them or they may not have access to some of the information or the journals that we all read and have access to. So, they blindly

implement these technologies thinking everything is fine and they wind up realizing that it's not. I worry about that. I worry about it for my kids. I worry about it for members of my family. That's probably the one thing that keeps me awake at night.

GR: I hear that a lot. If you could speak to a grandma or a teenager or someone who isn't cyber savvy, what's one piece of advice you could give someone listening about protecting themselves when they start implementing these smart devices?

DW: I'd say don't, but that's just probably not the right answer. I would say find someone you trust who is technology savvy to help you implement it in the right way. So, changing the passwords, don't allow the default passwords to stay in place. When your cable company comes to set up your home router, don't keep the default password in place; change it right away. I think that's probably the one easy thing people can do that gives them a layer of protection, so they aren't taken advantage of. Definitely try to find someone you trust, Geek Squad, there are a lot of groups out there to help you set it up if you're not comfortable or familiar with technology. And let them know security is a priority for you.

GR: I hear a lot of buzz about smart airports and smart travel involving the Internet of Things, whether it's like a luggage tracking device or anything that has to do with Internet of Things in the airport. Are there any technologies coming out that you're particularly interested in when it comes to that?

DW: Recently Delta made the announcement that we've implemented the first biometric terminal in the United States. When you travel internationally through Hartsfield-Jackson Airport, you will encounter a completely biometric terminal, from curbside to the gate. You can use facial recognition to check in without fumbling around for your passport or your driver's license. Then obviously we have partnership with CLEAR. Again, you can utilize biometrics to speed your process through the security line. You brought up bag tracking — RFID tracking of luggage from curbside check-in or the counter check-in, all the way to destination. It's a great feature that our customers really love.

GR: That's a lot of progress. Not only is it going to be easier for the customer to use the facial recognition, the biometrics, would you say it's more secure?

DW: I would. We obviously do a lot of vetting of the companies that we work with. In the case of facial recognition, yes, there are partners, and there's always the risks — we have risks, partners have risks — but I think we're all very cognizant of what's involved here, and we're doing a lot to evaluate and ensure the security of the data that is being passed.

GR: That sounds like an exciting initiative. I know a lot of smaller companies out there who are doing incredible things with new and innovative products, but they just can't seem to get to talk to CISOs. What advice would you give them? What is it like being a CISO with all of these different vendors out there to choose from and how has this

changed over the course of your career?

DW: When I first started in the field, there were maybe two dozen vendors that focused on any sort of product on security. Today there is over 3,500.

GR: That's a lot.

DW: It's ridiculous. Everybody thinks they have the silver bullet. Security budgets while they are growing are not infinite. When I look at a product, I need to ensure that it's going to cover a multitude of concerns that I have. It can't just be a point solution. There are just too many vendors with point solutions out there and while they may be really innovative and although they may be really great technology, it's kind of going to be a flash in the pan in a year or two.

I'm looking for technologies that allow me to address a broad array of threats and concerns that we have and integrate with other base products that we have in the environment. So, I tend not to engage with a lot of point solution vendors, because I'm looking more for the platform that I'm building capability on, or a tool that will do a multitude of things, or that can replace a multitude of point solutions that I may have in my environment.

GR: Possibly MSSPs.

DW: In some instances. We've looked at managed services where we know that managed service can bring either the skill set to the table that we're having difficulty finding or is going to be a complement to skills that I already have on my team.

As an example, we have a SOC, an internal security operation center, but we also leverage an external provider for off hours, weekend and holiday coverage. They also have some capabilities that we don't have internally. It's more cost effective for them to have it than it is for us, things like the education and the schooling and the training programs, they put their people through. For us to try and replicate that would not be cost-effective, but we benefit tremendously from leveraging their resources and their programs.

GR: I was curious if companies such as Delta has any kind of internal proprietary technologies that they use.

DW: We do, but not so much in the security space. Most of what we're doing in the security space is best of breed product that's readily available to any security organization.

GR: It's already challenging enough when you have 80,000 employees, plus all these consumers. The data, the technology, to have to kind of put together a bunch of point solutions to manage all of that is almost impossible.

DW: It really is.

GR: Is there anything else that you're working on with Delta that you're particularly excited about new technology wise.

DW: I think at Delta, we're in the process of going through a digital transformation, so we do a lot of work with Georgia Tech, which is where we happen to be today, through a collaboration called The Hangar. That's our innovation lab. Being that we're part of this digital transformation, we're bringing a lot of technology into Delta. Security is a big part of that, so we get to be a part of that innovation, looking at the new technology and helping the organization make a determination about where it's appropriate and where it might not be.

GR: What are some of the key security focus areas for you to 2019?

DW: Like a lot of CISOs, we're focused on operational technology. I think that's coming up more and more at the conferences I've been attending over the course of the last two-year period. We're very focused on our OT footprint. We're continuing to monitor the integration of things into our network and tracking how we secure those. We're always going to be very, very conscientious about third-party risks and vendor risks and insider threat management and monitoring. Those are just table stakes and we're very, very committed to those things, but I think if you look at new innovation, new technology, and where we're looking to get more involved, blockchain is certainly something that's coming onto the scene in the security space. We've been working with partners new better understand how blockchain can really help the airline but help security as well.

GR: Is there anything you could say about blockchain?

DW: I think it's early stages. We're waiting to see how it evolves and where it goes. There's a lot being done with blockchain in terms of identity management. We've been monitoring that. We're certainly not at a point where we would be implementing anything that would leverage it, at least not in the security space, but we are monitoring it very carefully.

GR: I'm really curious to see what comes of this in the next year or two.

DW: I am too.

GR: Briefly, I wanted to switch gears and talk to you, Debbie, about being a woman in cyber. We have a group on LinkedIn dedicated to helping women get advice — career advice, professional and personal advice — in the cybersecurity workforce. As a woman in cyber, what would you say to other girls or women who are listening and want to know what it's like to work in cybersecurity and is this a place for them.

DW: There are a couple of things I'd like to say. First, go for it. Don't let anybody tell you that you can't do it. Don't let anyone tell you that you need a certain background to be

successful. My team is partnering right now with a high school that has a work study program here in Atlanta, so we have a team of four school students that join my department every day. They work alongside my team. Three of those young people are young girls. When they came into our environment back in the August timeframe, none of them were looking actively at technology, let alone cybersecurity, as a potential career field. We now have all three of them very interested in what we're doing. All three of them have been exposed to a variety of aspects of cyber, so you see, you don't necessarily need a math background or a computer science background to be successful. You just need to bring a really good work ethic and a passion for what you do. If you can bring those two things to the table, the rest is easy to learn.

GR: That's great. Thank you so much for coming down today, Debbie. Is there anything that you'd like to say or leave off with to our listeners.

DW: Support young women who want to pursue technology careers. And to the CISOs out there, we're all in this together, so the more information sharing and collaboration we can do, the more successful we will all be.

GR: Thank you very much. I really appreciate it.

DW: Thank you, Georgia.

