CYBERCRIME MAGAZINE
CybercrimeMagazine.com

published by
CYBERSECURITY VENTURES

Page ONE for the Cybesecurity Industry
Cybercrime Facts, Figures, Predictions and Statistics

VIDEO TRANSCRIPT

INTERVIEW WITH JASON WITTY, EXECUTIVE VICE PRESIDENT & CISO, U.S. BANCORP, DEC. 13, 2018. ONE WORLD TRADE CENTER, NYC

Filmed and edited by Cybersecurity Ventures

Cybersecurity Ventures filmed an interview with Jason Witty, Executive Vice President and CISO of U.S. Bancorp, on Dec. 13, 2018, at One World Trade Center, NYC. A video of the entire interview can be seen on YouTube at https://youtu.be/QtlM3gHgGVw

A full transcript of the interview is provided here.

GR: Welcome, everybody. It's Georgia from Cybercrime Magazine. We're here for our first Ask the CISO event. It's December 13, 2018. I'm here interviewing Jason Witty. Welcome.

JW: Thank you very much.

GR: Thanks for coming down here today. Jason, you're the Executive Vice President and CISO for U.S. Bancorp, correct?

JW: That's right.

GR: How long have you been with U.S. Bancorp?

JW: It's coming up on right around seven years.

GR: How long have you been in cybersecurity?

JW: About 25 years, and 19 of that in the banking or financial services sector. Before that I was in aerospace.

GR: We're talking to a lot of other CISOs tonight on camera and this interview will be seen by a lot of CISOs around the world. What is it that you'd like to tell them?

JW: First and foremost, I feel your pain. We're all in this together. Obviously, there's been a lot that's been changing on the Internet, on the population of devices that are being connected, the type of devices that are being connected. All of that is sort of a large amount of stuff that we would have to deal with, and then we have an even more rapid pace of change of technology innovation that's happening that we're also having to deal with. It's constantly wearing multiple hats. That makes it pretty challenging.

GR: Pretty challenging, but also probably interesting and exciting. How do you go about finding the best professionals to work for you in this climate?

JW: I think that's one of the biggest problems all CISOs have is there is a shortage of talent. There have been different studies that have been out there. I've seen numbers like globally by 2020 we'll have a shortage of 6 million positions.

GR: We're predicting 3.5 million unfilled by 2021.

JW: There you go. There are different numbers that are published on that. There is a supply and demand problem right now. All of us are implementing some kind of a strategy for how to handle that. We've implemented sort of almost like a Disney branding type strategy where when you think about Disney, you don't think about — immediately, if I said the word Disney, you don't think …

GR: I'm thinking Mickey Mouse.

JW: You think Mickey Mouse. Then you're thinking the Mickey ears and the ears you see on stuff and then the theme parks cursive for the Disney word. It's a multitude of things. It's not one thing they did. For us, for example, we're always attending conferences on purpose, looking for talent. We're very specific about which conferences we want to go to. We are always looking for people and interviewing people even though we don't have positions open, or even when we don't have positions open.

We've also partnered with universities. There are four universities every year that we do scholarships for four people. That gives us 16 people per year that we're sort of watching from a pipeline standpoint. We pipeline those people into our internship programs, so that helps. Sort of try before you buy. It gives them an opportunity to see corporate life and gives us the ability to see how they are going to operate in it.

We also partner with military. We're one of the largest hirers of military leaders in banking. That's fantastic. We've gotten a few awards for that. But it's doing all of those things and then we're always looking for more ways that we can also fill a pipeline, whether it's participating in women in technology or targeting girls who code. We participate in that. We actually just did a cyber badge for the Girl Scouts. That was really cool.

GR: The CEO of the Girl Scouts will be here tonight.

JW: That's fantastic. I have to talk to her.

GR: She's Sylvia Acevedo. We've interviewed her. We nominated her Cybersecurity Person of 2018 because of those badges.

JW: Nice.

GR: I didn't realize that you were also involved.

JW: Yeah. We did that in the Cincinnati market, which is pretty huge for U.S. Bank. It went over really well.

GR: Do you agree that there's a little bit of a PR problem or branding problem with cybersecurity as a career?

JW: I wouldn't say that. I think it's a new field. It's an immature field. You can argue that cybersecurity has existed since the 1950s, but even as late as 1990, when you thought about information security, you probably thought firewalls and maybe a little bit of monitoring and probably access control, not a whole lot more than that. It's changed so dramatically. You need so many different simultaneous skillsets or to specialize so highly in order to be super good at one information security vertical that it's just finding those specialties and finding the people that thought about getting into a STEM type process in the first place, who then got interested in the computer side of that, who then figured out, oh wow, securing those computers is quite lucrative and/or interesting and important.

GR: Essential.

JW: Absolutely.

GR: Cybersecurity is changing a lot. I know we were talking earlier about a shift in Internet security to Internet safety. Can you elaborate a little bit about that?

JW: I mentioned the multiple hats thing previously. That's one of the toughest aspects of the job of being a CISO. You have to be a busy leader first. You have to be a risk manager. You have to be a compliance manager. You have to understand the compliance regime that your company fits in. But you also have to be somewhat technical in order to understand the nuances, and you have to be somewhat policy in order to understand the implications of those nuances on broader topics. Then you layer onto that the technology environment itself has been explosively growing but it is now even more explosively growing with the Internet of Things, with artificial intelligence, with machine learning, with a lot of these newer digital cloud technologies, continuous integration, continuous delivery type of modern software development.

With all these things happening, there is just a tremendous amount that's going on. Then you also have to speak Klingon all day and speak English to the board, and these other things that increasingly are important as a business leader.

GR: There's a translation issue, I'm sure, between technology people and business people.

JW: For sure.

GR: And the CISOs help kind of bridge that gap a bit. And we want to thank all of the CISOs who are participating in the Ask the CISO series for that. Tell me a little bit about this Internet of Things problem. What are some of the issues that we're going to see coming up as far as these safety concerns?

JW: It's really interesting. When I talk publicly about information security, I usually preface by saying, "I'm here to educate you, not to scare you," because we as information security people see what would scare normal people all the time. It's just not scary that there's some new malware that is jumping from computer to computer. It's always happening, right. But there are some things that truly are changing the game that are coming up. Self-driving cars is a complete game changer. If you design that for failure first, that can actually save tens of thousands of lives per month when you take out the human error factor. Personally, I think self-driving cars are a really good idea. I do think that you have to design for failure. You have to seek out people who are going to try and break your stuff on purpose. Get them the responsibility to disclose it. Try and design it right from the first place but recognize that you won't always compartmentalize your designs. Why do the brakes need to talk to the radio, needs to talk to the Internet? That type of thing. But done well, we can manage those types of risks. The more of those types of things that happen that aren't done well, society is going to struggle with the life safety issues that come with the Internet of Things, and when you have pacemakers with Bluetooth, and you have defibrillators that are connected to the network. The WannaCry virus shut down something like 65 UK hospitals last year. And they weren't even being targeted. That was sort of accidental. It hit the whole Internet.

I think that is going to be one of those game-changing things, when you have artificial intelligence that's actually operating to break into your network, and if you're not thinking about how you have defense in an artificial intelligence world, that's game-changing.

There was some really interesting research that a couple of researchers did, and then they had a TED Talk. It's about eight minutes. It's phenomenal. It's fascinating. They basically took a series of Google images of President Obama and then a series of YouTube videos that he had recorded. They fed all of that into an artificial intelligence machine learning engine and built a 3D model just off of the images of President Obama's face and mouth and jaw, from every angle. Then they took all of the audio and they chunked all that up into syllables and every intonation and every word and made it look like a real video. They did nine of them. You can't even tell that was not an actual speech. We talk about ransomware. We talk about business email compromise. Imagine how crazy that would be …

GR: If it looked like your boss was on Skype.

JW: Yeah, if your boss was Face-timing you or Skyping you or whatever, telling you, "I'm going to do this thing; send some money to China." That's what keeps it interesting. That's what keeps it exciting. It can be definitely exhausting as well.

GR: So, you're saying that as these inventions in Internet of Things devices come out, even if it's operational technology or a smart-driving car, whatever, you need to be aware of the supply chain, that every little piece could be a vulnerability.

JW: Absolutely. And you have to treat it like it's going to be part of a hostile environment and design accordingly.

GR: How many employees do you have who work in cybersecurity for U.S. Bancorp?

JW: For us, it's about 700.

GR: And then how many employees overall?

JW: 72,000, somewhere around there.

GR: 72,400. I could have just looked down at my paper. How do you train all of these employees to be aware that there could be business email compromise or there could be a ransomware attack or a phishing scam or any kind of thing like that? How do you go about training for that large amount of people?

JW: It's again back to the Disney analogy. It's multiple things at the same time. All financial institutions have mandatory training requirements on certain types of things; information security happens to be one of them. AML, OFAC, lots of other stuff too. Everybody's going to have some baseline of information security training. It's mandated. Above that, we focus on employee behavior and trying to make sure that we are detecting if there is some sort of massively wrong behavior. Somebody has a virus on their computer or something like that. Also trying to shape the behavior in a positive direction. Phishing testing is extremely educational. When you have that teachable moment, like, big U.S. Bank logo. This was a test. You failed. If this was real, your computer would be being rebuilt right now. You probably don't want that pain. I've been through it. Be more careful with what you click on.

We do that. We do a lot of webinars and that sort of thing as well. We have poster campaigns we do every quarter. We have the benefit that our CEO is really quite focused on ensuring that the management of the company is all sort of rowing in the same direction; it's a "One U.S. Bank" thought process. We all know what the goals are. And one of the routines for that is that there's a monthly call with most of the leaders in the organization. We're also able to get security messaging out that way. We've also obviously got things like board education and senior leader education, that sort of thing.

For us, risk is really at the core of our DNA. Just being able to manage risk is core to what we do. So then fitting information security into that overall risk message is a lot easier.

GR: A lot of CISOs say the same thing, no matter what vertical they work in, whether it's healthcare, finance, or anything else, for that matter, entertainment. Do you think that there is anything that differentiates the financial sector or the banking sector as a CISO in your job, other challenges that you face that are unique?

JW: Yeah, I would definitely say that there are. The first one is we're going to be attacked, a lot, with very seriously funded adversaries who are trying to get money. We are where the money is. That's going to be different. The other thing I would say is that because of safety and soundness and the fact that no bank competes on safety and soundness, we all share information with each other very openly when it comes to attacks, whether it's physical attacks or cyberattacks. The amount of knowledge that we all have collectively around what's going on in the financial services sector is just incredible. I think you know I'm the chairman of the Financial Services Information Sharing and Analysis Center, FS-ISAC.

GR: Is that based in New York?

JW: It's actually based in D.C., but a lot of members are in New York. That organization, if you were to print the amount of intelligence that's being shared — bank to bank, and targeted government products, law enforcement, to the financial services sector — it would be four realms of paper per day. It's quite a lot of volume. How we're all sharing, what subject lines are we seeing, or what bad hashes of the day are, or IP addresses that are trying to break in, that type of thing.

GR: So the private sector is helping the government as well when it comes to that stuff?

Jason: Yeah, it's definitely a partnership. The whole idea of the ISACs is that there is sharing within the sector and then there's sharing between the sector and the government and then there's sharing between the government and the sector.

GR: What technology business drivers and strategies are you working with right now to affect the security?

JW: I'd say that the whole financial services industry is going through a digitalization sort or — revolution is probably not the right word. It's explosively growing, how much we're digitizing. And along with that comes a lot of newer technologies like continuous integration, continuous development type modern software, application development, cloud technologies. Most of the large financials are experimenting with artificial intelligence machine learning right now. We have been since 2015. We have a couple of things that are really cool that are going on that I can't talk about.

Blockchain is another one that's a game changer. If you got blockchain right for a community, blockchain for different types of banking information, that could be absolutely game-changing in terms of no bank having to do settlement anymore. That would just be huge. You've got thousands of persons, teams, doing settlement. That type of thing is really promising. And then you've got things like everyone opening up automated programming interfaces so that your app can go find all the ATMS without actually having to log in to something and go find all the ATMs. You've already pre-authenticated that information and made it available. That then enriches the different types of things you can do app to app, or cloud to cloud, or bank to bank, or customer to bank. All of that is sort of revolutionizing the payments process in the future.

GR: That's super interesting. Are there going to be a lot more laws and regulations and audit processes around these things or is it pretty much free right now to experiment with these technologies? See how it goes.

JW: That's almost a comical question. That's one of the other differences. We're one of the highest regulated sectors.

GR: What about an access control system, or an app, or something that opens a bank door or an ATM vestibule, or anything that is a vulnerability?

JW: The way I'd answer that is we are already highly regulated for anything. Any type of big change has to go through a change management process, which has to have multiple types of reviews associated with it.

GR: Is that part of your role as a CISO as well?

JW: Absolutely. Any of the large financial institutions will have teams that do pretty much nothing but evaluate business change risk and figure out if it's within risk appetite or not. What I think's really game-changing though with these newer technologies is that we have the ability for the first time to not have all the legacy processes and the legacy systems and all that. We actually have an opportunity to build a virtual data center from scratch, from the ground up, in the cloud, while still securing the data, doing things like utilizing tokenization to pull the real data out, so that you just have a token that you're using in the cloud, or encrypting the data with keys the provider doesn't have access to. You keep those on premise.

There's a lot of cool things you can do where you bake the security in from the ground up and then automate it and have those controls continuously available and continuously evidenced as well. You have to do it right. You have to be very thoughtful about how you apply those sorts of things. But if you think back 10 years ago, security people were all freaked out about Wi-Fi.

GR: And the cloud.

JW: Right. And now, it's becoming securable. It's becoming safe. It requires that you're very deliberate, but there are certainly ways of doing it to enable the business to move a lot faster and make decisions a lot faster.

GR: Jason, this has been really interesting. I really appreciate you coming down tonight for our Ask the CISO series.

JW: Absolutely.

GR: It's sponsored by Fortinet. They are also sponsoring our event tonight, which I hope you'll stay for. Is there anything that you wanted our readers to know that you're particularly excited about before you go?

JW: The next two years, I expect to be such a high pace of change that that pace is going to eclipse the last 20 years in information security. There is just that much new stuff happening. That's really exciting to me.

GR: Thank you. I can't wait to hear more about it.