VIDEO TRANSCRIPT

INTERVIEW WITH SHAMLA NAIDOO, GLOBAL CISO, IBM, DEC. 13, 2018. ONE WORLD TRADE CENTER, NYC

Filmed and edited by Cybersecurity Ventures

Cybersecurity Ventures filmed an interview with Shamla Naidoo, Global CISO of IBM, on Dec. 13, 2018, at One World Trade Center, NYC. A video of the entire interview can be seen on YouTube at https://www.youtube.com/watch?v=qZ_ZWuU8Awc

A full transcript of the interview is provided here.

GR: Welcome, everybody. It's Georgia Reid from Cybercrime Magazine here tonight on December 13, 2018. I'm here with Shamla Naidoo, from IBM. She's the Global CISO of IBM. Welcome, Shamla.

SN: It's great to be here, Georgia.

GR: It's great to have you. You're here also for our Ask the CISO event, where we are going to have about 30 CISOs here from around the world talking about cybersecurity and sharing thought leadership and everything like that as part of our Ask the CISO series, sponsored by Fortinet this year. I just wanted to get the ball rolling and hear a little bit about you, yourself a woman in cyber, heading up one of the biggest technology companies in the world, household name, IBM. How did you come into cybersecurity?

SN: Interestingly, many, many years ago, I was responsible for a network that had an intrusion. There's nothing like accelerating your learning when you have to deal with a crisis, and that was just part of my normal technology job. It wasn't a security job at the time. In years after that, it became a whole profession on its own. I have been in the technology industry 35 years. I've been at IBM three and a half. I've been a CISO for about half of that time. I spent a lot of my years working in financial services and health-care, worked some time in hospitality, and now with this large technology company.

I feel so fortunate to be at a technology company because I really feel like I have the opportunity at IBM to change the world through cybersecurity practices, through cyber-security innovation, and through really all kinds of innovation that we can consume and use in cybersecurity to solve the problems that have been hounding us for such a long time.

GR: One of the things that we talked about a little bit was covering blockchain, quan-tum, artificial intelligence. Tell me more about these innovations and any digitization that you're using at your role at IBM.

SN: Yes, I use all of the innovation that IBM actually creates, so I get the opportunity to be kind of user zero before the technologies even mature, because it's great for us. We are IBM's largest customer. We consume all of the innovation and new technologies, and it gives us a unique opportunity to provide feedback, to tell them what works, to tell them what doesn't work, and more importantly, I think, to bring new use cases to the ta-ble for the innovation and for the technology. I'm in a very, very fortunate position where I get to use, touch, play, and consume all of that great innovation.

GR: So, you're also part of product development in a way?

SN: In a way. We give a lot of input. We work collaboratively with our research teams, so as they research new technologies, new solutions, new capability, we have a lot of collaboration.

GR: I'm interested to know, since you have a background in so many different verticals that range from hospitality to healthcare to finance and now technology, what are some of the similarities and differences that you've seen as far as attack surface or crown jewels for the attackers that are coming after these different verticals?

SN: I think attackers are going to be opportunistic. They 're going to go wherever the data is that can meet the objectives. So, if the objectives are let's create some financial crime, fraud, then they are going to go where data is going to actually support that initiative. In other cases, they're going to go to other companies that have data that will support them. One of the things that's interesting in my own experience, what I've seen, is that opportunistic gets combined with the ease of attacking intrusion. In some industries we've got more maturity, and you'll find that they will exploit those and change as they go along.

At some point, remember, financial crime and financial fraud was a big, big challenge. Then they moved to healthcare, and healthcare records can give you as much value in a different way, so let's steal it from healthcare. Then you would use it to create fraud in financial services, for example. So, I think that every industry has its own exposure; they have their own data that's valuable. Depending on what the attackers' objectives are, then they can be motivated to go to that industry.

GR: There's something I wanted to ask you about. I know the Internet of Things is a hot topic right now, the cloud, as well as operational technology, and since IBM is a manufacturer as well of product, a physical product, what can you tell us as a CISO what your role has to do with any kind of supply chain management, or making sure that in manufacturing there's security, physical and Internet security?

SN: What's interesting is that whether you manufacture or not, we all have supply chain providers and partners across the board, so partners and providers of services and technology can actually create a weak link in the chain. One of the things that I am a huge believer in is that these relationships are very important. The relationship itself is built on trust. Just like we trust everyone we work with and do business with, we also do have to validate though that the practices and the outcomes we expect are actually what we get.

So, from a supply chain perspective, I feel strongly about making sure we understand who our partners are and that we know we can trust them, and we want to do business with them. The other thing that's important is to recognize that providers and partners and people in the supply chain should not be in a position where they have to go out of

business in order to do and deliver services for you.

It's important that we don't negotiate with providers to the point where they have to really struggle to make investment in probably you good service. Because when they have to do that, they often will cut corners, and when they cut corners, they're going to cut in places you don't see.

GR: Security issues.

SN: Security is a place you're not going to see immediately. You'll see it at some point, but you don't see it immediately. I think we have to start being more fair in our dealings with our providers, to trust them, work with them, collaborate, co-create, but you also have to validate, and you do have to govern and oversee.

GR: So, you have some control systems in place.

SN: Yeah. For a third party who is providing us services, we want to make sure that they are treating our data, our systems, and our assets the same way we would. I think if you look at that and you ask your provider to give you what you would give yourself, then you ought to make the investment to get that outcome.

GR: Cybersecurity is not just an Internet problem anymore. It's way more; it goes down into every single part of every single product that you guys are creating at IBM, which is super interesting. I was wondering if you could talk a little bit more about the operational technology side of things and the industrial control side of things.

SN: Operational technology and information technology has converged to some large extent. A lot of the operational technology still is in a bubble, so my recommendation is to leverage as much of the information technology security practices that we have built, capabilities that we have, and to leverage those to protect those systems. For example, if an operational technology system has an IP address and is connected to the Internet and it is generating traffic, we have an opportunity there to treat that device the same way as we would treat a laptop or a server, for example, so the same kind of practices should apply. Now, in some cases operational technology might actually be insulated from the Internet, so it's not connected. We should make sure it's not connected by accident, and we should try to isolate them to work only in the operational area that it's intended to run. That would be something that we could do, is isolate them.

The other thing on operational technology is to know what the technology does. Often we would get operational technology that's in a box. You really don't know how it's configured, you don't know how it's set up, and maybe you don't need to know, but functionally you have to make sure that it does what it needs to do, and then we have to know where it is and we have to be able to track it and trace it. Sometimes operational technologies are so small and so prolific that you could lose track of them. It's important as an asset to know where that piece of technology is and what it's doing.

GR: You're wearing a lot of hats as a CISO.

SN: Yes.

GR: What is your favorite hat?

SN: I think it's about building strong, high-performing teams. One of the things I say to my teams all the time is I would be nothing without them. I would have no accomplishments without really strong teams who are willing to take risks to get the job done, to understand how to protect the company and our digital assets. It's really important to me that we have people with the right skills, they have the right aptitude, they have the right attitude, but more importantly, that they take ownership for the outcomes.

GR: How do you go about finding people? We have a cybersecurity work shortage right now.

SN: By all indications, it looks like by the year 2020 we said there will be 1.5 million jobs that would go unfilled. I think by 2022 that number is going to get closer to 2 million.

GR: Cybersecurity Ventures predicts 3.5 million.

SN: That would not surprise me because if you think about how the technology has grown, everything from your shoes to your refrigerator and your car is now a smart computer. What I think about that is these are not shoes anymore. This is a computer with a shoe built around it. My self-driving car is going to be a computer with a car around it.

Everything is getting digitized; everything is getting connected to the Internet. The more you have that, the bigger the threat is, the more you're going to need people to kind of manage the threat, so I think we have to think about this in two different ways. One is how do we create more of the talent we want? I don't think it's easy enough to go buy it, because if we could buy it, all of us would have it.

GR: And you get into a bidding war with other companies over talent.

SN: Absolutely. The only thing we do is we outbid each other, but we're not really making the world a safer place. The idea is for us to build more talent and to create more skills, so in addition to just the talent, we have to create more skills in the talent that we already have.

The way we've been thinking about this is twofold. One is we create new talent by training people who don't otherwise have the skills. So, we teach them the skills, we give them the experience, and we give them the opportunities to build on those skills and experience. The other thing we've done is driving accountability to the people who are doing the work. For example, whether you're selling a dress in Macy's or you're writing a

big application for a big manufacturer, you still have to do your job in a secure way.

If you're building a network, you have to build it securely. If you're writing a piece of code, you have to write it securely. So, if you're selling that dress in the store, you have to understand what the areas of issue are going to be in that transaction, and you have to take the steps to try and overcome those types of obstacles.

GR: And knowledge is power.

SN: Knowledge is power.

GR: Not a lot of people know that this is such an issue.

SN: One thing we have to do is teach the skills in the context of the job. If you are selling that dress in the store, then you should know and understand where the particular cybersecurity obstacles are going to be, where the potential opportunities for fraud and crime and other kinds of digital challenges are going to be, and you have to then learn how do you overcome that in your role?

At the end of the day, if you've got a compromised transaction for that dress, you who are selling that dress are in the best position to avoid that hum. You have to know how to, so we have to teach those types of skills in the context of the job. If you are designing the global network, you have to know how to secure that global network, and we have to teach you how to do that in the hope that as you do your day-to-day job, you're going to do the security for that job without it even becoming a separate exercise or a separate team.

GR: As naturally as breathing.

SN: Just naturally, it should be incorporated in what you do every day. I would encourage employers out there to think about how they allocate hours and time to different efforts. So that person who is selling the dress, they are allocating the entire 8 hours of their day to selling dresses. Somehow, we might have to think about how do we give them a little bit of time in that 8 hours that's allocated to making sure those transactions are secure, and the same with any other technology company.

I think that we have to do that, drive the accountability to the people who can avoid the bad outcomes, and then build more talent, build more skills. To do that we have to be inclusive; we have to be far more open than we are. If you show me a laundry list — I want 10 years' experience, 5 years' experience, 2 years' experience, these skills, this technology…

GR: It's going to be impossible to find that.

SN: Yes, it's going to be impossible to find.

GR: I hear that from a lot of people. They're willing to train someone if they have the right attitude and interest in it. I hope people that are listening answer that call, because we do need more cybersecurity workers — cybersecurity warriors, really.

SN: Absolutely, and we have to get creative about where we go source talent. You can't always go source it in the universities or you're not always going to go look for talent in other companies that are like you, your competitors. That's not always going to be productive. We have to get much more creative. We have done a few things at IBM. We have these P-TECH programs that support schools — high school students will actually get an associate degree while still in school.

GR: That's very, very good. That's excellent.

SN: And then we go out, we reach out to women who are rejoining the workforce. They've taken time off; they've raised their families; they've done what they wanted to do at that point in their life. They want to reenter the workforce. Our objective is to give them those opportunities. A lot of people have come in from those nontraditional places, whether it's veterans or women returning to the workforce, people coming from other verticals.

A lot of jobs are getting automated, there's a lot of displacement, etc. This is a great opportunity for people to retrain, reskill, retool, and move into this field. This challenge is not going to get overcome with the people that we have today. We're going to need more, no matter which way we look at it.

GR: It is inclusive, because we need you no matter who you are, your gender, what you look like, absolutely. I want to get more women involved in cybersecurity. What would you say to women who are listening to get them involved or interested?

SN: I would say first we have to get rid of that notion that cybersecurity is about hackers behind a mask sitting behind a dark keyboard with a dark hoodie over their heads. That's kind of the stereotype and we have to move beyond that. I think women have to see that there's something that's much bigger here. This is an entire career.

In fact, I would argue that this is one of the only professions that has almost every job within it. If you want to be an engineer, you can be an engineer. If you want to be a communications person, you can be a communications person here. If you want to be a developer, you can be a developer here. There are all kinds of opportunity, whether you want to write policy, whether you want to do governance, whether you want to do hardcore forensic analysis, this is an area you can do most any job within this field.

GR: Shamla, I can't thank you enough for coming down here tonight. These words are going to reach a lot of ears. Is there anything that you want to say to other CISOs who are listening before we go?

SN: We got to fight the good fight.

GR: We're all on the same team.

SN: We're all the same team, and just remember, cybersecurity is not a competitive advantage. None of us are better or worse because somebody else failed. We just have to support each other.

GR: Share the knowledge.

SN: Yes, share the knowledge, and we have to recognize that failure is only one click away.

GR: Very good. Thank you so much.

SN: Absolutely.

GR: I appreciate it.

SN: Thank you. It's great to be here.

