**RedZone Podcast Episode #80: How Do You Decrypt 29,000+ Computers? – with Raj Samani**

Bill: Okay, Raj, well I am super excited to have you on the show today. Welcome.

Raj: Hey, thanks for having me.

Bill:

[00:00:30] So, for all our listeners and to talk to you a little bit about the listener audience [inaudible 00:00:12], tell us a little bit about how did you get to where you are today? Is this something that you mapped as soon as you got out of university? How did you get to where you are, at the point you are? Maybe you could explain a little bit about your role now and then what was your trajectory? How did you get there?

Raj:

[00:01:00] So, the official title now is Chief Scientist, and I've got to be honest, I think it's literally probably the coolest sounding job in the world. To be honest, I didn't even know that Chief Scientist ever existed until ... Certainly not when I was in school. Now, obviously, I've got this wonderful role where actually I'm helping lead and drive McAfee who I think is ... I love working here. I'm getting the opportunity to drive this company forward from a technical perspective, from a technical strategy perspective. I've kind of got the job of my dreams. I kinda say it to my boss, "I could do this for free," but I kind of realize that I don't want to do it for free, really. I just say that.

[00:01:30]

[00:02:00] I started actually ... Well, gosh, it sounds a long time ago, but over 20 years ago. To be honest, security wasn't really a career path at the time. It was you can get into IT, and security itself was more of a hobby. So, I, obviously, began to focus on security really just as a hobby. I think as time went on, I became more and more interested in it. I remember, a number of years into my career, I'd been doing Help Desk and, as I was doing this Help Desk work, I kind of had this decision to make, which was, "Okay, look, I need to focus on something. I don't want to be a generalist." Everybody, at the time, was going through the Cisco certification, CCIE. You know, at the time it was [crosstalk 00:02:09].

Bill: Yeah, I remember that.

Raj: Right, you remember the certification? Everyone was an MCSE, and everybody was a CCIE. Actually, I didn't have a social life after I finished my masters. I did 34 professional exams.

Bill: Oh.

Raj:
[00:02:30]

[00:03:00]

[00:03:30] Because I wanted to be the best, right? I wanted to know everything. I'm kind of like an information whore, people say. But I kind of made this decision, which was, "Okay, there's networking, which is going to make me money, or there's security, which isn't going to make me any money, but I'm going to enjoy it," and I actually still remember the conversation today that I had with my wife. We were sitting there, and I kind of said, "Look, this clearly is the two paths, and I need to make a decision." She just said, "What do you want to do?" It was, "Well, I want to work in security." At the time I'd just read Cliff Stoll's the Cuckoo's Egg, and that book kind of cemented it for me, which was, "Okay, I'm going to do something I love. I realize it's not really a career right now, and it's not really seen as that important right now but this is what I want to do." So, I began to read and focus. I bought myself a Cisco router and I bought myself ... I had licenses for firewalls, and I configured stuff in my bedroom. I began to really focus on that. It was a conscious decision, absolutely a conscious decision to get into this industry.

Bill:

[00:04:00]

[00:04:30] I love that. And there's many that are listening that remember those days 20 years ago where security was ... We knew it was coming, but it wasn't really paid attention to. It's really interesting you made that decision, because it wasn't necessarily the obvious choice then, because you're right. I mean, all the respect was given to the rare CCIE and what number you were and the [MCSE 00:04:00] track. That is really interesting, the Genesis of a lot of the certification tracks and such. It's funny, a lot of the guys, even today, that we hire, if you really ask them, right beside their bed at home is essentially a plethora of different boxes and devices and things that they're breaking and testing in the evening. It really is a big differentiator between the guys that are really, really passionate about this industry and those that are just kind of showing up for a paycheck.

Raj:

[00:05:00] I kind of took it to the extreme. For my honeymoon, I took Bruce Schneier's Applied Cryptography with me. And I remember, at one point, I was sitting there reading the book on a sun lounge on my honeymoon, and somebody just turned around, looked at me, and just shook their head like, "What are you doing?" But I think that's kind of what it takes in some cases. It sounds quite obsessive, but, in this industry, and certainly in tech, but especially in tech, there's just a wealth of information. And, of course, this was, what, 20 plus years ago? Now, with the advent of social media, now, with the advent of every conference under the sun that you could possibly think of, I think it's got to the point whereby there's simply too much information to consume.

[00:05:30]

[00:06:00] I mean, I remember, back in the day, we had those few books. There was Bruce Schneier's books, there was books by Ira Winkler, there was Kevin Mitnick's books, but by and large, we were talking about a relatively small pool of information. There was the one or two conferences like, in Europe, we had Infosec. There was maybe one or two industry bodies like the ISSA, perhaps. CISP was just beginning to form. It was relatively quite small. Now, of course, it's an industry, and I think that's been the interesting change. We kind of had this as like a hobby where it was a small community, and now it's a wide industry.

Bill:

[00:06:30] So, you clearly went into the worms eye level of security first, and networking. And then you kind of came up to a strategy level and to a much different level. But you never lost that appreciation for the tech, the real tech part. Was that another conscious decision where you were going to elevate yourself to the strategy side of the fence? How did that start for you?

Raj:

[00:07:00] If I'm honest, I think it was luck, but I don't think it was luck, if that makes sense. At the time, I was consulting for one of the largest employers in the world. I was working for the big four at the time, and I'd done a piece of work for them, and I sat in front of their CTO, and I presented the research and technical findings that we had. The CTO turned around said, "Wow, the way that you communicate is really good. I've been looking for a CSO. Do you want the role?" Even before he finished the sentence, I was like, "Yep, yep, yep, yep. Of course, I do."

[00:07:30]

[00:08:00]

[00:08:30] While that sounds like luck, I kind of realized, when I was doing pure technical work, I actually had a real phobia about public speaking. I had a real phobia about speaking to the board or speaking even to the IT director. So, I began a path of trying to teach myself how to communicate, how to read body language. And actually I can still tell you, but the scariest moment of my career was at Infosec many, many years ago, and I'd agreed to speak at the conference. At the time, I'd begun to write articles and blogs, so they'd been asking me for some time. I agreed to do it this one year, and I've got to tell you, Bill, I barely slept for two weeks. The night before, I was in a cold sweat. I was physically and visibly shaking on stage. But I knew that I had to learn the ability to communicate. I had to learn the ability to be able to stand up and articulate to a broader audience. So, yes, okay, I got off with this role as CSO, but I think there was a lot of work and actually a lot of fear that I had to overcome in order to be able to communicate.

Bill:

[00:09:00]

[00:09:30] I think there's a couple themes that I'm noticing from you. I think it's a great message and a great reminder for myself and others is just ... So, communication is super important, and sometimes I think that's one of the things that get lost, especially in the technology side, because usually the guys and ladies are a little bit more binary. It's the cliché that the tech guys really don't communicate well. But you actually really approached that fear and that discomfort in yourself and really blew through that. I know you and I were talking about communication earlier, and even with children and such. It sounds like you've really changed that whole paradigm and decided you were going to be a great communicator.

Raj:

[00:10:00] Yeah. I mean, I think it was a conscious decision. You know, I'm quite logical in certain things. I don't like surprises, I don't like to realize that actually, I've got some issues which are going to hold me back in my career. And actually, I think back to your point, which is, whenever I interview for people, I always sit down and I'll test their technical skills, but I always try to understand the person. I always try to understand those soft skills, because I feel ... I'm going to get destroyed for this, but I always feel that technical skills are overrated.

[00:10:30]

[00:11:00] And I am actually a perfect example of that. I wanted to learn something. I got books, I learned, and I was pretty much a self-starter. Much of what I've done is self-taught, but I think what you can't teach from a book and you can't learn is the ability to learn, is the enthusiasm, is the aptitude to learn, is somebody that was willing to put themselves out there. Whenever I interview, I'll always give the basic test of technical questions, which is the baseline that we need, but at that point, I try to understand, "Okay, who is this individual? Are they willing to learn and do they have that kind of attitude and aptitude that really what we're looking for?" I think that's probably a key piece of advice that I give certainly to my kids all of the time.

[00:11:30] I remember my daughter said to me the other day, she said, "Daddy, I want Minecraft. Can you buy me Minecraft off the app store?" And I said no. She said, "Oh. Why not?" And I said, "Well, because I believe that if I buy you Minecraft, you're going to constantly and consistently ignore your homework." And she's like 10 years old, right? So, she looks at me and she goes, "Oh, okay." And I went, "[inaudible 00:11:23] you're just going to walk away and say, 'Okay'? You're going to accept the fact I said no?" And she went, "Oh, what do you mean?" I said, "Well, why don't you develop a case for me to try to change my mind?" I'm kind of trying to teach my kids this as well, which is, "Don't take no for an answer. Try to understand where the other person's coming from and develop an argument which can help you win your case." It sounds like really extreme parenting, but I'm trying to live it every day.

Bill:
[00:12:00]

[00:12:30] I don't think it is extreme. I think it's necessary because it's developing grit. You dove deeply and read 400 books and you bought equipment, had it in your basement. That was a different day, but the reality is that can be done today, and that's the type of determination and effort it takes to master a discipline, whether it's computers or whether it's painting. There's a grit, there's a determination. I just got out of an innovation conference in Singularity University in California last week, and one of the key things is not the ability to learn, but how you learn. Your unique learning style, and are you hungry to learn? Because we can't depend on our college educations anymore, or our high school, we've got to be always on learning.

[00:13:00]

[00:13:30] The thing is that everybody has a different gear for learning. Are they really interested in learning, or do they have to have information given to them because they're passive? It's really interesting and in security what's interesting ... I met with a very large association in DC the other day, and the CIO looked at me and she ... We were talking about innovation and her innovation labs and then it branched over into security. She goes, "Doesn't it bother you that the industry hasn't got together, and the world governments haven't got together to solve this problem?" She looked at me and goes, "Do you realize how much it's costing me to just chase all these security threats?" She goes, "Do you realize how many small businesses are going out of business due to ransomware?"

I looked at her, and I have my own thesis around it and such, but the reality is how many of us are actually approaching this to actually solve the damn problem versus just creating something for someone else to buy? It was a really interesting point. What are your thoughts on that?

Raj:
[00:14:00] I think we are. I can sit down and point to you multiple examples whereby people have left their egos at the door and are actually doing something to address and tackle this problem. One of the examples I'll give is a project I actually was co-founded with through McAfee but actually, we had Kaspersky Lab, we had the Dutch police, we had Europol, and we had Amazon web services and Barracuda. We kind of got together, just over a year ago, and we said, "Okay, this issue of ransomware, it's getting ridiculous. What can we do about it?"

[00:14:30] Whenever we do work like take down bad guys, when it comes to ransomware, sometimes we get the keys that allow people to unlock their data. So, we said, "Why don't we just pool our resources? Why don't we put all of the tools in one site and create a single repository where anybody freely, you don't even need to give us your email address, you can go to this site and we will give you the tools to decrypt data, assuming, of course, it's a variant that we know about.

[00:15:00]

[00:15:30] That was just over a year ago. We started off where there were six of us, now we're in excess of 100 partners with law enforcement from pretty much most countries all across the world. We've got a huge number of private sector companies now. The website's translated in 27 languages. The official figure is we've prevented 8.5 million US dollars going into the hands of criminals because we've decrypted 29,000 computers. The unofficial figure is way higher from that. It's just that some of the tools don't actually track how successful they've been in the past.

[00:16:00] This has cost the industry nothing. This is provided free of charge. I couldn't even tell you who we've decrypted because we just give it away free of charge. So, there are examples. We can sit down and complain and moan and say, "Things aren't the way they should be," or we can just stop moaning, and we can get up, and we can do something about it. I think No More Ransom, to me, is a shining example whereby we just put all of the commercial pressures to one side and did something. I remember we were trying to recruit a year ago and I had companies and people saying no to me, and then six months later some people came back and said, "Actually, yeah. We will join now."

[00:16:30]
Bill:
Wow. When I heard you speak at [inaudible 00:16:29] is that, the No More Ransom, is that the organization you're referring to?

Raj:

[00:17:00] Yeah. So, the website is nomoreransom.org, and you don't need to be a McAfee customer, you don't even need to have antivirus. You can go to this site, and if you've been impacted by ransomware, we'll tell you the variant that you've been hit by and if we have a free tool that can allow you to decrypt your data. You don't need to give us your email address, you don't need to have ... A salesperson won't call you afterwards. We don't track anything, it's just free to access. We've also got the ability for you to be able to report the crime back to your local law enforcement as well.

Bill:

[00:17:30] I love that, I love that. During the presentation that you gave, what was the tipping point ... How many companies are you involved in this? Would you call it a consortium or would you call it a loosely coupled confederation? What would be the right word to call this?

Raj:

[00:18:00] So, you remember Lord of the Rings? And I think it was the first film, and I think I did this analogy actually, a few times, but it's the analogy of Lord of the Rings. So, Gandalf and the Fellowship are crossing the bridge, and they're being chased by ... I think it was a dragon or some equally nasty thing. Gandalf says, "You go ahead," and he stops at the bridge. He puts his staff down, he says, "You shall not pass." This is what this is. This is a, "You shall not pass," moment.

[00:18:30] Like WannaCry, for example, in the UK, 8,000 operations were impacted. Like, medical procedures were not carried about because of ... I mean actually, I don't think it was ransomware, but something labeled as ransomware. That's the impact that it's having. People are not getting operations. Companies are going out of business. Large companies are actually having decrease in revenue, like quarter upon quarter results. This really was that, "You shall not pass," moment. We've got to do something about this, because if we, as the industry, with law enforcement, can't do something about it, who is? I mean, this is our job. This is what we do. This is what we're really good at. So, why don't we do something about it?

[00:19:00]
Bill:
Yes. I love it. I think it's fantastic. I'm so glad you shared that with the audience because I think there is a certain ... People don't know how to combat this, and they don't know how to take action. This is definitely stepping forward and giving someone a chance to actually bypass the paying the ransom and actually looking to see what they can do about it.

[00:19:30]
Raj:

[00:20:00]
Well, I mean, right now, if you're hit by ransomware, you have two options. Pay criminals or lose your data. That's really not a great set of choices. So, we kind of try to give people a third option, which is do neither. Get your data back, and don't pay criminals. To me, that's probably ... I think the greatest success is, finally, actually, we are directly impacting the revenue earned by criminals. That's what I'm particularly proud of.

Bill:

[00:20:30]

[00:21:00] I also noticed that it seems like this was an innovation. Actually, this is probably more of a transformation. I've been having this conversation with people. What does it really mean to be innovative? Painting a tree that's green, painting it green and orange and calling it something innovative is somewhat ... It might be different, but it's certainly not innovative. But it seems like this is a transformation that the industry really needed. Also, I look at your role in one of the organizations in your LinkedIn profile, you actually had innovation next to it. So, is this something that you really think actively about is how you innovate and how McAfee innovates, how you innovate or how you bring in innovative ideas to the marketplace. Do you actually think about that from a transformation point of view?

Raj:

[00:21:30]

[00:22:00] We've heard the saying that security is an enabler, and yet the reality is that most people listening to your podcast couldn't give you an ROI for any of the security technology they've ever bought. I mean, actually, it's quite embarrassing, I think, to an extent because you buy this technology and you buy it because you know that if you don't, there might be an issue or you may be on the news. It's always ifs and when's and maybes. For me, my biggest challenge today is, "How can I actually demonstrate and articulate that security ... Or not even security, that trust is an enabler for businesses across the world?" And I firmly, firmly believe that, because the reality is I'm not a security person. None of us are. There's no such thing as cyber security. It's a made up word. We are technologists. All of us are technologists.

[00:22:30] What we try to do is we try to manage and mitigate the risks that the innovation is clearly going to have. So, I'll give you an example. I mean, it was a few years back and I was out in the middle east. I met with an oil company, and we were talking about the evolution of oil and gas. One of the things that we discussed was this feasibility of developing what we call a digital oil field. Now, of course, what that means is that they're going to move away from a manual environment to fully automated digital systems. Because of the work that we did, we were able to increase oil production from 400,000 barrels to a million barrels a day.

[00:23:00] Now, that clearly introduced huge numbers of risks, right? Because you're now putting digital systems in which can manage equipment out in the middle of the Arabian sea. What we did was we actually considered what the risks were and we put in as many controls as we could possibly find to try to ensure that disruption doesn't happen. That, to me, is probably my favorite use case, because what it says to any business across the world is, "As an industry, we can revolutionize the way that you work, and just because it introduces new risks doesn't mean that you should just ignore it."

[00:23:30] Actually, what we should do is, from a trust perspective, we should look at ways to manage or at least reduce the risk to a level that we're comfortable with. That's kind of really the charter that I'm trying to do here within McAfee and with some of our partners and customers that we work with, which is, okay, look, this is the way that your business works. How can we revolutionize the way that you operate and use technology such that you can have 250% productivity gains as we saw in oil and gas?

[00:24:00]
Bill:
That's really interesting. So, what do you think it's going to take to ... Are you or McAfee kind of spending time educating leaders, technology leaders, CIOs, and CSOs about how to convert what they're spend is into a, "Well, this is communication, and this is communication in a different way." How are you educating about how the dialogue needs to shift?

[00:24:30]
Raj:

[00:25:00]
Well, in many cases, when organizations do something so disruptive for an industry or for a specific vertical, invariably, it kind of involves their senior leaders. For example, I wrote a book around smart grids, applied cyber security in the smart grid. I actually talk about this model whereby utilities don't make money through electricity, they make money through becoming a data broker. And, tongue in cheek, I say, " The company that provides you electricity in the home will have more data than Facebook in two to three years time," and, actually, is kind of true.

[00:25:30] So, what it takes to get organizations to adopt these disruptive technologies ... In many ways, it really depends on the leadership within that company. And then, of course, you're going to get other companies who are going to say, "Well, actually, you know what? I don't feel comfortable paying the kind of organization that's going to do something this dramatic. What we'll do is we'll wait and see what happens." So, in many cases, you'll find within industry, you'll find those companies that will be disruptive, that will do things, and that will be first out, and then you'll find that other companies or competitors will kind of follow as well. We've certainly seen that.

[00:26:00] I mean, when we developed this digital oil field, I remember I was talking at a conference about this. I was actually told, "You're crazy. You would never do this. Why would you have this type of connectivity? It's dangerous. It's risky," and then three years or two years after we rolled it out, there was a digital oil field conference. And, interestingly enough, they didn't invite me. I remember getting the phone call and they said, "Oh, would you like to come to this digital oil field conference?" And I went, "Oh, yeah. That would be great." And they said, "Well, okay. That's going to cost you this much money to speak." And I went, "Yeah, thanks very much. Good luck."

[00:26:30] But I think that's kind of what it takes. You'll have some organizations who are more than willing to kind of try something and do something like this and equally, there'll be other organizations that may well follow. And, actually, I'm quite fortunate that a lot of the people that I work with are kind of visionaries in their own field. They kind of come to me and say, "Well, actually, can we do something, and how can we manage these risks?"

Bill:
[00:27:00]

[00:27:30] So, I have a vision for security. I want to see how you respond to it because I think that the ultimate security is going to follow a biological model that ... Many of my listeners have heard me say this before. Where, if an ecosystem is disrupted by an invasive species or an oil spill or something that happens, normally humans apply a patch and then nature has to take over and heal. And that can be a wound on our body. It can be a cut, a sprain, a broken bone. We splint it or we put a patch or a band-aid and then the body takes over. So, I really think, ultimately, whether it's a zero to five, zero to ten, zero to fifty, is that we're going to have self-healing ... When you have these outbreaks, viruses, malware, infestation, whatever it may be, and then there's going to be maybe a human patch but then there's going to be a self-healing that takes over.

[00:28:00] Now, I don't know how that's going to work out with FBI and law enforcement and INTERPOL and UK and vendors and individual devices and such, but that's the vision I'm holding to. What do you think about that? Is there a macro vision upon that that we should be thinking about? Where do you see this ultimately going in the zero to one, zero to five, zero to ten year timeframe?

Raj:

[00:28:30]

[00:29:00] So, actually, interestingly enough, this concept of self-healing networks is something that, actually, in some cases, we have proof of concepts in place. If it's a known. So, for example, if it's a threat that we know about, a network should be able to respond and recover from that. That's kind of in proof of concept phase, but, for me, I think it's broader because we talk about security as a separate discipline. Even the word cyber is a separate discipline. You take the word crime and you put cyber at the end of it, you put the word war. You have cyber war, cyber attacks, heck, even cyber sex. And, actually, all they are is just an evolution of crime, an evolution of warfare, and evolution of ... Well, actually, I don't know if it's an evolution of sex or not, but [inaudible 00:29:00] satisfying to say, but I wouldn't know.

[00:29:30] Again, we kind of look at this as a separate discipline. And yet, within three to five years time, Bill, you're going to be sitting in a car, doing 70 miles down the freeway, and you're going to be sitting and talking to your children, and the car's going to be driving itself. The reality is ... In fact, just yesterday, we saw vulnerabilities in cardiac equipment, or we've had vulnerabilities in insulin pumps. Like, our dependency on technology is becoming almost ubiquitous. WannaCry was a great example of that, which was a vulnerability which hadn't been patched that was available for months before, caused wide-scale disruption, and I genuinely believe, actually, WannaCry was ... Well, certainly not Petya, was intended to disrupt anyway.

[00:30:00]

[00:30:30] So, I genuinely feel that, right now, we're kind of in this halfway house, which is security still isn't at the top table. How many CSOs do you know that are on the board? I don't know one today. And yet, every organization today is dependent on technology to the extent that, if they had a significant outage, it could be the death knell of the company. So, I genuinely feel that, right now, security, as an industry, maybe, isn't important enough. Maybe that's the job that we've got to begin to do. We've got to begin to be able to have that seat at the top table so that security is designed from the ground up.

[00:31:00]

[00:31:30] So that when you and I buy things from Amazon or wherever we buy this IOT equipment, that they have security and privacy built in. You know, it's ridiculous that companies like VTech can edit the privacy policy so they say that, "If your children's personal data is compromised, we're not held liable," and yet they can say that, and they think people will get away with it, and people still continue to buy. I think, generally, as a society, we need to be able to value our data more, and we just simply don't. I mean, I've seen people give away their personal data for a bar of chocolate. I see people giving away their data for nothing more than a bar of chocolate, and yet companies like WhatsApp are being acquired for billions of dollars, and they're being acquired for personal data. So, the perceived value of data is rock bottom and the actual value of data is relatively high. I don't think this model is going to continue for long.

Bill:

[00:32:00]

[00:32:30] I agree with you, and I think, partially, in many of the companies I'm still with and still work with, the CIO is still the CSO, even though they might have a CSO or an administrative staff or VPs or directors are playing a security function, it is still the minority of companies that actually have the CSO that's reporting into the board or reporting into the audit committee or what have you. It's becoming very, very expensive for companies to staff security operations from the way maybe some of the fortune 100 or fortune 200 companies can. But I do like the ability for people to learn, if they're listening on can you give me an RY in security? And I love that question you had. And using security as a trust enabler, and starting to change the conversation so you're having a much different communication about security and how you can enable it to play a part of the offense of your organization.

Raj:
[00:33:00]

[00:33:30] As a consumer, I want to know that the CSO for every single organization has been involved with innovation. That, to me, is what I want, as a consumer. Because I know that the CSO is going to say, "Well, okay. Have we considered the security risks and have we managed them? Have we considered the privacy issues associated with this device?" And, today, I don't believe the CSO, and not in all cases, but generally speaking, when an organization innovates, the CSO is contacted on a Friday. I mean, I remember I used to be a CSO myself, and I remember getting a phone call at 4:30 saying, "Oh, well, actually we've developed this new system and on Monday we're going to go live. We just forgot to send it to you. Can you please sign it off?"

Bill: Oh, jeez.

Raj:

[00:34:00] Yeah. And I'm sure there are people listening to this podcast now that will nod their head and say, "Yes." In fact, I'm sure there's probably one or two people listening right now, on a Friday maybe, and their phone is ringing and they're thinking to themselves, "Oh, my good God, is that the same call that's happening?" So, we need to be part of the business. The security team is a part of the business, and, actually, I would say, when it comes to trust in the digital world, we're more important than ever.

[00:34:30] I mean, Ponemon talk about this thing called the abnormal churn rate which is, if a company is breached, then an organization can expect to lose between 2 to 5% of their customers because of the loss of trust. Well, actually, that was 2 to 5% ages ago. You know, when [TalkTalk 00:34:23] were hit, it was reported they lost 90,000 customers. When [inaudible 00:34:26] were here, and they did their due diligence by the way, by [inaudible 00:34:29] they lost way more than 2 to 5%.

[00:35:00] So, I think the concept of trust in the digital age is not understood as well. Maybe that's something that we, as an industry, need to do, which is we need to join the grownup's table. We need to be able to articulate the value that we bring to the business, and more importantly, we need to bring innovation into the company so that when the company does innovate the consumers aren't going to be having issues whereby personal data is taken through the back door, which is what's happening now.

Bill:

[00:35:30] Yeah, and I think there's a way for companies defense innovation within security, or I like to say defense. To be able to move that, it's got to move at the pace of the offense of the business. I think that's a challenge for security, is to be able to move at speed and to be able to adjust its speed because of the accelerating way which companies have to test and test new applications. Nobody's really spending multiple millions of these framework projects. They're using more iterative designs and such, so security has to really adjust with that. That is quite a challenge for most security operations to do.

Raj:
[00:36:00]

[00:36:30] Yeah, and I think that's the challenge, which is, when it comes to innovation, when it comes to these emerging new business models, a company feels it has to move as quickly as possible, and the misconception that they have is that the security team may slow them down. But, quite frankly, doing due diligence is a fundamental requirement. It should be ... Sorry, is a legal and a regulatory requirement when it comes to handling customer data. I mean, I just wrote a blog today where my music system, the company that provides music into my home, have updated their privacy policy. What they said was, "We are now going to capture personal data from your house. Oh, and by the way, if you don't like that, your device will stop working."

[00:37:00] I mean, that's the world that we're living in, is that organizations are now ... To me that's unethical, by the way, changing the privacy policies, but that's the world that we live in, is that you have companies today making decisions about data about you, me, my children. To me, that's unethical. I don't believe for a second that a CSO, certainly any good CSO, would have said that's a good thing to do. We're seeing this happen time and time again, where pacemakers are coming out with vulnerabilities or cars can be remote controlled and so forth. Having the CSO as part of this innovation, I think, is not only good for the business but, quite frankly, is good for us as society.

[00:37:30]
Bill:

[00:38:00]
I agree. So, as we wrap up, I'd love for the decision makers that are listening to be able to understand where to go to learn more about McAfee and learn more about ... So, we've had some really interesting conversation about a wide variety of subjects, and McAfee's clearly a world leader in these areas. Is there a place that people can go to start learning about where the most appropriate tools, technologies, and approaches that McAfee is deploying now? And I can put this on my show notes as well. My team puts this on our show notes page, and so people don't necessarily have to memorize all the URLs and products. We'll definitely put them up there for people, but where would someone start, if they really wanted to kind of dive into the thesis more of where McAfee's going?

Raj:

[00:38:30] So, I think this is the most difficult question that I'm always ... Actually, this is my biggest challenge, which is we do all of this work, we'll take down bad guys or we'll create free decryption tools. How do we get the information to people? Now, of course, there's mcafee.com. There's the website, but, quite frankly, how do you stay up to date with data and information? Certainly, we're using social media like LinkedIn, and we're using Twitter. So, the website's a great place to start, but to stay up to speed with all of the latest information, we've got multiple channels. We've got McAfee Business, McAfee [Gov 00:38:49]. Dependent on what area you're interested in, you can follow the key accounts or join the right groups. And, of course, I'm on Twitter, so I'll post stuff as well, regularly, also.

[00:39:00]
Bill:
Okay. So, basically, whatever their platform of choice to receive information, whether it's LinkedIn or mcafee.com or follow twitter. And then they can follow you. Would it be a good place to reach out to you? What do you prefer? Twitter? LinkedIn? What's your preference?

Raj:

[00:39:30] Twitter of LinkedIn is fine, but just mention on the podcast, if you're sending a LinkedIn, because I generally decline if I don't know people, which I think is good practice. But if you mention the podcast, then at least I know that you've listened to this, at least, I guess.

Bill: Yeah, I mean, if you get several thousand, it's probably ... Most, I guess, default to Twitter, for sure. I'll put your twitter handle out there so they can follow you. So, is there any parting words of wisdom that you want to share with my audience before we go today?

[00:40:00]
Raj:

[00:40:30]
You know, I've got a number of ... Actually, I've got three children. I was going to say a number of children, then my wife is going to go, "Really? Hmm. Is there something you're not telling me?" I've got three children, and I'll be honest, I'm really quite nervous about the future. This is not meant to kind of sound melodramatic or anything like that, but a lot of what I talk about is we talk about vulnerabilities, but there's the vulnerabilities in devices that our lives depend upon. So, one of the challenges that I think we have today is we need to get more individuals and children really interested in this career. I would urge every single one of your readers and your listeners, please do everything that you can to just talk to your kids about the value of personal data.

[00:41:00] Also, more importantly, show them the career opportunities that exist here in this industry, because I speak at a school once a month, that's something I always try to do, I always try to speak at a school a month. Every single time, and I remember I went to a careers day just recently when I was there, they had a careers day, and they had a community support officer, so that was law enforcement. They had army recruitment and they had a local what we call a solicitor. So, it's somebody that would do conveyancing for homes and stuff. I turned around, and I remember saying, "These were the same people that came to my careers day like 25 years ago."

[00:41:30]

[00:42:00] It just staggers me that everything that we do is focused upon technology, it's dependent upon technology, and yet we're still not showing children or inspiring children about what the career opportunities here are. So, I guess my ask is this, which is talk to your children about cyber security. Talk to your children about cyber bullying. Tell them about the career opportunities that exist, and please do everything that you can to promote things like No More Ransom. Tell people not to pay, because we work in technology, but those that don't won't know where to go. All of us should be ambassadors towards getting more people into this industry, taking security seriously and our privacy seriously and managing our personal data as well.

Bill:
[00:42:30]

[00:43:00] I think that's a great message, and I just had a personal story with my ... And I think I might have shared this, but I don't think I have with my audience. My kids were coming back to me a little while ago, saying, "Dad, you're such a geek," and to my three kids, neither one of them is inclined to be breaking down computers and tearing them apart. They're just not inclined that way, necessarily. However, when we started talking about autonomous vehicles at the kitchen table, so they're learning certain things at school. They're thinking that's a real nerd thing to do, is tuning AI [LIDAR 00:43:05] on cars, and then that's where society ... That's the value.

[00:43:30]

[00:44:00] I said, "Well, hold on. The programmer's not tuning the choice of whether to hit the child that's walking across in front of that car or swerve over to the sidewalk and hit the four people that are walking along the sidewalk. Who makes the decision that that car will veer into the sidewalk to hit the four or just hit the one?" That's an ethical, that's a moral, that's a philosophical question. So, why can't they go into that side of the conversation? Why can't they go into the legal side of the question? Because some attorney's going to have to get involved, or the code review side. Certainly, there's the programmatic side. So, I think there's a certain education around what's available for participation in this conversation about data and data privacy and the like.

Raj:

[00:44:30]

[00:45:00] But I think that's what's so exciting about what we do. Because every single facet of society is evolving and changing. I mean, the way that we communicate has stood still for in excess of 2,000 years, and in the last 20, it's changed. So, the way that you used to develop social networks, for example, was based upon this concept of physical proximity. In other words, I knew my next door neighbor. I knew their neighbor. I knew the person down the street. I knew the butcher, the baker, and so forth. Now, your friends you've probably never physically met. If you went to a conference and the person that you'd been communicating with for five years over email, you may not even recognize them, they're sitting right next to you. Now, the way that we communicate and the way that we've built networks together and developed friendships is now based around common interests.

[00:45:30] The how we communicate has changed. How we work has changed. How we travel has changed. You know, technology has revolutionized every single part of us, completely, as a race. We've had more changes in the last 20 years than we've had in 2,000. The next 20 to 30 years, we're going to be faced with some of the most moral and ethical challenges that we've ever really experienced. I mean, you touched upon that, which is, at some point, you say that a car is going to have to make a decision. Does it run over one person to save potentially many or does it protect the person behind it? Well, actually, that's going to be based upon the code that's written in the application. So, who's going to be the person that's going to be developing that? Who's going to be the person developing the logic?

[00:46:00]

[00:46:30] Even more mundane things like, "Well, okay, if my credit card is cloned, will the bank refund me? Well, at what point does the bank say no? If my car is hacked by ransomware, then do I lose my car or will the auto company be responsible for preventing ransomware?" All of these fundamental issues that we haven't really got under the skin of actually, we put under the bucket of security. That's what I'm saying. The term security is ... We have to do away with that, because, fundamentally, the work that we do has far-ranging consequences way beyond just simply installing antivirus.

Bill:

[00:47:00]

[00:47:30] That dependence is huge, and I don't know ... It's an interesting question, like how the nuclear industry actually made decisions on how everything gets backed up. When you have a meltdown of a reactor and some of the actual supporting systems that go into backing up, essentially preventing a major catastrophe to happen ... Because if you look at that from how we've engineered complexity and backups into some of our more complex systems, planes and all sorts of medical operating rooms, hospitals, they're very complex, and we've engineered the best we can into providing some resiliency in those systems, but, for example, if a nuclear warhead goes off in the atmosphere and knocks out all of our GPS communications, that impacts everything from our gas stations turning on to our autonomous vehicles. There's a wide ranging impact, so that would drive decisions of how we build resiliency into the local fabric of society. It's quite interesting, these conversations, Raj, and I am really excited you came on the show today. I hope we can do a round two in the future some time.

Raj: I look forward to it.

Bill: Well, thanks very much. Enjoy the rest of your day.

[00:48:00]
Raj:
Thanks very much. Bye-bye.