02 Trust vs. Perception_Mark-nunnikhoven_v1.mp3

Mark [00:00:03] There is no wrong security decision except the one that you didn't make, because if you understand the risks, a perfectly acceptable security decision is I accept those risks but not understanding those risks, you are still accepting.

Robert [00:00:23] Welcome to episode two of Trust Versus I'm Robert Booker, I trust Chief Strategy Officer.

Jeremy [00:00:29] And I'm Jeremy Duval. I trust Innovation Officer. Today's topic is trust versus perception. On the show, we've got top cybersecurity myths and misconceptions. How both security and compliance functions desperately need a PR campaign. Our security theater is bad for airports and worse for your business. And the reason why every control has to be value. Add in both facts and perception.

Robert [00:00:53] That voice you heard at the top of the episode belongs to Mark Nina Koven. Mark's basically a deep thinker in the cybersecurity space. He currently works as principal for the Amazon security team at NWS.

Jeremy [00:01:04] Hey, Robert, why does perception matter? To trust? Like, why even give this airtime on the podcast?

Robert [00:01:10] You know, I think perception matters. It matters to security, it matters to compliance, and especially matters around whether I trust you or not. We could have the best program around, but still, fail of perception doesn't match reality. When that happens, stakeholders like the people I serve, the end users in the organization and the people that manage the company and provide funding for my programs lose confidence.

Jeremy [00:01:33] Yeah, well said. And so we cover a lot of ground on this interview. And I, I can't think of a better guest than Mark to talk about stuff like this with his been a security educator and practitioner for years. He's got a YouTube channel. He does a lot of interviews and he brought in some fun perspectives.

Robert [00:01:48] Yeah, it was a great conversation. Let's jump in.

Jeremy [00:01:56] Mark, how would you describe what you do? And you've got a lot of stuff online that makes it clear that you're passionate about cybersecurity and about spreading the good word of best practices and awareness. How would you describe? It's hard to put your efforts into one box.

Mark [00:02:13] Yes, it is very hard to figure out what I actually do. Unfortunately, my boss has also said that to me and I'm like, Oh, wait, no, not at all. No jokes aside, I've been doing cybersecurity like both of you for a very long time and realize that there is a lot of confusion, There's a lot of opportunity. It's something that I'm doing now, working for Amazon's security team, helping, you know, build the practice across all of Amazon and externally trying to be active in the community. Whether that's encouraging more people to get into cybersecurity, going abroad with, you know, public service announcements or sort of the in the trenches kind of education about tackling things like passwords or cloud security or what have you. So really centers around that education, understanding peace. I think the reality is that we love to talk about the super complicated or interesting or niche, you know, attacks or techniques. If you look at it in conference, it's almost always about the latest attacks. This threat actor, that threat actor not about like, hey, here's how to go

to have a conversation with people, to make them aware how much benefit they can get from making sure that people understand why they're taking certain actions. It's not directly a security thing, but it has way more impact than a lot of security stuff.

Jeremy [00:03:28] One of the things that we've been kind of foot stomping as of late is the foundational cybersecurity controls being just so much more important than some of the more sexy stuff. To your point, hey, we've got a new quantum cryptography standard that you as a small business need to start thinking about right now. Well, maybe. But maybe you should make sure you've got the foundations nice and buttoned up before you chase kind of the more exotic risks. Not to say that quantum cryptography is not important, but for the small business and for the everyday business, for everyday risk assessment, there's something to be said for just the let's not overcomplicate it. Going to be more.

Mark [00:04:05] You know, the quantum cryptography thing is very interesting because from the math perspective, yeah, we need to start worrying about this right now. But that entire threat model is based on somebody being able to store today's encrypted communications long enough to actually get a quantum computer with appropriate algorithm, which isn't that complicated. It turns out the algorithm, the quantum computer part is quite complicated. But once that's in place to then decrypt those old communications and, you know, Jeremy, you spot on a small business, not really worrying about their data today being accessed in a decade from now. Someone else maybe, but most people know.

Jeremy [00:04:46] Yeah, yeah. And risk assessments are hard enough to get right.

Robert [00:04:50] We were trying to think of just possibly fallacies or areas where people might just have assumptions about, you know, what do you need to do to establish trust? And this topic of perceptions came up and we actually had a debate as we were preparing for this episode. Actually, it's like, are we talking about the perception of the consumer? You know, do they care or not care? Or are we talking about the perception of us as practitioners who are responsible for doing something important to secure the company? We think about what the public thinks about this and like, do the people we we serve, are they are they fully on board with this concept of, you know, being secured or maybe the overcomplicated aspect we we put into it and what's their perception of risk?

Mark [00:05:31] And that's a really good and I think profound question because I think people fundamentally do care. But I also think they have a radically different view of technology than those of us in the field. Security is based on the assumption that things don't actually work the way we think they do, right? We have an inordinate amount of complexity in our technology systems. Even just recording this podcast, the amount of things that have to go right and the amount of different protocols and technology stacks and things that we're relying on to make this work. You know, when you step back for a minute, you're like, it's kind of miraculous that it actually works at all, let alone works as intended. And really security is that aspect of making sure that it does continue to work as intended and only as intended. And from our practice, like from from the security practitioner perspective, you go, okay, I know all these different things that go wrong. I know all these different types of attacks and things like that. Whereas from that consumer perspective, I think it's almost the opposite. It is just like how this works. I press a button and I'm having a video chat with somebody across the world and they assume that that's all that is possible from that. Like you take out a fork and you know what that fork is capable of. You're like, Great, I can eat my food with this. It's not a question of like, Hey, if I was really evil, what could I do with this fork?

Robert [00:06:57] It reminds me of the very first red team engagement I ever contracted early in my career. And the. Yeah, they were successful, as most red teams are, at least when you start a program. And I remember looking at the looking at the challenge, the facts don't matter, but the how they, how they penetrated the system and it was it sophisticated. It was literally the thing kind of the backdoor thing that everybody would have assumed was okay. And but then you look at you say, who would have thought to go and look at a system in that way? And I think goes to your point about, you know, we assume it's going to work as a security leader. I had to learn that lesson the hard way, you know, through testing and validation, thankfully, not the really hard way like some others have.

Mark [00:07:38] Your example reminded me of one that stuck with me and has stuck with me for, you know, two decades now. I was in a training session here in Canada with our RCMP who were teaching. We were learning about doing physical threat assessments on buildings and facilities, and the instructor of the time had said he had been given this course for years and he had yet to enter a non high class classified building. So just the normal public service government buildings, he'd yet to actually enter one on the books. Every time he gave the course in those buildings. He just found a way in and then showed up and everyone was always like, Oh, what are you doing here? We thought we'd have to come down and get you is like, Yeah. So lesson one, what you've thought about, like in this being, you know, an access only flaw. It's not. It was super easy. I got it in 2 minutes and I like Yep, that's a great example of everyone thought you had a bad gym and everyone knew that, you know, it was only people were allowed to be here. This person just kept walking and.

Jeremy [00:08:42] So the users assume that this thing works because it's the on the box that says it's secure and product can't be wrong. And then in your case, we're assuming that those controls, at least for the people who own the controls, I think there might have been an assumption that those controls worked. What cybersecurity fallacies or myths or assumptions that are wrong do you think are out there that both individuals and businesses step in more than they ought to?

Mark [00:09:12] There's two that popped to mind all the time, which is passwords and phishing. And so we teach people two things time and time again about passwords and about phishing. And the first four passwords is the absolutely absurdly ridiculous needs to be, you know, at least a capital symbol, a number in there, eight characters or more. You know, we've all seen the basic standard. This password needs to be secure. And then there's a whole bunch of calculators for different uses. It'll say, hey, you picked a really good password. We've known for a long time that that is not actually true. It doesn't hold up mathematically. It doesn't hold up through practice because that generates for a number of reasons, but primarily it generates bad user behavior. We all know people as, you know, password, whatever, one, two, exclamation, just keep pouring in there, you know, to make it memorable. And so the reality is, the longer you can make a password, the stronger it is in honest. Finally updated the guidelines a couple of years back to include, you know, say, hey, go up to 256 characters. I've no idea why they actually put an upper bound on it should be just go as long as you can. It it's funny when you trace the history of that back is it goes back to a very early elder directory implementation that ties into like Novell and Early Windows for Workgroups Day where they couldn't store a password past a certain size. And that was given those technological constraints that the programmers had decided the password formula made the most sense and sort of delivered the best mathematical results at the time. That was 35 years ago. But things

have changed technologically that's been ingrained in us. And so we've been hit with that time and time again. And the second one that really gets me is phishing, because we tell people when you're looking at an email, look at the URL and determine whether it's bad or not. Now, first of all, the being very generous and polite to to my colleagues and friends within the security community. Obviously, none of us have ever looked at an email from a marketing department because those are all ridiculously long, complicated, like basically someone's writing a novel in a URL with all the tracking codes. There's no way you can figure out if that's a legit or not, let alone all the top level domains were over 200. Now it's just not a human solvable problem to look at a domain and say, That's a good one. I'm okay with clicking on that. Yet we continue to teach people to take that action, which is frustrating for them. I think a better approach for that one where, you know, passwords change to longer, the stronger for phishing. If you click on something it asks you to take an action, then you should probably stop it, click on a link and it says, Hey, log in to Gmail, Stop. Download this file, stop. If it goes to a web page, so long as you've been doing some other security hygiene stuff, you should be okay. But the biggest thing for phishing is we have tools and controls that should catch that because it's not really a human solvable problem. So I think those are, for me, the two biggest myths that continue to perpetuate. But I'm really curious, you know, for for both of you, for Jeremy and Robert, what have you guys bubbled up in your discussions, especially around fallacies and myths?

Jeremy [00:12:20] One of the one of the fallacies and I don't know if these follow really that clean definition of fallacy and the thought fallacies, but the one about my security is strong because I haven't been breached. There's there's this maybe more in the executive space and less in the CISOs space. But look, we make these investments at the same level approximately every year and we haven't been breached yet. So that level of investment and that level of controls is good enough because we haven't been breached. And the fact is you maybe haven't been breached because you're good enough, but you maybe haven't been breached because you're lucky and you just haven't come across the radar yet to that particular threat. Actor who might be perfectly capable of stomping you. Right? There's this myth that says, I'm too small to be attacked like I'm a small business, that the bad guys don't care about me and they have bigger fish to fry. That is such an easy thought trap to fall into, and it's just not true, especially with stuff like, I don't know, I assisted spear phishing now where the bad guys can look so tailored at scale, where they haven't been able to before is as easily at scale. So I think this I'm too tall, too small to be attack mentality. While it may have worked for a lot of people for a long time, it's eroding.

Robert [00:13:40] It's interesting to me. I like I like the way you framed it as a maybe a management conversation, because I think perceptions will be different for the consumer from management teams. But I the one I think we heard earlier, maybe it's maybe we've move past it now, I hope is that cybersecurity is an IT issue. You know, I'm going to have my technology team have it or or frankly, even the seat I've sat in. It's the it's the CISOs problem and I think most people that a set the seat would say I can only do it with the support of the organizations. Yeah. The other one is like in chair I mean we struggled with this when we built some of our recent essentials capabilities, like, you know, which what were the most essential cyber controls that organizations needed assurance around. And so the fallacy of just having just the minimum is good enough. And, you know, I think sometimes and even auditors in the past, they said, well, you know, you have antivirus, you have anti-malware, you mention phishing, marked phishing, you know, phishing prevention program, or you have good security awareness training. That's good enough. You know, you've got the basics covered. And you I think we might agree those are those are not complete enough.

Jeremy [00:14:42] Yeah, that's an interesting one, too, because I think there's there's sort of this corporate policy trap that people say, if I comply with my corporate policy across all my systems, my policy has got to be right. Therefore, my security is good enough. And I don't know, like an easy example is password policy. If my password policy says I got to have complexity and 12 characters and it's got to be, you know, change that often and I apply that corporate policy across all of my systems. You could be failing to match controls to the risk of the system, the inherent risk for the system. So if my current policy is the same, regardless of whether my system is Internet facing or whether it houses electronic protected health information or cardholder data, maybe those minimal password controls aren't good enough and maybe you should be doing MFA. So this is fallacy of like minimal security controls being good enough, but they don't match the risk. I think that could be a common problem too, that people are stepping in and every day and don't know it.

Mark [00:15:40] I think, you know, the way you just phrase that, I think it really highlights. There is a the way I would sum that up is there is a fundamental difference between CIA and actual security. Right. And so I have met the minimum bar will be, you know, you can straight face that on a press release, right. Or to the board or whatever the case may be. But as you said, it's not good enough. It doesn't match your risk model. But you did everything that you were supposed to it. Then you realize I go, wow, no, I did not match at all what I was supposed to be doing for my risk model, you know? But also I get it because the you know, to your point, Robert, when the view, you know, that myth of the View that it sees the CISOs problem or the security team's problem and that's, you know, on us as a security community as well, for the longest time, we haven't brought people into the fold. But when you do the math on that one, as far as the number of people on your team versus the rest of the company, there's no way that holds up. So if you sit there, go, okay, you know, Mr. or Mrs. C, so your response or your team of ten is responsible for all of our security needs for our enterprise. And our enterprise has 6000 people, which is about the ballpark ratio, by the way, 1 to 600 for security people to to normal non-security employees. There is no way ten people can be accountable and responsible for the systems, work output and safety and security Of those 6000 people, it just doesn't make any sense. Yet everybody is sitting around the table going, Oh, that makes sense. See? So it's your problem.

Robert [00:17:16] Yeah. A follow up I have on this, this whole theme, the perception of compliance versus the perception of security or cybersecurity or both. Thoughts on that.

Mark [00:17:27] Many. Jeremy, do you want to jump in first?

Jeremy [00:17:30] So I'm a bit biased because I grew up in the compliance world and not necessarily the security world, and I used to think of myself as a security and risk management effort doing our doing compliance gap analysis. And since sort of graduating from compliance, I've, I realized that it's a much bigger elephant to eat than just I have to comply with HIPA or I have to comply with PCI or I have to get my SOC to I got to pass my HFCS assessment because those are tools toward a much larger end. And for a long time coming up, I thought being a compliant state was the end goal. And if I do this, I'm doing the right thing. And it's not to say that those aren't admirable goals that should be strive toward, but security should be the goal and compliance should be the milestone along the way.

Mark [00:18:22] Yeah, and I will say this having considered my word choice carefully and fully aware of the context of the podcast and say this with all support for the communities involved, the only people who have done worse at positioning themselves in the

functioning of a modern business than the security team is the compliance team. And by that, what I mean is compliance serves a valuable role. And it's not simply to get somebody off your back or to be able to point and say we are compliant with this. Compliance to me is a larger community or groups or PCI is a good example, right? Simple to understand for people who aren't in the weeds payment card industry, the major players have come together and said this is the minimum bar we will tolerate for you handling this type of data. You need to adhere to this if you are going to be processing payment card information. But then compliance plays a more important role than just meeting that minimum bar. It is filling in a major gap in security and that it's checking our work. We've so rarely check our work in security. We go, Hey, we rolled out all these controls. We're done. Like we'll know. Are they working? Are they actually actively doing what you think they're doing? Because things change, right? And by the time, especially in a larger corporation, you roll out of control by the end of that weekslong or month following effort. Things have changed as is still the appropriate control. Is it doing its job? You know, is the environment in which it's been configured different now? And so compliance gets you in that attitude and in that practice of checking your work. And, you know, Jeremy, you phrased it quite well, is that it's a milestone. I like to think of it as an output of a well-run security practice. If you're doing all the security stuff correctly and in line with your intentions. Compliance is just a matter of making sure you're checking the boxes of Yes, I verify this. Yes, I verify that. It runs very similar to some work we're doing at Amazon around formal proofs. And our automated reasoning group has done a bunch of the work. They published a lot of academic papers and there's quite a few around automated reasoning and how they are using formal mathematical proofs to prove the security models are doing what they expect them to do. And then that surfaces in a bunch of products that ADA abuses or tools that ABC has specifically released in the Analyzer series. But I think that type of effort is very complementary to compliance in the, Hey, we need to do more than just roll this stuff out. We need to make sure that this is doing what we expect it to do. Compliance is that first step. It's that community agreement. All of us working on health information have agreed HEPA is the standard is the baseline for this do more, but at the very least you have to legally do this. But I think we can keep taking that further to make sure that what we're actually think we're doing is actually what we're doing.

Robert [00:21:12] Wow. Mark sure covered a lot of ground on that one. Yeah. I'm a little confused, though, about his point about how security should be based on the assumption that things don't actually work the way we think they should. Jeremy, what do you think?

Jeremy [00:21:25] So my take is that it's easy human even to have the perspective that something will work as advertised. So if I buy a new product and it says it's secured in this manner and is locked down in that way, you know, the inclination is to believe. A Yeah, that's, that's who is secure. Even if I give that aspect of the system thought at all, I might be more excited about the functionality it brings and less confused or concerned about the security. But if I read the side of the package as a as a human, as a regular user, my inclination is to just trust that. Yeah, okay. But security professionals, security leaders don't have that luxury. They can't just assume that just because it says it's secure in this way, that it actually is. And further, security professionals don't have the benefit of assuming that it will continue to operate in the way that it initially operated, meaning systems change, processes break, and it's the security team that has to come in and make sure that those breakdowns and those changes and that drift doesn't create, you know, the vulnerabilities that the big doorways that the bad guys can come in through.

Robert [00:22:33] Yeah, it almost falls into that category of myths or misconceptions. We talked about that as well, Jeremy.

Jeremy [00:22:40] The one that stuck with me from this conversation was this perspective that stronger passwords equate to stronger security. And I think that's a common myth. A lot of people still believe that if I just had made my my password stronger, that bad thing wouldn't have happened. I think about the newest 1863 release and I was looking today, can you believe it's been five years since 863 B was published and that's the NSA's special publication that challenged a lot of longstanding, longstanding password norms, like password complexity is actually harmful and not helpful. And it makes me wonder how much longer the world will keep holding on to these kind of legacy password controls everybody thinks are good and keep getting perpetuated through key controls, lists and needs need to be challenged. Which ones have stuck with you? You know, I.

Robert [00:23:31] Think about this one about identifying phishing emails. You know, the the whole concept is we have a security breakdown and let's go look at which user was using the weak password to the point you just made. Or that was foolish enough to click on a phishing email. And you know, I'm red faced enough to admit that I have been Phish before. It was Christmas time. It was probably 2010 or 11. I don't remember what year. And I got a link from Amazon saying that my package had been delayed because of a weather event. And click here to see what order was delayed. And I clicked on it. And immediately, I mean, I immediately knew I clicked on it. It opened this isn't the right site. And I went, Oh, and I'm like, okay, I know everything I should know. I'm careful as can be. And I still got got bit, I do, I got bit and I was able to not, you know, not, not fall prey to it all but yeah, kind of embarrassing.

Jeremy [00:24:31] I immediately think less of you.

Robert [00:24:32] Well my credibility is damaged forever, Jerry.

Jeremy [00:24:36] This makes me think of a joke we used to tell each other when I worked at helpdesk, is that, hey, this would be a pretty secure company if it wasn't for those pesky users. Like, why do we think users should be the front line against all phishing?

Robert [00:24:48] It they can't.

Jeremy [00:24:51] The bad guys are getting too good at writing these things. And you remember the time whenever you have to look for the misspelling and you knew that that was a fish to like filter out all the smart people and only be trained on it. Yeah, we trained on phishing and I'm immune now. So let's get back to the rest of the interview with Mark.

Robert [00:25:09] I wonder about how security professionals can think of security programs from an operational lens. You know, especially in large, complex corporate environments, you know where to work. We're drumming all the time on revenue and, you know, NPS and all all the things we use to measure customer engagement and all those things. But here security is sort of out here focusing on the compliance island. And, you know, I think we could argue that we could do so much more as a as a as a discipline than that.

Mark [00:25:39] I think we've come at it. I mean, we are where we are, so we need to work from there. But if we had it all over to do all over again, I don't think we would we would take what is essentially the insurance based approach. Right. Because even insurance does it better than than cybersecurity does. You know, so if you try to get car insurance and most jurisdictions, depending on the country, you know, you're legally required to get

some level of it. But when you talk to the insurance company, they've got so much data around the demographics of the neighborhood you're in where you're normally commuting, the likelihood of that vehicle being in an accident. Like they have all this information to be able to do a very solid, quantifiable risk assessment. And then they attach a dollar figure and say, you're going to pay us this much per month and we will insure you for this amount if something bad happens. That is not a great place to be from a customer perspective, from a business perspective and quantifying risk, that's a really nice thing because you've got really solid boundaries, but your customer interaction there is I'm paying you because I legally have to and because I'm afraid if something bad does go wrong that I'm up the creek, so I will pay you. It doesn't make you feel good. Nobody's like, Yeah, I get to pay for insurance today. Security isn't quite that bad in its pitch, but it's very similar. This ties back again. I'm just going to keep hitting on this because you phrases so well, Jeremy, of that myth of like, well, nothing bad has happened yet. So we'll continue to invest at this level, that is. And that's where compliance has seen that advantage. Well, we know we need to invest more because otherwise here is a very quantifiable number. That's all from a negative perspective. If we had it all to do over again, I think coming at it from the positive of saying, you know, look, this is all really complicated stuff. All of the as far as technology goes, the security controls that we'll put in place from a technology perspective and also from a procedural perspective for people are going to ensure that we can move forward as a business safely.

Robert [00:27:31] So when I kind of take us a little bit, when I want to talk about the concept of security theater, and, you know, we just we just went looked at, you know, Wikipedia, a security theater, the practice of taking security measures considered to provide a feeling of improved security while not providing value to achieve it. We think of the example of airport security in many countries as it really make us safer. I would argue it does make us somewhat safer. But, you know, the perception of people having about this is good security because I see stuff happening.

Mark [00:28:03] It's funny, you know, robber you went right to the airport security. So I spent some time at our equivalent of the NTSB here in Canada working with airline investigators and stuff. And it's absolutely fascinating how that culture works. But from the people side of things, the thing that always stands out to me is the requirement to take off your shoes. When it comes to America and it's only America as far as I've ever encountered traveling the world and all that comes back from one case. Right There was the one case when someone tried to smuggle or smuggle an explosive through their shoes, and it failed. And it was caught in security before people were required to take off their shoes. But the response was, we need to do something. What we're going to do is we're make people take off their shoes. So for one case, millions and millions and millions and millions of travelers since then, in the 20 years since then or however many it's been, have had to remove their shoes in order to prevent something that was caught without somebody removing their shoes. And I think the challenge with that, I understand the psychology requirement, and I'm not advocating for, you know, removing any of these measures necessarily. But I think from a security practitioner perspective, this ties very much back to the core audience that we're trying to talk to in the show of people within a in an organization, in an enterprise is you have to be very careful as to what you impose on your users or try to implement within your environment because you only get so many things you can do. And get people to buy in on, you better make sure they're worth it. And I think that's the challenge, is sometimes we do things either in public scenarios or within our companies that we think is going to make people feel better or is going to have the appearance or drives a nice metric, but it doesn't actually move the needle for us or raise the security bar. And I think that actually has an adverse effect. It's going to reduce your

security bar because it erodes that trust. And the next time you try to do something with value, people may not be paying as much attention as they should be.

Jeremy [00:29:58] So, Robert. Do you think? Third party cyber security questionnaires. Our form of security theater. Could they be or could they be implement in a way that they're not? Do they add value in the way that they are intended to? All the time? Some of the time? None of the time.

Robert [00:30:17] I think I you know, as you know, Jerry, binary questions are hard for me. I'm not going to say it's impossible. But it ultimately comes down to what level of. Sure. And does it offer me around the actual effectiveness of the answer? So I would say you give me an answer. What's the proof behind the answer? If the proof is absent, then I don't know if the answer is real or not. So I would say in that in that aspect, not much. I think in the aspect of a system that goes beyond the questioning or possibly, but then you into assurance and there's so much more involved in the assurance than just the question and the answer. So, yes, probably more security theater in my mind.

Mark [00:30:59] I think the challenge with survey questions in general is you got to think of the context of the people answering it. As soon as somebody says, I know I'm supposed to answer this as opposed to this is my answer. Weird example. You probably figured this out for a while now. I love weird examples. I read an absolutely bizarrely fascinating essay, a breakdown of the smiley face rating system for airport bathrooms. The reason why that's effective is the sheer volume. It's a very simple interactions either one one, two, three or one two, five. Was the bathroom clean and acceptable? Yes or no? We're not Yes or no, but one, two, five, you know, smiley face, happy, no, sticky face, green. They individually they're meaningless because it depends. Somebody could having a bad day. Most of us traveling are having a bad day. Could be just a bad time before the clean, whatever the case may be. But the point of the system was they gathered just a sheer volume of metrics, gave them enough accuracy, Of course, that over the trending that is very subjective measure actually turned into something valuable. And I think the challenge with the survey stuff is it's always scale. We go too deep, too far and we can't scale it up as well as broadly as we need to to eliminate those biases. Because if you send me a survey question and I know the context of the survey, like, well, I know Jerry's running the survey and it's about Robert's program and I want Robert to look good. So, yes, best answer is going to be given as opposed to my actual answer is like, Oh, Robert really messed up this quarter. Right? And so I'm going to give that because I don't I have a personal connection to Robert and I don't want him to feel bad. And I think that's where things get really muddy.

Robert [00:32:35] So, Mark, as we as we approach the end of our time together, I'm just, you know, what have we not asked or talked about that you're thinking, wow, they should have asked me that or we should have talked about that.

Mark [00:32:43] I love it that we focused on sort of the bigger perspective. I think the one that had sort of been tossed around that we didn't get to was the question of, you know, is security everybody's responsibility going to ask both of you, is security, is everybody is the responsibility? Is that a myth? Is that bull? What what's your perspective on that, Jeremy?

Jeremy [00:33:07] I'm all in on the user having a responsibility to not be the weakest link. But it's also I think it's it's too easy sometimes to say, look, if we get breached, it's going to be because a user made a mistake and not because our program had a problem. So I don't know, sort of I guess I think it's safe to say, yeah, I'm in the boat of it is a safe thing and not a myth.

Mark [00:33:32] Robert. Security is everybody's responsibility. Yes or no? Maybe I'll bu.

Robert [00:33:38] I'll never be attacked from stage for saying it, but it's cliche. There's so much more. And yes, the people are part of it. And awareness is great. Let's engage our people. Absolutely. But there's so much more. It just it's an easy answer.

Mark [00:33:53] Have we done enough to make that cliche a reality?

Robert [00:33:57] No. No, I don't think so. I think engaging the organization around the problem is valuable. How many bullets in our gun? How many arrows are in our quiver? Firing the right arrows for the right problem? Not not wasting them. I think that's that's the opportunity is to engage everyone on security on the right part of the problem.

Jeremy [00:34:18] Yeah. And I don't know that we can ever do enough when it comes to educating our users and helping them understand how to use the tools made available. This is a constantly moving target and will never be done. But I think that the programs that equip their users with the right endpoint tools and make the users aware of them. It's one thing to say, right, we're going to do a phishing simulation and if somebody clicks on it, you know, shame on them and stop the risk. It's another thing to have sort of the gusto to say, I will cut off that person's Internet access for this period of time if they click on it twice in a row.

Mark [00:34:57] It's very similar to eating healthy. But if we don't provide easy access to healthy food, simple recipes for people to follow, quick ways to get healthy take out, then we have failed, you know, to to enable that. And it's the same for security. If it's everybody's responsibility, it's the security teams. It's incumbent on the security team to make sure that it's possible to do that. And it's through education is through easy controls. And but really, it's about communication.

Jeremy [00:35:25] So thanks to Mark for chatting with us today. You know, Robert, we really cover a lot of ground on this episode. And you said it once, but it's true.

Robert [00:35:33] Yeah, we really did. I mean, perception in practice almost. If you look at the topics around any security conference, it's usually the latest attacks, the threat actor, the threat actor, you know, the new exploit. It's not about having a conversation with the people to make them aware of how much benefit they could have if they looked at their controls in a different way. The controls mandated by security policies, making sure that people understand why they take actions the way they do and how are they doing the right things. By the way, it's not a security thing alone. I mean, it's just life, you know, making sure you, you know, what your risk are and you're you're implementing good, you know, good health practices. You're staying on top of the things you need to do to keep your family safe. You know, all that stuff.

Jeremy [00:36:17] Yeah. And I know we talked about it about this sort of cybersecurity cliche that security is everyone's responsibility. And Mark challenged us. He asked this question. He said, Do you think we are doing enough to make that cliche a reality? Do you think we're doing enough to make security everyone's responsibility? I don't know the answer, but I think it is it is a good challenge to us all to say, you know, what am I? Am I reminding my users enough? My equipping the users with enough tools and perspectives to make sure that they understand that, too?

Robert [00:36:53] You know, I think the last thing I want to cover is the topic of security theater. You know, this act of creating an appearance that we're doing security that's going to keep us safe, maybe it doesn't, but it looks like it does. You know, Mark, I use the example of airport security. I think probably many of us fly. Millions of people take their shoes off every day because of an incident that took place years ago. Kind of makes me wonder, you know, where are we using security theater type controls every day, you know, outside of the airport, inside of businesses. You mentioned some today, Jeremy. I mean, password length is probably one of those controls today.

Jeremy [00:37:32] Yeah, well, password links. I like password complexity. Password expiration. I like those less. Yeah. This is all kind of in the realm of opinion, but my personal opinion, bad or outdated or ineffectual cybersecurity awareness trainings can for sure be a form of security theater information security questionnaires as well, if used incorrectly to me, top the list of security theater type of activity where there's a lot of effort going in, there's a lot of organization and there's a lot of pressure to do them. But, you know, how is the output of that actually affecting security and is it consistently affecting security the way everyone wants to and think it should? And I'm not creative enough to think of other examples of security theater in the business context, but I'm sure that there's others.

Robert [00:38:21] Well, that's all the time we have for this episode. Thanks again for listening to Trust verses presented by I Trust. Make sure you follow this podcast on whatever platform you're listening to to see how we're going to challenge trust next. Take care of away.