04_Trust vs Breaches_John-Overbaugh_v3.mp3

John [00:00:04] When I think of the word breach, fear is the word that comes in most cases. I think a strong, successful CISO approach is that without emotion, someone needs to be the calmest person in the room. [00:00:18]And oh, and [0.5s] by the way, that's the CISO's job.

Robert [00:00:27] Welcome to episode number four of the Trust vs podcast. I'm Robert Booker, strategy officer at HITRUST.

Jeremy [00:00:33] And I'm Jeremy Huval, chief innovation officer at HITRUST. The voice you heard at the top of the episode belongs to John Overbaugh, CISO of Alpine Software Group. John's a long time friend of HITRUST and just an insightful guy.

Robert [00:00:44] Today's episode is a conversation all about security breaches.

Jeremy [00:00:49] That's right. We wanted to cover this topic because to us, this is the why of it all. If all these controls and compliance requirements and assessments and everything else isn't about preventing breaches, at the end of the day, what's what's the point?

Robert [00:01:02] Yeah, for sure Jeremy. And just note for all the listeners, we set some ground rules for ourselves in this conversation. It's a super sensitive topic and the people dealing with these issues deserve a lot of care and a lot of empathy. We're not talking about this to ride any wave of headlines about the latest security breaches and we're not trying to benefit off anybody's misfortune.

Jeremy [00:01:22] Yeah, and to that end, we don't go into the specifics of any breach and you won't really even hear us name the company that was breached or any companies that were breached except for one or two parts, which I think we're complimenting an organization for how good they did on their process breach communications. And as we're recording this, we're aware that there's yet another really big mega breach hitting the headlines right now. And there are plenty of avenues to get details on that, if that's what you're looking for.

Robert [00:01:51] Yeah. So just to set the stage and there's a lot here, but I'll try to get through it because I think it's really valuable. The frame around which we're airing this episode, just some stats to let you know just how big an issue this really is. So, you know, in the last 20 years, 20 years have been more than 20,000 reported data breaches in the US alone. And that comes from a site called Privacyrights.org.

Jeremy [00:02:12] With numbers this big, I mean, to me that that says the cybersecurity industry still has a ton of work left to do for all of our advances. There's still more work in front of us. The cost of getting breached isn't cheap either. So in the cost of a data breach report for 2022, IBM Security and the Ponemon Institute found that the global average cost of a data breach reached 4.35 million. And that's like the cost that the organization breached would have to incur eventually when it's all said and done. So that's an all time high since they've been calculating that stat. So that's the global stat. Now in the U.S., the average cost hit 9.44 million. So in other words, if an organization in the US has a reportable breach and they've got to go through all the all the impacts associated with it, financial cost 9.44 million on average. So it's just not cheap. And these things happen.

Robert [00:03:06] It's big numbers. But you know, people also think about the cost of getting our security systems certified against something like an ISO framework 27001 or the HITRUST framework. And, you know, people will claim it's not cheap, but, you know, as the numbers show us, the neither is the breach.

Jeremy [00:03:23] So with all that said, let's get into the conversation. I really enjoyed talking to John and hearing his perspective around breaches. He's been doing this a long time before being a CISO at ASG. He was also VP of InfoSec at CareCentrix and he's worn many security hats over his long career. And he also spearheaded high trust adoption in many different places.

Robert [00:03:46] We hope you enjoyed the conversation. John was really interesting to talk to.

Jeremy [00:03:56] Why don't you introduce yourself, John, and tell us a little bit about the company you're with.

John [00:04:00] Sure. My name is John Overbaugh. I'm the chief information security officer for Alpine Software Group. We are a private equity firm that purchases SaaS based companies in vertical spaces such as health care, transportation, logistics, hospitality and so forth. So interesting company in that we focus on growing and pulling these companies together and taking the vision of our of our founders to that next level. Most of the founders have come to us, have have reached the point where they can take their companies and are looking for a partner to help them achieve that next step in their vision. So that's what we do.

Jeremy [00:04:37] In addition to made an accomplished CISO you're also a photographer, so you've got a you've got a photography blog and a recent sort of recent post. You said something that stuck out to us. You said some photography is purposeful, some photography is art, and some photography is being in the right place at the right time. Can the same be said for cybersecurity? If so, why or why not?

John [00:05:04] Yeah, maybe maybe wrong place, wrong time would be more frequent. So first of all, I would say for me, cybersecurity in my career was the right place at the right time. I was working in product groups at Microsoft starting in the mid nineties and had the opportunity to lead the first product group through what was then called the Secure Windows Initiative and is now the the what is it, the Microsoft SDL. And so right place, right time, like I got exposed to information security and application security, and I was like this is fascinating. The many ways that someone can hack your application just opened a whole new world to me. And defending and protecting your application from those attacks was like just sort of the coolest puzzle I could ever find. So that for me was right place, right time that got me into my career. And then, you know, I don't I don't know if I could ever charge someone with being in the right place, right time. And information security is, like I said, it's probably more wrong place, wrong time, right? So I often look at security as really there's two kinds of of targets, a target of choice and a target of opportunity. In both cases, you're in the wrong place at the wrong time, right? Unless you have the right set of protective measures in place and detective measures and so forth.

Jeremy [00:06:22] Yeah, I appreciate them. Hey, remember Mad Libs help us out here. Breaches are blank.

John [00:06:29] Oh, scary.

Robert [00:06:30] Is it an emotional response that that would be a scary or is it is it analytical? Is it thoughtful? I mean, when you when you think about just in broad terms, we hear we hear about another company that had a bad day. You know, what is as a CISO what does it do to inside of you?

John [00:06:46] When I think of the word breach in the context of a of a corporate leadership team, fear is the word that comes in most cases. I think a strong, successful CISO approaches it without emotion. Right? So it's very you have to be analytical. You have to set everything, all of your emotion aside because you someone needs to be the calmest person in the room. And oh by the way, that's the CISO's job. When you first hear that news, you know, inside you get this little sinking feeling in your heart, probably, but but the first thing you have to do is step back and remember, look, you know, if we're a responsible company, we've tabletop this. We have documented policy and procedure and how to approach this. That's what we are going to do. We're going to get to the bottom of this and then you move forward. There's a saying if you're prepared, you shall not fear, right? So the more prepared a company is for the breach, then the better off things will be and the better you can handle that. And preparation is in a number of forms, right? We already talked about having policy and procedure, having things documented so you can pull a script up and follow it in the midst of all of that emotion. But I think also good preparation comes in terms of having excellent logging, exhaustive logging and knowing how to use it. So someone says breach. First thing I do is say, you know, that word is reserved for the c-suite and council to determine. We use the word incident and that's how we're going to handle this to begin with. And we'll let the leadership decide whether it is actually a breach.

Jeremy [00:08:26] The words we use to describe a situation matter a lot. And I think this is especially true when you're talking about a breach. And so you just said the only people are going to call it a breach or, you know, the c-levels and up. And to outsiders terms like security event or incident or breach or concern even they all sound like code words for the same thing. And while the insiders know that using the wrong word can lead to difficult consequences, the outsiders, they don't they don't get it right because it's just not something that these sentences don't have value.

John [00:09:01] When we see the word breach on an email or security incident or whatever else that's sent to us, because it's our record that's real. And that is also an emotional thing. Right? And it's frustrating. You know, we entrust our data to a company and the company didn't didn't fulfill their side of that trust. That can be that can be frustrating if you're going to force me to talk about it. Right. How do I handle that? I think the number one most important thing is to be forthcoming when you're when you are talking about that kind of security incident or or security event. I think what we've seen over and over again is the companies that try to sweep it under the rug or underplay it or, you know, pretend it isn't a serious issue. Those are the companies that really get sort of castigated in the press down the road. Right? So whereas the companies that are upfront about it and really open about it as open as they can be, those are the companies that weather it best and are best able to restore trust, right? I mean, the trust is lost no matter what the situation. But there's a there's a responsibility here to restore that trust with your customers.

Robert [00:10:12] There's this whole perception around companies that have had bad days or had breaches or had events. Yeah. Are they are they competent or not? I mean,

you have a breach, so you must not be competent, which really as a practitioner really offends me. But that's me, you know.

John [00:10:27] So the immediate tendency for most people is to probably think, yes, you are incompetent. And I think there are a lot of nuances. In, you know, in the world we live in today, especially in the news. Anything that hits the news, we want to boil it down to a quick [00:10:43]news [0.0s] soundbite. Are there companies that are incompetent in their information security? Absolutely. They're out there. Right? And they unfortunately, you know, they have shiny logos and they look to try to present themselves, just like the companies who are competent. Very hard to tell the difference unless you dig into it deeply. And that's that's one of our jobs in the information security world is to do that assessment of the companies we're going to do business with and make sure we're only choosing competent companies. Are there companies that are fully competent in our tech? Yeah. I mean, this goes back to the idea of a target of choice versus a target of opportunity, right? So the way I try to explain it is a target of opportunity is, you know, when a thief walks into a parking lot, wants to break into a car, they're going to wander around the parking lot. They know the telltale signs of what car to break into. And they didn't they didn't show up thinking, oh, I'm going to break into that 1978 Ford Escort. Right? But it it happens. When you are a target of choice that's when you're rolling into the parking lot in your, I don't know, Mercedes or your Explorer or whatever. And and the attacker says that is the vehicle I want to break into. And they will be patient, they will be persistent, they will look for the right opportunity and they will break into to you. And this is where a comprehensive security strategy is important because, you know, look, there are zero days announced on a regular basis. And if there are zero days being announced on a regular basis, that means that there are other zero days upstream in the pipeline, if you will, that we don't know about, that attackers do. And they're leveraging. So a security program that relies entirely on prevention is not going to be as effective and may come across as incompetent simply because even though it was a very advanced attack, it went unnoticed. The the best approach to protecting yourself and really developing your competence is to have a good preventive program, but also to have that detective program in place that that sees that anomalous behavior after access is gained and is able to close it down. That detective side of things is the difference between a security incident where someone gained unauthorized access but didn't make it very far and a full on breach where they owned your network for months and operated at will within your network and you never detected them. Right? So so I think I think that the competence thing is a branding problem in some cases. In many cases it is a problem that companies are just purely incompetent, completely negligent, that their security. But I think there are a lot of companies that are just a target of choice. A persistent actor goes at them, you know, month after month after month. And the best defense in that situation is to have a good detective program in place. So you can you can catch it when it happens.

Robert [00:13:42] You know, John's an interesting guy, and I can tell he's been doing this for a long time. I really loved his tip about reserving the use of the word breach for just the c-suite and council only. It's an important definition.

Jeremy [00:13:55] So here's a question for you, Robert. Can any good come from a cyber security breach for the company involved? There's definitely a lot of bad, but is there any possible good that can come out of it?

Robert [00:14:07] You know, I've talked to a lot of CISOs that have done this, been through these issues, experienced the pain of it. It's just no fun. And I think at the time, it just seems like there's no good that can come out of it, at least for that company. But, you

know, if we actually rise back up, we talk about trust in establishing trust, you know, sustaining trust. I think there is some good in the long run. Yeah. I think first and foremost, breaches come from vulnerabilities oftentimes that were not previously known to the company. In fact, you know, if I look back over the last five years, we've got two or three major system wide breaches that all began due to a vulnerability that was unknown. So it's kind of a zero day issue, and it created a whole class of engagement and energy around getting after that problem. So, you know, if we can learn from that and obviously patch the patch the software that's vulnerable, that's that's job one, obviously. But I think you have to go beyond that, say like, okay, if a vetted software is having unknown vulnerabilities, you know, what more do we need to do around the trustworthiness of vetted software? And I don't know that that's necessarily the victim companies issue. I think it's an industry wide issue to to get after. And if organizations can apply pressure and encouragement to the companies they buy software from to identify weak points, enhance their security as a result of these issues, it just leads to a stronger system and potentially better detective controls and the risk of future attacks being reduced across a whole all companies. What do you think about it, Jeremy? I mean, you know, what do you think in terms of good that can come from a breach?

Jeremy [00:15:45] So my first thought is about sort of the process that the organization goes through when responding to the breach and containing it and remediating it. It's not done alone. So they bring in experts. They bring in help from the outside. And in doing so, they benefit from the knowledge sharing and the collaboration it takes to get through it. And then when they get past it, the better ones are the ones who share what they've learned to the extent they can with peers so that others in the industry can avoid making those same mistakes. And they do that through participations in like ISAC groups and InfraGard and whatnot. Information sharing like this is what contributes to a healthier cybersecurity ecosystem for everybody involved. Given the choice, though, you know, it's still want to find other ways to benefit, obviously. And then I guess the other one I'm thinking of is at the macro level, all this breach stuff makes noise in the media, rightly so, but it creates the backdrop that's often needed to get cybersecurity regulation enacted where historically there might not have been enough momentum to get something over the finish line, but it was still very much needed. This kind of contributes to the momentum. It's necessary to get some of those rules that are desperately needed in place.

Robert [00:16:56] We cover even more with this and other topics in the second half of the interview, so let's get back into it.

Jeremy [00:17:04] So think about companies that that actually have seemingly robust information, security certifications and like they've got this compliance page that's stacked with all these factoids about they've got this cert, they've got that cert, and they look from the outside looking at that page or reading their, you know, audit opinion or certification report. That company looks like they got it together, and then they get breached anyway. So from the perception of the the relying party of those reports, the people reading those reports and then seeing that company's name in the paper a week later, can information security certifications sort of give false assurances if the company gets breached while they got a live certification?

John [00:17:50] Yeah, I see where you going. That's that's kind of a can of worms actually to open up. So, look, there are some assurance programs that are like, well, you tell me what security controls you want to have in place. I'll check in and see if they're in place in an effective manner. In an egregious example, you could see a company that doesn't really look at that collection of controls and say, oh, this seems like a reasonable set of

controls for what you do, right? And they just assess on what's there and we're done, right? And there's a big gap, right? That's egregious. I think in most cases we do see this happen a lot. We've seen some really interesting things occur with this, right? There was a PCI breach where the you know, they had been issued a certification. Once they breached, the certification was revoked. And they were it was instantly assumed that they falsified their information to pass the certification. Right? And I think that that's a that's a false conclusion. But again, if you have a persistent actor that is incredibly sophisticated, you could follow to the letter every single cybersecurity certification there is and still be successfully attacked. In fact, it doesn't take that much sophistication to fish your employees. Right. So you may have all of those certifications and your your loose end is in your in your employee group somewhere. You can look at assurance in a variety of levels where the first level is just I saw that they have a SOC report. I didn't read it. I just assumed it meant they were good. Right? And you can progress from that to oh, I read their SOC report. You know, I had them answer a few questions for me. I had a I had them provide some evidence of their answers or I had a third party go in and rigorously test them. And, you know, there are based on the risk of the data that you're sharing with that company, then you have varying degrees of assurance that you want to go through. Right? So if I have a company that's storing historical podcast for me and they get breached, I'm not really that concerned about it. So I'm not going to put that much effort into vetting them in the first place. Whereas if I have a company that's processing PHI data for me, yeah, you can bet that they're going to get a very rigorous review and have high expectations on an ongoing basis.

Jeremy [00:20:12] As it should be. Yeah, different inherent risks for different organizations you share data with and that the strength of the assurance needs to match. And yeah, we've talked a lot on this podcast I'm sure will continue to about kind of the different assurance mechanisms out there, starting with none when they should have had some and all the way up to really robust assessments backed by teams of assessors sitting in the conference room months and months. And that spectrum in between is tough for companies to navigate.

John [00:20:40] Let me- let me do a follow up on that answer, actually, and go a little bit deeper, though, because, like, you know, the question is if if you passed an assessment and you get breached, was the assessment false or what? And look, I think, again, this really calls out the need for a broad security strategy. A lot of our assessments assess primarily for the presence of certain technical controls. But really, again, if you're managing security from a risk based perspective, you should be looking at all of your risks and you're going to look beyond technical controls. You're going to look at your policies, your procedures, your processes, how you treat your employees and how you educate your employees. You're going to have a wider range of of controls in place beyond just the technical controls. And so that really like from one you know, from one perspective, from looking at a company to do an assessment of them to do business with them, if I hear that they have that kind of maturity in their program, I'm feeling good. Secondly, if I look at a security assessment framework that requires that level of maturity in the program, I'm also happier about it, right? So end is more descriptive or prescriptive in the program, right? So I don't know if this is a place to make a pitch for a HITRUST or not, but the thing I like about HITRUST is that it is more prescriptive. It doesn't say, "Hey, you tell me what controls you want, and I'll tell you whether they're there and they're effective." It's more like, look, you know, based on the data you have and the industry you're in, these are the controls that you really should have in place. So I feel there's more confidence in that kind of assessment.

Jeremy [00:22:19] Yeah, I appreciate that. The breath of HITRUST assessments is pretty consistent, and it's the depth of HITRUST assessments that differ based on whether you're sharing PHI or not, cardholder data or not. But that breadth of where I was going to ask about the information security program, I was going to talk about a bit about privacy, about TPI controls and, and on and on, there's this breadth. And you're right, you can't take just logical security as a slice and expect to extrapolate that across the maturity of the whole companies. You just can't do it.

Robert [00:22:47] Thinking about public perception around all this. You know I guess two questions. The first is maybe something that is surprising to you about public perception and media treatment of breaches has been changing over time. Do you do you see it changing? And if so, how?

John [00:23:03] Okay, first I'm going to put my grumpy old man hat on, and I just I just cannot stand the fact that every major security thing now gets an icon.

Jeremy [00:23:12] What you mean?

John [00:23:14] Right? Like like Heartbleed got an icon, in Log4j got an icon. It's it's like, really? Come on. I don't know. Anyhow, that's.

Robert [00:23:22] It's like a marketing program for breaches.

John [00:23:24] Exactly. It's like a marketing program. It's so sophomoric, right? I mean, it's just literally so sophomoric that like, okay, you know, we're going to we're going to we're going to rally around this image. Anyway, so that's that's neither here nor there.

Jeremy [00:23:36] Well, it's it's not a black hoodie with just the back of the the head on the keyboard in the dark room.

John [00:23:41] There you go. I mean, I think look, we live in a we live in a especially in the United States in a very litigious society. Right? And we live in a society that the shrillest, loudest voices heard the best. And we live in a society where media is driven by clicks. So I think there there one thing that you can see happen is that a major breach ends up in the spotlight. And I don't want to try to undersell the impact of the breach, but what I would say is that people are just dragged through it. Organizations are dragged through the mud in this process. Right? So the scrutiny there's a couple of problems here. Number one, there are a few reporters who are very aware of cybersecurity, cyber overall information security practices. And you can trust articles that these individuals will write. In many cases, though, reporters are not really sure what they're talking about and will jump to conclusions. And we'll sort of make it seem like it's worse than it really is. I think, though, key here and we've talked about this a little bit early on, how the company responds to that breach and to the publicity around that police breach really determines that company's future in many cases. It is somewhat surprising to me, though, how many companies just get to move ahead and, you know, so they do behave egregiously. The breach happens and then it all goes away and they manage the PR campaign pretty well and they move forward. So I know I'm kind of talking out of both sides of my mouth here, but I think we just see some cases where companies are overly beat up and then there are cases where they're they're they you know, maybe they should have been beaten up more. I think, and Robert, you could probably talk with this to this with me a little bit. You know, back in the 90s and 2000, especially the 2000, we talked a lot about how a breach is a is like a company changing event and it costs a fortune. And we use fear, uncertainty and doubt to

sell security programs or tried to. What was interesting is you look at the major breaches that happened and there aren't as many publicly traded companies that went out of business as you would expect based on the fear, uncertainty and doubt that we talked about back then.

Robert [00:26:02] You know, it's a a sure reputational risk.

John [00:26:06] There are companies that do go completely out of business, right? So we had the we had the collections company from a couple of years ago that suffered a catastrophic breach. And they they filed for bankruptcy. Right? So these things happen. And it's the smaller companies that get it the worst. And in many cases, they're companies that are either not insured or are underinsured for the event that they that they experience.

Robert [00:26:32] Yeah, we typically don't talk about specific companies here. I am going to talk about two companies for a moment because they both chose to engage the public domain. I go all the way back to the beginning of what we call advanced persistent threats when RSA had their event. And I remember I remember very distinctly them taking a leadership position in the industry to say, this happened to us. We consider ourselves pretty credible and we're going to teach the industry how it worked and why it happened. And I really thought, I've always respected the leadership that Art Coviello was the CEO there at the time, the leadership of him and his team on that. And I remember Mandy had just a few years ago as well, having a similar situation where, you know, they stepped into it and, you know, said, hey, this is happening and we're going to be really upfront about how the attacks operate and how they're exploiting us. I've always felt like companies that took that approach, you know, were seen as engaging in social good, trying to make good come from these bad things, which I always respected.

John [00:27:31] And I think in both of those cases, they had a little bit of an advantage and an easier ability to take that approach because their audience was technical and understood what they were talking about. If, you know, if a if a major automotive company went through a similar breach and tried to come into the public domain and start talking about these attacks that had occurred, you know, I think that they would lose the attention of the press and people would just be buried in information and wouldn't understand it. So it's a it's it's a good strategy. I think it can't be copied exactly. But what can be followed is an open strategy where there's good communication, here's where we're at, here's the situation, here's what we know, with, I think, less of an emphasis. I think what you see in the communication that comes out today from most breach companies, you can see that the that attorneys have written that with the future in mind. And and that is I think the tension. It's like how open can I be without putting my company at further financial risk in the future for class action lawsuits or other sorts of fines and penalties because I admitted something early on. Right? I think the other problem with this is, well, there are some companies there was a company that went through a breach recently and their breach notification process took over a year. They put on the air of wanting to be very open about it and they would produce releases that talked about, gave an update and there was nothing in them. They were like a nothing burger. Right? And that went on literally for almost 12 months. Right? And that kind of made that company a laughing stock in terms of the way they did it. So this is very nuanced. And I think in this situation, companies, companies need to be super careful about how they communicate. And that's why I said, like, you know, as the CISO, I don't want to be the one writing the communication because it has to be, I don't want to say wordsmith carefully, like we're trying to use words to hide what happened. It has the communication has to be crafted correctly for the target audience. And you may see multiple communications, right? One that goes to government

agencies and says, Hey, this happened. You would have won that goes to your customers and you might have one that goes to your providers.

Robert [00:30:02] Given the number of letters I've received personally, you know, I think many of us have seen those letters. Yeah. The question I have is, you know, do people still care? You know, is there still the same level of, you know, I had an issue, I got breached as a feel good, or is it just sort of like another thing I get in the mail.

Jeremy [00:30:18] Or is there just this gradual numbing that we're nearing the precipice of.

Robert [00:30:23] Maximum breach? That's a terrible thing to say, but yes.

John [00:30:26] Yeah. So I think don't care applies in a certain way. So I think everyone cares. Like if I if another company breaches my data, I care. At the same time, I think people are at the point where they're like, what's the impact? Like, you know, major credit unions who have all of my information have been breached. What more can be released to the general public. Like maybe an updated photograph that shows how many more gray hairs I have now. But, you know, like that data is out there already that that that that cause already out of the barn, if you will. So I think they care. But I think people recognize like that the impact is already pretty high because of what's been breached today.

Jeremy [00:31:11] So this this week this as we're recording this really recently there was a state the DMV got breached, and I have a lot of my family lives in that state. My aunt calls and she's older than me, younger than you guys, just to gauge where she's at. And she said, "Hey, I don't, I got this letter and I don't really know what to do with it. You're in security, right? Apparently, my data got breached. What do I do?" And I'm okay. I think I'm pretty sharp on this, but I was kind of at a loss. I told her, like, accept the credit monitoring when they offer it, because they will, lock your credit. Like you should lock your credit anyway. Freeze it, I think is the word at the top three. I really know what else to say. Like, I'm not going to say stop using that company because they can't. It's the DMV of the state, right? Yeah.

John [00:32:00] DMV. What choice do you have?

Jeremy [00:32:02] So did I miss the opportunity to give a nugget of advice that I should have?

John [00:32:07] I would say the one piece of advice I would given in addition to that, you know, you've already said like, okay, you know, get your credit monitoring going, lock your credit. But I think also would be increase your vigilance in your email and in spam in text messages and and things like that. Like be on the lookout for people using your data to address you and try to fish you or social engineer you into doing something. That would be the one the one additional piece of information that I'd offer.

Jeremy [00:32:39] Do you feel like there's there's ground that we need to cover that has to be said by way of breaches?

John [00:32:43] No, I think I think the only question I think that I would have thought you would ask that we did and we still kind of touched on and that is like, what's the first thing you do when you suspected a breach? And my answer is breathe. Right, stop and breathe, count to ten, and then go to your policies and procedures. Follow it. You have a plan for a purpose. Follow the plan and you'll get through it. Right? Ask for help. Right? If

there's if there's two kind of insurance policies that you can spend on in your company, one is cyber insurance, the other one is incident response. Find someone who knows how to do this and does it day in and day out because, you know, your company's future may depend on it, but also the data that you're entrusted with, you know, there may be ways to contain and prevent additional breach and protect the rest of the data. And there may be ways to really figure out who actually got breached and who needs to be notified versus we're just we're not sure, so we're going to tell everyone.

Robert [00:33:49] You know, thinking about all this, there's an asymmetrical advantage at play here. It's kind of a cliche, but I truly believe this. You know, defenders must get it right every single time. But attackers only have to be good once.

Jeremy [00:34:04] But attackers aren't the only cause of breaches. But, you know, sexy to think, you know, the James Bond guys coming after my network and I got to do everything I can to defend it, but it's not always the case. So I recently finished this book, great book from 2021 called Big Breaches: Cybersecurity Lessons for Everyone. And in the book, they did a bunch of analysis of all this publicly available breach data, and they rolled it down to six main root causes that contribute to the vast majority of breaches out there. Phishing, malware, third party compromised, unencrypted data, software vulnerabilities and invert inverting employee mistakes.

Robert [00:34:42] What this really tells me is pretty much the stuff you can take care of by basic blocking and tackling stuff. You know, the stuff that's just good hygiene and maintenance. And lack of security, hygiene and lack of security foundations has led to many, many breaches.

Jeremy [00:34:56] Yeah, and that's the root of the problem, I think. No one wants to do the boring hygiene and maintenance stuff. Even though hygiene is foundational to cybersecurity, it's not hard to see why is ignored. Given the choice between spending time building an inventory of all the assets and endpoints in the environment, or building that same time innovating around a new feature that your customers will get excited about. Most organizations are going to pick the latter.

Robert [00:35:21] And Jeremy, you and I learned this, there's no common definition of good cybersecurity hygiene. There's a few attempts at it, but there's no consensus yet. And that made it really hard for for us to do the work early last year to decide what to include in our essentials assurance level, a one year certification we introduced very early this year.

Jeremy [00:35:40] Yeah, and building the control list for the e1. We did a whole lot of research into this question of what constitutes cybersecurity hygiene and kind of what the general perspective is for what's in and what's out. And in that we got a lot of input from CISOs and auditors and vendor risk management teams. We also pulled in a lot of threat data available to us and all that stuff together really heavily influenced the control selection for our Essentials Certification. And that's why you see stuff like anti-phishing and anti spoofing controls like DMARC and DKIM. But again, that's a real challenge. What constitutes good cybersecurity hygiene, knowing that it's a major contributor to breaches?

Robert [00:36:21] I've done a lot of third party risk management throughout my career, and we oftentimes think of third parties as just the vendors or just the suppliers, not that they're just anything, but it's really too narrow a view. I mean, if you think about, you know, the way systems are put together, you know, third parties can be can be everybody and

everywhere. And when it comes to preventing breaches, you know, anybody that's in your system or making up part of your system, whether they're a supplier or they're just another constituency that you work with, is a door to your data. And, you know, everyone thinks about and accepts that you vet your security suppliers, everybody thinks about it, sort of accepts that you vet your supplier security before you give them sensitive data. But what about the customers that are coming in and working around your system or the joint ventures or the partners where you exchange industry data between several companies? That's a system and it has vulnerabilities potentially.

Jeremy [00:37:16] Yeah. Your customers is is an interesting one is one of my big takeaways from the book. I'd never, the lightbulb never went off that there's a scenario where you have to reach out to your customers and say, is your security good enough? There's a good example in that book, and it was it helped me a lot understand even that scenario in the customer's scenario, it can matter sometimes. So there's a very large data broker selling marketing databases back in 2017. One of their customers bought this enormous database from them and that customer was breached, and it was really clear where that database came from. Big player in the space, no question. It was that, proprietary data set that was breached. When that breach happened, it wasn't the customer's name in the headlines, it was the data brokers. It was their set. So it's not always just downstream to your suppliers and vendors. It can be upstream to your customers too. Something else I want to bring up from that book, let's take a long view of things. So the Internet was born in 1983 and it's been sort of commercialized for the last 20 years or so. Cars were invented in 1886, but rearview mirrors weren't invented. It was patented until 1921. And rearview mirrors didn't even become standard equipment until the mid 1960s, like 80 years later. And three point seatbelts weren't patented until 1955, and they weren't mandatory until 1968. So another 80 years, Right? So from that perspective, how many of the most important anti breach safeguards haven't even been created yet?

Robert [00:38:51] You know, thinking about car safety, the sentiment and momentum needed to push through regulations, it wasn't possible until there was just enough evidence that it was needed. You know, unfortunately, enough car crash data and enough preventable entry and death. A super sobering thought, but here we are.

Jeremy [00:39:09] And what was that stat was said at the start of the episode? 20,000 reported breaches, which we think is just the tip of the known iceberg. The knee-jerk reaction from punk rocker [00:39:19]Rebel In Me [0.4s] is to fight against anyone telling me what to do or how to operate. But with numbers like those, it's it makes me wonder how this whole self-regulate and self secure model of I.T. security is really going.

Robert [00:39:31] Thanks again to John Overbaugh of Alpine Software Group for a great conversation.

Jeremy [00:39:35] Yeah, thanks John.

Robert [00:39:37] We sure hope you enjoyed this episode of Trust vs and we hope to see you again. Have a great day.