07 Trust vs_Omar_v2.mp3

Omar [00:00:02] I found that it's really, really hard to figure out how to actually risk stratify your vendors, especially when you start to look at the data and when you look post-incident, does it actually past your past your test in terms of how you adapt risk stratified it?

Jeremy [00:00:23] Welcome back, everyone, to another episode of Trust Vs. I'm Jeremy Huval, innovation officer at HITRUST.

Robert [00:00:29] And I'm Robert Booker, strategy officer at HITRUST.

Jeremy [00:00:32] In today's episode, Trust Vs Third Party Assurance and the voice you heard at the top of the episode belongs to Mr. Omar Khawaja, a highly respected CISO in the industry.

Robert [00:00:42] That's right, Jeremy. Omar has been a trailblazer in the cybersecurity field for many years. He's currently field CISO at Databricks, a leading organization that does data and AI. And it's just always a pleasure hear his insights and learn from his experiences. I think his experiences are really valuable because prior to Databricks he was the CISO of Highmark Health and he's been a member of several boards, including the HITRUST Board of Directors.

Jeremy [00:01:07] Yeah, and I think the FAIR Institute as well, they focus on quantitative risk analysis in that key space. Yeah, and these are just examples of how Omar has been an advocate for effective security assurances and effective IT risk management for a long time now. Today, we're discussing with him, like I said, third party risk assurances and how third parties can better communicate the strength of their security system and cybersecurity programs to customers and other stakeholders. And we talk about the fact that these kind of assurance communications are not all the same. Some are good, some are not so great.

Robert [00:01:43] Yeah, it's a really important topic and and one that's really at the top of mind, given everything we're seeing across the industry right now and have been seeing for the past few years. As you just said, it's not a secret that these reports and assurances are not all equal. Some are quite good. I mean, some can get into incredibly valuable insights, help install confidence, help all parties in a relationship, know whether systems are mature or not, but others just aren't enough fall short. And I think Omar really gives us a great lens on the essential elements of what makes effective communication and how to look at the whole system across build through such assurances.

Jeremy [00:02:21] Yeah, and we talk about how to balance this or that, the ask around strong assurances with the risk kind of introduced by working with that third party. So, you know, it's a long standing approach to where you ask less of your lower risk third parties and ask more assurances, stronger assurances, harder assessments, longer assessments of your higher risk third parties. But it's kind of cool to hear Omar challenge that whole concept, and I think it's time to challenge that concept because we see more and more big breaches happening from organizations, third parties, suppliers who nobody was calling high risk, right?

Robert [00:02:59] I think that's right. And, you know, just looking at the past models, it's very obvious that we we need to think in a different way about these problems. And, you know, we also need to just think about what we mean when we talk about third party risk. I mean, you know, am I talking about vendors? Am I talking about suppliers? Am I talking about business relationships I have we're we're equal parties, but we work in a system? Is it the vendors of vendors, what some people call fourth party risk? You know, it's it's just a really complex space. And I think for the purpose of this conversation, let's just let's just refer to anybody that I exchange information and connect my system to is a third party, regardless of who they are and even regardless their risk classification, how did Omar gets into some of that and just I think it's an area that we can all learn from.

Jeremy [00:03:42] Yeah, I like that. So we're kind of scoping out the people that are pushing the lawnmower out front, but we're scoping in, you know, systems that maybe host your podcast or update your website that might not touch in traditionally covered data. We're acknowledging that even parties like that still have a risk. Right? Yeah, Omar's got some practical application of his learnings that in the space throughout the years that he shares with us and we talk about. For example, questionnaires are the good or bad, do they fit and they need to go away And we got some opinions on that that we shared and it was cool to hear his thoughts on that. We steered the whole conversation toward pragmatism and sort of how we apply this.

Robert [00:04:22] Yeah, I think I think that notion of finding the right approach to streamline the process is right for all of us. And it was a great and informative conversation. So let's just get into it.

Jeremy [00:04:33] Yeah. Without further ado, here's Mr. Omar Khawaja talking about third-party risk management.

Robert [00:04:42] So, Omar, it's really, really great to to spend time with you again. We've we've done a lot together, I think shared the stage at least once, you know, talking about CISO stuff. So thanks for, thanks for being with us. And and thanks a lot for the energy and the leadership you've given the industry for a long time. I know you've been out there kind of, you know, blazed the trail with a lot of a lot of things that you've done with your company and and now your new company. I know, I know you're with the new organization Databricks. So, you know, tell us tell us a little bit about kind of the Omar story, where you're from, what you what you've done, you know, what you're doing now. You know, just be curious to kind of get an update on kind of the world around weather and what's going on.

Omar [00:05:20] Yeah, Robert, it's it's great to be here and I've always enjoyed working with you and I've done things until I felt like I got bored and I got pretty good at something and I realized I wanted to go do something else. And I had a variety of different roles across security for many years until I became a CISO and every role prior to becoming a CISO I did for less than less than two years because that's pretty much how long it took me to get pretty decent at those roles and get bored. But it took me about nine years before I felt like I was I was a half decent CISO and I didn't feel like I had nearly as much to learn in the in the subsequent years. So I said, I'm going to, I'm going to go try something new. And the data and AI thing has been pretty big for the last couple of years and it's been bubbling and I just had a lot of FOMO around everything that was happening in the data and AI space and I felt like I didn't know enough about it. I didn't understand it well enough. And having an opportunity to work for an organization like Databricks, that is one of the leaders in the data and AI space providing enterprises with the platform on which to do analytics and machine learning, it sort of forced me to really understand the data in AI space, and now I get to work with CISOs and organizations across the planet and help them go down the data at [00:06:49]AI journey [0.0s] and help them with what their challenges. So I feel super fortunate that I get to now make make an impact across more than just one organization.

Jeremy [00:07:00] What makes a good assurance mechanism? What are the things that are essential to delivering good assurance versus deliver a message just off the mark? What characterizes the sort of the mediocre trust in assurance communications from those that are really meaningful, impactful?

Omar [00:07:18] Yeah, I think a few things. I think, one is understanding, you know, why you need assurance, why you need confidence or trust in a particular system and how it's going to perform and how it's not going to do the things that it should not it should not do. And once you understand sort of the implications of poor performance or adverse adverse reactions or adverse outcomes so you understand the risk profile of that system, then you could say, look at this system, I need a lot of assurance that it's going to it's going to operate appropriately versus this other system here. Maybe it's a dev environment, maybe it's got a smaller customer base, maybe it's we're operating at a non-regulated, regulated customer base, whatever it is, it's low risk. So one is aligning the assurance level with the business value and more importantly, the negative business value that can be created if something goes awry. And then being able to demonstrate that the assurance level that you're picking, the controls that you're picking, and then the process that you're going through to validate that those controls are in place are appropriately tied. Sometimes as a security person, it can be very compelling to think the more controls the better. But the reality is, as CISOs, we shouldn't be thinking as security professionals. We should be thinking as risk professionals, because too many controls means that the business is using resources in a security program where they're probably better being used elsewhere. So your security should be at the risk tolerance level of the organization. Not much higher than that, not much lower than that. But in the case of health care, in the case of financial services, in the case of any sort of organization that is working on systems and working with data, that's fairly consequential, that's fairly sensitive. In those cases, what you're looking for is you are looking for a high bar. If I'm going to give you my sensitive data, I want to make sure that you're setting a high bar for yourself. I you know, the conversations that I would have with my vendors that would be most concerning were the ones where they would tell me that security is hard. Right? That is the fastest way of eroding trust with your customer is to tell them it's too hard. And my response to them would be, "Hey, if you're telling me it's too hard, it's too expensive for you to adequately protect my data in the way that I and my customers expect it to be protected, I think you might be in the wrong business." Like, if this is hard, you should not be in this business. On the other hand, you have vendors that you come across that are always trying to raise the bar, trying to do more, and I leave in conversations with them feeling like, "Wow, these folks care about our data just as much as we do. And that that feeling that sort of is to me, the ultimate in how I build trust or how I, I perceive trust with my vendors. If is if I feel and if I'm convinced that they care about my data more than I do now, I'm willing to trust them because they're working hard to earn it.

Jeremy [00:10:40] Yeah, I can appreciate that. And you brought up an interesting area dealing with sort of the way trust is communicated between vendors and you as a business. Right? And we hear a lot about, you know, organizations. We're going to focus a lot on the higher risk vendors. We've had previous conversations about maybe that's not always the answer because insurances can be important to classically defined lower risk vendors. I think there's been a lot of high, high visibility breaches of maybe made that more apparent. Can you speak a little bit about that?

Omar [00:11:12] This was one of the learnings. Early on I did what made perfect sense, which is you stratify your vendors and you've got your high risk and you've got your medium risk and low risk and you apply the greatest effort to the highest risk ones and the least effort to the lower risk ones that makes perfect, logical, rational sense to do until you start paying attention to the vendors that have breaches. And you realize that almost none of the vendors that you put in high risk are having the breaches. A lot of the vendors that are having breaches happen to be in low risk. So if you, you know, look at a UKG or Kronos for for timesheets and time management or you look at SolarWinds for network line or during network management or you look at log4J or you look at MOVEit that for file transfer. I don't know of many if any programs where any of those vendors were classified as high risk by any of their customers, yet they happened to be very, very consequential. Now, you know, there's one of two things going on. Either we're doing such a good job protecting our high risk vendors that none of them are actually having breaches or we're doing a poor job classifying our vendors and many of the vendors that are having breaches. We learn after those incidents that they work more consequential to the business than we thought that they were. And so I, I found that it's really, really hard to figure out how to actually risk stratify your vendors, especially when you start to look at the data. And when you look post incident, does it actually pass your past your test in terms of how you adapt risk stratified it? So I find that most programs that risk stratify vendors do it fairly poorly. I could tell you when I did it, I did it pretty, pretty poorly, and I ended up just throwing that out the window. That's and the other reason is I may have a vendor that the business starts off by saying, "Hey, they're only going to get 100,000 records of PHI we're doing a small test with that." I don't know many organizations that are that good at figuring out when the business goes from 100,000 records to a million or two or five or ten, because once the approval is done, you know, it's a slippery slope. Stuff happens. Not that anyone means what it means ill or is being malicious or being deceptive. That's just the way large enterprises work. And so they go and become a big vendor. But you classified them as a small vendor. Now, how do you solve for that problem? And I think if our asset management is imperfect, our data management is imperfect, we most enterprises operate in an imperfect world, I think taking the approach to say, you know what, I'm going to try to figure out how to scalable address more of our my vendors and effectively set the bar pretty low for what it means to be a high risk vendor.

Robert [00:14:14] Yeah, you said something interesting scalabily address. My vendor set the bar appropriately for the vendor so that that makes a lot of sense to me. So the journey from where you were, you said, okay, I'm going to move from stratification to where I believe you went. How do you make that journey happen? You know, what's the message? How do you talk to your board? You know? Well, what was the process behind all that?

Omar [00:14:40] Yeah, Robert, I think the first part was figuring out how to set my ego aside and, you know, going from trying to build a third-party risk management program whereby I've got a team, we've got a team in the enterprise that is doing all of this work, doing it by hand, one vendor at a time, one questioner at a time, one onsite audit at a time, and realizing that that isn't working as well. And I think that's one of the hardest things as a leader to do, is to accept that I got it wrong and now I'm going to pivot and do it in a totally different way. Like the conversation went something like. I think for me the aha moment was right after a lot of health care organizations were having breaches and I got asked to get in front of many, many of our customers and talk about what we're doing to adequately protect the organization. And as is the case with security, you know, whenever you solved one problem, then you have a next problem to solve. And so I hadn't I was running a pretty strong security program, and I felt pretty comfortable going in front of our customers and talking about our security program. And I could wow them with charts and numbers and data and roadmaps and accomplishments. And I had a customer ask me this one simple question. They said, "Omar, if you're saying that the HITRUST common security framework is the highest bar in the land when it comes to security controls and protecting data within the four walls of Highmark. Well, why isn't that the same bar you're setting for your third parties? Like, why does it matter if our data is within Highmarks data center or Highmark sends it to one of their third parties and it sits in their data center or their cloud". And I had no good answer for that. And what they basically pointed out to me was the flaw of my thinking of within my four walls I set the bar way up here, but outside my four walls, I just have a contract and a questionnaire. And I basically set the bar an inch from the floor. That just made no sense. And the moment that sort of question, I internalized it. I was like, I could not think of any logical response to that other than if the bar to run our security program effectively was for it to be HITRUST certified, then the bar for any third party to have access to our customers PHI should also be for them to be HITRUST certified. And that's sort of the conversation that I took to my fellow executives at the company, and that's what I had the conversation with the board. And when it was framed that way, the answer seemed very obvious to everyone.

Robert [00:17:19] I'm going to pivot a little bit and get into a little bit of the mechanics of all this, because I think some of our audience are people that just want to figure out how to get it done, get it right. And so kind of stepping into that space. So some of these may be areas where maybe we still need to get it better as an industry. So maybe not just depends on the topic, but, you know, like we we know from talking to a lot of companies, there's all these tools out there, you know. You know, there's different kinds of assurance reports or compliance reports or even compliance as a system at large. Thinking about questionnaires, for example, you know, to the point earlier, maybe lower risk, we do less. So we send out a questionnaire, we get an answer back. You know, how how do we think about the value of a tool like a questionnaire, you know? Any thoughts on that?

Omar [00:18:02] I used to think highly of them in the beginning. And then when you're sending out questionnaires, it feels like they make a lot of sense and we send them out like they're amazing. But when we receive those questionnaires, it becomes very obvious that they're a waste of time. And most organizations do both. And yet there's such a schizophrenic relationship with questionnaires. When you send them out, you feel like they're valuable. But when someone else sends you their questionnaire, I've yet to meet any security organization that says, "We love getting all these questionnaires and they're such a great use of our time." And then, of course, I'll ask them, "Do you send out any questionnaires?" And they're like, "Let's not talk about that." And, you know, that's that was my organization. We would send out the questionnaires and think that was an awesome thing to do. We would receive them and think that they were a total waste of time. And that dichotomy, that just felt odd. And so we reconciled that by saying, if we don't think they're good to receive and fill out, then why are we forcing and victimizing our partners to do the same? And I think part of it was thinking of our vendors differently. So if you think about your vendors, as, you know, we pay them a lot of money and they should do whatever we tell them to. I think that's the wrong mindset. If you think about your vendors as these are organizations outside of yours that different parts of the business really find that they deliver value uniquely, that cannot be gained organically within your own four walls, and you start to think of them as partners and you start to have empathy for them and you start to have some humanity for them, you realize, well, why would I inflict pain on you just because I can? How do I do this such that the ecosystem benefits and not just do something because it's convenient, because it's easy, do it because it's actually going to deliver value. So so I am so we very quickly ended up pivoting away from questionnaires, primarily because, you know, I mean, I'll give you one simple example. In the early days back when everyone didn't have encryption at rest, you'd get a question that would say something like, "Do you encrypt data at rest?" And I remember once saying to one of the engineers on my team, "Hey, can you just go to Best Buy, get a USB drive and put TrueCrypt on it?" Check. Yes, we have encrypted data at rest. Right. But is it the right data? Where's the data? Where's the key man? I mean, there's like ten other questions you have to ask to see if there's actually real value there. But a questionnaire, you can say yes to everything with very little effort. It turns out that, you know, if we're thinking that that's what every other recipient of a questionnaire is thinking too.

Robert [00:20:54] Yeah. So, yeah, we thought a lot about the the basis behind people checking the box on a questionnaire. Like, you know, it's almost giving, you know, giving the respondent the opportunity to say, well, you know, I know what the context is, I must say yes. So I could find that. Yes, I could find that yes at my organization. So that's great.

Omar [00:21:14] So yeah, and I think like this goes to Robert, almost like that bigger question of, you know, it's stuff like this that gives compliance a bad rep because now you're doing something for the sake of the check in the box versus recognizing that, you know, every control that shows up in any compliance regulation, any compliance standard. Someone genuinely believed that this is going to help deliver more value to an organization, reduce risk, increase availability, increase reliability. There's going to be some kind of value if we don't understand what that value is. And oftentimes we just focus on can we just get it done? Can we get the check in the box versus asking the question, what is the value? What is the point of it? When we ask that question, we almost always find that there is some business value in compliance. And and I think sometimes as leaders, we allow our teams and ourselves to get away with with devolving compliance to just the check in the box when it's absolutely not intended to be a check in the box. It's actually intended to deliver value. But when we continue practices that we know in our own heart of hearts that they deliver zero value, then yeah, of course, who's going to enjoy being being compliant versus actually reducing risk? One of the things that I've always grappled with and I feel is fairly unfair is when we talk about incidents, we don't make this distinction. And I think whenever an incident happens in an organization, it likely happens because of one of two reasons. It happens because the organization had a weak system of controls in the environment where the incident happened or it happened in spite of the organization having a strong system of controls. However, the adversary just happened to be very persistent and very willing to use lots of resources and time to to break in. And I think that's an important point. So, you know, I always I would say to my board, if if we have an incident because I'm running a negligent program, that's horrible. If we have an incident in spite of us running a strong security program, I'm not going to enjoy that day, but I'm going to be willing to sit in front of the board, in front of the judge, in front of the customers, in front of my boss, and explain very confidently, here's what we did and here's why we thought that was reasonable. And I don't think in the press, in the media and in the world of sound bites that we live in today, we make that distinction. There's sort of is this almost automatic conclusion. If someone had an incident, it must be because they were running a poor program. And not that there's any shortage of organizations that are running poor, programs that have incidents, but occasionally there are organizations that are running strong security programs and still have incidents. And, you know, the metaphor I use is even Volvos get into accidents.

Jeremy [00:24:25] There's an acknowledgment that, look, we did a risk analysis, our likelihood of that threat, we pinned it and that threat came to fruition. Now we've got to readjust our perception of the likelihood that threat. And it's got to be evolving, but there's acknowledgment, like you said, that, look, Spider-Man can climb over any wall no matter how high. And there's Spider-Man's out there.

Robert [00:24:49] So, Jeremy, always great insights and talking with Omar. So just reflecting on all that, what did you take away from the conversation?

Jeremy [00:24:57] Yeah. Underpinning all of it is the importance of creating a good, strong working relationship with our vendors and third parties. And one that's sort of equitable and fair, and Omar talked about empathy and it's something we kind of forget about as we try to stand up these rich, robust processes to, you know, chase down every corner of risk. And you can't go into it with the mindset of they need to do what we ask them to do because they work for us and they pay us a lot of money. That's that's a flawed approach. And you also can't expect of your third parties more than you expect of yourself. So you can't say you're going to get the most robust, stringent cybersecurity certification there is, where you also don't expect that of yourself, right? You tend to prevent them from being the lowest, weakest link in the chain, and they're not going to be a stronger chain than you. That's, you know, you can't expect that. That's not how positive working relationships are built. Instead, I think you have to remember that their partners, their collaborators, they're important to your business. If we really want to get the right level of assurances in line with the risk that they really carry, you have to work with them to make that happen. And you have to have the right assurance mechanisms at our disposal that you can mutually agree upon.

Robert [00:26:13] I don't think we can set a high bar for every single vendor because they have different levels of inherent risk to the business. You know, they are different, they do different things. And at the same time, you can't just rely on a very low bar for vendors who have historically been considered, quote, low risk in quote. And I think Omar really nailed that point when he talked about how low risk vendors experienced breaches. And if you look at the recent high profile breaches he mentioned, you know, involving things like web based file transfer apps, which we're dealing with at this moment when we record this episode, you know, the size and scale of those breaches show us and show the industry that even those lower risk vendors have a super big blast radius when they explode. So I think we've really are learning and continuing to learn that, you know, letting low risk vendors just get away with a pretty low intensity or low level of assurance approach, you know, maybe even just a, you know, answers without validation to questionnaires and assessments, just not the right approach.

Jeremy [00:27:16] So what's the fix, though, for those low risk vendors that we're kind of collectively acknowledging they're, you know, maybe more consequential than we thought they were? You can't put every single third party in the critical category and expect the highest for [00:27:28]area on. Can you? [0.4s]

Robert [00:27:30] No, no, that that's not going to get us through, I think. So, I think we need to think about vendor tearing with a more pessimistic view of what could go wrong, you know, because of an unexpected, you know, outcome. So really thinking about it from a business risk perspective. So, you know, I think most everybody does here their third party relationships using inherent risk factors. You know, we advocate for that. But, you know, it's it may not be sufficient to consider factors only focused upon data exposure, like how many thousands of records of information do we share with them. You know, if you look at ransomware, you look at some of the data extortion events that are occurring, you know, it's the it's the catastrophic impact of business operations that really impacts the industry. So, you know, you have to think about like does the visibility of the vendor and the the fact that they are granting a high level of access to the management plane of the system, you know, create a valuable target that attackers would use, you know, to attack hundreds of thousands of organizations. So if you look at some of the management, management infrastructure vendors being attacked and, you know, correlate that to the fact that some of those attacks are impacting federal government and state agencies for example, you know, you could say, well, those are probably attractive to certain certain malicious actors. And, you know, companies can get caught up in the blast because they're using the same technology.

Jeremy [00:28:55] Yeah. Is the system potentially a beachhead or is springing off point where an attacker can attack one system and get thousands of successful, you know, unauthorized entries? That's an inherent risk factor that I think often we haven't had to consider. In this new world is that everybody should be considering. And if you do that, I think you'll start to see that your lower risk vendors might not be as lower risk if you have these right kind of inherent risk factors. Continuing to evolve our risk based thinking around those, that's going to help us properly align the assurance expectations with that negative business value that can be made if something goes wrong. And that journey toward getting stronger security assurances and certifications from third parties who haven't historically been asked for it, it's not an easy one.

Robert [00:29:44] Yeah, and I know, I know there are some that will listen to this and you know, people that are well-intended that they're going to push back on this and say, you know what, we can't ask more and more of people that, you know, that haven't been asked to do this before. You know, it's it's already a hard problem. We're just making it more difficult. And I get it. I mean, that's the that's the human nature of the change management consideration around it. But, you know, facing the real truth here, I mean, cybersecurity isn't easy. And unfortunately, the risk are getting greater every day. And Omar talked about this, you know, easy isn't why we're here. So in in this world, you know, anticipating the worst case scenario and taking a reasonable and prudent approach to to learning from experiences being open to new approaches, being willing to adopt new strategies, you know, I think we have to be continuous learners. And, you know, that's that's I think, a really important part of, you know, what Omar has brought to the table as he's continuously learned as a leader.

Jeremy [00:30:41] Yeah. And that adaptedness that continual learning mindset, I think that's equally important for standards setting bodies and certification bodies like HITRUST, as it is for organizations that work with third parties. At HITRUST, we worked really hard over the past few years to expand our assessment and certification offerings specifically so that lighter weight assurance mechanisms are available when needed, but still provide meaningful reliable assurances that something like a questionnaire just can't.

Robert [00:31:13] Our questionnaires, I just I just love the approach Omar talked about to justify his views here. You know, he simultaneously viewed the ones he sent to vendors first as value add and the ones he got from his customers as a waste of time. And then he evolved. And I wonder how many other organizations have the same dichotomy and don't take the step of challenging the status quo like Omar did at his company. You know, the truth is we do a lot of things, and sending out questionnaires can make us feel really productive. But receiving and filling them out feels like a burden. And especially when you say, you know, I could just answer the questions and move on. So I think we all have to take away from this that we need better approaches that provide different and appropriate levels of meaningful assurances for third parties of all shapes and sizes. Let's let's build a system that provides the level of transparency and integrity that we're all seeking.

Jeremy [00:32:02] Oh. Robert's drop in the knowledge. Well said. And with that, I think it's time to wrap up this episode of Trust Vs. Thank you all for tuning in. And thanks to our special guest, Omar, for sharing his insights and experiences with us.

Robert [00:32:15] Yeah, thanks Omar for joining us today and for your continued leadership across the industry. It's been a great time to have you on the show and I want to thank all of you for listening in as well. And we hope you found the discussion on communicating security assurances valuable, and we hope you join us on the journey to get better in this area.

Jeremy [00:32:32] Stay tuned for more episodes of Trust Vs, where we're exploring the evolving world of cybersecurity and the delicate balance between trust and security. Goodbye, everyone.

Robert [00:32:42] Bye, folks.