Trustvs 08_Montage_v3.mp3

Jeremy [00:00:10] And welcome back to Trust vs. I'm Jeremy Huval, innovation officer at HITRUST.

Robert [00:00:16] And I'm Robert Booker, strategy officer at HITRUST.

Jeremy [00:00:19] So here we are, our final episode of season one. This season we've had a chance to speak to many cybersecurity leaders and experts about different aspects of trust in the area of cyber security.

Robert [00:00:31] That's right. And in this final episode for season one, we wanted to do something a little bit different. You know, we've been talking to one guest or a couple of guest about the topic each episode. But, you know, as we were as we were having these conversations, you know, we asked all of our guests during the season their thoughts on the same topic. You know what that means, right, Jeremy?

Jeremy [00:00:51] Clip show.

Robert [00:00:52] Clip show, that's right. And so the topic that obviously comes to forefront is this little thing that no one is talking about called artificial intelligence or AI. The topics so big, so impactful and so nuanced that any one guest or one voice just won't do it justice.

Jeremy [00:01:12] With the amount of airtime AI has been getting everywhere lately, there's no way we're not going to talk about AI on this show, but if I'm being honest, I really didn't want to, Robert.

Robert [00:01:22] Yeah, why? Why not, Jeremy?

Jeremy [00:01:24] Two reasons, right? The first for me was like, "Here we go again." And over the past, I don't know, five, ten years, thirties waves of AI media hypes that come and go every few years. And the last one I really remember was around 2016 and 2017, and it got a lot of air time then about how great the generative AI models were getting. And and just like all of those waves, this wave that I'm talking about in 2016 and 2017, it promised some kind of imminent Jetsons like future paradigm shift that was about to happen. We were on the cusp of it and it was going to completely change the way we work. And if you're a knowledge worker, your job was going to shift dramatically and then it didn't happen. So fast forward a few years and here we are again. Admittedly, though, this one feels a little bit different as now I actually have APIs to hit and sandboxes and playgrounds to play in. Yeah, and like recently I saw ChatGPT actually write code for the first time in a language that I can code in, and I was floored because it committed the code better than I actually come at the code. So it feels a little bit different this time. But here we go again is kind of one of the first reasons.

Robert [00:02:35] Yeah, you know, there's there just seems to be these hype cycles in technology in general. And I, I kind of share your your perspective and maybe a little bit of your pain as you think about the past here. You know, and to your point, it is it is really compelling to see the number of companies actually doing something this time. Like we're not you know, we're not dealing with sort of abstract this may change your world. Maybe think about it. You know, I, I honestly can't think of a leader I've talked to in the past, you know, probably a year of time that isn't telling me they're doing something now, usually with ChatGPT. But, you know, generative AI in general is just everywhere these days. So

you said two reasons, though. What was the other reason? You know, Jeremy, you were thinking about not covering it.

Jeremy [00:03:19] From a security perspective. I kind of worry that this AI hype distracts from the fundamentals. Yeah, we should invest in innovation using emerging tech like, of course. Right? But what about those investments and stuff like endpoint security that might have already been to been deferred a few times so far? And so ChatGPT and other generative AI models that are shiny objects right now are sort of still getting the focus. And while it's important, like I'm an innovation guy, I think it's important. I just worry that these new toys, they're going to distract from like, you know, the brushing and the flossing and all the hygiene stuff that is so critical to, you know, protecting the house.

Robert [00:03:59] Yeah, I think that's that's just a real risk in general. You know, it seems like we we see all the new shiny things, the toys as you describe them being the, you know, the next thing people want to invest in, you know, we can go get capital, we can buy a new totally could buy a new capability. And you know, I don't know I'm I guess I'm gray enough and and senior enough in my career trajectory to to think that AI is really valuable. But I don't know that it's going to it's going to just change everything the way people describe it as I think it will change the way technology is delivered, will change the way people interact with technology. I think all that. Not sure I'm ready to say it's going to change security at some kind of I'm kind of cynical as skeptical, maybe reinforcing your point, Jeremy.

Jeremy [00:04:43] But yeah, and you remember from one of our earliest episodes, maybe episode three or four, so we talked about breaches and one of the one of the final points we made was I wonder what anti breach safeguards have yet to be invented. And, you know, maybe AI will help fill some of that void about some of the key capabilities that will help us prevent those breaches because so many are needed. But with all that said, yeah, let's let's get into the episode. So, Robert, like you said, we've got several bits of conversations that we've had over the season, but we'll start with a conversation we have with David Houlding, who's a director of Global Health Care Business Strategy at Microsoft from our first episode. And let's hear his thoughts about the double edged sword that is AI and emerging tech.

Robert [00:05:35] You know, I think about the world in front of us. We we hear terms all the time, like AI, you know, blockchain. Those things we could begin spent an hour just defining those terms, I think, in many cases. But, you know, the world is changing quickly. And and I think about the leadership that organizations have to partner with in order to to do that in any perspective on the future where the world is going. Terms of those technologies or others.

David [00:06:01] Yeah. No it's it's really interesting. Things are moving faster and faster. There's really exciting changes like AI but blockchain, many others that are essentially bringing are promising some very compelling new benefits, including to health care and the quality of care and, you know, basically empowering health care professionals to make better decisions faster and improved quality of care, lower cost of care, that that kind of thing. So really exciting. But these these new technologies, like any technology, can be a double-edged sword. It can be used nefariously as well as for good. And AI is no exception. And you know, it can be used in things like phishing and spear phishing and deep fakes where they're audio, video, etc.. And so as cybersecurity compliance professionals, I think we all need to be thinking about like how can we ensure that we enable the good, maximize the good and minimize the risk of the bad? The interesting

thing is because I mean, very often I know I'm preaching to the choir here, but very often there's a lag time between compliance and controls and requirements within a given compliance sort of authoritative source and where the industry actually is in terms of, you know, IT landscape like as it's shifting from on prem to the cloud, is it are there new risks from AI and so forth? Very often there's a lag time. Is it six months, is it multiple years for the regulations and so forth to catch up with, hey, this this new technology or the shift as introduces new new vulnerabilities, new risks? So so I'm really excited about some of the cyber adaptive stuff that's happening at HITRUST and, you know, tracking those kinds of shifts much more closely on a like monthly basis and and being able to to deliver new intelligence and updates to organizations that are HITRUST licensed in terms of helping them, helping them see what they need to change in their what controls are they complying with are getting in place to to adequately mitigate the latest risks that are relevant given what's happening in I.T. and with these new technologies?

Robert [00:08:12] Yeah, it's a it's an exciting space. And I think the technology and automation can benefit. But as you said, there's a risk there. We have to really watch carefully and try to keep up. But we've talked so much about the the positives. So can you think of incidents or, you know, industry trends where things didn't go like we'd like and compliance and regulation became more of a priority as a result? You know, anything come to mind there, David?

David [00:08:37] Yeah, unfortunately. I mean, compliance can be a proactive thing, but so often it's a reactive thing and it can occur as a result of some incident that's occurred like a breach or ransomware and the disruption and the negative consequences. So I think too often that happens with organizations either not not complying with what they need to comply with or not complying with enough for a sufficiently a sufficiently high level of compliance like maybe they were just hit by before, but they really needed to be high trust to sufficiently mitigate risk. And, you know, because they weren't they had a breach or some adverse event that very often impacts the in-patients. Right? So to the extent we can all be more proactive about information, privacy and security and compliance is a big part of that, as is risk management. You know, we can we can mitigate risk of those those things faster, sooner and and reduce that window of opportunity for adverse outcomes and security incidents like like breaches and ransomware.

Robert [00:09:45] So I really enjoyed hearing from David in episode one and great input again on this topic of AI. So now we're going to hear from John Overbaugh, CISO of Alpine Software Group, who we interviewed in episode four. For those of you that listened, we had a great conversation with John about Trust vs Breaches. And it's actually one of our most listened to episodes. So if you haven't gone in and grabbed it and listened to it. I highly recommend you do. I think John has a great perspective on the topic that many people care about.

Jeremy [00:10:12] Yeah, and here coming into this part of the conversation, we had just asked John his views on emerging tech and new and emerging AI kind of stuff, but more importantly, how that will affect the [00:10:23]Bruce [0.0s] landscape. So let's take a listen.

John [00:10:32] I'm going to unfortunately say we will see, we will 100 percent see an increase in breaches. Those breaches, though, won't necessarily be nefarious actors. Those are going to be breaches where company you know, where the compliance team finds out that a member of the company leveraged AI to analyze data and they shared confidential information with that AI solution. That's where I think we're going to see the breaches. I think I think the HIPAA wall of shame is going to be on fire with with

announcements over the next two years or so. I think we'll see similar things happening around financial information and so forth. So so I see that happening. Will our defenses improve? Yeah. Yeah. I mean, in fact, you know, I was just looking at a at a solution from my former employer, Microsoft, which will scan data that uses AI to scan data to look for PII. Right? So it's doing more than just a simple grep or a regex, It's actually using artificial intelligence to recognize PII. Tools like that can really help us. I try to tell my team. So first of all, I'm a huge proponent of AI in certain circumstances. I will say grumpy old man hat back on. You remember the Disney movie WALL-E, where where everyone was just like massively overweight and they flew around on these little floating scooters like. Yeah, exactly. I see our society going in that direction mentally. Right? I mean, if, if, if all I have to do is ask an AI think to write an essay for me or do this out of the other thing, like I'm going to lose my ability to develop critical thinking. That's my grumpy old man essay. So let's go back to this. I see AI helping us be more productive. And I see AI as a massive opportunity for companies to jump ahead from a from a competitive perspective, I was at a risk management seminar put on by Wall Street Journal a couple couple of weeks ago, and they pulled the audience. In only 34 percent of the attendees were planning to do something in with AI in their product offerings in the next year.

Robert [00:12:42] Wow. Really? That low.

John [00:12:43] Yeah. Which so I'm like, sweet. Like, this is a great competitive advantage and it's hard to take advantage of, right? So I see a lot of value in AI, in making our lives more efficient, doing some of those easy things for us. The risk here is in not understanding how to use AI in a secure and compliant manner. And that's where that's that's my concern is just how quickly can we educate our employees.

Jeremy [00:13:10] Yeah. And there's there's more and more awareness of AI, risk management frameworks and AI governance frameworks. I think this published one in January of this year, 2023. And peeling the onion back on it, there are tons. There's almost too many. So there's not like there's a lack of guidance on how to evaluate and consider risks in the air space. But for the common I.T user having that sort of basic cybersecurity hygiene awareness, they shouldn't click on that link. I wonder if that level of awareness will need to continue to continue to evolve as the AI based spear-phishing comes out and stuff like that. I think it will.

John [00:13:49] Well, that's something I was talking to a relative of mine who had was receiving a lot of spam and they were asking me how to stop the spam. And then they said, you know, well, at least with phish I can detect them because they always have grammatical errors and things like that. And I said, "Well, that's the case now, but with AI, that's going to change." Like, you know, I'm surprised it hasn't already. Like phishers just don't seem smart enough to go and say, "Oh, have AI write me my phishing email so I can get rid of the punctuation errors or just use a third party product that reviews your text for grammar errors before you submit it.

Robert [00:14:29] Yeah. You know, I agree with John. Their awareness is increasing, but, you know, probably just not quickly enough.

Jeremy [00:14:35] I think that point is an excellent segway into our next interview with George DeCesare, Chief Technology Risk Officer at Kaiser Permanente. We talked to him earlier in the season about cyber risk management. So AI is definitely a current buzzword. And when it comes to AI risk management, it's on everyone's mind. As John mentioned

earlier, there's a lot of new risks on the horizon. So here we pick George's brain about the changes he thinks we'll see in the next three to five years. Let's hear George's comments.

George [00:15:08] Let's start with the a the AI question is really, you know, right now we're sort of at the cusp of what that impact is going to look like. And, you know, the federal state governments are looking at regulating it, and we don't know what they're actually going to go and how much regulation. I mean, California is talking about having an opt out, you know, option for consumers, you know, residents of the state of California, that they can opt out from the use of of automated decision making businesses. So and that's health care is included in that. So if we are adopting artificial intelligence to help us in the clinical decision making and things like that, it becomes a very complex environment to maneuver as these new regulations start to evolve and come out is how do we deal with it? And in some terms, I mean, if you think about what that means, you know, if a patient comes in and says, I want to opt out from any of that, now you have to, you know, separately track what you're doing there. And the other the costs of health care increase because we're we're trying to become more efficient, more effective and quicker. And and unfortunately you now have [00:16:21]to get it keep. [0.9s]

Jeremy [00:16:22] [00:16:22]Of band and the normal. [0.7s] Yeah.

George [00:16:24] Yeah exactly. And so that becomes a very complex environment to maneuver through and manage, you know, and that's just excuse me from the regulatory standpoint. Have the look out, you know, things like, yeah, but how do we use that technology to help us make decisions, you know, and think about the ethical, the bias pieces of, of the risk involved in that. How do we make sure that the decision is still that human decision, that it's not just completely 100 percent relied upon from the technology? So it's it's process. It's it's you know, the practice of it becomes very key in how you, you know, adopt these these technologies. Otherwise the risks of of just you bringing in a technology and using it as your end all you know that's not the right thing to do.

Jeremy [00:17:23] Yeah. Keep it in the realm of a decision support system as opposed to a decision maker helps address some of the risks associated with the biases in the underlying data, for example. Yeah, that's right. But it will it will cross that horizon eventually. It has to.

George [00:17:37] Gosh, what was it? There were about four or five years ago, we were having a little think tank session just strategizing. What does health care look like 20 years from now? And my team came up with the sort of out a few. There was a movie. I can't remember what it was. I think it was Elysium.

Jeremy [00:17:55] The city in this. Yeah.

George [00:17:57] Yeah, that's right. Yeah. But one of the things they had was that the doctors were no longer in place.

Jeremy [00:18:04] The robots that came in service.

George [00:18:06] Yeah. And you basically, you know, sat in, like, kind of an MRI tube. You got a scan and everything then was corrected to determine what was wrong with you. And then you were diagnosed. And then given your treatment right there without any human involvement. And I thought, you know, 20 years from now, that that could be something. In fact, you know, we saw what it was a ChatGPT that passed the medical bar

and the and and so it is it is getting to know the cusp of something that that could evolve into something like that, that could make things much quicker, much more precise. But, you know, in that there's inherent risk. And until until that risk is mitigated through, you know, the learning process, the elimination of that bias, the other those things that will well, I think we'll eventually get there. But it's it's not here today.

Jeremy [00:19:03] Yeah. The optimist in me thinks that having some of the automated decision making around health care will help create a more equitable health care environment for those that traditionally can't afford to get access to that kind of care. On Elysium, that's where it ended up. They unlocked the city's drones and they all went down and treat everybody. So hopefully there's a utopian future in there for somewhere.

George [00:19:22] Yeah, exactly. It was just the the, the folks up in the and whatever that was that city in the sky. Yeah. Yeah.

Jeremy [00:19:28] As we look to that future, you know, George, we're talking a lot in about assurances around this, you know, how will how will a system that relies heavily on these tools, you know, evolve from a policy and practices and maturity and assurance kind of kind of model? Is is anyone really wrestling with that yet? Or is it still embryonic or, you know, what? What do you think is going on there or may go on there?

George [00:19:55] I know there's groups now and consortiums are coming together and health care to you know, on the topic of AI in its use. But they're coming together and they're they're in the initial stages of what's going to be important in this. How can we use this? What are the ground rules? I think they're talking quite a bit about evolving this in the care delivery space. But like I said, it's embryonic at this point. It's it's sort of, you know, looking at what's available today. And I think, you know, one of the things that that was I was having a discussion with somebody and said, I think we need to look at it from the perspective of not what's available today, but what is it going to look like tomorrow and how is it going to evolve to this point? And then how do we use that? How do we, you know, take advantage of what that evolution is? Because today it's you know, it's it's basic. It's it's you know, we're sort of touting the what it does and we've got the generative AI capabilities that, you know, anybody can now use and take advantage of. But that's therefore, that's the beginning. And we need to think about it as what what that can say there's an end game, but there's certainly a, you know, that that and sort of that junior varsity varsity game that we have to think about.

Jeremy [00:21:20] Yeah. Thanks to George for that that look into the future. Thinking about AI and the enterprise risk management dimensions around AI and kind of pivoting to our final look into this future of AI. We we asked Omar Khawaja, Field CISO at Databricks about his take on AI. And Omar said a lot of what we're thinking. AI is a new tech that many of us are suddenly have to become experts on. So it was it was refreshing to hear from Omar that we're not alone and and feeling like we have to keep up with what AI is kind of forcing upon us. It's just a rich conversation, and it's great to hear from someone so knowledgeable. So let's take a listen.

Omar [00:22:03] I'll share with you maybe the the double edged conversations I've been having with many CISOs over the last month, month and a half. On the one hand, almost every CISO will admit that they're not an AI expert. They don't even actually AI expert is maybe too much, but they don't even understand the foundations and the basics of AI And and to be clear, had I not come to a company like Databricks, which focuses on AI, I would absolutely be in that exact same cohort. So at the beginning of the year, if you ask me,

Omar, what do you know about AI, I'd say, I'm pretty sure I know how to spell it and I think I know what it stands for, but I wouldn't know many of the details. What are tokens and what's featurization and what is feature engineering and you know, what are transformers? And there's a whole world of jargon that had been sort of building itself up over the last 15, 20 years while I've been heads down learning and trying to keep up with that with cyber. And so on the one end, the typical security leader, a CISO understands and accepts that they're not an expert on it. The part that is really concerning for me is that the knee jerk reaction, which I would also say would be my reaction if I was a CISO, but now being sort of at AI company, it's easy for me to for me to judge other CISOs. The knee jerk reaction is Omar, it's not really that different. We don't really think we need new controls if our employees are going to it. It's all talk on our website, it's all data. So we know that we've got web proxies and we've got DLP and we've got training. And if it's the, you know, our products are building AI into them, we've got product security and we've got SDLC and we know how to do that. And it's data going into some kind of code and it's [00:23:55]building [0.0s] something else. We've been doing that for 10, 15 years or so. Yeah, we don't really think we need new controls and if we do, we'll look at it later. And that sort of is the reaction I would have because I would look at my already oversubscribed plate of things to do. And the last thing I want to do is admit and acknowledge that I've got this whole new field that I've got to go figure out. Because the way I think about thread modeling, the way I think about risk assessments, the way I think about assets, all of those paradigms are built for a fixed world where code doesn't change by itself. It's not accessible to the entire universe. And now I've got to go rethink my own paradigm, which I spent ten, 15, 20 years developing. And you want me to throw that out the window? I'm the frequent CISO I've got Chief in my title. And if you force me to rethink all of this, you're telling me I need to go back and be an intern? So I think that, you know, if I'd say to answer your question, Jeremy, if I'd say there's one thing that's really important is for every security leader to be thinking, I do need new controls, I do need new paradigms, I do need new ways of protecting AI, of enabling the business of effectively managing risk, as every business is going and deploying LLMs and using AI and going to this brand new world. I may not know exactly how to do it. No one may know exactly how to do it, but I should at least go into this with an open mind and eyes wide open that I am going to need more controls and incidents will happen and I want to be as prepared as I can be. But no one has a crystal ball to say these are the three controls that would be magical. So, you know, for instance, ten years ago no one knew the value of something like MFA. We had MFA and we used it here and there. But over the last four or five years, it's sort of become this magical control that in many, many scenarios serves as the closest thing we have to a silver bullet. But we didn't know that ten years ago. Similarly, in two or three or four years, we're going to find out that there are certain controls that are just applied in the right places are going to have tremendous value. But having that open mindset and the CISO setting that tone for the security organization and with the business, that's really important.

Jeremy [00:26:26] I'm really interested to hear your thoughts on if you had a crystal ball looking into the future a year or two. What are the AI driven risks that you think people should be thinking about now?

Omar [00:26:38] I fully expect there to be many incidents and high profile incidents coming out of organizations using AI and it behaving in ways that they just did not anticipate. And they did not that they did not plan for. I'd say I expect things like more more poisoning attacks where you're able to train the AI in ways that are malicious and then for it to spit out responses that either divulge information that shouldn't be divulged or for it to impact the integrity of the AI model. I expect that to happen. I expect the other thing I expect to happen, which is one of the things that really makes AI different compared to other

applications, is, you know, the hallmark of AI and machine learning in particular is that it learns. And so when you create an application, an application is static. So once I do a code review of the application and I put it into production, I don't have to worry about that application behaving differently than when I did a code review and I did a pen test and I did all my other assessments. But for for AI, that's not the case. The AI model could be changing every minute. It could be changing every day. And so there is some level of drift happening. And how do I monitor that on a continuous basis? That's a very different paradigm than the paradigm I have for how I monitor applications, how applications I monitor for malicious behavior. But here, if I'm not even quite sure how the AI is making decisions and based on what data and the provenance of that data and all of that becomes really hard because you've got so many parameters and such deep neural networks that are operating at the core of this. Then how do I know that that AI model hasn't drifted further away than what I'm willing to tolerate.

Robert [00:28:42] We just heard from four experts, you know, about a topic we're all thinking about and what a fantastic way to wrap this season up. So I just really learned from all these people about the impacts of AI and just thinking about the future that we're all creating together and also reacting to together. So. So, Jeremy, we we are privileged to set in a place where we are a part of, you know, this, this change is happening around us. So, you know, what is HITRUST doing to help companies address this risk and that risk we were just talking with these guests about people incorporating AI into their platforms and then perhaps seeking certification validation of those platforms.

Jeremy [00:29:22] So in a word, a lot which two words? But we've we've been working on this for a while and we have a lot more to do. But here's just a few of the things that come to mind. We've currently got a patent pending with the US Patent Office about using natural language processing and AI to help map an organization's written policy documents to control requirements to help evaluate, you know, does my written policy content address everything it needs to address and natural language processing to help us maintain the HITRUST CSF. So we stood up within our standards tooling the ability to compare text against itself. And we use that by basically saying, "Hey, I've got this." Authoritative source like, HIPAA or GDPR or whatever. How tightly is it reflected in the HITRUST CSF? So we've been doing that a little while and we've gotten some good return on that. Most recently we've added the NIST AI risk Management Framework into version 11.2 of the HITRUST CSF. We're also adding an AI risk Management guideline. I think it's [00:30:26]23894 [0.0s] into v11.2 of the CSF as well. So I'm pretty excited about this because both of those standards I mentioned are really new. Like for example, the NIST AI Risk Management Framework was published in January of 2023 and we've already pretty much wrapped the mapping of it. I think we did that in May of 2023. So really quick turnaround and coincidentally it's the use of that AI and our mapping tech that helps us map this AI content into the framework faster.

Robert [00:30:59] Yeah. So we're really we're really talking about how we use AI to help our customers do the work they do to help us maintain our framework, the CSF. And then that last area, Jeremy really to create that foundation of having AI risk management principles in and the risk management framework in our, in our CSF specifically. So all those things really cool. And actually we've been playing with it for quite a while and getting real value from us. So we're, we're super excited about that. So we've known for a long time with things like service providers and specifically cloud service providers that shared responsibility and inheritance are really valuable tools When we think about how AI systems are built, you know, you have the consumer of AI, then you have the supplier of AI and the company or companies that built the language models seems really ripe for a

shared responsibility and an inheritance, you know, opportunity. So, you know, how do we think about all of that?

Jeremy [00:32:00] We're currently expanding our Shared Responsibility and Inheritance Program to specifically include the acknowledgment and the formalization of responsibilities shared across the AI service provider and the AI user. And it's not an easy problem to solve. We feel like it's really important because if you can't solve this, you can't give the higher level of assurances around the use of AI that includes consideration of whether the model provider, the AI service provider is or is not performing their end of the bargain. Like, for example, there are several AI controls that deal with the quality of the training data that goes into the large language model. And you know, for that run of the mill user of a large language model who is not doing fine tuning and is not training the model themselves, they're just using it. They expect that training model to have good controls around it, but they expect those controls to be performed by the provider, not themselves. But how do they get assurance that those controls are being performed? And the AI share responsibility model is a key input into solving that problem. But it's not something that we're just having to figure out [00:33:07]net new [0.8s] HITRUST has been doing share responsibility and AI over I.T, service provider and cloud service provider stuff for a long time now. So we've got a lot of machinery, a lot of processes, a lot of relationships that will help us move quickly on it. We're already underway. So yeah, really exciting problem to solve. It's like it's the cool kind of problem that I personally like because it's controls focus is tech focused and it it's, you know, it's new.

Robert [00:33:36] You know I think we see lots of articles and lots of input being being written about how to be safe with AI, how to do AI with quality, how to make sure it's not it's not biased that those things are taken care of. And so, you know, it ultimately comes down to the larger problem being trust and being assurance. So back to our podcast, Trust vs so, you know, it really becomes foundational how we provide assurances over how AI is used, how it operates at scale, how organizations like you just said, Jeremy, actually test and validate that their service providers have done the stuff that's necessary to to make sure this is a safe and appropriate system that you get the outcomes and the the enhancements in the value you're seeking and you don't get outcomes and and answers that are far from what you need and expect and really set that acceptable bar over the risk management around. AI mean, sorry, it's a brand new area. We were really excited to be a part of it and to help lead as we look at the opportunity going forward.

Jeremy [00:34:37] Yeah, and there's a lot of work that I think collectively the technology and risk management assurance industry still have to do around and giving guidance and establishing sort of what right looks like when it comes to controlling the risks of AI. And if you look at the ISO risk management frameworks that are out there right now, there's not that many. And if you look at the AI Risk Management Frameworks, it out there right now, there's a few that I mentioned earlier and they're all like brand new. So this landscape will change dramatically in a year from now, in my opinion, as more and more standards and assurance mechanisms like HITRUST really step up and say this is how right looks like and how will implemented at scale with reliability, etc., just rapidly changing right now. But it's it's a fun kind of a fun thing to look at in my opinion.

Robert [00:35:27] You know AI is definitely a new technology and something certainly we have to think about all the time these days. But, you know, at the risk of oversimplifying all of this new technology, at the end of the day just brings new risks to the organization. And just like Omar said, you know, now we have new controls needed to address those risk If they're being performed by a service provider, like an AI large language model provider

like Jeremy was just talking about, we're going to need those assurances that that service provider has implemented those controls. All that requires a control framework and an assurance system that provides you that trust and integrity that you're expecting to know that the technology is up to the task. So really happy to be part of that journey, working with some other great companies, also looking at leadership in this realm. And there's a lot of work ahead of all of us. So it's all good stuff.

Jeremy [00:36:15] And that's a wrap for this season of Trust vs. HITRUST's very first podcast. So a heartfelt thank you to everyone who's joined us on this season and listened along the way. We had a bunch of fun on the side of the mic recording it and strengthened our relationships with with others. We hope you enjoyed listening and we hope that you took something away from it that helped you in your in your day to day, day to day working efforts. And. Yeah, thank you. Thank you.

Robert [00:36:42] And Jeremy, thanks to you for joining me. This was fun. I enjoyed it a lot. Thanks to Quincy and Dillon our producer joined us as well and to our guest along the way, each of which I think are just true leaders in every right in this industry. And we're so grateful, have relationships with people like that. If you missed any of these, please go back and listen. We're proud of each and every one of them. And I think there's something you'll find in each episode if you take an opportunity. So we invite you to join us.

Jeremy [00:37:07] And if you enjoyed Trust vs, this is so important, we'd appreciate it dearly if you left a rating or review on your favorite podcast listening app. And listen, I've got another very big ask if you enjoyed the podcast and you want us to keep doing it, please let HITRUST know. Robert and I are on LinkedIn as well as the rest of organization. If you got a relationship at HITRUST, hit us up on LinkedIn and say, "Hey, I want more of that Trust vs." Since smoke signals across the great divide if you need to, but it would help us help you have a second season and if you want to listen to the transcripts or the recordings again, find them on our website. Thanks again.

Robert [00:37:47] Thank you, Jeremy.