## 05_Trustvs_George_v7.mp3

**George** [00:00:03] What do we need to do to protect the organization? And you kind of get in this mode of not only talking about the management of the risks, but you're also talking about the direction of the organization.

**Robert** [00:00:21] Welcome back to another exciting episode of Trust Vs. I'm Robert Booker, strategy officer at HITRUST.

**Jeremy** [00:00:27] And I'm Jeremy Huval, innovation officer at HITRUST. You know, it's always a pleasure to be here talking about cybersecurity.

**Robert** [00:00:34] That voice you heard at the top of the episode belongs to none other than George DeCesare, the chief technology risk officer at Kaiser Permanente, a giant in the health care industry. George has been of the HITRUST board of directors for quite some time and a long time friend. And what we learned in talking to George is before he joined Kaiser, he worked with the Los Angeles County Sheriff's Department doing forensic investigations, identity theft. And before that, he was a CISO and privacy officer at Dignity Health. So George has a really rare mix of skills, being a lawyer, a cybersecurity expert, and having worked on the law enforcement side, he's kind of got the triple threat going on there.

**Jeremy** [00:01:12] The theme of our conversation was George, Trust Vs. Cyber Risk Management. So as cybersecurity professionals and risk managers ourselves. This conversation struck a chord with Robert and I. George provides some insights into how he approaches managing cyber risks in a huge company and in a very interconnected industry.

**Robert** [00:01:33] Yes, we we think a lot about the importance of cyber risk management within the broader enterprise risk management framework. Not a new term to this podcast. We've talked about enterprise risk management several times, and it all ties into the overall value creation of the organization.

**Jeremy** [00:01:49] Yeah, and we also talk about the evolving threat landscape and how it impacts cybersecurity, which is something we continue to touch on on the podcast. And George here shares his perspectives on staying ahead and how critical that is to ensure you're protecting data like you like you need to.

**Robert** [00:02:05] We also cover third party risks and the challenges organizations face when they think about and manage those external partnerships. And lastly, we touch upon the significance of industry governance and the critical role that partnership between organizations and the regulatory bodies they work with together with partners in managing cyber risk. So, Jeremy, give me your thoughts on why this is such an important conversation.

**Jeremy** [00:02:28] Sure. But let's zoom out for a bit. Think bigger than just managing the risks of technology. And let's think bigger than just managing the risks within a particular business. Let's talk about the concept of risk management for a minute. To think we as humans can somehow manage risk takes this acknowledgment that the future is something that we can shape and even bend in our favor when we try to manage any kind of risk, regardless of whether it's the risk of a lost hard drive with lost data or even lost crops of corn. We're operating under the belief that we can determine our future state instead of being victims to whatever nature or Lady Luck has in store for us.

**Robert** [00:03:10] It's such a great point, Jeremy. It's such a human consideration, and it's good to think of risk management about trying actively to shape the future. If risk management's our game, the future is the playing field we're running on. Without an uncertain future, there's no risk or any need to manage it. So risk and time are really two sides of the same coin.

**Jeremy** [00:03:28] And because none of us can see the future, at least nobody that I know, any risk management decisions we make are based on two inputs. One our subjective belief about what will happen in the future and two our knowledge of the past. I think the tools that exist in the risk management space try to bring those two inputs together to optimize our decision making. I think those tools are just fascinating. So we talk about a few in this interview, tools like Quantitative Risk Analysis and the Fair Institute's tool set and the methodology they bring to the table. And HITRUST has a patent pending in the science and the space around Quasi quantitative residual risk analysis and how to use HITRUST analyzes to sort of do a quantitative risk analysis. Shout out to Dr. Bryan Cline there, but I'm a tool guy and sort of the the ideas that underpin these tools in the space are just fascinating to me.

**Robert** [00:04:22] Yeah, and I think I think it's really interesting how you talk about the human dimension in the tooling and there is a lot of science in play at risk management and as we dig in, it seems to be continually evolving. I think some people do it better than others, and I think George probably is one of those people. And but I'd argue that there's a lot still happening. And in terms of art, you know, not just the science but the art of it all. So without further ado, let's just dig into the interview and listen to George DeCesare, the chief technology risk officer at Kaiser Permanente.

**Jeremy** [00:04:58] So George, thanks so much for spending time with us. And I know you from your role in HITRUST board. I think you've been a board member for maybe seven years, just about. Can you tell our audience a little bit about who you are and what you do and what you focus on day in, day out?

**George** [00:05:13] Sure, sure. So I'm the senior vice president chief risk, actually, chief technology risk officer for Kaiser Permanente. We're a 100 billion dollar revenue integrated delivery network, having both the the payer, the providers and and of course, the hospitals and medical office buildings. We're practiced in a number of markets throughout the United States. We are a US based company, about 220,000 employees and but 30 I think it's 39 hospitals.

**Robert** [00:05:52] George, one of things I'm so fascinated about with your role is the the breadth of the role that I imagine must be, you know, the chief technology risk officer role for a company as distinguished as Kaiser. And when we think about, you know, Jeremy and I both worked in this sort of cybersecurity cyber assurance space, and we're definitely in that area all the time. But, you know, you you know, I would I would presume your role goes can go much broader and deeper than that. So when I think about it, you know, how are how do we think about cybersecurity and cyber risk, you know, as a part of a larger enterprise risk framework. So it's foundational, as you said. But how so? And what do we need to be thinking about there?

**George** [00:06:30] Starts off with where your organization is. And really an organization with a mature risk management program has a good idea of where, you know, its risks lie and what its tolerances are to accept those risks or or even deal with those risks, you know, and cybersecurity being one of them. But, you know, you've got particularly in today's day and age, many health care organizations are struggling financially with CEO, even even the hospitals that are closing. We just had one recent hospital that can't remember that closed down because they were hit by ransomware and shut down for for several months. I think it was in their accounts receivables were just they're falling behind and they ended up having to close their doors, you know, unprecedented but but know really realizing, you know, what I use, there's a gentleman that I've I've worked with in the past by name of Bob Zukis. I don't know if you're familiar with a certain number of books, former PwC gentleman and one of his stories that I have gone to our board and talked about is know, understand what your O-ring is. And by that it's the story about the challenger space shuttle mission. Now, what happened in that and, you know, that explosion, that accident, and it turned out to be a small, tiny little O-ring that was subjected to think it was lower temperatures or higher temperature I can't recall then it was tested by a few degrees, but that caused a systemic failure of all of the shuttle systems. Similarly, it's like, you know, in health care, you have to understand what is that O-ring, what's tied together. And there's a lot. You know, you look at who you do business with, you look at what you do, you look at your in the care delivery space. You've got legacy clinical systems that don't have the capability of accepting agents or being monitored. So you've got all these things that come together as you're O-ring, you know, in which one can cause a systemic failure in your environment, you know, financial situations. You know, those are right now something that health care is looking at. Sure. That, you know, leaders in that space are looking at the industry as a whole and saying, what can we do better so that we don't fail? So those are the things that we're, you know, that come down across the board are systemic in nature. And cybersecurity is a piece of that that can cause a failure if there is an impact to to that [00:09:06]virus. [0.0s] So there's there's quite a bit from my perspective. And what I do is I have to look at that holistically and and be able to determine what pieces fit together, where that O-ring sits or which O-rings we have throughout our environment, in which things we have to deal with. Yeah, again, everything has a cost to accept a risk because that cost versus the benefit isn't just equal or greater.

**Robert** [00:09:34] You know as you were explaining those examples. You're talking about the you know, the the business risks, the the enterprise risk dimensions. Not not purely the quote unquote cyber or technical risk, which I think, as you noted, is a is and then is a component of that. But it's it's really the broader impact to the enterprise. So you're is it fair to say you're thinking about it from a you know, the the the enterprise value that's being created and how the technology risk broadly, you know, impacts that value? Or maybe said another way, what would keep it from being successful or would help it be successful? Do I have that right?

**George** [00:10:10] Yeah. Most organizations today invest heavily in technology. And, you know, in many aspects, there's stuff there's multiple risks that are introduced in the in the introduction of technology. Know, you know, if you don't change your process before you invest in the technology, then you're just kind of adding layers on top of broken things. And if you don't reap the benefits of what you invested in. Meaning, you know, it doesn't provide efficiency, it doesn't provide, you know, speed as there are things that you see as a benefit to this investment and that's not delivered. That's a risk. Yeah, but then we look at it too, from the aspect of the risk to an organization is a part of the risk to the industry. Because if you have a failure in a system, a health system, it's going to impact everybody else. Patients have to go elsewhere. Costs need to be absorbed. So there's a lot of things that we have to look at holistically, how it impacts not just your organization but the broader industry in general.

**Robert** [00:11:20] What are some ways to measure and, you know, communicate that? I think I think health care, you know, one of the reasons I'm in health care is because of the mission, I think many of us are. But what are the ways you actually translate that? You mentioned earlier, you know, the CISO serving as kind of a point of translation, you know, communicating with the board, such I mean, taking that and kind of I'm almost thinking in practical terms, how do you how do you measure it? How do you score it? How do you report it? I mean, maybe I'm being too tactical about it, you know, how do you think about that when you communicate and a company, you know, that does all the things Kaiser does when you sort of translate that, you know, upward and with your colleagues. I mean, what's the conversation sound like?

**George** [00:11:59] And I would like to see you got to keep it simple because there's a lot in that conversation and you can really get into the weeds. It depends on who your audience is. So if you're talking to your board of directors, that's one level of conversation. If you're talking to your leadership, that's a different level. And of course, if you're talking to to the, you know, the staffing and and just the broad spectrum of your organization, then that's a completely different level of conversation. So it's it's really, you know, who your audience is. And if you start, you know, start at the at the top with the oversight, it's really, you know, they want to know what should they be worried about. You know, what risks exist, what risks are being introduced, and how is the organization dealing with. Most of these boards are made up of folks that were finance, CFOs and and coming from that that point of view. So a lot of times you that conversation is about money. It's about, know, quantitative risk modeling that that helps them understand what the impact is. And then typically it's [00:13:07]dollars, [0.0s] that translates well in that conversation. You know, if you're talking to leadership, it's it's really impact not only financial, but they're looking at the operations, the clinical space, the administrative areas, and, you know, what impact can they have by, you know, the risks that the company bears. And then, you know, to to the different levels of of folks within the organization. It's about the tactical pieces. What what do we need to do to protect the organization? And you kind of get in this mode of not only talking about the management of the risks, but you're also talking about the direction of the organization and you're kind of there delivering a message on behalf of leadership as well.

**Robert** [00:13:52] So what are your takeaways from all this, Jeremy?

**Jeremy** [00:13:54] So I was sort of intrigued about George's example of that hospital system that had a ransomware attack be successful and ended up going out of business. I ended up looking up some stats about how often this happens. I was really curious. This happens a lot more than I thought it did. So I found an article from Cybercrime magazine from back in 2019, and even then they were saying something like 60 percent of small businesses will end up going out of business within six months if they fall victim to a cyber attack or have a data breach. So for me, that was a good reminder that cybersecurity is an existential threat for a lot of companies, and it makes cyber risk management a practice of organizational preservation. What about you? Any key takeaways?

**Robert** [00:14:40] You know, I couldn't get past the the example that George gave about the O-ring bringing out Space Shuttle Challenger, I mean, something that small and eventually that tragic and just yeah, thinking about all that and what it means for our business processes, you know, what are the O-rings that we have and you know, what do we need to be thinking about. You know, and just thinking about it maybe from a bigger picture, you know, something that we talked about was, you know, the risk of automating bad business processes, not something we talk about a lot when we talk about cyber security. But it's a real example. So, you know, imagine we put in a new ERP system, we spend even more money, you know, customizing that system to align with our legacy business processes. And then we do accounts payable just the way we've always done it, you know, with the legacy processes we built over the years, because we've always done it that way. You know, if you add all that out, we're not going to be in a better place. And, you know, instead we have just a more efficient legacy process. And I guess if you take that all the way to the end, you could even get better at being bad or having a bad process, which isn't really going to be what you're seeking.

**Jeremy** [00:15:45] Yeah mission failed successfully, sir. Yeah, George said it pretty well when he was talking about that. He said something like, "If you don't change your process before you invest in the technology, then you're adding layers on top of broken things and you don't get to reap the benefits of what you invested in." It's pretty cool.

**Robert** [00:16:03] Yeah, it is cool. And, you know, we think about the importance of cyber risk within the broader enterprise risk framework, how it ties in to value, the value of the organization's delivering. And, you know, I think that's really important thing for us as cybersecurity professionals to constantly remind ourselves about, you know, we are here to balance business security with business goals. Business outcomes are what we deliver, and it's what we're about. And we've heard it from other experienced guests as well. So if I want my program to be successful and effective and and frankly, to also serve the needs of the business, I've got to find that right balance of maximizing my security and enabling the business objectives through my security program. That balance is going to be different for every company, and that's okay.

**Jeremy** [00:16:43] Yeah, totally I remember. I remember my first internship in college. It was with an insurance company in Baton Rouge, and I was helping administer a Novell Network as part of their electronic data processing department. If you can believe it, the CIO at the time was trying to explain to me is like a college sophomore or something how information security worked. And she said something that's always stayed with me. It was something like this, We could make the company as secure as possible. The most secure company on the entire planet. We'd be able to guarantee that it will never be hacked and we'll never be robbed. A picture of this, right? No Internet connection. No doors, no windows. Actually, no employees sitting at any of the desks. The data will sit on the computers and stay there, and it won't be at risk at all. Mind you, nobody, no customers are getting served. No processes happening, no transactions get through the machine. We'll go under really fast, but we'll be super secure doing it right. So the moral of the story, of course, is you don't want to lose the baby with the bathwater when you're trying to manage IT risk. You can't make an overly restrictive system or take an overly restrictive approach that hinders operations or like, for example, slows down innovation.

**Robert** [00:18:01] Yeah, it sounds like a great internship because you learned something that stayed with you even now Jeremy. So that's really cool. So and I think just getting it out, risk management is it's not about chasing every last bit of risk to the ground. You know, we're, you know, we think about enterprise risk in the way that George does it because he's an enterprise level risk manager. You know, he's looking at the major risk that stop the organization which are having objectives. And you know, his point was look at those big risks. We could get distracted by the little risk and wrap all kinds of red tape around them. And I think at the end of the day, that's what makes the O-ring analogy so on point, a little thing with a huge impact.

**Jeremy** [00:18:38] Yeah. So let's get back into the conversation with George. You mentioned quantitative risk analysis. I'm curious, in your view, do the traditional tools of risk analysis and risk management like, you know, defining risk thresholds in the traditional risk analysis approaches, do those help us in managing cybersecurity risk? Are those tools up to the task or is there still more work to do in that area and developing the capability of managing cyber risk, measuring cyber risk, etc.?

**George** [00:19:12] Yeah, I think they're a good starting point. You know, if you don't have something, I think the traditional ways of doing things with looking at exposure, the the, you know, the likelihood, the impact and you know, coming up with your heatmaps that show where things sit. I mean, that's that's good. I mean, that's a good start. And it's a good blend, too, because you're not going to, you know, risk analyze everything and not everything falls into a neat package of quantitative risk. So you got to have a blend of both. And, you know, again, you know, it's again who you're talking to and who your audience is and what's important to them. Quantitative risk modeling. We are very familiar with the Fair Institute model, something that a lot of organizations have adopted, and that has been very successfully carried through where that message really becomes very important to the business, knowing, you know, how that model works. In fact, it was interesting when we first started pitching that model, it was sort of the business or leadership wanted to understand more about it. So how does this work and have more questions about the process than the output? How does it calculate? How does it as we continue to evolve it? We actually put certain things into the model. The events that happened within the organization and within the industry actually were fairly well represented in the model. So they started seeing the value of it and it started to expand not just from the technology area, but it's used across the board now. And we, we, we process this for a number of of other departments, including corporate risk and others, our supply chain. And in fact, interestingly, it's become sort of the fact of how we calculate risk transfer, become very, very accurate where, you know, in the past, as a lot of organizations did, was know it's already a cyber liability insurance. You kind of went after what you could afford. You know, it was at the right amount of coverage. Yeah, but if you if you use a good quantitative risk model to sort of figure out what you need to transfer, you know, what's what's acceptable and what you need to transfer, then you actually you're going after the right amount of coverage for the organization. We were able to reduce our cost significantly in that space because of that.

**Jeremy** [00:21:36] Wow. Yeah, a very desirable place, because I think a lot of organizations are struggling with the increasing costs of cybersecurity insurance and the risk transfer mechanisms available. Just keep getting more and more expensive, as you know, that area matures.

**George** [00:21:50] Yeah, less coverage and much more expensive.

**Jeremy** [00:21:52] Yeah, absolutely. So that's interesting. You mentioned risk acceptance earlier in addition to risk transfer. And in Robert nice world, we hear a lot of organizations say, you know what, we're choosing to accept this risk or we're choosing to accept that risk, which is a bit tougher to do without the really tough quantification of the risk. How does it hit your ear if you, for example, are vetting, I don't know, a third party organization and maybe looking over their assurance mechanisms and you see that they've accepted a lot of risk. Are there situations where companies are accepting too much cyber risk, not enough risks? How mature is that space, in your opinion? Do you think it's accepting the risk becomes a risk of itself sometimes?

**George** [00:22:33] Something a mixed bag organizations that have sophisticated practices will, you know, understand that better. Some organizations are just you look at it from the perspective of where that organization is and the maturity of that organization, you know, where they need to be, where they are financially, you know, because if if they're willing to take more risk, you know, whether it's the new investments, new new business dealings, things like that, a lot of times they're looking to expand. They're looking to generate more revenue. So they're willing to take more risk if they're if they're struggling. Same thing. Yeah. When you're in a good place and things are stable, you tend to not take as much of risk, especially if you're dealing with a third party. That risk becomes your risk. If you deal be do business with them. So you need to be able to now understand your risk tolerance when it comes to their risk tolerance.

**Robert** [00:23:25] That's a topic that's come up several times in these conversations George is third party risk and third party risk management. And I think you said it well. I mean, their risk becomes your risk. But I think a little bit about the system of the system of health care. And I think, you know, you probably are super well-placed to talk about how complex health care is, but. It's a it's a it's a network of different companies coming together around a patient, whether they be people providing or paying for care or, you know, engaging in, you know, biomedical science and technologies. I mean, how do how do you approach the the the thinking about the system of risk around your organization or just in general terms, how should we think about it as an industry?

**George** [00:24:06] It's well, I think you kind of yeah, set it to it to begin with. We're we're all in this together. We're it's it's an industry that's intertwined. You know, we deal with the same third parties that most other health care organizations. We deal with each other. We're integrated in health information exchanges. And we're, you know, we're sending information across the board to other health care organizations, the government. So we've got ties everywhere. Like you said, it's, you know, the risks of one organization, you know, kind of trickle over to the other organizations that are tied to it. And you have to yes, you have to be able to conduct business. You know, you have to be able to to provide care and you have to be able to to generate revenues so that you can continue to provide care. But in that there's a lot of risks that you have to be able to, one, understand, do as much as you can to mitigate that exposure for your respective organization, because if everybody does their part in that way, it impacts everybody else.

**Robert** [00:25:13] That's that's great. I think it really is a risk system. And we continue to we continue to want to work on ways to help the system become stronger across the system as a something certainly we're working on HITRUST. But I think as just industry partners, keeping everybody focused on that problem, you know, hopefully yields some good benefits for us in time so.

**George** [00:25:32] Like as we said earlier, we're all intertwined in this and we need to act together, you know, work with the ISAC. So the it's become part of this was, you know, the ISAC had, you know, some level of of information sharing that that they were getting and distributing. So how do how does the federal government do that better? How do we contribute to that? What's that avenue that we as the private sector need to take so that what we learned, you know, everyone else is aware of and can take action?

**Robert** [00:26:06] Yeah, it's really it's really the private sector, you know, leading alongside and with our regulatory partners and how do we together [00:26:13]solve, solve what unsolved [2.1s] it easily but lean into it easily I think is a better way of saying it so.

**Jeremy** [00:26:19] Exactly. It's fascinating how much information sharing, the lack of information sharing can hinder achievement of goals and really lead to disasters. And to bring back to your O-ring example, I think the the Challenger disaster was predicted by a booster rocket engineer who knew the tolerances of that O-ring and try to communicate an acid. But it wasn't the information sharing wasn't effective enough so that information sharing can be a deal breaker moment in a big, tragic way. That's interesting.

**Robert** [00:26:51] What a great conversation with a great guest.

**Jeremy** [00:26:54] Yeah Sir Robert. George has some good insights because he's lucky enough to have a full time job doing nothing but cyber risk management. So given that you were a CISO in a Fortune Ten company, how does hearing George talk about his experience at Kaiser parallel with your pirate prior experience? And I guess more importantly, do you think it should align with everyone else's cyber risk management experiences?

**Robert** [00:27:18] Yeah, you know, we talked earlier about humans wanting to try to control the future. Right? I think it's also pretty human to look at the world through the perspective that we each have. So. So I think it's a terrific question, Jeremy, because the world that Kaiser lives in, the world I lived in are, you know, they're they're different than the world that many of our listeners live in. So, you know, it's important to acknowledge that oftentimes it's only the largest companies that will have very dedicated and many, you know, cyber professionals working in the organization. And they may have lawyers helping them with the regulatory considerations, you know, partnering every day with many privacy professionals focused on that risk. But everyone has the problem, and it's why I love your question so much. So, you know, for the majority of companies, cybersecurity is something they spend what they can spend on trying not to be negligent, never being compromising. But it's that balancing act every day of risk management deciding how much to invest in their security program, how much can be good enough this year. And they may not call it risk management. They may not cause cyber risk or enterprise risk management, but it is what it is. It is it is risk management. So the challenge for those smaller folks is, is that it's getting more dangerous all the time. And, you know, I think we can agree that everybody needs somebody that know they're focused on the problem. They own this problem for their company and they're communicating with the company leadership, how many leaders there are or how few leaders they are about the problem and and making those decisions together.

**Jeremy** [00:28:44] And with that, we're coming to the end of our episode. If you've been listening, enjoying the show would really appreciate it. If you leave us a rating and review in your favorite podcast app.

**Robert** [00:28:54] Yep. And we sure appreciate all your for listening and joining with us. So have a terrific day. Thank you.