s01e06_Trustvs_Chris-Kevin_v4.mp3 - EDITED TRANSCRIPT

Chris [00:00:03] So what you want is an idea of communication between the cybersecurity organization and the board that bridges that gap, that expresses cybersecurity as a business operational, financial, regulatory, legal impact. Unfortunately, most of our cybersecurity that operates within its own silo, and that's not good for effective communication with the board.

Jeremy [00:00:32] Welcome back to Trust Vs. I'm Jeremy Huval, chief innovation officer at HITRUST.

Robert [00:00:37] And I'm Robert Booker, chief strategy officer at HITRUST. Today's topic, Trust Vs The Board.

Jeremy [00:00:43] And the voice you heard at the top of the episode belongs to Mr. Chris Hetner. He's incredibly qualified to take on this important topic. He previously served as senior cyber advisor to the SEC and currently advises the NACD, in addition to a bunch of other stuff that he does. In this episode, we have not one but two guest interviews though, and we'll talk about our second guest in a bit.

Robert [00:01:06] Jeremy, I was already the CISO in a large company, publicly traded company, when cyber risk rose to the level that they really gained board attention. And at that point the board began asking for regular updates from me. And over time, it became a really critical part of the role. And I spent a lot of time working on doing that and keeping in front of those requests. And I remember at the time talking to other CISOs in various companies about, you know, the fact that they were also getting these requests from their board. And at least one of them told me that they felt like the neighborhood dog that had been perpetually chasing the cars down the road, they finally caught one. And the question became, "So what do I do with it now?" So, you know, there were some articles, a lot of articles back in the beginning days with this this career field where, you know, you'd see things like chief security officers or chiefs information security officers have chief in the title. And, you know, we're pretty vocal about, you know, we should be we should be reporting at the board level were enterprise executives, you know, seeking more enterprise visibility? Well, we got it. And the question, you know, I think to explore, at least in my mind today, is, you know, what do we do with that visibility to help our organizations earn and sustain trust? You know, CISO serving as a risk executive, not just a technology leader.

Jeremy [00:02:28] Yeah, I can only imagine how those first presentations to the board must have felt being traditionally viewed as part of the IT group and then kind of evolving from the kind of the black hoodie and the hacker perspective to truly a, you know, a member of the executive leadership team and being viewed as a risk executive and not just an IT expert. So I imagine there's some growing pains along the way. Tell me a little bit about that.

Robert [00:02:52] You know, I was I was really fortunate. I was with a mature company with great leaders, Fortune 100 company. And, you know, when when this request was made of me, I had other executive partners, the company who were very experienced working with the board and kind of kind of, you know, put their virtual arms around me and said, "Hey, you know, we got you. Here's here's what, here's some advice that maybe will help you be effective in this responsibility." And I still remember you take a lot of a lot of different things. You boil it down to really two things that stick with me to this day. And kind of the first piece of advice is, you know, board members view you as the expert. They they

want to learn from you. And they, they also want you to earn their trust. You know, you are the cybersecurity professional expert on the management team. So they they they want you to be the expert and want you to be be there with them. And the second is kind of related. They want you to do well and be competent at the job. Ultimately, they're responsible for governing the company and making sure management is in control of the risk. And they want you to be successful in that mission because ultimately we want to be good at risk management for any company.

Jeremy [00:04:03] I totally agree, Robert. It can be difficult to articulate to leaders how cybersecurity ladders into business goals and the importance of investing in a robust cybersecurity program. Luckily, we're able to speak to two experts about these very issues. First, you'll hear our conversation with Chris Hetner, who I briefly introduced earlier. And then we're joined by Dr. Kevin Charest, CISO and CTO of HITRUST, is equally qualified by his career experience and two major organizations and tenure with ISC².

Robert [00:04:32] Yeah, I think two great guests and we have lots to discuss, so let's get right into it. Hey, Chris, welcome to the podcast. Thanks for being with us today. You've done a lot of things and I'm just really curious about your background and also kind of what you're working on around this problem today.

Chris [00:04:51] Yeah, I've been in space for about three decades that I was in the underbelly or in the belly of the cyber security market within Wall Street Financial Services, New York based mostly on the infrastructure security ops side of the house in the mid-nineties and then shifted to banking global CISO for GE Capital and it's a management consulting for EY, Marsh & McLennan company in New York focused on the financial markets, wealth management, hedge fund, private equity, some healthcare, actually. And then I spent four years within the Securities and Exchange Commission as senior advisor to the Chair's office. So I was appointed by named by Mary Jo White and Jay Clayton as the senior cyber security advisor to the SEC. And now back in the private sector for the last four years, largely focused on cyber security, risk management, governance. I support the NACD community as a senior advisor. So we've got about 24,000 corporate directors in our portfolio. We deliver insights, education awareness, risk reporting, and I also chair the NASDAQ Insights Council on Cybersecurity and Privacy and I also sit on the board.

Robert [00:06:18] Yeah, a bit of the space for a while. So the evolution of the space is fascinating to me. I am and just the fact that, you know, NACD is working in the space and, you know, you're there obviously leading inside of that. And the fact that we continue to see more and more guidance you're being being issued, you know, tells me we're growing up as an industry, although I think we've got a long ways to go, at least from my perspective. And I'm sure you've seen where it's worked perhaps and where it hasn't worked. But for a security leader or an executive in general meeting with the board, you know, what are some key principles or best practices that that they should keep in mind? You know, where do they start? How do they effectively communicate?

Chris [00:06:57] This is more of a business resiliency, so to shift that conversation and that that dynamic from cybersecurity being a traditional tactical issue to now it's really costing our business, whether it be business interruption, disrupting our operations, introducing financial cost, introducing, you know, legal regulatory class action suits, targeting directors and officers, you know, as this masses and creates more of a global systemic risk. Now suddenly we've got some other very senior folks that are going to be held accountable that are more interested in assigning resources. And and ultimately, at

the end of the day, you have to sign off on the information security policy. And so what you want is an ideal communication between the cybersecurity organization and the board that bridges that gap, that expresses cybersecurity as a business operational, financial, regulatory, legal impact. Unfortunately, we're out there to point most of our cybersecurity organizations and the supporting infrastructure the teams are still deep tactical. They treat cyber with a tactical hammer. I call the cyber security industry an echo chamber. It's self-perpetuating. It operates within its own silo, unfortunately. And that's not good for effective communication with the board because the boardroom is looking for more of a business oriented dialog. So that's where I think we have an opportunity to grow, evolve our industry, and it's got a long way to go.

Jeremy [00:08:40] You know, if I think about the traditional measurements of security, it's it's often for better or worse, [00:08:46]view it [0.2s] as sort of the outcomes that it creates in the absence of a more generally accepted measures and metrics for how good the security function, whether the organization is doing things like, you know, achieving the outcome of compliance with a particular regulation or I'm meeting all my privacy expectations. Is it is that fair or is there a different or better lens that should be used to communicate sort of the outcomes and how good the security organization is doing, addressing the risks it's meant to address?

Chris [00:09:16] Look, cyber compliance regulation does not necessarily translate to effective resiliency, and resiliency is really the centerpiece here. It's it's all about realizing that you're going to be attacked, you're going to lose data, you're going to have some type of interruption introduced by. And by the way, you know, it doesn't always have to be malicious. It can be an insider that just introduces erroneous code, accidentally sends a thousand records to a counterparty that wasn't encrypted. You know, we're humans. We're imperfect. Right. And so realizing that the events will occur, it's analogous to like driving down the highway, drive 85 miles per hour. You probably some point going to hit another car or realize like [00:10:04]back seat accidents [0.5s] occur. So so how do we create resiliency that is just to to to realize that the attack is going to occur, the events going to happen. What do we put in place in order to recover? There are metrics and measurements that are foundational. I use the analogy if you build a house, you need to have a sound foundation and that structure needs to be have maintained a level of integrity to ensure that you survive, whether it be a flood or an earthquake, whatever the event may be. In cybersecurity is very much similar. You need to have those foundational hygiene measures. So it's having that that ability to communicate the relationship between business outcome, the relationship of those exposures to where you have potential integrity issues with your hygiene.

Robert [00:10:55] If I'm sitting in this seat as a security leader, you know, what should I be thinking about to ensure that I'm meeting my obligations to the company, but I'm also supporting the management team in their obligations. You know, is this going to be a new place for all of us?

Chris [00:11:10] There's an expectation that the companies is taking the right level of measurements to make sure that that you're reducing the extent possible, the amount of risk. And through that lens where the SEC disclosures come into play, ensuring that transparency is really the centerpiece. You know, if you're a CISO or a publicly traded company or any company for that matter, or any organization and you feel that you're underinvested, you're missing core pieces of your cyber hygiene and basics and because of that can introduce material harm to your to your organization, your business, then that conversation needs to be had as soon as possible, upstream to the management team, to

the CEO and the board of directors. And so I would lean on transparency if your organization, your team, to go through a new in the role, you feel like you're not necessarily running on all cylinders in terms of capability. You may want to hire an outside firm or somebody independent to provide a view as to how effective your cybersecurity program is. And then present that upstream to the board of directors and then put together a game plan for strengthening your posture and your remediation.

Robert [00:12:31] And it really leads me to the question about in dealing with a security event, I'm paraphrasing heavily, but, you know, it's not a it's not a if it happens, but when it happens kind of scenario. So the first question might be one of competency. You know, I trust the security leader and now we have a security event. You know, should I continue to trust that leader? Is it this transparency you're describing that is really the key to that being transparent with the board as you work through the event? You know, how do I engage my board on that tough day?

Chris [00:13:01] It's an area that's understated, underappreciated, the level of reactiveness that occurs within a cybersecurity organization, particularly within the CISO function. And so what I what I encourage folks to do and I've done in the past in my previous roles and even in my role with the Securities Exchange Commission, working with the U.S. Treasury Markets and the financial regulatory bodies is we've ran a series of exercises. We call them tabletops. We've done drills. We run different scenarios that introduce the cyber event into the organization. Well, that does it provides the training and the muscle. Whether that occurs and you're in the fight, you're in the battle that there's an understanding that, wow, yeah, we've actually done this to where it's at the top now. It's a real time event and it's time to execute our our management response plan. And I typically lean more towards a crisis management response plan. So again, it's it's diverts the sole responsibility of the event management, from the CISO to enterprise risk management to a broader crisis management team and so you're able to bring in folks such as compliance public relations, you know, general counsel, outside counsel, and this becomes, you know, more of a team sport versus the the individual, that's that's the proverbial putting out the fire.

Jeremy [00:14:40] [00:14:40]It's pivot, [0.0s] and talk about board composition. There's been a lot of talk in the past year about what the SEC may or may not require in terms of transparency about cybersecurity composition, cybersecurity skills on the board. What do you think that's going?

Chris [00:14:56] So there's a few things there. Cybersecurity was in the boardroom. Number one, first and foremost needs to be addressed regardless of whether you have experts or not. And the SEC in the investor community wants to see the substance of the reporting and engagement between management and the board. What's the frequency? Where do you roll into from a board perspective? Best practice suggests there should be a risk committee with a subcommittee of risk focused on cybersecurity and like minded risk domains such as supply chain, geopolitical privacy risk, maybe artificial intelligence type of exposures, or what I would call more advanced technology. As you're bringing these advanced technologies into the mix. It's the reporting as well. So it's bringing forward. And this is actually specified in in the not only the proposed rule, but I've been very vocal about this. The 2018 interpretive guidance clearly states that bringing forward cybersecurity risk as well as events or incident disclosures through the boardroom needs to be funneled through the lens of how these events or these exposures introduce material business. These are very concrete costs that need to be contemplated and brought in to your board deck that create more substance and in addition to frequency, where you report into the

overall touch point, the substance of the reporting they want to understand also, which is fairly new in in the whole proposed wall spaces, what level of expertise do you have on the board. So those are the types of disclosures that the SEC is proposing and wants to see in relationship to cybersecurity competency within the board of directors.

Robert [00:16:57] Are you saying in your experience areas where board members may have common misconceptions or misunderstandings about, you know, what the role of a security leader is or what the security leader deals with every day? Do you see some of that? And if so, what would that be?

Chris [00:17:14] You need to as a community be more be more expressive to the non-technical folks. And because this is now becoming such a broad systemic issue across our economies, across our enterprises, and was starting to see requirements being put forward, such as the SEC requirements on cyber competency and oversight beyond just tactical is bringing more of a business context. So so I would encourage CISOs to participate in other events beyond cybersecurity. There are no shortage of financial markets, events, accounting events, conferences that look at a wide range of risks such as ESG principles or perhaps there's something on regulatory. And what that does is it broadens your aperture, it broadens your muscle. You're now more communicative beyond just having the cybersecurity conversation.

Jeremy [00:18:19] It was really great to chat with Chris and get his unique insight into communicating with the c-suite in the board. So a key takeaway as I learn more about the CISOs board interactions specifically and sort of what the CISO needs to hear about the cybersecurity efforts of the company is that, you know, the CISO isn't asking for permission to go out and do this or that. Instead, the CISOs communication to the board is one of information sharing and informing. Right?

Robert [00:18:46] Yeah. I mean, the board is the governance function of the company and at least four publicly traded companies they represent the shareholders and they're responsible for holding management accountable. So where a CISO needs to gain concurrence and permission to proceed in a certain way, that's permission and concurrence with the management team. And so, you know, that's where working with the management every day is really critical. So when you step over to talking to the board from a governance perspective, you know, you're talking to some incredibly brilliant people and well experienced business leaders who really aren't afforded the time to get into the weeds of any issue in the company. You know, management has the responsibility to run the company and the board holds management responsible and accountable. So short of requesting a change in management, which certainly the board has that that authority with regard to like the executive leadership directors oftentimes don't get it operational details. I wouldn't say it's exclusive, but in my experience, they're really they're really interested in risk management. And, you know, I, I have been incredibly blessed to have directors that have been good partners at risk spotting. I can think of times when they ask the question that caused me to say, "Wow, that's an interesting perspective, not one I had explored or possibly one that was related to something we did. And we could use the question to explain how the program works in practice". Bottom line management's dedicated 100 percent of the time 24/7 to managing the risk, the board is responsible for governing the company and governing management.

Jeremy [00:20:18] So we're now going to our interview with Dr. Kevin Charest. Kevin's our CTO and CISO here at HITRUST. That's not the only reason why we thought it'd be great to talk to him on today's episode. Kevin served with distinction as the CISO of HHS for a

while. He was also on the board of ISC², who is one of the largest security certification bodies for cybersecurity professionals in the world, and he ended his board tenure there as chairperson. So it was chairperson ISC², that's a no joke job, as well as being the CISO of HHS. So he's got a lot of valuable insight into sort of the cybersecurity landscape as well as the health care cybersecurity landscape. He's got a lot of experience developing and supporting security leadership and practices globally, and he's no stranger to boardrooms. Let's go to Kevin.

Robert [00:21:06] So for a CISO, that's meeting with the board, starting that relationship. Yeah. What are things you think about as a leader that's been where you've been that we should be thinking about as security leaders to earn that trust, to get the support needed to do the work we have to do.

Kevin [00:21:24] You know, the board is expecting you to be an expert. That doesn't mean you're supposed to know everything, but they are expecting you to be the expert in the room and to be most competent and capable, but also recognize, generally speaking, we're talking about publicly traded companies and or even privately held. But the reality is the board is there to handle that that governance oversight [00:21:50]unreflective [0.0s] team. And so we're looking for the chief operation security officer to be pragmatic as well. Right. So can't walk in with disguise following. There's always an attack. There's always a new attack. There's always an emerging threat. There's always a crisis to endure, if you will. So what they're looking for, I have found very often is to understand that you you both understand the landscape, but you also understand the [00:22:21]internal [0.0s] business. And furthermore, that you have in your ability and by you I mean the entire information security structure of a company smart mind and body in one person, obviously. But then you have the the team, the tactics, the procedures, a plans in place to address a myriad, you know, a number of factors. So from that standpoint, it's it's a wonderful opportunity to engage in a really deep conversation about risk and how does it feed how do cyber security risk fit into the whole enterprise risk management as well. And then for those companies that have strong compliance requirements, you know, whether they be from federal or other or under or state, local or compliance requirements, you can really paint the picture of how all of that remains together. But to do that, you have to understand it yourself and you know you have to come equipped to have that dialog.

Jeremy [00:23:25] Yeah. So thinking about what boards often view as outcome based achievement based measures in a business, so I'm meeting my sales goals, I'm meeting my profitability goals. Security is tougher to measure in terms of concrete, quantifiable measures and metrics. It's one thing to say yes or no. I'm achieving my compliance goals, but that's only part of security. What are the appropriate measurements and measures that a CISO can bring to a board to help communicate the effectiveness of his or her program?

Kevin [00:23:57] Yeah, that that's a great question, Jeremy. You know, because we often joke about, you know, we spend our lives trying to prove a negative.

Jeremy [00:24:05] Yeah, it's tough to prove that the attacks that were attempted didn't happen.

Kevin [00:24:09] But if something bad happens to somebody else, well, the first question you're going to get is, well, are we having that problem? Are we having that challenge? And when you say no, we're good, the question becomes, why do you know? Well, and therein lies a whole a whole dialog, a whole conversation, because it is difficult to prove a negative. So the way you do that, in my opinion, is to talk programmatically, right? It is to

speak about, as you said, well, compliance probably is more easily quantifiable than other elements, you know, of the various security domains that need to be in place for a quality information security program. And so that's really what I always relied upon was speaking your cross those pillars, right, those those information security domains colors whichever phraseology, you know, might work for somebody. But it's really about understanding the full spectrum and then being able to show not only that they exist, but that they work together, you know, that they work in tandem with one another in order to have that full securing programmatic view.

Robert [00:25:28] So, Kevin, to just just maybe reversing the hat, if know from a perspective of a person that may be sitting on a board, you know, based on your experiences, you know, what are what are our board members thinking about when they're hearing an update from a security leader?

Kevin [00:25:43] So I think they're listening for a number of things, you know, in their role. We're listening to you, frankly, the level of support that the the CISO is giving, that experts giving, they're listening for gaps in what they're hearing, you know, are are is it complete relative to the business that to protect entreprises conduct. Sometimes what you don't say can speak louder than what you do. And so we're looking for some of those potential omissions as well.

Robert [00:26:15] You know, public companies need to have cybersecurity expertise on their board at the board level, you know, and we certainly have recently also seen companies that were breached a couple of years ago, have situations where their CISO has been notified that they may be in violation of SEC regulations, you know, quite recently. You know, what are your thoughts on all that, the role of security leaders on the board? You know, where where do you think that's going to go?

Kevin [00:26:41] I think it's a it's an appropriate response. I think it's particularly appropriate for a publicly traded company. So I would suggest that anyone would benefit if you really want to look for that more well-rounded, pragmatic approach. You know, as a as a long time professional in this space, I have to acknowledge that there's a certain reputation for being sort of the nights of no. And when you say no, and that's so we protect. When in fact, I would argue, good cyber security professionals building strong programs that provide excellent assurance, do it by not saying no, they do it by saying yes, but we need to consider these factors. Yes, we can enable business. Yes, we can enable innovation. Yes, we can enable new lines of business. But we need to do it with these elements in mind. And so I think having that kind of expertise on the board because, again, that the the strong cyber leader is a leader, right? He's an executive leader. He or she has got those experiences.

Robert [00:28:01] We're so lucky to have had both Chris and Kevin with us on the podcast and I enjoyed our discussion with them both. It's really cool to see that while they come from different backgrounds and have had different experiences, they mentioned a lot of the same points around security hygiene, security as part of enterprise risk or organizational risk management and strong communication. Said another way, we're starting to develop common science around this problem.

Jeremy [00:28:25] Tying it all together for me is remembering that the board has a much broader perspective of risk across the entire business, while the CISO has a more narrow but deeper focus on just a subset of enterprise risk, which is cyber risk obviously. So when communicating to the board, the system needs to build up the cyber risk, dialog and

narrative in a way that the board members can understand so that they can use that understanding to make them to help them make informed decisions around the whole of the businesses risk landscape.

Robert [00:28:54] Yeah, and I think, you know, we talked to some about cybersecurity leadership and, you know, you have to have a lot of flexibility and a lot of agility in your leadership approach because, you know, when I'm talking to the board, I can't talk about cybersecurity risk to the board, you know, the same way I talk to my colleagues and the IT team or at the Enterprise Risk management team or how I talk to my organization that runs and operates our security program. You know, if I go in at that level of detail, which is certainly important for our operators, yeah, I'm going to lose the board. It's just it's a different language or a summarization of that stuff. Yeah, there was an article back in April this year at the Forbes Technology Council that had a study that said that 90 percent of companies in the Russell 3000 lack a board member with cyber expertise, and only about 50 percent of Fortune 100 companies have even one. So, you know, our job is to communicate risk to the board. And we do that, to tied the business objectives. It's the business objectives that are the common language.

Jeremy [00:29:57] We focus on the solutions and technologies. But you know, the rest of the business, they want to hear about the outcomes, everything about why a lot of times that is to support the needs of the business, to help them move into new markets or to support a new business strategy. Yeah, but so that stat from the Forbes Technology Council article you talked about that helps me appreciate how impactful these upcoming SEC rules over cybersecurity governance might be for public companies and broker dealers and other kind of regulated entities.

Robert [00:30:27] So with that as the last word, we'll wrap up another edition of Trust Vs. Thank you all for listening to us. We're so grateful you're here taking this journey with us. If you enjoyed today's episode, we'd really appreciate it if you'd tell us what you thought, leave us a review or a rating in your favorite podcast app. We definitely want to learn and look at the things you are seeking us to look at. Thanks so much. Have a great day.