#117 - Good Govenance (with Sameer Sait)

[00:00:12] **G Mark Hardy:** Hello and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy, and today we want to share a special episode with you on good governance. Now, if you're like me, the term governance might give you a little bit of a post-traumatic stress disorder, because a lot of people have had management promise good governance in the past, which only resulted in creating a large committee that took everything under further study and consideration and now they have channels and long speeches and irrelevant issues, and they haggle over the precise wording and they really don't produce anything of value. So our goal today is to learn what good governance is while avoiding bad governance that falls short. So why do we even need governance in cybersecurity?

And the simple [00:01:00] answer is that governance emphasizes outcomes. If you can deliver great outcomes, then you become extremely valuable to an organization. The International Organization for Standardization, ISO defines governance as a following quote. "The system by which an organization is directed, overseen, and held accountable for achieving its defined purpose"

now that definition is exactly what C Suite executives want from cyber organizations right now. Executives wanna hold the CISO role accountable for understanding, managing, and mitigating the risk of critical data being disclosed (Confidentiality), altered (Integrity), or denied access (Availability). Now, if you wanna find a cheat sheet for getting really good cybersecurity governance, we recommend looking at the Cyber Risk Institute's website.

We'll put a link in our our show notes. And there you can find something called the Cyber Risk Institute Profile. Workbook or Profile is this commonly known? And just a quick background about the profile. It was produced from a partnership of over 150 financial institutions, [00:02:00] and you can think of the profile as the financial sector equivalent to ISO 27002 or NIST Special Pub 800-53. It's a list of 278 controls called diagnostic statements. And each of these diagnostic statements provide prescriptive guidance that organizations should follow to meet legal and regulatory requirements. And one thing that's particularly helpful is that, Each diagnostic statement shows examples of effective evidence, and this is helpful because you can show that your evidence meets the standard versus arguing with auditors about what's needed for each control.

So if we dive into the profile, we'll see that governance is broken into eight categories. One, strategy and framework. Two. Risk management. Three. Policy. Four. Roles and responsibilities. Five. Security program. Six independent risk management functions, seven audit, and eight technology. Now, rather than bore you and just kinda read through this whole episode, we're gonna do a [00:03:00] little something that I think you're gonna find a lot more interesting.

We've got an expert here who's done an awful lot of work in governance and is gonna be able to provide us with some insight in terms of how to do it right.

I'm pleased to have on our show today, Samir say to give us some insight in terms of good governance. Samir, welcome to the show.

[00:03:16] **Sameer Sait:** Thank you. Thank you so much. Nice to be here.

[00:03:19] **G Mark Hardy:** Can you tell the audience a little bit about yourself, your background, all the kind of cool stuff you've been doing?

[00:03:24] **Sameer Sait:** Absolutely. I'm a seasoned CISO, have been a CISO a few times. Started my career in risk management in financial services. Worked at some large enterprises, became a CISO at Aero Electronics. That was my first CISO gig. Then became a CISO at Forcepoint and then finally a CISO of Amazon's Whole Foods Market.

And then I decided to take the big plunge and start my own venture. So I have my own startup now in the identity governance space. So I guess I'm all about governance right now.

[00:03:55] **G Mark Hardy:** So there actually is life after being a CISO.

[00:03:58] **Sameer Sait:** Barely. Yes.

[00:03:59] **G Mark Hardy:** But of course [00:04:00] you get all burned out and things like that, you're like, but anyway, that's pretty cool. So you've had a lot of these great experiences. Well, what caused you to wanna get involved in governance and then focusing on that as a cyber professional?

[00:04:11] **Sameer Sait:** Yeah, it's a great question. When I started in the risk and audit space it, it was interesting because we would do these assessments to meet a certain compliance requirement. Typically, at that time it was SOX 404. Now we've got a whole lot more. PCI 4.0 came out, etc..

But I think that by meeting those compliance requirements, we got a false sense of security and we got a false sense of completeness of our security posture. And in, in general, I think governance kind of ties security to the business, to IT ops, to IT in general, or technology in general, where if you don't have those interlinking.

I'll use the word controls or capabilities. You tend to have a false sense of I'm good, right? And so for me, governance [00:05:00] became this kind of rallying cry for good strategy and good execution of that strategy at a more business and tech ops perspective.

[00:05:08] **G Mark Hardy:** So really governance, execution of strategy and being able to go ahead and ensure that things take place and that makes sense to an extent because if we don't have a way to oversee what's going on, it just wanders often in different directions, and there's no way that we can hold ourselves accountable to senior management of what's going on.

If we don't even have controls in place to make sure that we're getting done what needs to get done. Make

[00:05:32] **Sameer Sait:** Right. Makes complete sense.

[00:05:34] **G Mark Hardy:** So as you, as you look to develop a governance program, probably one of the first things that's gonna be required for any CISO is to come up with a cyber strategy and a framework. Now, of all the things that are out there, what would be the criteria that a CISO should use to try to select a cyber strategy in a framework?

[00:05:51] **Sameer Sait:** That's again a great question because I think it and I, I hate to say it depends, but it, first time CISO, small company. Versus a [00:06:00] Fortune 500 public trade company, right, with a board, etc. I think you can't go wrong by looking at NIST and what NIST offers, because the NACD refers to it, and the board is well-versed in some of the terminology NIST. I've worked with large companies that are global and they've adopted ISO before I got there. You can look at that. I've seen some things, really great things from the financial services industry on their control frameworks. So I think it, it depends on the industry. It depends on the the maturity of the organization or the expectations more than the maturity of the expectations, right?

You really wanna work backwards from what the board and the executive team expect and the language that they use. And we'll get into more of that, those details, but NIST has been my go-to for the last, I wanna say two jobs.

[00:06:43] **G Mark Hardy:** Yeah, and I guess I had on last week, it was over in Austria and he's basically saying, well, NIST is what you Americans use and ISO is what the rest of the planet uses. Well, not, he didn't quite say it that way, but it was sort of implied that we have our own little area, and yet if you take a look.

At some of these strategies and frameworks, they're [00:07:00] not radically different. Now in the this world, we sort of focus on here's how to do things as compared to, as Michael had said, with respect to the iso, here's where we want you to be. You figure out how to get there. And. In that regard, it suggests that there are things that you have to think about.

If you're an international company, you may be required to meet a compliance requirement for an ISO standard. If you're a federal contractor with a Department of Defense, we see CMMC coming along requiring compliance with the NIST 800-171 set of controls and things such as that. So there's a lot of different templates that are out there in the selection of them. All things being equal. If you don't have a legal requirement and you don't have a contractual requirement and you don't have a existing requirement, then it seems to, as you had suggested, be based upon how big is your organization, how complex do you really need to get, because it doesn't make sense to build a massive governance [00:08:00] operation for a 50 person company.

[00:08:02] **Sameer Sait:** Absolutely. And I wanted to add one more comment to that. I think there's some of the frameworks that I was not exposed to till I worked in international development organizations like the World Bank, right? They had INISA and that would come up a lot when we talked to our European peers. And as a bunch of controls in that, again, Terribly different than what you mentioned earlier with ISO and nist, and sometimes it's just about, making sure we're all speaking the same language.

And maybe even for the sake of continuity, just tying it back to the original framework that everyone is so comfortable with. Right. At the end of the day, it's all about the same outcomes and, and that's the, that's the end goal.

[00:08:38] **G Mark Hardy:** and and that makes sense. I mean, once, once a CISO has selected a strategy and a framework, let's presume that you either didn't inherit one that you had to use, or perhaps you have, there was one from your predecessor that didn't really make sense, but at that point in time, you need to be in the convincing mode.

You have to convince the executive leadership team [00:09:00] to buy in. What are thoughts about how to do that? To make sure that they say, yes, Sameer, that makes sense. Let's go ahead and and use this governance model.

[00:09:08] **Sameer Sait:** Yeah. , Great point. I think I've seen this happen and play out when we've done M&A activities where the company we're buying has a different approach and framework, etc.. What I've learned through this process is, If it aligns with the industry where you can factually say, 80% of FinTech startups are following this approach.

Right? And this is a Gartner survey, PWC survey, etc., as one approach. The second is the framework we have or the way we've adopted it, is overkill, right? And we need to scale back to really focus in and meet the business and operational risk that we are faced with, and then add on layers as we mature, as we get bigger.

I've seen different approaches work, but if anytime you ask for more work from a company or a team you have to have a very good reason. And usually it's a benchmark of some sort.

[00:09:59] **G Mark Hardy:** [00:10:00] So being able to refer to that then allows us to then also have an objective measurement. And if somebody is pushing back, well, why do I have to do that? Why are you making me do these things? As well. It's actually an existing framework that's industry-wide or national, or even internationally accepted.

And so to a certain extent it sounds like that makes it a little bit more sellable to somebody who's gonna push back.

[00:10:22] **Sameer Sait:** Right, exactly, the other one is explaining why. I think a lot of times early in my career as well, I would say we have to do this just because everyone else is doing it. Right. Versus, and that might be a good starting point. You have to kind of position it to why this is important, why.

Us speaking the same language, having the same framework to, to play off of and defining ownership. Not to say it's all on you, like it could be you're responsible, I'm accountable, this is who's consulted. It gives a sense of partnership, right and sometimes I've noticed that by having the pre-meetings, with the board member, with the executive team explaining them, getting them on on your side.[00:11:00]

And if you don't get them on your side, then you have a different kind of set of discussion items, right? But when you get them on your side, it makes it much easier to have that dialogue of that change because for me it's change management. Change is hard. Just any company doesn't matter if you go to the CEO and get him to buy in.

But getting more people to buy in to the change is always better.

[00:11:19] **G Mark Hardy:** And that's always, of course, the CEO's challenge is setting a vision and trying to get everybody to follow it. And of course, as CISO, we may be facing that same issue, even if we can convince the CEO O, you're still only at block two out of a hundred steps instead of it being far down along the line. But if we think about boards and executives, and one of the things that they need to do is take measured risk.

That's how you grow a business. That's how you maintain things, is you accept some amount of uncertainty in exchange for the opportunity to do well. And so as a result, we have different metrics like risk tolerance and even risk appetite. So if we look at an organization's risk tolerance or their appetite, how might [00:12:00] that change the cyber strategy of an organization?

[00:12:03] **Sameer Sait:** This makes me think about things like budget and headcount and outsourcing versus insourcing and, capabilities. It's a broad question, so I'm gonna do my best to kinda keep it in check, if you will, to what's relevant. I've seen people take a top down approach of these are the best measures of these controls that come out of this framework, and let's leave it to the teams, the individual leaders.

If you're a large organization to find the best way to measure it, right? Working with their IT brethren and outsource provider, etc.. I've also seen, and this is where kind of the Amazon mindset comes in a little bit, which is what are we seeing? What are the details? Let's start working backwards from the details and then let's create better governance measures.

Let's say, is our threat intel program working effectively or are the signals we're getting valuable for our business unit? Right. And I think that's where, again, the culture comes in. I do think it's important to stress test everything. So if you do get governance level [00:13:00] metrics, running it by your team and seeing how they would measure it.

And how often they'll measure it and if they get value from it as well, right? From measuring it, not just you being able to go and turn it and throw it in front of the board, then you've got a win-win situation and vice versa, right? Smart people will come up with different ways to measure the efficacy and efficiency of their programs in your organization.

How can you turn that into a story that the board can understand? And when I say story the reason I bring up the word story is because just throwing a metric without context without good, bad, ugly, without an outcome that is moving the needle. And we'll get to what kind of needle we're moving will result in more questions and more alignment.

Right? And, and you don't want that.

[00:13:41] **G Mark Hardy:** Well, it's interesting what you mentioned because as you're explaining kind of the Amazon way, it sounds to me it's more of an inductive than a deductive process. Deductively, I would say, let me start at the top level. Come up with some sort of framework, some governance model, etc., and then go ahead and work out the details.

What you described is, let's look at the [00:14:00] details and see what would fit those details. And since you've been in more than one CISO role what would cause you to choose one approach over the other? Is it just culture or is there something that's a little bit different that would allow someone to say, Hey, this is a better approach then that.

[00:14:15] **Sameer Sait:** I think culture is only part of it. I think you're right now that I consider some of the situations I've been in, I think for a first time CISO having to come in. Without a lot of security DNA within the company would probably take that more top down deductive approach, right.

To start and say, this is what, best practice aligns with, right? With a company that's more mature, that has security built into the dna, of like an Amazon or, think about large companies that have spent a lot of money on security over the years. I think there's a little bit more negotiation on the inductive side because measurements have been put in place. Now, are they valid? Are they not? Are they valid maybe in the future? Is that a leading indicator that we wanna talk about once we have some of our baseline metrics in place? Those are discussions I felt [00:15:00] were very valuable in a company like Amazon.

[00:15:02] **G Mark Hardy:** Well, that makes good sense. Now, another thing I think is really important for CISOs to establish is an effective risk management program. Now, have you found any helpful ways to ensure that business priorities, constraints, risk tolerances, and even assumptions effectively support the operational risk discussion?

[00:15:20] **Sameer Sait:** So it's interesting you brought up the operational risk piece because. Having worked in financial services right early on, and it might have changed since then since I've been a CISO, but cyber risk was always a line item with an operational risk. Right? And over time, I think having talked to a number of Fortune 500 CISOs in the financial services space, I think cyber business continuity, resilience, disaster recovery areas that were quasi IT run and quasi cyber run and quasi business risk run Right. Became part of the same dialogue for operational risk. Right. And so, [00:16:00] again, going back to culture, I think financial services companies that have an operational risk committee or ORM function operational risk management function will have some ways of working some expectations on how you fit into their larger reporting and data collection mechanisms.

And that's where you have a little bit less leeway. In bringing your risk management mantras, if you will, right? I think in places where a tech company, let's use Amazon, Google, etc., I think cyber risk measurements become a much more quantitative discussion because you're working with a lot of engineers who really want, fine grain data to work with and they want, they want everything automated, right?

So they can kinda get it real time. And then you've got everybody else in the middle. And I don't mean this in a bad way. I think healthcare might be closer to financial services, but you've got a lot of, the 80 20 rule, right? A lot of folks in the middle. Who will look at this and say so I've got a framework, I've got some governance controls now, which are my key controls that [00:17:00] I wanna measure that will align with two things, right?

One is, My day-to-day operational activities, keeping the lights on with a cyber bent of making sure those lights keep, keep on right and don't go off. And the second is business activities, right? I've got a, a one year goal or two year goal to move seven applications to the cloud, right?

Cloud native we're looking to do some M&A activities, right? And so how do you measure that cyber risk findings were closed in a timely manner? Accepted, blah, blah, blah. You have to have those two modes of operating, right and that's where risk management measurements of those key indicators, key controls come into play.

[00:17:40] **G Mark Hardy:** So we look at the. When we look at measuring them, but there's also the concept of a risk register, and sometimes we find that, could the cyber function just simply be a collection point for risks? For example, a business goes out and buys some software, but it doesn't support SAML. But that's a standard.

But yeah. So what, or the vendor doesn't have a SOC two type two report for review, but [00:18:00] we go, yeah, but so what? I mean, at some point in time, does the business need to sign off on these risks as being accepted, or is it not even worth documenting?

[00:18:10] **Sameer Sait:** That's such a great question. I, I've been on both sides where I've had a never-ending risk registrar that goes back seven years with no closures and having to look through that and get alignment. On the other side, being the annoying CISO that sends auto emails to the owners of those risks to remind them that they still have an open risk.

Right? I, I don't, again this is a tough question and a good question, but I'll say this. Visibility at multiple levels is important. I, this is why I think the CISO job is so hard, this exact reason because exception management, risk approvals the ownership of risk. The mindset I've noticed is when the word security and risk are used, or cyber risk is used, there's an automatic assumption in a number of organizations that the owner of that risk is a CISO.

Right? Which is completely in my mind not accurate, right? And [00:19:00] so, I found the best way to deal with this is to document everything. And this is something I learned from Amazon as well, is to document everything but have enough committees or mechanisms of committees that you don't even drive or own, let's call it the operational Risk Oversight committee.

Right. Or the privacy council, or I, I can name any number of councils that have already been set up in certain organizations. If they haven't been set up. The CISO should set one up to provide that visibility. Take a non-confrontational app approach to talk about how this is a shared business risk. That whether technology owns part of it and cyber owns part of it doesn't matter.

And what are we gonna do collectively to accept it? And what are the outcomes that we're accepting? Right? The potential outcomes. I mean, not every outcome is gonna be bad, but there's good, bad, and ugly. I always say, you, you never go in and say, well, the world is gonna fall apart if you don't approve this or, or you or you don't.

You don't fix it. So, I think that that's where the negotiation [00:20:00] and the political savvy of a CISO comes into. To get things done.

[00:20:04] **G Mark Hardy:** Got it. Now, another thing I'm seeing that CISOs use as a resource to help get things done, are there cybersecurity policies? And if we have, let's say, go to Fortune 500 company tomorrow as a CISO and I walk in the door, what recommendations do you have for me to assess the state of the cyber security policy library and knowing whether it's good enough or whether it's missing something, and then in anything particular you would recommend looking for, other than simply perhaps, is it, does it have a lot of dust on it?

They haven't looked at it, or has it appear to be dogeared and are they using it on a regular basis?

[00:20:37] **Sameer Sait:** Again, I think if I'm coming into a CISO role and I'm documenting new policies that haven't been put in place, the first question I ask is, by documenting this and working with legal, I wanna understand, is there any exposure to us for not being compliant? And I get it, it'll take 3, 6, 9 months to meet the bar of what we've documented, right?

It's okay. There's a vacant period. I get that. But if the [00:21:00] measurement against the policy. Is super painful to the point where my 2, 3, 5, 7 person GRC team is just chasing data collection to measure policy compliance. Then it's not worth it, right? So I wanna make sure if I'm working backwards again are we capturing this data?

Are we sure? Are we sure there's only one way to to push code to production, right? And so once we get that alignment that there's only one way, and we're meeting that baseline of let's say code deployment then I can measure it. I can get data, I can get metrics, and I can say we are, we are compliant.

The second thing is coming in. Not writing policies for the sake of writing policies. It, it's very easy to get frustrated. I've been there where you're not getting traction with your business teams and you're like, I'm just gonna write a policy on, B Y O D and that way they can't go out and buy tools and technologies, etc..

Right. I think writing. In partnership with the people that are also in a difficult spot, right? What I've learned is sometimes IT, or your CIO doesn't have control over it. So how do you partner with your [00:22:00] CIO and say, when we write this policy, how do we get the engagement? And then how do we make sure we're doing it with the right intent for the business in mind, which is cost controls, data control, data loss prevention, etc., etc..

I think just thinking back I've written policies to meet compliance requirements, ISO, NIST, etc., but then I've also pulled back and said, let's not make this into a policy. Let's make it a standard operating procedure or a guideline and get buy-in, and then as we mature, move it into a policy.

So I've taken some of those approaches as well.

[00:22:32] **G Mark Hardy:** Right, so basically started a lower portion of the policy pyramid and work our way up now if you get partial buy-in. If you get some business units that go, okay, fine, but you get in a couple other business units, they're like, well, forget that. How do you create accountability and ultimately push for a bit of a culture change in a way because that's ultimately how are you gonna happen?

I mean, I think it was Peter Drucker says culture, each strategy for breakfast. And my corollary is culture eats policy for lunch.[00:23:00]

[00:23:01] **Sameer Sait:** Nice. I think there is where you take some of the 80 20 rule and say there's 20% who are going to be naysayers feel like we will slow them down. The previous CIO, CISO, it ops guy, was so hard fast that we had to do it our way, otherwise we'd never get anything done in this company.

And so, again, going back to is it measurable? Is it consumable? What do we have to change in it and security to make it worth your while? Right? Is it centralizing the cost structure. I've used this tactic and said, I'm gonna work with, my executive, the COO, the Chief legal Council and say let's centralize how we do certain things.

And so, they won't have to spend it on their P card. and have to buy laptops, right, for example. And so, they don't have to hire three people to do provisioning for example. Right? And so, and that can be a different challenge because some people want to hold onto their headcount, right? And so how do you negotiate those things?

They take, they take a little bit longer. And then when you really have stragglers, that's when you call out the [00:24:00] exceptions. And I think it, that's where it calls out. This exception has a medium risk. Right. Be, be factual, be honest and say it might not be a high risk, but there's a medium risk and this is why they want to continue on this path and then get approvals.

Right. For that exception.

[00:24:14] **G Mark Hardy:** And as you said earlier, the CISO doesn't own that risk, and we gotta be careful to avoid somebody trying to go ahead and dump it on you and said, well, okay, you're the chief scapegoat officer. And like, no, no, no, no. I'm, I'm, I'm here to ensure that, that this program has run effectively, but you identify the risks for them.

They make a business decision as a business unit manager or above to accept the risk. And if things go well, great, you got, lucky you. You rode around without a seatbelt at 90 miles an hour on the ice and you got lucky. But sometimes you find that luck is a very poor strategy and as a result that's that accountability that we're talking about.

And as long as senior management backs that up and you say there, I'm here to. Executives make informed risk-based decisions, [00:25:00] then that's my definition of what effective cybersecurity executive does, is you just make sure that other people, you're not making the decisions for 'em, but you're not letting 'em make it in the dark.

[00:25:09] **Sameer Sait:** Right.

[00:25:10] **G Mark Hardy:** So as we look at roles and responsibilities for an organization, if an organization appoints a CISO, which a lot of 'em are doing these days, then how do you assess if that role has the appropriate amount of authority to get the job done? You may be responsible for things, but responsibility and accountability and authority are all three different things. Responsible means you're the guy that we hang if something goes wrong, the authority means you can direct people to make it done, and the accountability is that you're on the hook for it.

[00:25:37] **Sameer Sait:** I think a lot of organizations make the mistake of make the CISOs accountable for everything, but responsible for nothing. On the flip side, make them accountable and responsible for everything, but not give them the headcount or the budget or their resources to do it.

But they have to go and influence teams that don't report to them, which is also very hard. Right. I think that again, starting off first time CISO in a new company that [00:26:00] has never had a CISO before or a company maybe not new, but has never had a CISO, I think drawing those lines of demarcation, the seize is one, the boundaries is another.

Right? The handoffs, if you will. And I think if a CISO is coming in and you're just dumping on few headcount and saying you are accountable for all security, I think even that has a, potential bad connotation because at the end of the day, You might give me a bunch of security operations guys who find a bunch of issues who discover a bunch of vulnerabilities, but the people actually making the remediation is not in your team.

And then you go out and have to report and say they didn't do their job, which is not fun. Right. So I think What I would say is to aspiring CISOs or CISOs in this position is to not take on more than they can chew, because it's not always fun to be the guy making the change in a system that might go down.

Right? They might be tried and tested procedures, but I think providing the team that you have to work with, the fact that you're accountable for reporting the risk, [00:27:00] which is not to put them under the bus, but you have to give visibility on the risk posture that these are the kind of metrics we're looking for, and these are the kind of SLAs we're looking for, and building those partnerships and having a couple of those rough meetings, it's okay to have a rough meeting where you show up and you're like, well, we didn't really patch or, we got a third party and they didn't go through the third party risk assessment process and we missed it and we collectively will go fix it.

When you say we. And then you negotiate what you do versus what your counterparts do and come back in a better spot. Right? It's okay, but there's visibility that things need to be fixed. The last thing you want is for leadership to think, oh, we gotta CISO, and everything works amazing, right? I always say, let there be a little bit of friction early on.

And you will work through it. Sometimes a good place for change.

[00:27:51] **G Mark Hardy:** Yeah, that makes sense. Now, what if you don't have the resources to get things done? You've got all these opportunities, you've got everything cleared out, but you're horribly understaffed. And we're not [00:28:00] talking about just the lack of people out there and all these open jobs, but what if the organization just has said, not so much that you can't find them, but, well, we don't think you need these people.

How do you convince a leadership team that you need these extra resources to get the job done?

[00:28:16] **Sameer Sait:** Yeah, this is great. And I think, again, coming in as a new CISO, right, the expectation for a lot of leaders who don't understand our industry and we don't understand some of the things they do. So it's, it's a give and take. Is, well, IT has 20 people doing helpdesk, why can't they do monitoring? Right?

I've heard that kind of thing. I've heard, well, we've got a compliance person. Why can't he or she do a cyber risk assessment. Right? And so you don't just talk about a skills gap. That's one easy way to say, well, they don't know cyber, so ah, we can't work with them. The better thing to do is to work with those leaders who own the help desk, that own compliance and legal and say, do your folks even have the bandwidth?

to support my needs as a dotted line, [00:29:00] right? And then we can get into the skills discussion and more of the granular discussions. The second thing is, what is the volume of work, right? So I've got 500 vendors, 10% of them have gone through a third party risk process and we missed five controls.

So I almost wanna create a pyramid funnel and say. This is the landscape of what I'm dealing with. This is what's been done. This is what's been done partially. This is not what's not been done, and this is where we'd like to be in order to get a handle of our environment. And, I'll say this out loud, but unfortunately, or fortunately for large companies, I've had to bring in consultants to validate and verify what I'm saying.

Right and the big four well-known cyber risk consulting companies will come in and benchmark you and say, Hey, he's right. Early on we did the whole BitSight thing that didn't go great. It wasn't too happy with us, but you have to find ways to get external data to support your assertions as well.

[00:29:51] **G Mark Hardy:** And with that data, what we're able to do then is provide some sort of metrics to say, Hey, our security program, we're measuring it. And of course we want to measure it, we wanna [00:30:00] improve it. And so, Other than, as you said, no prophet is honored in his hometown, and you gotta bring in that external consultant.

What have you seen as effective ways for measuring cybersecurity across an organization? Insofar as it can then be used to help address making some corrections or changes or modifications to the, to the entity, rather than just simply you fill out a report, you got a number, then it goes into a, into a bucket.

[00:30:24] **Sameer Sait:** I know. I think and again, I always talk about influencing peers first and, and then talk about leadership because I truly believe it's a, it's a team sport. And so, I'll use an example of an area that I'm passionate about, which is identity governance or identity lifecycle management, right?

There's a cyber risk component of somebody having too many permissions. There's a customer impact of somebody not having the permissions they need to do their job, and there's a productivity component of people not being able to be onboarded in a timely manner with all the permissions they want. And so when you think about the measurement and you add risk to it, right?

First you measure the process, which is [00:31:00] how long does it take when someone joins to get all the birthright access they need? Once they get their birthright access, how do we audit to make sure. that it's not over permissioned over time, right? People who've been there longer. And then when people change or leave, how do we make sure those permissions have been removed in a timely manner, say less than 24 hours, right?

And how good are we against this end-to-end workflow and process? And when I think about this process, you're including HR. You're including IT ops, you're including security from a risk perspective. And you're including your customers who will fill out surveys hopefully, or will give you some data as well to say what happened and why they got the wrong set of permissions, etc.

And so I think when you audit that end-to-end, you can then start calling out, this is the risk. Right of the end to end. Right. And I think it applies to a number of areas. Yes. There's obviously areas that are only cyber focused, right? I got threat data, I did action on it, and then there's a vulnerably exposed, right?

That's a little bit less involving of HR and it maybe a little bit legal, [00:32:00] but if you can start with the ones that are well known to the company, right? Introducing a new concept like, oh, I need a threat intel operations team to measure a risk around that. People are gonna look at you like you've got three different heads on, right?

And so starting with knowledge and experience of people that are already there that know a little bit about it, risk and governing that, and then expanding on that would be a smart move in my eyes.

[00:32:22] **G Mark Hardy:** Well that makes good sense. And so we're influencing, if you will, our peers and then maybe, semi subordinate organizations, not because they're below you, but you said it's an influence operation and that's really one of the, the critical skills for a CISO, because rarely do you have the line authority over all the people whose behavior needs to be changed.

But let's talk about going the other direction, because a lot of times regulators wanna. Cyber has an important reporting line up to the executive and senior leadership team. So how do you ensure that you could report risk findings in an independent manner without having it filtered as it goes along the way by the CIO or the COO or whomever you report to?

Because those people don't wanna [00:33:00] look bad, and quite often to accomplish their tasks and their missions, they may have to blow past security. To meet a deadline, and yet that's a risk that may not be effectively communicated to senior management. How do we get that independent communication?

[00:33:13] **Sameer Sait:** To the board you mean? Or to audit

[00:33:15] **G Mark Hardy:** board.

Yeah.

[00:33:15] **Sameer Sait:** Yeah.

[00:33:15] **G Mark Hardy:** Up, up, to the top because they need to know that, hey, there's been unrealistic expectations placed on my fellow executives. And so this isn't you running around and tattletaling on your boss, rather, this is a matter of you trying to cover and saying, Hey, do you really realize that if you want this thing deployed by the 30th of June, that we're gonna have to skip all these security controls and things like that?

And if you're willing to live with that risk, we can be up and running on one July. , but the thing could go horribly wrong if something went off the rails. And so as long as you're informed risk-based decision, you're good. But how do we keep that communication open to senior management?

[00:33:51] **Sameer Sait:** I think about when I first presented to a board or an audit committee subset of the board I think the world has changed since then. I think there's a lot more [00:34:00] transparency through the NACD and other periodicals that have been published to board members to understand what their role is in managing cyber risk as well.

Not just our roles as professionals. I think the first board meeting for me has always been about the 30 day learnings of the organizations, or 60 day learnings of the organization's security posture. Getting the nomenclature right. What does a crown jewel mean, right? I've, I've used that quite a bit.

And typically being ready for the, I'd say the top five to 10 questions that always end up coming, right? It's open-ended type questions. How do you know we haven't been breached? Or how do you, how do you feel about our ability to detect breaches? I think the framework is a big one.

You, you asked about that. I think measurement is another one we talked about, but I think the big one that always comes in the audit committee where we have to be prepared in advance is where does external audit see your deficiencies? Right? Are you in alignment that those deficiencies that they've rated as a high risk are your high risks and why not?

Right? So funding that alignment is super important before, and so that executive leadership discussion before [00:35:00] the audit, meeting with the auditor to get that alignment is important. The second is as you said, you're a steward for the risk. So you bring up, this is why I think these are the top three things we need to work on as a company using the data of alignment.

And then oftentimes I've been in situations where I've come in where there's been a breach already, right? And so there's ongoing dialogue around what are we doing to resiliency and hardening. Ensuring that doesn't happen again and all that stuff. That tends to be a little bit a different mindset with the board.

They're much more involved in, is this vulnerably exposed anywhere else? You have asset management and they'll, they'll start getting really deep into that stuff. So you have to have those additional, I'll call them supporting artifacts, right. To prove that we are getting there if we haven't already got there.

The mature companies. Now let's talk about where I'm coming in CISO number four, right after been around the company's been around, has CISOs for many years. It's more around alignment with business objectives, right? That's when it becomes more interesting about we assume you're aware of this [00:36:00] M&A acquisition.

Where do you see the cyber risk? And those get into, know, the more transactional and, and more deep dive into the, into the particular scenario.

[00:36:08] **G Mark Hardy:** Right, as you say. So aligning with the auditor is important because a, you don't wanna get blindsided, but also you want to be able to almost present. United front to the senior management to saying, Hey, I'm the person who is going to be able to implement these. The auditors are able to, create findings and as they like to say, findings get funded.

And so there's one way to go ahead and do it that way. And so don't see the auditors necessarily as an adversary, but again, Aligning with that, just realize that you both have a similar objective. That is to protect the organization and again, inform senior management of where the risks may lie. And one of the places risks may lie in newer emerging technologies, we're seeing an awful lot of change taking place like that.

How would we take a look at governance from an IT security perspective? In the technology space, is it applied? Do we wait till something grows and gets big enough to worry about it? Or are there ways that we can influence and be [00:37:00] involved from an early stage for companies that are doing technology development?

[00:37:04] **Sameer Sait:** No, that's a great question and I should have piggybacked off of that when I talked about the audit committee. I think there's a concept, especially in companies in technology where we talk about emerging risks or emerging threats or emerging trends. Not even using the word risk, but, or threats.

It's trends, right? For us in cyber and how do we take a high level defined control from a framework and apply it to an emerging threat. Right? And how do we look at it from a risk Acceptance, which is ideally not the case, but minimization, mitigation, and or transference.

Right. And so, laying out these options in advance, as you mentioned, as people are thinking about these emerging technologies that might enable their business, you start thinking about the emerging threats and risks that. Could disable the business, right? And then when they're thinking about, do I fund it here?

Do I outsource it? Do I work with a partner? Do I use chatGPT? I had to throw that in there. . This is where [00:38:00] this is where some of the concerns lie.

[00:38:02] **G Mark Hardy:** I had that on my bingo card, by the way.

[00:38:03] **Sameer Sait:** There you go, I think again, those alignment discussions will typically happen with your legal counsel because they're thinking privacy, they're thinking protection as well.

A risk committee prior to going to the audit folks and then getting that alignment before the audit committee. So you say security is involved with this from the get-go. Right. And does security have the biggest stick in the room? Maybe not. But we do have the ability to state our voice and be one of the seven or 10 players in the room.

And that's important. And that's why I think the audit committee likes to see engagement.

[00:38:36] **G Mark Hardy:** And that's some great insight and I think we could probably go on talking all, all day long, but I see we're just about out of time. And so, to go ahead and respect our, our listeners here, I'm gonna go ahead and, and put a wrap to the show. But Samir, this has been awesome. I think your insights in terms of good governance have been tremendous and for our listeners, if you'd like to learn more about our podcast, make sure you go [00:39:00] ahead and subscribe to us on your favorite podcast channel, or go to LinkedIn and follow us on there because we do more than just put out the podcast. We have a lot of good material and things such as that. And if you have noticed, we are now on YouTube, we're now doing our visual recordings.

This year, and if you're a visual person, you like YouTube, either go to CISO tradecraft.com to get the link, or just go to YouTube and search for CISO Tradecraft, and you'll find shows like this. So thank you again for being a part of our show. Sameer, thank you for our listeners for being a part of our audience.

This is your host, G Mark Hardy. And until our next time we get together again, stay safe out there.