CTL-CISO-Bill-Harmer (1)

Sat, Oct 04, 2025 11:21AM 12:50

SUMMARY KEYWORDS

cyber security, business impact, risk management, AI adoption, financial risk model, CISO role, startup advisory, cyber risk integration, acceptable loss, business shifts, SaaS contracts, AI governance, compliance frameworks, cyber threat, financial decision-making

SPEAKERS

Jo Peterson, Bill Hammer

J **Jo Peterson** 00:07

Hey everyone, thank you so much for joining. You're here today with us on clear tech loop. We're in the know and on the move. I'm Jo Peterson. I'm the vice president of cloud and security for clarify 360 and the chief analyst at Clear Tech Research. And I'm here today with Mr. Bill Harmer, who is the V CISO of Kill Switch advisory. Hi, Bill,

B **Bill Hammer** 00:27

how you doing?

J **Jo Peterson** 00:28

I'm doing great. Thank you so much for giving your time today. My pleasure. My pleasure. Yeah. So in case folks are new to the podcast, clear tech loop is a focus podcast series, and we're delivering sharp, real time insights at the intersection of cyber security, cloud and AI security, and this session is part of the series of conversations with it and security leaders that are navigating a new era of risk and responsibility. But it's not just about protection. We ask what they see on the horizon and how they're preparing for it now for a three question lens. But before we get into the questions, Bill, tell us what you're doing with Kill Switch advisory.

B **Bill Hammer** 01:09

So I started Kill Switch advisory to bring an adult in the room to the startup world. You know, I have, I have nearly 30 years in startups and cybersecurity. I have four exits out of six startups, and I'm looking to bring that to the community and help startups grow.

J Jo Peterson 01:32

I think it's it's a great niche, and you can bring a wealth of experience. So let's get right into the questions.

B Bill Hammer 01:41

Sure.

J Jo Peterson 01:42

Thanks. From a CISOs perspective, how should you be thinking about cyber security in terms of dollars and business impact?

B Bill Hammer 01:51

Cyber security should honestly be proportional to the risk accepted. What is it that you can and can't accept? I think looking at it as a percentage of IT budget is a bad way to go. I think looking at it as a percentage of revenue, maybe the honest truth is, CISOs need to look at their business and understand how they make money. They need to know exactly how they make money, because that'll tell them what they can and can't survive, just because. And I've used this example before, and I'll continue to use it, because if you look at General Electric when they're looking at what intellectual property is important to them, the washing machine division is not terribly important in the sense that, you know, it's colors and features. And if something happens, it's, it's, you know, it's going to hurt the bottom line, but it's not going to hurt it the same way that the jet engine. That the jet engine division would. So that gives you the the idea of how you should be allocating your your cyber security dollars, against the risk to it's not the risk of something happening, it's the risk of what you cannot survive. So that's more the way I think you should be looking at it,

J Jo Peterson 02:58

right. And that, you know, to your point that changes by vertical

B Bill Hammer 03:03

right? And it changes on a daily basis too. You know you may have a shift in your business model. And this is, again, you know why CISOs absolutely need to have a seat at the table, because those business shifts sometimes don't get trickled down to the the personnel as quickly as they should. And if a CISO is defending or putting money into or building a program which are not typically easy or agile and can't be adjusted super fast, you can't suddenly change your strategy. But you know you and you don't know that the board has decided, Oh, we're going to focus on Division A instead of division B, because we know in the future, division B is going to have some resource issue that's going to cause problems. So we're going to get out of that business and get into this business, but you're still thinking B is important, and

you're sinking your your dollars into that. That's why we've got to be there understanding what is happening with the company, and how are we driving this company so that we can properly protect it.

J Jo Peterson 04:01

That's great advice. And I, you know, just made me think about a CISO that I know, quite clever gentleman, I think. And he, he has his whole team read the 10k there you go. Because you know and you know it, and I know it, we do a really great job of training technicians, but we have a hard time helping them make that next leap to leaders in terms of their communication sometimes and what they should be focused on. And I thought that was a great way for him to sort of teach them to think like the leaders of the organization were thinking,

B Bill Hammer 04:44

Yeah, you know, read the 10k listening to the forward statements for a public company, private companies, it's a little more difficult because they're not around, and that's where you got to figure it out. That's, I think, a big challenge that we have. But no, absolutely, it just makes them more adaptable. So the security world, I don't know how well a lot of us deal with acceptable loss, but that should be in our lexicon. We should be talking about acceptable loss. We should look at our business and say, It's okay if I lose my marketing department laptops, they get compromised, big deal. Format them and go, unless I'm a marketing company, right? Like, I mean, that would be a horrific thing if I was a marketing company delivering marketing services to my clients. So, so understanding those types of situations and being current. It's this is not static. We don't fire and forget here. You know, we have to be looking at this every day to understand what's happening.

J Jo Peterson 05:38

Yeah, really. Great point. So next question, in your opinion, what is the best way to integrate cyber risk into the business's overall financial risk model?

B Bill Hammer 05:48

Truthfully, cyber risk is the financial risk model like it. We need to,

J Jo Peterson 05:55

well, some would argue with you,

B Bill Hammer 05:57

yeah, I know. I know. We just need to get away from sort of looking at the numbers of vulnerabilities and the potential that's for us to decide how the risk gets addressed, but we

need to be having the discussion and understanding, how do we tie our actions back to the dollars of the company? So if we're looking at, you know, let's go to the washing machine division, and we think that there's a potential vulnerability in the washing machine division that could cost us. And it's not that we would get attacked and something would happen. Boards don't care about that. They want to know that if they get attacked and something happens, how much does it cost? Right? So you can do the financial modeling on that side, and that's when I start looking at new software coming out. I am asking every one of these startups, how do you tie my financials into this? How can you tie my financials into this? Because then I can look smarter and make a better decision when I go back and I can say, Look, I understand if we're going to we're going to pick up and move our manufacturing out of China to Alabama, because we need to bring stuff back on shore. Whatever the decision is, there's a financial cost to that, there's risks, there's logistics, there's a whole bunch of stuff that goes with it. There are cyber issues that happen as well, because anytime there's disruption, there's a potential for a cyber attack, and that's, you know, any good cyber threat will come during a point of transition. So you should be in there having that discussion around well, here's some of the risks that we lose. We lose some of the risks that are inherent with being offshore in another country. We lose the risks of being offshore in a country such as China, which has a higher known issue around threats, cyber threats, bringing it back onshore, but being onshore, we're going to have other issues, and that's how we should be integrating cyber risk into the financial risk models, because that's how we make decisions on the business. Those decisions to move a manufacturing plant, to open a new line of business, or to change code, right? We're going to rewrite everything from Ruby to go. Those are decisions that are made for reasons, whatever the reasons are. I don't care right now, but they're going to have financial impact reasons, and we discuss them, usually around the financial aspect to say, okay, you know, it will make the code, the recoding. It'll make the code faster, better, easier to support. The easier to support means it's cheaper to support. That's really what it is. But we'll, we'll couch that and cover it up in the it makes our customers happier, but making our customers happier is better for the bottom line, because we don't churn as fast, right? So everything's a financial decision, and that's how we just have to bring cyber into it as well.

J Jo Peterson 08:34

Yeah, and yeah, no, that's, that's a great answer. Last question, yeah. How should the CISO be thinking about AI adoption in terms of its use to secure emerging threats, and then from an organizational governance perspective,

B Bill Hammer 08:51

that's a really interesting one, because we are if you had walked around RSA and you saw, yeah, you saw all the AI security solutions out there, right? We are still discussing, how do we secure AI? Yet every security vendor is selling AI solutions and having not figured out how to secure them. I think the way to look at this is, this is the time, you know, there was all those discussions for years around CISOs should not be the Department of No. They should be the yes and they should be open, etc. Well, we're way past that now. Ai adoption is there. Don't even try to stop it. Find ways to to to integrate it and to allow the adoption to happen in a framework that you can at least see and have some modicum of control over it. And you know, that could be as simple as saying, look, okay, we understand that. There's all sorts of solutions out there, but we're going with and pick one, Claude, open, AI, whatever. You know, here's the one we're going to use. So for you to play and try and do all those things, do it in one get in. Enterprise

version, have some control over it, so you're not doing all the the personal ones on the apps that are bringing in the copilots. The first thing I've said, and this is a PSA to anybody that's listening, go back and look at your SaaS contracts with all of your vendors, because all of your vendors are going to bring copilots in if they bring copilots in, and they have that standard clause in a SAS contract, and I put these in my contracts for 15 years, it said, I will not use your data for any other purpose than stated in the services that you have purchased. But I always had a carve out that said, except I can use it for performance related metrics to or performance related upgrades to make the systems better. And that was honestly built for things like disk, read, write, query, speed, network bandwidth, all the stuff that I needed to do to make the environment better. But if that Contra, if that clause still sits in there, and they open up a co pilot. Then that training that database, training that LLM is making the system better. So theoretically, they can use your data to train their llms. So that when I say, go back and look at all of your contracts you've got, you've got work to do there, but absolutely get through and just have the llms carved out, have aI carved out of that performance piece, or have find a way to change that, because that, you know, it's not malicious. On the vendors part, there's no, I don't think there's a vendor out there that went, Oh, you know, we'll plan this 10 years in advance so we can sneak it in. But it is in there and you want to get it out. That's, that's what I would say, and then from a from a governance perspective, I'm not sure right now, I think, I think you really have to look at what your governance framework is for your company and see how AI fits into that, because there's so many different ways to govern. There's so many different perspectives on that that they will, that will slide into some very easily, as just another system with another data point, and in others it will not work at all. Like, you know, when you look at things like HIPAA and some of the more rigorous frameworks that are out there for for compliance, there's, there's just too much looseness in AI right now for it.

J Jo Peterson 12:22

Yeah, that's a really good point. And what a great PSA for everybody about their software contracts. That was a nugget. So thank you for that nugget, and thank you for the time today. I had so much fun talking to you as normal. So everyone, thanks for tuning in, and we'll see you next time you