Show Me the Money with Nick Vigier

[00:00:00]

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 more effective cybersecurity leader. Today, we're gonna talk about money. Basically, as an executive, you need to be able to run an effective budget. But what happens is as CISOs, we spend the majority of our career learning technology skills and tool sets and managing our people perhaps, but budgeting and resource management sometimes comes as an afterthought, but being able to do it effectively could be a key performance differentiator in your job as a security leader. A lot of what we've learned in the past has pretty much come from on the job training we figure stuff out, we get it right, great, we get it wrong we pay the penalty, and then [00:01:00] maybe within the next year or so we get to try to correct that.

G Mark Hardy: Our goal today is to be able to give you some insights by talking to an expert who's been through a number of CISO roles, but also learned an awful lot about budgeting. And originally we're gonna give you a big, long episode with the whole preamble on it, but my guess was just so eloquent that you know what, we're gonna give him the whole show.

G Mark Hardy: And so to help with this podcast, let me introduce you to a special guest after we hear from our sponsor.

G Mark Hardy: Meet Nucleus, the only risk-based vulnerability management platform purpose-built for the world's most complex enterprises. Nucleus takes the mountain of vulnerability data that's produced by your security stack and unifies it into one clean dashboard that helps you make sense. Of your assets and vulnerabilities with nucleus users, you get a normalized and de-duplicated list of vulnerabilities across network devices, clouds, applications, and more.

G Mark Hardy: And next, they layer in risk and vulnerability intelligence from sources [00:02:00] like Mandiant to help you prioritize the vulnerabilities that matter most. Ready to see how Nucleus can help improve your vulnerability management program? Head to nucleussec.com today. And I'm privileged to have today a special guest, Nick Vigier, who's gonna share some tricks of the trade that he's found to be helpful in his role as a ciso. Nick, welcome to the show.

Nick Vigier: Thanks a lot. Pleasure to be here.

G Mark Hardy: Yeah. Hey, can you tell us a little bit about yourself and the audience and about your background?

Nick Vigier: Yeah, absolutely someone who's passionate about security but didn't know it at the time, but I started my career in, , as a network engineer for the New York Stock Exchange. Started doing some security work. About three years into that, I was sitting next to the security team and started doing pen testing, and then spent about 12 years in financial services.

Nick Vigier: Where the next gig was basically doing everything security. So I was fortunate enough to work for someone who really saw the full breadth of what security and risk management is, as opposed to just like InfoSec and just doing what some people think that security is. So I learned how to do bug sweeping, right?

Nick Vigier: Pretty [00:03:00] cool. I was there for about seven years. And what I came to realize just from a rounding out perspective of what I wasn't learning was budgeting. I was actually germane to this. I went from a small financial services company. It was like 400 people to Sony and with a very specific goal of learning, budgeting and what it was like working for a huge company.

Nick Vigier: And I got thrown right into it. And there I was paired up with a forensic accountant who taught me the ropes and learned to appreciate it. And then also just got to work with an amazing team. And build up my network. And then since then I've had a few different CISO roles, a CIO gig mixed into there and have done some advisory work, at a few different companies.

Nick Vigier: So it's been an interesting journey and I'm now the CISO at Talend, which is a French data ELT company.

G Mark Hardy: That's fascinating to see all the plays. You've gone and I don't see any gray hair on you, . It's okay.

Nick Vigier: I know

G Mark Hardy: It's like you're waiting all of a sudden, like this Dorian Gray picture is getting older and older somewhere in a closet, and you keep going. But that's some fascinating background, particularly in [00:04:00] the budgeting and then working in the security and seeing is an expansive type of a, , experience.

G Mark Hardy: As I say, bug sweeping and things like that. It's not typically what you'd find in the cybersecurity role, but it's neat stuff. And so from your perspective, can you tell me a little bit more about what you perceive as CISO does? The real role about.

Nick Vigier: So for me it's really fundamentally, my role is about facilitating informed decision making, right? mean, We have the base, the cybersecurity that is like the protect the house side in my mind, right? The security and risk management hat to me is really what's much more important on the CISO side, and that's about bringing truth to the business and helping the business make informed decisions about what risks they're , and then know, businesses make money by taking risk. So then our job is to try to help mitigate that as much as possible within the bounds of a risk appetite. So for me, it's about. understanding the entire organization, understanding how it makes money, what all the different teams do, having relationships in all the different teams [00:05:00] across the entire company.

Nick Vigier: And then having, uh, I, I typically build it out as having certain silos. So product security, if you're a product company, Uh, where my company now is a SaaS company, it is having the, the platform security. So the product security side is focused like how you build the things that you sell.

Nick Vigier: The platform security side for me is,, know, where the things run that you built and then got the enterprise security side that secures how the company does its work. So you've got all your know, SaaS apps and everything else. And then you've got the, and security operations, and then you've got your GRC side that kind of overlays on top of everything and provides the the guardrails.

Nick Vigier: And so my job as a CISO is to basically help the organization figure, understand what it has, understand where the gaps are, and then figure out, hey, how do we make decisions about what to address or not?

G Mark Hardy: And I agree with you very strongly. First point I, I tell people our role as cybersecurity professionals is to help our management team make informed [00:06:00] risk-based decisions, and you've reflected that, that well. But of course, with all the varieties of tools and activities and the people we have working for us.

G Mark Hardy: That's not free. It'd be nice to get every, yeah, it's all free, but it's not, and so what turns out is we really need to have a good understanding of budgeting to be able to do this effectively if we wanna enable our critical resources and be able to get the right things online when we need them, instead of being a panic situation.

G Mark Hardy: What type of a budget process knowledge as a CISO really need to have to be effective?

Nick Vigier: Well, First off is understanding what a budget is, right? of the basics things that I didn't really understand until I went to go work at Sony, where it was know, oh, let's break it down to opex and CapEx and what's the narrative and what are the metrics that the company is know, trying to hold to, know, all those elements.

Nick Vigier: And I think it's really about, first and foremost is understanding what that, what a budget. , right? And then it's a matter of figuring out what do we need to, what do we, what is a spend that we need to do? But there's also the [00:07:00] framing of it, right? is it spend or is it investment? And I think we always look at it as a spend.

Nick Vigier: We al And when you talk about spend, you're talking about overhead. , right? When you talk about investment, you're talking about growth. And so for me it's about know, if you understand how budgets are constructed, if you understand what drives the business and what the metrics are that the business is being held to, then you can frame your budget in that same way.

Nick Vigier: And I think that's what's really becomes most important, is making sure that you're able to communicate that.

G Mark Hardy: Yeah, so as you'd said, there's a couple dichotomies here. The operational expense or the opex, the capital expenditure of the CapEx, and we can either spend things or you said we're gonna. For overhead, at which point it's gotta get done. We gotta keep the lights on, don't want to be like Bob Cratchit and sit there shivering in our office, trying to go ahead and make things work.

G Mark Hardy: Roaming our hands over our server, cuz we're now gonna try to mine cryptocurrency to heat that thing up and get a little bit more in there. Or the investments from a growth perspective. So if we're looking at this and being able to communicate effectively to [00:08:00] our CEO, to our CFO, we need to help them not only understand how much money we want, but really what's the importance of our program and our program initiative.

G Mark Hardy: So how do we translate our strategic vision as a cease of what we wanna accomplish, as well as the tactical stuff we gotta get done into a budget and make that understandable to our executives who ultimately are gonna make a decision as to whether they approve it.

Nick Vigier: Yeah, I, I, so you it comes back to that framing, right? There's what buckets your budget goes into. So is it g and a? Is it that overhead? , is it cogs, is it part of the things that you're selling? Is it part of the know, the margin calculations and all of those things or is it r and d?

Nick Vigier: Is it research and development where you can actually write that off from a tax perspective? So it's really about. How you're making sure that you're framing it in that same way. So for me, looking at it as, okay, what are the table stakes? Okay. Yeah. We need like CrowdStrike on the end points.

Nick Vigier: That's a table stake, that's [00:09:00] overhead, that they're just things that you have to do. You have to have asset inventory, you have to have that vulnerability management and some basic protections in place. , but then the question comes in like, Hey, what is the right amount to spend and how do we communicate that?

Nick Vigier: And that's really where you start talking about business cases. And I think that's where, what we're not doing as an industry, in a lot of cases, we're just coming and saying, Hey, here's how much I have to spend, or, Hey, here's what my envelope size is, and so I'm gonna see how many things I can jam into that envelope.

Nick Vigier: and instead of looking at it as a, if I looked at this as a business, if we looked at this like a p and l perspective, a profit and loss, like what is a revenue I'm generating from this? Can I show And that I come back to again, what we're the what I, I just said before, which was know, is it a spend or is an investment?

Nick Vigier: And there are opportunities that we have to frame some of these things as investments versus framing them as risk mitigations. And so the, you. One of the, one of the mantras or things that I like to think about is [00:10:00] the business has a limited appetite for risk management, but they have infinite appetite for profits and making money.

Nick Vigier: And so if you're able to take some of these things that need to get done, but you're able to frame them as how they're actually going to help accelerate the business or improve the business that brings the CEO and the CFO along on the journey, that you're not just there to lock the doors, you might actually be there to help put another floor on the. and that's a very different conversation. So it's a matter of balancing all this together. If you're able to establish the, risk posture, risk appetite, help guide the conversations around what it means to make an investment or not, or make, do a spend or not, and then help the business make a decision about what those trade-offs are.

Nick Vigier: I think that's where know, you're having that conversation the way that everyone else at at the table is having that convers.

G Mark Hardy: And I think one of the things we've done here at me, CISO Tradecraft, is looked at the role here as saying, as a CISO, we're really in the business of revenue protection. For the enterprise. That's a different take [00:11:00] entirely than we're here to consume resources and just to be a spending line that doesn't generate anything.

G Mark Hardy: Because if you become just a commodity spend line you're like the toilet paper, they're gonna buy the cheapest stuff they can get to meet the compliance. Okay, fine. And then it's a hygiene factor. If it's their okay. But if it's not, their people complain. But you're not gonna, you're not gonna score points by getting the triple ply that the bears like to.

G Mark Hardy: You get to the executive washroom, which is why we wanna all go up there. And so that is very important in the communication, as you say, the business cases, being able to translate that from a risk appetite perspective. I like your distinction that unlimited appetite for profit. More limited appetite for risk, although rarely do you tend to get a lot of profit without risk.

G Mark Hardy: And as we've seen in some particular cases, and we were talking earlier before the show about cryptocurrency world is, for a while it seemed like that was it, like the no risk way to get rich. And of course all that runs out very quickly because everybody comes in and it normalizes. [00:12:00] But as we look at the budgeting, assuming that we've been able to get resources, typically as we come toward the end of a fiscal.

G Mark Hardy: there's user lose money. Now, in the federal government, it was a double sword because what would happen is if you didn't spend it by the end of the year, not only would you not get to roll it over, but they would take that off of your top line next year. And so for the first 11 months of the fiscal year no.

G Mark Hardy: And all of a sudden September, bye bye bye bye bye. And everybody kinda goes crazy. Sometimes you buy stupid stuff. What'd you do? We bought 18,000 ballpoint pens, cuz you never know when you're gonna need them. There you go. You're good until Armageddon. But it's probably more important for a CISO to have a strategic arsenal of things that might not have gotten approved.

G Mark Hardy: But if you had to do a snap. and a quick fire, something you could close the deal in 24 hours. How would you put that together? How would you put together a quick spend? Is [00:13:00] it you just gonna wing it? Do you take whatever didn't get approved last year, you take the top three things?

G Mark Hardy: Or is that dynamic how, what are your thoughts on that?

Nick Vigier: Yeah. I mean it, it all depends. I. Always a stable of things that you have lined up that you know you have a business case ready for, you've already gone through, you preemptively do the due diligence on, and just make sure that you have it in the stable, ready to go. mean, The things that are, I have cash right now that needs to get used and you see this a little bit less maybe like in the commercial world.

Nick Vigier: Definitely in the government side. And September is definitely you know, free for all timeframe. But the private sector side of things, the, there might be some extra money at the end of the year. It usually doesn't affect in the same way from a, like cutting it off the budget for next year type of thing.

Nick Vigier: the the simple wins for me are, is there a quick win to get from a hey, there's a pen test we've been holding off on, there is a contracting engagement that we can have someone come in and do a quick uplift for us. know, Things like that. So [00:14:00] having a bench of initiatives or pre-clear. things that you can get done quickly, and I think having a partner in place that you can use to help execute quickly, I think become the key element.

Nick Vigier: So I think it's really about having those that optionality available to you, but always having, if you a strategic plan, you know the things that you would like to get done if only you had a little extra cash. but don't wait until you have the extra cash to figure out what those things are or to get them.

Nick Vigier: Through the paper trail or paper process that you need to go through, try to work on that preemptively. So then you're not, if you're at the end of the year and you're suddenly trying to get something done, guess who else is trying to get stuff done at the end of the year? Everybody else.

Nick Vigier: So if you make that process go smoother, you get your stuff faster, and you get through the process as opposed being stuck at the end of the year and not having gotten the deal.

G Mark Hardy: now, when I was in the government in the military, we had a term called the color of money. We had blue dollars and red dollars and green dollars and what essentially [00:15:00] that meant is that certain things would either fit into opex or CapEx and you couldn't. Across the stream, so to speak.

G Mark Hardy: But we find out is that one of the things potentially toward the end of a fiscal cycle is to say hey, if you got lose or use money, how about a training voucher? We'll go ahead and you can buy training for next year. You pay now and then you can cash that out. And I've seen some training companies be very effective at extracting a lot of money that way.

G Mark Hardy: And then of course producing some value later on. Is that something that you can recommend

Nick Vigier: That is definitely a great option. I think there are other examples too, where. know, Especially with cloud, now you've got AWS marketplace, you've got committed spend, things like that. And then maybe you're not gonna hit the committed spend level that you anticipated, but hey, we really have to hit it so we can get the discount levels, that we negotiated.

Nick Vigier: There's another opportunity there to help. each other out. I think that's from a budgeting perspective, this is another really important thing for CISOs to understand, is that your s r e counterparts, your infrastructure, your know, C [00:16:00] I O or c t o have spend that they have to do. And if you're able to execute your spend in their lane, it actually helps them right? And then it's a win-win. You can get a deal done faster because you're going through a marketplace and you're helping them hit the commit, the committed spend. So they get their discount levels for their infrastructure. So it's to have those relationships to understand it's more than just like, oh, I got the a deal sign.

Nick Vigier: It's figuring out which avenue is what's gonna help execute on that. And those become those weird dollars how do I manipulate that in the right way in order to get the job done and help the business.

G Mark Hardy: Now have you run into commercial organizations that have similar, if you will, buckets of money or spending targets that we find the federal government, for example corporations or minority owned, or in my case, a service disabled veteran owned small business and S D V O S B That in a way, if you can say, Hey, I have a vendor, and they offer something that we have, and oh, by the way, [00:17:00] it helps you meet your spending targets.

G Mark Hardy: You actually, oddly enough, become a bit of a hero helping somebody else spend their money on your stuff, which sounds like a perfect type of a storm.

Nick Vigier: And it's a great way to get your spend done. mean, You're absolutely right if you're getting government funds and now you have maybe webi requirements and things like that, it's super important to do the right way to, and to get done. And if you have an opportunity to help that metric, and this is really important, what are the businesses metrics as it relates to the financials?

Nick Vigier: That's a metric, right? You may have a metric around only a certain percentage of spend can be for g and a or overhead or a certain metric around margin. And so, you wanna make sure that as you think about budgeting, that you are using those and taking those into account cuz that's what's gonna help you be part of the business conversation.

G Mark Hardy: Now, one of the things is that as we spend given, let's say we have a one year budget, and okay, fine, here's your money, execute. It never usually shows up on day [00:18:00] one. You don't get this giant pot of money. But usually your comptroller is somebody who's going to meet his out to you at regular intervals. And I learned early on in my career that you.

G Mark Hardy: Kind of need to spend as you go along and I tend to not waste resources. Therefore I was, if you will, well below glide soap. But the idea was I had some major purchases coming up a little bit later. I am going to really cut down on my opex so I can have more capax. And then what I found out is after the first budget review, about a quarter or two into it, one of the other department heads was spending like a drunken sailor, if you pardon the term.

G Mark Hardy: And they're like he needs more money. We're giving him your money. It's but wait a minute. I'm a better steward of the resources. Yeah, but he's spending faster, he. And he had a few more years experience than I did, and he kinda looked at me like, yeah, Hardy, you're an idiot now. Now I know better, but rather than, blow through money and buying boxes of pens or that you don't need.

G Mark Hardy: How would you [00:19:00] recommend organizationally that CISO assess where they're at? Do they have to always spend it all ago or is there a political element, layer eight that's involved? Or how would you recommend somebody feel that out to make sure they don't inadvertently shortchange their own budget?

G Mark Hardy: Because in their mind, they think they're saving up for a rainy day.

Nick Vigier: This is where having a strong partnership with your, financial planning and analysis team is really. key, right? It's really about having that relationship where you're managing the p and l with your fp and a representative and keeping track of how that monthly spend goes. Like for example, you might have someone leave your team.

Nick Vigier: Well Now there are crude salaries and getting paid out to anybody cause you haven't replaced them yet. So now here's a whole bunch of money that's going back into the OPEX pool and so trying know, you gotta manage all of those things together to figure out how you're executing, but working closely with your fp and a team is gonna help protect you.

Nick Vigier: I think the other, for [00:20:00] me, the other thing is, I think a little bit to your point, is one of my goals as a CISO is to make sure that my budget isn't subordinate to somebody else's budget. That someone can't just come in, like the CTO can't like come in and. Hey, by the way, that headcount you had, yeah.

Nick Vigier: I'm taking it and I'm moving it over there. like, well the headcount I have is because the business was addressing a risk item and we now have to go and adjust the risk statement at this point. And things like that doesn't, this isn't just like moving a developer from one team to another.

Nick Vigier: This is, there's an actual business reason why we're doing this, and so making that that budget stays, atomic helps to keep a little bit of that independence and a little bit more of that control over how you're

G Mark Hardy: executing.

G Mark Hardy: yet, in a way, it'd almost, I'd almost be inclined to say, here, sign here that you are accepting this risk on behalf of the organization and you're doing so personally, and if things go sideways because you pulled the resource and we don't have it anywhere I'm not sure where you're gonna be working next month, but yeah, most people don't wanna do that [00:21:00] rather than go into that contemplating the, oh wow, we could do this, or whatever.

G Mark Hardy: If we think about it though, we brought up a number of ideas so far that it's a bit of wisdom, based on experience that you've figured out. over the years, but what are the things that going into, for example, a first CISO job that you really wish you knew about budgeting that maybe took a mistake or took some hard learning, or just sometimes, what wisdom can we impart now to people so they could give 'em a jump on doing it right.

Nick Vigier: I think it's really around, I think what one of the things I said before was it's around the framing. It's around how you tell the story around your, your, around your budget. I I don't wanna say your spend because it's that difference between investment versus spend. It's that difference of where I'm allocating my funds so that I make sure I scale with the business.

Nick Vigier: So Yeah. And I know, I very much looked at it as of the same way that you get in all of the surveys, a percentage of it spend, or percentage of like total revenue or whatever. like, well that's great, but a [00:22:00] security team's budget is actually split out across a bunch of different areas.

Nick Vigier: You know how one percentage works against one metric versus another is gonna be very different from company to company. Forget about industry to industry. And so for me, it's now more. Making sure that I understand that context and that I'm also telling the full business story around it. Like how much revenue can this actually generate?

Nick Vigier: like, hey, we're bringing in a tool to eliminate answering security questionnaires. Well, Great, that's a lot less pain, but hey, that's also accelerating the deal cycle and bringing customers on board faster, which actually generates revenue. So how do you have that conversation? to show that you're actually driving the business forward instead of just mitigating risk or minimizing bottom line impact.

G Mark Hardy: And so it's really partnering with the business. As a ciso, you can't be in your own little silo of excellence and just focus on the technology. Really have to understand at a [00:23:00] business perspective. And that's why I recommend if you wanna be successful there, if you haven't had a lot of experience at the business level at least an MBA gives you book knowledge.

G Mark Hardy: But I remember one of the things I think I got out of my business degree, one of the most important things was becoming fluent in business. and the language of business and it's a real mindset change. You really can't go back and look at it a different way because you now have a much more expansive view and your perspective is much more understandable to the executives who are gonna be working with you and they get it.

G Mark Hardy: You get it, and you're really more of a member of a team now, I remember looking. Surveys of budgets what percentage of it spending goes to it. Security. And I remember Richard Clark used to complain years ago, he says, more money is spent on coffee than on cybersecurity. And that probably was true about 20 years ago.

G Mark Hardy: Maybe not so much today. But how important are these benchmarks? And is benchmarking a percentage [00:24:00] of an IT budget the correct thing to be looking? , or is it raw dollars or dollars per employee, or dollars per revenue generated, or dollars per profit or convert to whatever currency you're operating in.

G Mark Hardy: What's the best way to look at these things in terms of these benchmarkings, if at all? Maybe it's not useful.

Nick Vigier: I struggle with this. And I think a little what I was saying before, which is like it's what we do is so nuanced and transversal across the entire organization and their individual like impacts and buckets, right? So to say like, Hey, You know, let's just use it as a metric against it spend.

Nick Vigier: Cause we think that security's more like it. okay, great. But if I look at my actual budget, 60% of my spend is more related to cogs and the cost of goods sold. Like what it takes to actually deliver our products. Like you can't use that metric at that point. It doesn't make any sense because it doesn't actually tie back to what the business is doing and [00:25:00] how the business needs to scale.

Nick Vigier: Cause that's the other thing, when you pressure test these things is. If a part of the business grows, like let's say your arm grows, one arm grows faster than the other, right? You're not, you have to be able to grow with it. And you have know, pants versus shirts might be a better analogy. Like, Let's say my arms get longer, faster than my legs.

Nick Vigier: I need new shirt, but I might not need new pants. If the shirt is, is your products and your cogs, but your pants are your it why am I measuring how big my shirt is by how big my pants need to be? You know, they're, they're unrelated to each other and I think that taking a view that is not nuanced is, I think naive in terms of just trying to put a number on it.

Nick Vigier: Just know, let's just try to measure something and maybe that's not the right thing to be measuring or the right approach. So I think that for me it's trying to figure out what are the, what should those metrics look like? The cog security side of percentage of the total cogs know, and then the overhead side be a percentage of it or [00:26:00] what have you, and trying to figure out the right dials to tell a story in a more universal sense.

Nick Vigier: I don't think we've gotten there yet.

G Mark Hardy: Yeah and for me personally, I dislike those from a couple of perspectives. One is you may be doing just as well as everybody else, as everybody drives over the cliff, you're running just as fast as a lemming next to you. And are, we're running faster than the other lemmings. It doesn't necessarily mean you're doing better, but if you focus on the mission first, executing the business, as you said, delivery of revenue, what does it take to be able to provide that enhancement?

G Mark Hardy: How do we get deals closed faster? How do we reduce our overhead and our cost by reducing the risk and things such as that? Now you've got a winning combination, and when the person says what does everybody else get this? It doesn't matter. I don't wanna be like anybody else. We're better than they are. And if you measure yourself against the people you're beating, That's not the way benchmarks work.

G Mark Hardy: Benchmarks are supposed to be. Find the level of excellence in your industry [00:27:00] and try to equal and then exceed that. And so from that certain perspective, you wanna look around for everybody says, oh. So you're admitting that you're really not excellent already, that you're actually just a runner up and we could do better.

G Mark Hardy: We need somebody else to show us how to do our business. And again it's not trying to be confrontational, but you can turn these things a little bit sideways. It's hard to diffuse them early on to. , what we're doing needs to be done effectively in our environment, and our environment is what matters most.

Nick Vigier: A and what might be really interesting is instead of trying to take it as a, let's measure the exhaust, but let's measure the actual gas in the tank, it might make more sense to say, why won't, why not measure the level of risk being accepted? By the organization compared to its peers, right? Is your organization taking more risk?

Nick Vigier: And that really then should dictate how much you spend in different areas and everything else. And so maybe that's a better way of measuring though again, there is no know, gap of risk [00:28:00] risk management and risk scoring and things like that within security. But maybe those are better things to measure in terms of like how you're operating directionally rather than just a pure dollar spend.

G Mark Hardy: That's actually an interesting perspective. I hadn't really, I'd like to think about it a little bit more, but I'm not gonna waste time on it now. , but focusing upon how well are we managing risk relative to our peers? And someone says, oh, we wanna spend less. This says, okay, fine. You're gonna spend less. You're gonna accept more risk. How much risk is too much? How much uncertainty do you want to add to us making our numbers this quarter? But let's move on for that. And let's think about people, because as we find out in cybersecurity, there seems to be this universal. Gap of talent, and I've done a talk that I put out.

G Mark Hardy: I even put together one of the episodes here called the Demise of the Cybersecurity Workforce, where I put together a contrary argument that says, just because you throw money at a problem doesn't mean that. People magically appear with the right credentials. It doesn't generate new humans with new [00:29:00] knowledge.

G Mark Hardy: And it takes time, and particularly when you get to more senior ranks. But for those of us who are doing our best that we can to attract and retain talent, how do we ensure that A, we're paying them the right amount of money that we're recording with hr when they say, what do you mean you want somebody in their twenties?

G Mark Hardy: And we're gonna be paving them more than the people that have been here for 20 years. They've been here longer than this kids have been alive, and yet the value that we. Is usually relative to some other positions quite high. How do we communicate that effectively to HR who might not necessarily see things our way initially?

Nick Vigier: I think this is one of those things that I do in every role that I take, is really that level setting around. Helping hr, helping finance understand that, especially for security talent and because we have so many distinct skillsets that the. Salary bands are very different than know, just, oh, hey, I'm gonna go hire an sre.

Nick Vigier: But even [00:30:00] SREs now differentiate between assists, admin and an S R E, right? These are very different types of roles and functions, and so HR and finance haven't really kept up with that. And I think our job , as CISOs and as leaders, is to come with the data to show this is what the market's bearing. I think the.

Nick Vigier: The most challenging thing right now with the economic climate is that it used to be very much an employee's market, right? People could just hop around and do whatever they wanted, demand ridiculous salaries, know, and so it just led to this inflation. But now with companies know, going under and doing layoffs, it's a question of like, how long is it gonna take for these salaries?

Nick Vigier: Will they normalize, will they come down, right? Or will they just plateau versus continuing to go up? And then how do Not overpay. And I think that's what companies are really scared of right now like, okay, we acknowledge that they get paid more than everybody else, are we overpaying them to where they're, where the bands are going to be in a year?

Nick Vigier: [00:31:00] Because you can't really. Do pay cuts usually. So I think that's, we're in this really weird state right now where companies don't wanna overcommit on salary spend. We have numbers and metrics, but they're all about eight to nine months old. , Because these SA surveys happen once a year and know, how do you properly do the framing?

Nick Vigier: But I think it's super important as security leaders to be the ones that. HR and finance understand the nuances of these roles. That these roles aren't interchangeable parts. Like I can't take a GRC person and put them on cloud engineering. Probably not gonna work out very well. They're very different skill sets, very different mindsets, very different everything. , So it's trying to manage that expectation and help them understand uh, because fundamentally the problem we have is because they just don't know. And that's okay. So we need to educate.

G Mark Hardy: What's some good insight now when we're talking about know, budgeting, of course, it's really what we're talking about for the show here. Sometimes the [00:32:00] company executives say we're gonna do a holdback, we're gonna hold back 10% of your budget across the board just in case we need it later on.

G Mark Hardy: And therefore, you're supposed to, you fight for your budget. You barely eek out what you. You gotta fight with one hand behind your back. H how do we, what do you think about that practice? And as a ciso, is there maybe some way we can answer that in a way to say, okay, you're special. We don't do that to you.

Nick Vigier: It's challenging. Some of it is just the business reality, right? And saying, Hey, the business needs to save money. Where, are there places that we can save money? Is there spend that we can defer? mean, I think everybody's going through this right now. And as partners in the business, I think it's really a matter of saying, here's the trade-off.

Nick Vigier: Yeah, I can delay that spend, or I can buy fewer licenses, or I can delay that higher. But here is the effect, and here's how that affects our risk management process our risk uh, appetite and maybe the company's risk appetite has gone up because revenues aren't where they need to be [00:33:00] and they need to save some money, and that's okay.

Nick Vigier: No one wants to slow down. No one wants to give up budget. No one wants to have to back off their plans, but, sometimes it's just the reality of business and right now it's a reality for a lot of businesses. So it's a matter of realizing that we can have a different kind of conversation than the rest of the business because of the whole risk appetite conversation.

Nick Vigier: Because of the fact that we oftentimes have visibility all the way up to the board, and sometimes the board is making the decision on whether or not risks are acceptable. And. We're empowered to have a slightly different kind of conversation about those holdbacks, but the reality is they may very well still happen, and then it's a matter of just figuring out, Hey, where's the right place?

Nick Vigier: How do I help without sacrifice, without doing too much that's gonna hurt the business.

G Mark Hardy: Yeah, and again, you don't wanna, you don't wanna be difficult, but in a way it's a little bit like. Since we are providing the assurance of being able to execute [00:34:00] to mission from an IT perspective, if you wanna cut back 10%, then here's the equivalent. Every other Friday, you may not put on a seatbelt. You have to, and you gotta turn your bags off.

G Mark Hardy: Now go out and drive down the highway. Do all the stuff you do. Put your family in there. Put your kids in there, and tell all the kids no seat belt. and let me know how that works out for you. And again, I just tr you gotta re it's a way of reframing things cuz I have found over the years that if you do that, it's no.

G Mark Hardy: And you talking to the executives like, isn't this company important to you? Because it's feeding your family and it's the future for then why would you treat them when less carefully.

Nick Vigier: The answer to the business well, then we won't take the car and we'll walk. And that's okay. And and I think that's where we end up in a lot of situations where we take on too much of a sense of responsibility for saving the business. And in reality, it is a business decision.

Nick Vigier: It's why defining that risk, appetite and risk tolerance is super important. Why triangulating that with the board is [00:35:00] super important and making sure that everyone understands the implications. And maybe there's another route to take, but we get very we get very emotional or Bought into our own approach of things, and I think that sometimes we have to just maybe become a little bit more disconnected from that emotion so that we can really be true stewards of the know, risk of risk management for the business.

G Mark Hardy: And that's a good point. Cause I said I I get a little bit excited about trying to protect the know, the enterprise. I That's what we do. We're there as guardians. If we take that role, but in, in doing so, we have to do a lot of stuff and we get projects and we got Rollouts and we acquire stuff and sometimes not everything goes according to budget.

G Mark Hardy: Sometimes it goes over time, over budget, sometimes it goes way over budget. And there's one of the laws, I read it the other day and I forgot the name of it, but it's basically the more people you add to a project, the longer you'll delay it. And I'll have to look that up to see what that is. Some people may know it off the top of their head, but it's true in a way.

G Mark Hardy: So if a project is [00:36:00] starting to slide. If it looks like this is one of those things where you want to obey the financial rule of don't throw good money after bad. Okay. Then what? What, how can you tell if that thing is happening?

Nick Vigier: I mean, I think so when you're actually you know, in the middle of the project. mean, That just to me of like good project management. I think the fallacy that we put ourselves into is this whole notion of sunk cost or that's the way we've always done it and things like that where technology changes, cost change, approaches change.

Nick Vigier: It's okay to say, Hey, you know what, yeah, we spent a hundred thousand dollars on that risk management solution, but it's not doing the job for us. , let's get rid of it. It's okay to get rid of it just cause we've already spent $200,000 on it over the course of the last two years doesn't that that justifies its continued existence.

Nick Vigier: And I think that's what we have to have the courageous conversations about. There's the know, is this thing going off the rails and implementation it's just a matter of like how you're tracking it to [00:37:00] execution and your success metrics. But I think it's the same thing to always being willing to take a look. If I had to make the same decision today that I did back then and I had the information that I have now, would I still have made the same decision? And if the answer's no, then having the courage to stand up and say, you know what, that thing, it was fine and, or we thought it was going to deliver a certain outcome, but it hasn't. We either get rid of it or we pick a different path. And that's okay. That has to be okay because otherwise you're gonna be stuck in this analysis paralysis mode and or not accepting the fact that you're wasting money and both of them are losses and so it's a matter of figuring out how do you move with alacrity.

Nick Vigier: While having the flexibility to make a change or make a decision later on, that doesn't put you in a blame situation. You have the psychological safety to go and, actually course correct.

G Mark Hardy: And as a result, what we want to be able to [00:38:00] do. Is have a pulse on all the activities that are going on. Some of them are gonna go well. Some are a low burn rate. The big deal ones probably require greater scrutiny because from that perspective, there's more risk involved if you're spending more money.

G Mark Hardy: And some of them, there may be a lot of spend of money, but fairly low risk. It's a well established contractor or vendor. They know what they're doing. They've delivered for years and very unlikely it's gonna go sideways. And in other cases, Innovation brings with it its own risk because we've done it before, that's why it's innovative and it could provide a huge benefit for the business or it could bottom out and things like that.

G Mark Hardy: And so as you look at all these different. Programs and things like that are out there. How do we focus our attention among all the other things we need to do as a ciso, at least from a budgetary perspective on what we should be looking at the most carefully, not necessarily micromanaging it, but giving it an additional scrutiny.[00:39:00]

Nick Vigier: I think it's our responsibility as leaders kind of have a pulse on that, right? And keep an eye on where things might be going sideways or need a little bit more attention. And I think to your point, there's some proven. Some people that deliver in a proven fashion that can be trusted more and more of a leash.

Nick Vigier: And then others where you're like, Hey, this is a higher risk project and I need to keep a closer pulse on it. I think it's just a matter of, of having that level of awareness. And this again, comes back to where know, as a ciso you're working across the entire business and I think that we have this really unique vantage point where, and I've actually said this to some finance folks of if you want your ultimate set of business efficiency consultants, it's gonna be in your security organization. Because we see everything and we also see where efforts are being duplicated or where things are being missed or where things are going off track.

Nick Vigier: And we're often the ones to try to help get it back on track or try to mitigate the risk and whatnot within that. So I think [00:40:00] that we're uniquely equipped to spot. and to provide the support to the business to address it regardless of whether it's a security project or not.

Nick Vigier: It's being able to anticipate where things are gonna get complicated becomes really important.

G Mark Hardy: It is. And we have to mi manage among budgets, our time budget here, and this has been awesome. We're getting close to the end of the show. So any thoughts in terms of other tips or tricks that you've observed over the years that could be leveraged by our listeners?

Nick Vigier: What I've thematically been saying is take a dispassionate approach to things is really, for me, the biggest thing. The decision is the businesses. It's not right, it's not wrong, it's just different.

Nick Vigier: It's theirs. And when we have too much of a emotional stake in it, we take on too much responsibility for the decision itself. Our responsibility lies in the quality of the decision, not the decision itself. And so the ability separate ourselves from that, I think allows us to [00:41:00] manage our stress levels a little bit more.

Nick Vigier: Perhaps it allows us to deliver more effectively and act in a more balanced way. And I think that to me is the biggest tip, is make sure that you're not getting into the amygdala, hijacks and getting into the emotions of it. But we wanna make sure we're, we're passionate about the subject, but we're not emotionally vested in it because the business may make a decision, I think, to your point, that, Hey, we have to cut things back.

Nick Vigier: All well that's not an affront against security. And the business might be willing to take some risks and that's OK, And I think that's really know, we as an industry need to realize that we are not the here to save everyone from themselves. We're here to make them aware of the risks that they're taking.

Nick Vigier: And I think that's the biggest thing for me, for folks think about as they go through their security careers. We're not Superman, we're not Captain America. Our job isn't that our job is to be amazing professionals. .

G Mark Hardy: I love that idea of it's the quality of your decision rather than the [00:42:00] actual. Content of the decision that matters. We do the best we can and to help out. I've learned a lot from you. This has really been one of my better shows in terms of having a guest on. So I do wanna thank you for taking the time and the insight and if listeners wanted to hear more from you or learn more any place else that we can come look stuff up.

Nick Vigier: I don't post on social media nearly as much as I should. mean, I should be uh, posting some more on LinkedIn. I still don't know how Twitter works and know, definitely don't ask me about Instagram But yeah, you could find me on LinkedIn or hit me and uh, I'll be posting some more things over the course of the coming months. That's awesome. So Nick Vigier, thank you for being on our show and for giving us the insights on the budgets, the insights and things like that as a ciso and for our listeners, if you've enjoyed the show, and if you haven't rated us already, please consider rating us on your favorite podcast channel.

G Mark Hardy: You know, five stars and follow us if you're not following us, and let other people know where you get your insights from. CISO, Tradecraft, because that helps us reach. Other people as well. So thank you for [00:43:00] listening, and until next time, stay safe out there.