#207 - CISO Burnout (with Raghav Singh)

[00:00:00]

Introduction and Guest Welcome

[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. I'm your host for today, and our special guest is Raghav Singh, who has been doing some research on CISO Burnout. If you're thinking of becoming a CISO or you are a CISO, this is definitely something you'll want to listen in on. I think you'll find this is a fascinating episode. Before we get started, let me point out that CISO Tradecraft is partnering with CruiseCon, which is a cybersecurity conference held on a luxury cruise.

And normally events like this are reserved for Fortune 100 CISOs, but we've worked a deal for CISO Tradecraft listeners, so you can join us for I'm the Royal Caribbean Voyager of the Seas for the 8th to the 13th of February, 2025. [00:01:00] As I mentioned before, in the last show, Admiral Mike Rogers is going to be there.

So I'm not going to be the senior officer afloat, but if you want to beat the cold, get some great networking done, please go ahead and head over to cruisecon. com and use the special code CISOTRADECRAFT10 for a 10 percent discount to this exclusive event.

And then on with our show. So anyway, Raghav, welcome to CISO Tradecraft.

[00:01:27] **Raghav Singh:** Thank you so much, Mark, thank you for having me, we, we had a chat earlier as well, but, really stoked to talk about my project and get some feedback from you on that as well.

[00:01:39] **G Mark Hardy:** Yeah, so what happened was, is that I was in one forum and somebody had mentioned, I think it was on the WeedRam forum that was run, by J. C. Vega, and someone said, hey, I know this guy, he's doing his PhD thesis, he's up at the University of Buffalo, and he is, looking for input, and I said, wait a minute, I'm gonna be in Buffalo next weekend, I'm up there

[00:02:00] visiting my Mom. So I gave Raghav a call and they said, can we meet?

And we did. We got together over a cup of coffee and had a fascinating discussion. And I think that what you're talking about is going to be of general interest to an awful lot of people. So first of all, can you tell me a little bit about yourself and how did you end up where you're at right now?

[00:02:17] **Raghav Singh:** Yeah, absolutely. so I'm a, three, I'm a third year PhD student at, UB's, MSS department. That's the Management Science and Systems department. And, most of my work has been in the information security area and leadership dynamics around it. apart from a couple of projects here and there in healthcare IT and chatbot space as well.

But, my thesis right now consists of essays in which CISOs are the focal point. So a couple of things that I have been working on, which may interest you are, one of the projects where we explored what the stresses are that contribute to burnout in CISOs, such as, lack of executive [00:03:00] support, resources, related stresses, and whatnot.

And, another project where I'm exploring the power dynamic between CISOs and CIOs. So I'll be happy to explain more, more about, those two projects, later on in the podcast, but, yeah, that, that's pretty much it about me.

[00:03:20] **G Mark Hardy:** No, but you're doing a PhD, which I think is great. And I've got three bachelor's degrees and two masters and everybody's saying just put a PhD, like a cherry on top, but it's not for the faint of heart. It's not something that you do on a weekend. Yeah. That's probably going to take you at least three years, maybe four years or longer.

How do, for those who have thought about maybe doing a PhD program, but weren't quite sure how they worked, what insights could you share about the sacrifice you have to make and then the commitment that you're going to do to complete a program like that?

[00:03:49] **Raghav Singh:** Of course. so yeah, PhD is tough, but it's like, you, have, to embrace it. You have to be fascinated [00:04:00] by, by the reasons why you want to do a PhD, because, from the conversations that I've had with fellow PhD students and a lot of faculty members as well, what I've gleaned is that the people who struggle in the PhD are the ones who do it for the wrong reasons.

So I feel that if you have to, do a PhD, be fascinated with, the subject matter, at hand in which you want to, finish your PhD in. So personally, for me, it just started with the fascination for. How technology drives organizational efficiency and shapes decision making, right? as I gained experience, as a product manager a couple of years back, so I became increasingly aware of, how critical cybersecurity is in this equation. And the fact that cyber threats are constantly evolving and, companies nowadays need to stay one step ahead, not only in terms of technology, but [00:05:00] also in terms of strategies. that realization really drove my interest into diving deeper into the field. So the decision to pursue, this PhD was really fueled by my desire to contribute to, the existing literature and to this growing field through research.

I would say just, having the zeal to explore, your subject matter deeply and granularly is something that you really need to have before you embark on that PhD journey.

[00:05:32] **G Mark Hardy:** I think there's some really good words of wisdom there. Now, I have worked with some friends who have become ABD. we joke about that euphemistically, but what is somebody who is ABD?

[00:05:45] **Raghav Singh:** ABD basically, stands for All But Dissertation. so you can just, say that, they have pretty much fulfilled all the criteria, but they're yet to finish their dissertation,

[00:05:59] **G Mark Hardy:** And what's [00:06:00] involved in a dissertation? Is it just like writing a giant white paper? Or is it, does it have a minimum requirement of being 250 pages? It's a little bit like Rodney Dangerfield back to school. Ah, it doesn't weigh enough. go ahead and write more pages. How, what is What constitutes, if you will, the standard for a dissertation?

I'm asking this quite genuinely because I don't know.

[00:06:21] **Raghav Singh:** right? So strangely enough, I do am still, searching for that answer be because I'm yet to, start working on my dissertation. I've started putting my essays together. but yeah, I do meet, we meet with my faculty members and my advisor regularly just to get a feel of, what the expectations are.

but my initial thoughts on that is, at least for our department, that you need to have three essays, which constitute. a theme. for me, for example, since my three essays are revolving around CISOs, so they make a pretty nice theme about [00:07:00] how CISOs navigate the, the multiple challenges that they

face, be it in terms of just the power dynamics between themselves and the rest of the C suite or, or even how they manage their burnout effectively while contributing to the business and being a business enabler while also keeping up with the pace of the rapid technology innovation and being agile.

just having a coherent team and, ensuring that, you're providing enough evidence of you, you having done enough in depth exploration of that subject matter.

[00:07:46] **G Mark Hardy:** So what you're really doing with a thesis is, or a dissertation, is to create some additional knowledge into the knowledge base of the subject. So you're pushing forth the boundaries of what we know. [00:08:00] Which would mean that the very first person who ever did a PhD in something like computer science or computer, cybersecurity, would have had Greenfield, pick anything you want because nobody's picked anything.

Now, do you get to a point after a while where all the corners are painted into, and then you're just trying to carve out this new little tiny corner in something that, has been well established for a long time or is one of the advantages in cybersecurity, as I've shared before with G Mark's Law, half of what you know about security will be obsolete in 18 months.

That seems to create an ever renewing opportunities to come up with new ideas that you could do that weren't around three years ago.

[00:08:39] **Raghav Singh:** It's actually pretty interesting. the way that I look at it is that, your aim should, at least, in academia, your aim should be to advance the existing literature and advance the existing knowledge. I'm sure at the outset, you can say that, the person who did his PhD first in [00:09:00] computer science, he probably had it easy because there's so much to do.

but then again, if there wasn't enough literature or enough research done, so I think he or she would have had to lay down that groundwork on that own, which is quite a feat. so I think in that way, we are, we, PhD students are quite lucky right now because there are so many existing theories that we can lean on and so much existing literature to, to read.

but at the same time, it also creates a bit of a challenge just to identify. Gaps in the literature because everyone is doing so much research nowadays. It's a challenge to understand, understand the subject matter and identify what the gaps are and how they can be filled effectively. Because if there's a problem at hand, in research, there's no one single [00:10:00] approach to solve that

problem or to address that problem. for example, you can, look at a problem and try to, try to address it quantitatively. But then again, if you want to get more granular, you can always, talk to a lot of people and conduct qualitative work just to get to the, get to the bottom of, that problem.

So that, that's something that excites me.

[00:10:24] **G Mark Hardy:** So when you're dealing with the question of CISOs, and we're talking here about potential burnout, do you find out that the research you're doing, is it more qualitative or more quantitative? How

[00:10:36] **Raghav Singh:** So as it stands, it's much more, much more qualitative. So right now, what I do is I reach out to a lot of CISOs and I talk to them about, about different, different issues. for example, burnout, where we first, what we do is we get an IRB approval, which means that whatever they say in the interviews, all the [00:11:00] personally identifiable information, doesn't get leaked.

And what we do is after the interviews are done, we simply just transcribe the interviews, analyze them. Get the insights out and then destroy the data. So once that is done, that really helps us, into getting some sort of, some sort of, teams out of all that data. So I use something called a grounded theory approach where we are building the theory from the data.

So that's primarily what I do in the qualitative work.

[00:11:32] **G Mark Hardy:** So then the data then sets the direction rather than the other way around. Do you start with a null hypothesis, for example, saying, I presume that this is the case. And then you go out and you gather data and you either prove or disprove your hypothesis. did you start with a null hypothesis and then from there look for data that validated or invalidated it, or do you start with kind of a blank and then let the data fill things

[00:11:57] **Raghav Singh:** Yeah, you can have a null hypothesis [00:12:00] for sure. So for example, there were a few assumptions that we made. before the, before the CISO burnout study. So one of the assumptions that we, that we made, and we even validated with, with the CISOs, we conducted a couple of unstructured interviews just to validate that.

so one of the assumptions was that was being, was that burnout is a multifactorial, phenomenon. So we assumed that from the outset. CISO burnout would not be caused by a single factor, but it's really a product of multiple

factors and multiple interrelated stresses. So given the unique pressures that are associated with the high stakes that CISOs and the other C suite members play with day in and day out, our assumption was that the multiple job related organizational [00:13:00] and external factors would interact and contribute to burnout.

So that was one of the assumptions. we also had a couple of other hypotheses about, the role of organizational culture. So we initially hypothesized that the organizational culture would play a significant role in CISO burnout. So that is something that, you know, we. basically came up with based on, based on the prior literature.

and another, one was seeing burnout as both a personal and an organizational issue where we assume that the burnout among CISOs would have implications not just for the individuals themselves, but also for their organizations. So that pretty much led us to examine how different factors like, like communication issues or, just the lack of resources, how [00:14:00] that would impact, both the CISO's well being and also the overall security posture of the organization.

[00:14:09] **G Mark Hardy:** So the idea that burnout is not just a personal issue, but an organizational one, it's interesting. And does that suggest then that if you tie that back to the culture, that you could look at it, for example, A lot of organizations say, Oh, we believe in quality of life and personal life work balance and on.

But what I suggest is that go ahead and look at the executive compensation plans and see where their bonus comes from. If the bonus comes from producing more revenue or higher profits or better margins, then that is in direct contradiction to these stated goals. And then it looks like some sort of almost disinformation that's put out by an organization promising you this wonderful, bucolic, wonderful lifestyle that when you get there, [00:15:00] it's just grind, grind, and off you go.

As compared to other organizations, when I used to work at Ernst Young up in New York City. we were expected to be there and you'd start to work about eight o'clock that evening, cause you only work half a day, 12 hours. The partner would come around and gather up the, the senior guys and said, all right, come on, let's go out for dinner.

And then you go there and you'd be out till 10, 10, 30, 11 o'clock at night. And so you'd end up basically working about 15 hours a day, as a cycle. And we see

that in other areas such as working in merchant banking and in the financial sector and the like. CISOs, we joke that it's not a 40 hour a week job.

Again, you're only doing half your work, but let's take a look at some of the concepts that you have come across and some of the ideas. Let me just start with that. Work hours. What have your research found in terms of CISOs? What are the expectations that perhaps CISOs come into a job and then what are they actually finding are the demands of the job?

And is [00:16:00] that mismatch causing? Yeah. The stress and the burnout, or is it just the actual fact of the workload?

[00:16:08] **Raghav Singh:** so there were a couple of interesting findings that we had. so before I get into that, what you talked about, the work hours is actually pretty valid, because one of the reports that we, we went through before we embarked on the study That stated that CISOs in particular tend to have shorter tenures compared to other C suite roles.

So for CISOs, on average, the tenure was just over two years. So I think around, yeah, just over two years. Whereas for other C suite executives, It was more than five years. so that, that is one of the reasons why, you know, that there's higher turnover, which means that the organizations are constantly facing the challenge of finding and keeping the right [00:17:00] cybersecurity talent as well.

And, burnout is a significant factor here, because it drives many CISOs away from their roles, which only makes it harder to recruit and retain the skilled cybersecurity experts. so what we found basically was that, organizations should first recognize burnout as a real and pressing issue.

And the leader should also, work to understand what the causes of burnout are and create support systems that help, help, the employees and specifically, at least in this case, CISOs to manage their responsibilities effectively. so we conducted this study. And, what we found was that CISOs are pretty different from other C suite members because they come in with a very strong, like they mostly [00:18:00] come in with a very strong technical expertise and they gain managerial skills as they advance within the organizations.

It's clear that CISOs. At least for CISOs, the burnout isn't usually just about lack of skill or preparation because we looked at a lot of burnout literature that exists in academia and of it points at burnout being a factor of lack of skill or preparation. But in CISO's case, it's not that.

So instead, what we found was that Instead of just the lack of skill or preparation, there are other factors at play that contribute to the burnout, and these stresses don't operate in isolation, they often overlap and, even, intensify one another, sometimes.

we conducted a thematic analysis, and we uncovered, six, Main sources of burnout among CISOs, so one was the [00:19:00] stress linked to organizational culture, then resource limitations, the burden of job responsibilities and, we also had communication and relationship management changes and, also the, the hurdle of, or the need of constantly keeping up with the emergence of new threats and external pressures. Apart from that, the findings, went a bit further where we analyze how these stressors interact.

And we found some notable, patterns with that as well. so for example, in organizations, there is a lack of understanding of the CISO's role, and that sometimes leads to, insufficient, executive support So at least with the CISOs that I interviewed, that we interviewed, for the study, we saw that [00:20:00] CISOs often, need, they want a seat at the table.

but what happens is CISOs sometimes report indirectly to the board. And they have to rely on other intermediaries like the CIO or the CTO. And oftentimes what happens is that it can create tensions and, diminish their authority. then again, there are resources, related stresses where a lot of CISOs struggle with the lack of investment in essential resources.

So for example, if a CISO is reporting to the CIO, there are times when they have to compete for the resources. Because since they don't have a lot of autonomy in that role, they pretty much have to, for the lack of a better word, they pretty much have to grovel for their share of the budget from the CEO, from the CIO. other than that, since the nature of the CISO [00:21:00] role, demands constant vigilance. The job is pretty interruption driven, if it makes sense, because like you said,

[00:21:08] **G Mark Hardy:** definitely makes sense.

[00:21:10] **Raghav Singh:** yeah, because like you said, they have to work long hours. And, sometimes CISOs are even required to be available 24 7 for potential breaches and that a lot of time. It can just, strain their work life balance and it just requires continuous learning to keep up with evolving threats. So similarly, just keeping up with, with newer technologies. like AI and just the shift, shift to remote work due to COVID 19 that, that also, introduced evolving

security risks, which, CISOs had to constantly adapt their strategies to address these emerging threats.

apart from that, a couple of CISOs [00:22:00] even alluded to, facing pressures from external sources, such as, You have persistent vendor outreach that distracts them sometimes from critical tasks, especially during incidents. so I remember one of the CISO talking about how when they were encountering such as such a situation where, they were trying to fix something and the vendors were constantly spamming their emails and their phone messages and the calls during that incident, which can become pretty annoying.

so additionally, just the jobs, growing demands and, the limited recognition, that has led CISOs to sometime question their long term commitment to their role, and thereby just resulting in the career dissatisfaction. I'm sorry if I just,

[00:22:53] **G Mark Hardy:** No there's a lot to unpack for us,

[00:22:55] **Raghav Singh:** but yeah.

[00:22:56] **G Mark Hardy:** but, yeah, I'm trying to take notes here. So here are the six [00:23:00] main sources of burnout. Tell me if I captured them right. It could be related to the organizational culture, which we discussed a little bit. Resource limitations. Sometimes you don't get the budget. You have to go grubble in front of the CIO to be able to fund what you need.

The job burden, just the fact that this is a very complex task, requires constant, learning and, involvement in a lot of things. communications and relationship changes, if I caught that where it's a dynamic flow and all of a sudden, Hey, we have to go ahead and make this, work out, or we have to talk to that person.

a need to constantly keep up with external pressures. And that could be the changes in the threat landscape primarily, but also you'd mentioned vendors, and of course vendors always want a piece of your time on your budget. And then insufficient executive support, which is a big deal because a lot of times we talk about CISO as a C level executive, but a small C instead of a large C.

So for those of us who grew up in the United States at Thanksgiving, we used to have the grown ups table. And the kids table. [00:24:00] And sometimes as a CISO, you don't get a chance to sit at the grownups table unless you're standing at the end of it, getting chewed out for something that went wrong and went sideways.

Did I capture those correctly?

[00:24:11] **Raghav Singh:** Yes, you absolutely did. And, I 100 percent agree with that point of the capital C and the smallest c when it comes to, comes to CISOs. And, just a point, just a quick point about, the stressor that you talked about where communication and relationship manager management is a problem. and the reason why it's a problem is because It requires balancing just the technical communication with business language, which can be challenging.

what we noticed was that quite a few CISOs, they faced a few challenges communicating to the board because they did not really understand how to talk in a business language. So when they are presenting to [00:25:00] board members would want to, get the data in dollar amount, and they would want, the communication to be done in much more of a business sense, where a lot of CISOs, since most of them come from a very technical background, all they could talk about was, technical jargon that the board couldn't really understand.

[00:25:28] **G Mark Hardy:** And that's one of the things we've been really trying to address over the last, now we're in our fifth year of doing CISO Tradecraft is providing those resources to say part of what you need to do. is mostly focused on communicating in the language in which your audience is going to understand. And when you're dealing with the board or senior executives, it's primarily risk.

What are the uncertainties that the organizations face? What are the potential threats that could materialize and then interact with our Assets to create these types of risks and those [00:26:00] vulnerabilities or those exposures to those threats, and then focus on that and, not coming in and saying, we've got CVSS 9.6.

It's coming in here through the 37 60 golf router, which is obsolete because Catalyst went out of no. They wanna know that, which you need to be able to come in and be able to say something that not only points out the problem, but I always tell people, be solution oriented. Don't come into my office and tell me there's a problem.

Sir, we got a problem. No, what are you gonna do about it? that's why we're talking to you. if you find out that if you're the CISO and everybody has been trained that you will become Solomon and you sit there with your sword waiting to slice babies in half when there's disputes, or you're waiting to make great pronouncements because you are the wisest of all in time, you're going to train your people not to solve their own problems.

And they're constantly be lying outside your office waiting for you to make a decision. And so empowering. Your people as a CISO to make the decisions. [00:27:00] Now, if they're going to be bet the farm decisions that have, we have to keep in mind that what I said as a guidance is if you're going to delegate decision making, the value of that decision that you delegate should not exceed that person's budget approval authority.

I say that again, do not delegate decisions. that exceed that individual's budget approval authority. Meaning what? As a certain level, as a director, you might be able to spend 10, 000. As a VP, you might be able to spend 20, 000. As a CISO, you might be able to spend 50, 000. As a CIO, you might be able to spend 250, 000.

Or whatever, before you have to go up to the next level. And so when we look at things such, for example, rogue trader Nick Leeson, who took down Barings Bank back in the day, and here's a guy making billion dollar bets. or Billion Pound Bets, way above what that person could approve. He might not even be able to buy a box of paperclips in that [00:28:00] organization.

And yet there's a fundamental lack of oversight there. So as a CISO, we are responsible for providing the oversight for our teams. Whoever gives your oversight is a different question, but think about developing your people that way, where you entrust them to say, go ahead and give me a recommendation.

Now the recommendation might be a bad one and you don't necessarily have to follow it. But you might say, at least, you gave it a try, but let's correct that and do it this way. As compared to a type of a situation where, okay, just do it and, we'll come back. I think one of the things that we find, and this helps with burnout, by the way, is that having an appropriate span of control.

It's a term we mean, which is the number of people that are reporting to you. And realistically, you can get up to about seven people or so. And when you get beyond that level. and Spanning Control, you're going to go yeah, this is not going to work. This is going to be such the fact [00:29:00] that too many activities, too many moving parts, you can't track them all.

Life just gets completely difficult. And it's yeah, we can't handle this. And so that burnout perspective is say, you know what? I can't deal with all these moving parts. is going to work against you as compared to somebody who says, you know what, I have got sub and then sub delegations, certain levels of authority, because if you think about it, a CEO who's running a multi billion dollar company can't control all the vertical, can't control all the horizontal.

And so being able to restrict that, and it's almost getting back to the one minute manager, you go back and look at Hersey and Blanchard or some of their ideas like that. makes sense. What are your thoughts on that as a way of not just diagnosing the problem for CISO Burnout, but actually prescribing some ideas of ways to potentially improve on that.

Thoughts on that?

[00:29:57] **Raghav Singh:** Yeah, [00:30:00] So I do have thoughts on that. so in our paper, we also, another thing that we do is we have practitioner points. so basically points that CISOs can use and not just the CISOs, but the organizations. leadership can use just to, just to address the burnout a bit, And, provide the CSOs few, not leeway exactly, but, provide them more resources to help them do the job a bit better.

so we do have some of those practitioner points, in some of the work that we are continuing to do. Yeah.

[00:30:40] **G Mark Hardy:** And other points as well. In addition to going ahead and having a more streamlined strategy for managing your direct reports, what about information flow? Have you looked at that as a potential CISO being a bottleneck for all these reports and things like that and having to adjudicate? Is that a contributor to [00:31:00] CISO burnout?

And if so, how would one simplify that? Think of a

[00:31:04] **Raghav Singh:** Yeah. To be very honest, we haven't looked at it yet. yeah, that, that's a very good point. But, we should

[00:31:13] **G Mark Hardy:** SOC, for example. Now what happens is a security operations center What you want to do is you want to reduce the number of false positives. That is to say, if I'm getting 10, 000 alerts a day, but only a hundred of them need to be followed up, then there's a 99 percent waste and that is just digging through it.

It's almost like having spam all day long. And although deleting spam in and of itself isn't a stressful activity, Just dealing with the fact that you've got the horrible signal to noise ratio. So I think one of the prescriptive things is to find ways to organize your information flow, to improve your signal to noise ratio.

So you're not sorting through junk. You don't get involved in decisions or meetings that are using a military term below your pay grade, because it's I don't

need to [00:32:00] know about that. When I brief, my, my boss, client environment like that, I do weekly updates. Just say, here's what's going on.

But during that, I don't, put everything in there. They don't care about the fact that, oh, I had to rewire this particular hot point, or I had to update this here, but what's more strategic? And if you can work on those communications as a CISO, your bandwidth requirements of communication start to drop down.

to something that's a little bit more manageable. Now, I remember when we met a couple of weeks ago, we kicked around some ideas, and you thought some of them were pretty good ones. And I didn't write them down, but I think you did. And so is there anything from that discussion that came to light that you think would be of value to discuss with our audience?

[00:32:47] **Raghav Singh:** Yes, definitely. And I think it can be a two way communication. so I'll tell you what exactly I talked about. so one of the things that, I brought up was. [00:33:00] How we, at least for the research, researchers purpose, we had, come up with a CISO maturity level as a coping mechanism.

I had mentioned that how we see CISOs, at least in the framework, was that there are three levels to a CISO, like a CISO 1. 0, 2. 0, and a 3. 0 with Each phase representing a big shift in, not just skill set, but also the mindset and that this journey doesn't just impact the CISO, but it influences the entire cybersecurity landscape.

so just to be, just to, explain what CISO 1. 0, 2. 0, 3. 0 is in short. So CISO 1. 0 is where a lot of CISOs start, so they are very IT centric and they are very heavily, heavily focused on the technical tasks like, your network monitoring and [00:34:00] vulnerability scanning. So at this stage, the focus is pretty narrow and a lot of CISOs might struggle with the broader organizational awareness or, business communication.

So they are incredibly skilled technically, but Translating that into the boardroom language is something of a challenge for the CISO 1. 0 and it's in this phase that the CISOs can feel being pretty isolated because they lack the business acumen to connect meaningfully with the other C suite members.

But then, if you move into being a CISO 2. 0, that role evolves from being just very IT centric to be, to being more risk oriented where the CISO still leverages a lot of, technical expertise, but they now prioritize [00:35:00] identifying and mitigating risks that could impact the organization.

So there they start to think more strategically, they start aligning cybersecurity with the risk management. but then again, the shortcoming of 0 is that the communication challenges, they still persist and a lot of CISOs find that they don't have the same status as the other, C suite executives.

So it's like a step forward from 2. 0, from 1. 0, but still not quite at the executive level of influence. finally CISO 3. 0 is. something that marks a major transformation where the CISO becomes a true business enabler. So what they're doing is they are fully integrated into the organization's strategic planning, actively contributing, the insights to help drive the business goals while also managing the cybersecurity risks.[00:36:00]

So they are the ones who adopt the, the language of a boardroom and they are on the equal footing with. A lot of, C suite members as well. a good way to, think about CISO 3. 0s is that they're no longer the security guard of the organization. Instead, they are somebody who are trying to propel the business forward, which ultimately reduces the feelings of isolation and increases the job satisfaction.

so basically, yeah, sorry, go on.

[00:36:36] **G Mark Hardy:** Yeah, no, excellent. So what have you seen then in the progression of the sense of burnout as someone goes from CISO 1. 0 to 2. 0 to 3. 0? Does this become a nirvana of sorts that, hey, everything is fine, or is in fact it's all appearance like a duck who's calm on the top and paddling like crazy on the bottom?

Where does the burnout hit? Is it uniform throughout the [00:37:00] 1. or does it peak in some place?

[00:37:03] **Raghav Singh:** So it's, It's generally, so let's, let me put it this way. CISO 1. 0 is much more prone to face burnout, right? And, an interesting way to look at it is that burnout can happen to all three of them. It's the fact or the art of managing that burnout, that really is helpful. And the art of managing burnout is more in CISO 3. 0 rather than 1. 0 and 2. 0. So basically CISOs progress through these phases and they develop better coping mechanisms for managing burnout. So a CISO 1. 0 and 2. 0, they would often rely on emotion based coping, such as overworking or handling the stress through their individual efforts. And that in turn can lead to more burnout because they are handling everything [00:38:00] themselves. but for the CISO 3. 0 phase, You see not emotional based coping, but you see something called problem based coping. so in problem based coping, what they do is they are leveraging the team

resources. They are aligning with the organization's culture and addressing the root causes are the root issues rather than just the symptoms. so the, that particular strategic approach from CISO 3. 0 that allows them to manage their workload better and, feeling, feeling much more, integrated in the executive team and ultimately that helps reduce burnout.

[00:38:49] **G Mark Hardy:** That makes good sense. And so now you had pointed out an interesting statistic a little bit earlier, your average tenure of a [00:39:00] CISO is just barely over two years. And yet you've described three phases that I don't know if that's, if one is going to promote or advance or grow to level two, level three in the same job.

So do we find a correlation between somebody. in CISO 1. 0 and then timing out because after two years they just burn out because they don't have the skill sets. Maybe they get another job, but when they get to the CISO 3. 0, are these the people who can tend to persist for longer? They become the long tail statistically because they're where the organization needs them to be, but they're also where they need to be.

Do you see that correlation?

[00:39:40] **Raghav Singh:** yeah, but I believe we do, because, a lot of, not a lot, but a good chunk of CISO 1. 0s, they keep, they have to change their job because of burnout. And a lot of them even contemplating, they even contemplate not being a CISO anymore. But the problem [00:40:00] is, there's no natural career progression from a CISO role. So a lot of them, what they end up doing is that they go to another organization where they hold a position of, both a CIO and a CISO. Or maybe a CTO and a CISO because, because that at least gives them more job autonomy. So yeah, there are lesser CISO 3. 0s than CISO 1. 0s. so yeah, you can see that tail that you just spoke of,

[00:40:38] **G Mark Hardy:** and I think you, what you talked about is a rather important thing as often. If you're a technical person and you're working there and you say, Hey, someday I want to be in management and then leadership and then learn the political system. That's the apex is that, Hey, I've made it up here to the top.

I'm the CISO. I'm not a director, VP, senior leader for that. But where do you go from here? I've had some [00:41:00] friends who have popped over to the CIO job. As you mentioned, some hold both hats. I work with organizations where I hold both hats. but at that point in time, you often don't see A CISO saying,

we'd like to announce the selection of our new CEO, the CISO, or the new chief operating officer, the CISO.

it doesn't seem to happen.

So what we have then is a situation where CISOs may be facing the fact that they're at the apex of this. They look around, they don't see any other mountains other than similar mountains to the way they're at. And so what happens at that point? Do they simply say, I'm going to go ahead and get into a long haul trucking.

I got this matchbook cover and it says, learn how to be a long haul trucker. I wonder if I can do that. Where do CISOs go after being a CISO? If they're not old and retired and headed off to Florida to go ahead and live on a condo someplace.

[00:41:56] **Raghav Singh:** That's actually a great question and I think you'd be the perfect person to [00:42:00] answer that, rather than me,

[00:42:01] **G Mark Hardy:** So I'm still working. So I'm not the right answer.

[00:42:04] **Raghav Singh:** Yeah, but then what I, from what I understand is that, the CISO community is a very closely knit one. So I'm very sure that you must have a lot of CISO friends and peers who may have been through certain situations, but, but at least from, the point of our research, what we have seen from the, different CISOs that I've talked to is that a lot of them can just feel stuck and they just persist with being in that role. and it's not really a happy place to be in for the CISOs. so their work, work life balance, and, even the relationships in the families, even they can break down because of that. but then yes, a lot of CISOs, like you correctly pointed out, They just transitioned to another role, like a CIO or a CTO.[00:43:00]

but then, yeah, that, that's what we have primarily seen, at least in the research in the, with the CISOs that we've talked to.

[00:43:09] **G Mark Hardy:** So as we get close to the end of the show here, as you're working through all of this. When do you think your results will be available? I'm not trying to put any time pressure on you, but I'd be really fascinated to, to read what you come up with.

[00:43:23] **Raghav Singh:** Sure. so there's a conference, so there's a conference that we presented our findings in recently. so the conference version of this paper is already out there. I'd be happy to share a link with you,

[00:43:36] **G Mark Hardy:** Send it to me and I'll put it in our show notes.

[00:43:38] **Raghav Singh:** Sounds good. And, we, we also, we've also, added on to our existing work, so we, connected a few more interviews.

came up with a few other themes that contribute to CISO burnout. And that version is, we are still trying to work on that and publish it in the journal. So there's [00:44:00] still a bit of, time for that left. but I'll definitely, pass it on to you once we published that,

[00:44:07] **G Mark Hardy:** So Raghav, it's fascinating the work you're doing. And if somebody would like to be part of your study, because I know you're looking for inputs on the CISO burnout, what should they do? How would they get in touch with you?

[00:44:19] **Raghav Singh:** Thanks for bringing it up, Mark. So yeah, to all the wonderful CISOs out there, I'm always, looking to talk to, Talk to you, guys. And, there are a couple of projects in the works where I would love your feedback on. I'll drop my, email ID with, Mark for this video, and we can put that in.

And if any of you want to help me advance knowledge and provide your, inputs on my projects and get interviewed and be a part of my projects, that would be highly appreciated.

[00:44:55] **G Mark Hardy:** I hope anybody who's out there who is interested and feels passionate about the subject of [00:45:00] CISO burnout would be very happy to contribute to your program because I think you're adding a lot to the community. So, thank you very much for that kind offer.

[00:45:08] **Raghav Singh:** Thank you so much, Mark.

[00:45:09] **G Mark Hardy:** So we shall stay in touch and I'll look forward to it. For our listeners out there, thank you so much. We've had as our guest Raghav Singh. He is a PhD candidate at the University of Buffalo. He is looking into the Topic of CISO burnout. Something that we have shared some ideas on the show about both some of the symptoms and possibly some of the antidotes that we could do for it.

So we hope that you've found this very valuable. If you have found this valuable, send us a note, go on LinkedIn, connect with us on CISO Tradecraft and follow us if you have not, because we put out more than just podcasts. We have a lot of extra information. If you're listening to us on your favorite podcast channel, give us a thumbs up or whatever feedback so other people can find us because we The more people that say, yay, this is good, the more people are able to find us.

And we hope that you've found this valuable. So I thank you very much for being part of the show as an audience. Raghav, thank you for being our special guest. [00:46:00] And to everybody else, this is your host, G Mark Hardy. And until next time, stay safe out there.