Reimagining Cyber Episode #17 Transcript | Cybersecurity and the Modern CISO | Guest: Parham Eftekhari

Mon, 7/26 1:32PM • 24:11

Listen on Soundcloud

SUMMARY KEYWORDS

ciso, business, parham, cyber, role, cybersecurity, technology, organizations, private sector, security, government, cfo, companies, public sector, conversations, focused, business leaders, critical infrastructure, board, executive leadership

SPEAKERS

Rob Aragao, Stan Wisseman, Parham Eftekhari

Parham Eftekhari 00:00

I think the government needs to do a really strong job advocating and educating the CEOs of major companies that this is an area where we actually need your help. It really should be, I don't want to go down the patriotic route, but I think it should become a part of corporate responsibility and corporate ethics. I'm not sure who should be responsible for it. I believe it should come from the White House and kind of some sort of major national initiative. But I do think that cyber should become part of a company's corporate responsibilities.

Rob Aragao 00:37

Welcome to the Reimagining Cyber podcast where we share short to the point perspectives on the cyber landscape. It's all about engaging, yet casual conversations and what organizations are doing to reimagine their cyber programs, while ensuring their business objectives are top priority with my co-host, Stan Wisseman, Head of Security Strategist, I'm Rob Aragao, Chief Security Strategist, and this is "Reimagining Cyber". Stan, who do we have joining us?

Stan Wisseman 01:04

Rob, our guest today is my friend Parham Eftekhari. Parham was the co-founder of GTRA as well as the Institute of Critical Infrastructure and Technology, also known as ICIT, where he is still the Chairman. But last year, Parham took the role of Senior VP and Executive Director for the Cybersecurity Collaborative, which is part of the CyberRisk Alliance program and is great to have you as part of our podcast, my friend. C an you expand on your background and the current role that you have for our listeners?

Parham Eftekhari 01:37
Sure, for the benefit of the listeners, I've been in the technology in cyberspace for about 15 years now. A lot of that has been working with the public sector and the federal government more specifically, in general with organizations, some of which Stan has mentioned, to create opportunities for federal technology and cybersecurity leaders to collaborate and share best practices and come up with solutions to solve the needs facing the government alongside their technology partners, like CyberRes and others. And so been doing that for a number of years. At ICIT, we were focused on producing research objective, nonpartisan research, that we shared with Congress, with federal agencies with the private sector, our critical infrastructure, owner operators, and so we've created a lot of great education and opportunities to partner with institutions like Congress and some of their projects, like the Cyberspace Solarium Commission, and other other agencies across the government. Now at the Cybersecurity Collaborative, and at CRA, I've kind of shifted gears a little bit, I'm primarily engaging with the private sector. And so I'm essentially tasked with, among other things, leading a group of CSOs as part of our peer to peer CSO community, which is what the Cybersecurity Collaborative is, essentially, we are a community that believes that some of the best insights and knowledge that can be used to support and improve security across organizations come from peers. And so we have a built a community and a series of services where executives can come together, we identify the top issues and challenges they're facing. And then we help them share best practices among one another. And more importantly, we capture that knowledge into guiding documents and tools and policies, which we then put into our members portal. And we democratize access to that information, if you will give it give it not just to the enterprise level members, but also, you know, small, medium businesses, state local government members as well. And it's just a great opportunity to have some trusted dialogue and help tackle the face, you know, face the issues of the day.

Stan Wisseman 03:59
Well, Parham, it's great to have you here, you as you've mentioned, you know, you've had the chance to work with a lot of executive leadership, not only in the public sector side, but also on the industry and academia. What have you seen change as far as cybersecurity leadership in that role of, you know, the CISO in the last decade and a half?

Parham Eftekhari 04:19
Let's start with what has changed. I think that the role of the CISO and really, depending on the size of the organization, those who are tasked with being leading cybersecurity and leading risk, I think, what we see, is that they are they're becoming more and more business leaders and business executives. At least, I think the ones who are more effective and efficient in their role understand that it's less about them actually implementing the technology and kind of doing the blocking and tackling themselves. They have teams to do that. What's really important for the CISO to do is understand how to navigate the business side of the organization to make sure that the priorities that they have as the head of the security shop, get elevated to the business leaders, right? The Board, the CFO, the CEO, the President, all the business unit leads within their organization. And that CISO really acts as that liaison between these these roles. So I think as you go up, kind of the food chain, so to speak, and organizations become larger, have more employees and more endpoints have just a more, more scale

to them. You see the CISO becoming more involved in and being a business leader, I think that's really been the most stark evolution and how that translates into what they do,

Rob Aragao 05:45
Thinking about the CISO role and the conversations that you're having more so on the private sector, you know, most recently, what are you seeing out there as relates to the kind of challenges that CISOs are having in conversations with executive leadership? With the Board? You know, a lot of things we've kind of discussed in the past is almost a tactical but technical, right? They come at it as like technology will solve the problems, the technology will protect this. Sure. But the translation of that doesn't make any sense to the Board level, it's what's the business outcome that we're going to achieve? And how are you going to enable us from a cyber point of view? I guess, what are you seeing as the key elements and best practices that are resonating when the CISOs are having the right type of conversation with executive leadership?

Parham Eftekhari 06:30
Yeah, that's a great question. I think, first and foremost, it's about understanding what's the priority for your business leadership and executive leadership? And speaking to those priorities. At the end of the day, very few business leaders are going to be interested in and how you're achieving those outcomes. They don't care about the the solutions, the technology, your layered security strategy. They may want to see it on a slide just to know that you've thought through it at the highest and highest levels. But the conversation that needs to be had is based on who you're speaking with, and what their priority is end of the day. Each of these business leaders has a Scope of Work, they're getting compensated, and, frankly, bonused, on certain certain meeting certain business objectives and certain business outcomes, a lot of time tied to revenue. And that revenue on those outcomes can be impacted negatively, due to digital risk. And so if you can come to them and say, I've identified these risks to the business to what you're responsible for, and I can help you mitigate those risks by implementing some security strategies, and here's what they are in business terms I can, I can reduce the risk of hackers attacking the network. That's all I got to say, a lot of times, I think if you leave it at that level, and speak about it in the terms of that they're interested in, and what their understanding, and then tie back to dollars and say, you know, here are some scenarios I've built out. If you're in a manufacturing facility, you say, if we're down for one hour, we're going to lose X amount of revenue. And you know that most, most recently, here's five recent examples in our industry of ransomware, or whatever, whatever incident has happened, that has caused our competitors X amount per day. That's hard to argue.

Stan Wisseman 08:24
I think the other challenge sometimes is where as a leader you report into so for example, classically, the CISO reported up through the CIO, and the CIO is more of a technology leader, right? And how they then will expect you to represent things up is sometimes with a technology focus, because that's how they view things. I'm sure you have seen and talked to lots of leaders and have various different reporting structures, whether it be through the CFO, through the CRO. Where are you seeing things evolved to? Or is there a best practice? Is it just personalities? You know, it works best if you have worked better with your leader, no matter what their role title is.

Parham Eftekhari 09:10

I think the things that matter in terms of the impact the CISO can have, and you know, where he or she can have the most impact, and where it makes sense, are things such as is the person you're reporting to going to have going to be personally impacted based on the recommendations that the CISO is making? You know, I've heard so many stories that the CFO will report to the CIO, and we all know we've all heard this, right. The CIO says, Well, I don't want you to make give this report to the Board because you're basically pointing out all these potential flaws and issues with the technology stack that I've built, and I don't want that. So they put a kibosh on it or in other instances, the CISO reports to the CFO and the company had a bad quarter, and so the CFO is like I need to save some money and the easiest thing to do is to cut security because you know, that's it's a nice to have, it's also in the security budget, the security requests get slashed. In my opinion, one of the things to look for is who can the CISO report to who's where that individual's perception on what's being recommended by the CISO won't be skewed based on their personal objectives. Because the role of the CISO, which is why I think we're all saying, you see, so should have report to the CEO or the president who's responsible overall for the company. I personally think that's where this should be heading to. And I'll give you another interesting example we're having, we're having conversations right now about, at the Collaborative, one of the big things that we're talking about is that you know, IT modernization, everyone's modernizing their their IT infrastructures. So particularly at larger companies, you have all these business unit leads, who are out there, either migrating to the cloud or investing in, you know, cloud-based applications and all this and the CISO, saying, I want to make sure that I have a seat at the table. So when these decisions are being made, we are whether we're going to be developing, you know, custom code, or there's an API or even just negotiating with the cloud contractor, or cloud provider, I can manage this third-party risk. Right. It's being introduced into the ecosystem. And to do this, either the CISO, you know, him or herself needs to be have the, you know, the perspective or the personality, frankly, to be able to go out and reach out to these business unit leads and just foster those relationships and, and get the buy in individually, which may or may not be realistic and may not be always be feasible, or you need somebody from the top to put in governance and put in policies and mandates the business unit lead saying, if you're going to spend money, one of the things you need to do is make sure that the CISO is, you know, signs off or reviews the contract or something. And so, I mean, these are the way in which where the CISO sits and how he or she is involved in the process really is going to ultimately have the biggest impact on on the resiliency of an organization.

Rob Aragao 12:04
One of the things Parham, as you were alluding to, on the business side of things that I I've seen in working with the different financial service organization that was extremely effective and pretty mature, was the buy in at the executive level. The organization had seven different lines of business. And one of the things they did to drive, the effectiveness of their cybersecurity program in each of the different lines of business was they tied a portion of the annual bonus for the business leaders across each of the seven lines of business, to their cybersecurity program profile and risk measurement. And I've not seen much of that out there. And I think that's, again, a way to really move the needle. The other thing that you alluded to is that the CISO have in the business conversations. And in some of the again, maybe, let's say more pioneering organizations and financial, for example, we see the role of the BISO, alright, the Business Information Security Officer becoming much more prominent, and kind of that layer of let me go as the BiSO aligned to a line of business and meet with those owners of the business specifically to translate, right, what the actual needs are from them, their initiatives are working on what

cyber's impact, the risks potentially could be, and mutually build that partnership to be successfully putting the cyber program to support them in place. What are you seeing out there? Are you seeing that really take off to look at other verticals and some conversations you're having? I mean, it's it seems like a very prominent role that is helping move things in a positive direction.

Parham Eftekhari 13:30
Bonuses are there to incentivize behavior. And so I one of the best things I think that cybersecurity practitioners and executives can do is get their Board to incentivize the right behavior by tying a portion of a Business Unit Lead, you know, bonuses to different types of responsiveness or compliance with what the CISO is asking for what I don't mean compliance in terms of regulatory I mean, compliance with the CISO's action. So I think that's great. And I think we should see more of that kind of innovative thinking. And, and, and, and partnership between the board and the CISO and the Business Unit Leads. And sometimes maybe you need to strong-arm it a little bit, but I think the stakes are too high not to make that a requirement. I think with in reguards to the the second question, I definitely see that as as an evolving role that's being, you know, that's increasing in organizations around the country and even internationally. I think that the reality is most likely we're just going to see more enterprise level companies take advantage of that because it is something that I think we have, we struggle with mid and certainly small sized companies even budgeting for, you know, a large security staff and funding with the security organizations asking for, so I think that the a Business Information Security Officer is going to be critical, I think is valuable. I think as a full time role, probably the bigger companies will do it. I speculate what if this becomes another, you know, "as a service model," where you have consultants that can be brought in to help kind of translate and be that be that, you know, liaison between the business unit leads and the CISOs, maybe that's an emerging, I'm speculating that, you know, I could see where that becomes an emerging field of consultancy in the near future.

Stan Wisseman 15:26
Hey Parham, to shift gears a little bit to the work you've been doing with the ICIT, which is as a focused on critical infrastructure protection. We've had some developments over the last few months around, potentially, that would help us boost our protections in this space. And we had the executive order from Biden, on the NATO agreement, do you think these are the going in the right direction? What else is needed, in your opinion?

Parham Eftekhari 15:55
I do. I think it's going in the right direction. The White House announced the stopransomware.gov website. I don't know if you had a chance to take a look at it yet. But it is I think a very well organized, you know, website that aggregates all of these different resources that the government has out there. The government certainly has an a very important role to play. I was meeting with with some of citizens leadership was, you know, interesting to hear their perspective on how to leverage legislation as a role in moving and advancing critical infrastructure resiliency, both in not just you know, the public sector, but obviously the private sector and critical infrastructure. Personally, I think you need a couple of things. I think you need more corporate responsibility to say that, hey, this is a priority, we need to take that whole of nation approach that I mentioned earlier, I do think that we need to go from just recommendations to requirements. CMMC is doing this by saying, you know, if you want to do business

with us, you have to meet these certain standards. I know, people have varying opinions on how effective it is. But I think overall, we have to start somewhere. And CMMC is a wonderful way to start.

Rob Aragao 17:09
Parham, you know, one of the things that we've discussed in the past is kind of the influences from public sector on to private sector. And there's been a lot of pushback, right. But I'd be interested to get your perspective, since you're kind of straddling both sides. right. What you're seeing out there, as far as you know, some of these conversations are happening more from a legislative perspective, the EO is obviously driving a lot at the federal sector, but what are you hearing on flipside, right? is public sector saying, Yeah, you know, not only pay attention, but we're planning on taking similar action, or we're going to continue to do our own thing?

Parham Eftekhari 17:46
Government has not been perfect like, like private sector. I think they have always been focused on cybersecurity. I think that it's very visible when they're not because they're required to do GAO audits. And so all of their dirty laundry is kind of aired to the public, when private sector companies aren't necessarily, so I think we got to remember that. And I think that moving forward, you know, you will see, particularly with some of the new new positions that have been created by the new administration, and these executive orders, and just a flurry of legislative activity, I think a lot of these bills eventually get bundled up together and become one, you know, one, one bill that eventually get passed. And I think this is a maybe an interesting kind of comment to make, but I think one of the things government could should do a better job of is just promoting and socializing what they do, because everyone else was focused on the things that that goes wrong.

Stan Wisseman 18:38
It's funny, we had Michael Echols friend of yours, yeah, on a previous episode, and he made the point that he could walk around all around DC and not see any sign or any kind of indication of cybersecurity, as far as awareness, yeah.

Parham Eftekhari 18:53
Yeah.

Stan Wisseman 18:53
And that's to your point, we need to raise that bar. Hey, so to wrap up, you know, one of the things you've said in the past is that, and maybe this is the context more of the private sector, but it's acceptable today to put profit over security, right? And and we've come a little apathetic, as far as cybersecurity incidents. Now, ransomware may change that, right? Because they really had to focus on how to continue to operate in the face of these kind of attacks. But you know, what are some of the ways in which you would incentivize, we talked about how would you incentivize business leaders in general, but how would you recommend changing those priorities?

Parham Eftekhari 19:35
Yeah, that is the million dollar question. I think that we're a capitalist country. We enjoy our liberties and our freedoms, and this democracy that we live in, but because of that, these corporations that are

thriving right, in this in this system that we live in, need to understand that when it comes to this particular topic, Security, or national security, is not something that our government can handle for them, right. There is there is a certain place that, you know, our physical borders can be kept safe by our government, but our digital borders really cannot because it is majority-owned by the private sector. And I really think that going back to this messaging campaign, I think the government needs to do a, a really strong job advocating, and educating the CEOs of major companies that, you know, this is an area where we actually need your help, and it really should be, I don't want to go down the patriotic route. But I think it should become a part of corporate responsibility and corporate ethics, just like many other things have come over the years. I think, we will, that's that's a very large order. I'm not sure who should be responsible for it. I believe it should come from the White House and kind of some sort of major national initiative. But I do think that cyber should become part of a company's corporate responsibilities. I think from the bottom up, it starts with consumers, whether it's individual or you're a you're buying on behalf of your company, whether you're, you know, medium sized business or like the DOD is doing, and we just start to demand and change our buying habits. I remember speaking of GTRA (Government Technology Research Alliance), I remember, you know, this was, I don't know how long ago but, and one of our GTR events, it was the Colleen Coggins, and she was a CIO for the transportation agencies, I believe, and she gave a talk and it was when cloud was first happening. And I remember that she gave a talk and said, and I'm very much paraphrasing, but she kind of talked about how she negotiated this contract. And she her one of her points was that I had security requirements, and they didn't want to give it to me. And I said, Well, I'm gonna take my business elsewhere. And her point was like, we have buying power as particularly this government, but companies do too, if you're not getting what you want. Take your business elsewhere, from manufacturers and cloud providers and whatnot. And, and, and I think that we just need to speak up and say, you know, if you're not going to give me the confidence and the risk appetite that I have, I'm gonna take my business elsewhere. And I think these are the types of things that need to happen in parallel to ultimately change. This is a major societal shift. All this technology is new. And and we need to just educate companies that what's acceptable for us and what's not, and where we see them playing a role in all this.

Stan Wisseman 22:22
Yeah.

Rob Aragao 22:23
I think you just hit on a key chord there, the collaboration requirement between public and private sector, we were kind of alluding to this. But true collaboration like enough is enough, right? Share the best practices, what works on the private sector side of things to help both public sector and then over the other way. There's some good intel sharing, I get it, but not great, right. But it's again, beyond that, the best practices that are actually being implemented to support just an overarching improvement are just so critical to our advancement in cyber. Parham, you've been even excellent and sharing that whole connection point back in, especially with the business aspects of what we're seeing out there, right, the structural kind of change and cultural change needed. And in cyber, we've, we've all come to agree, I guess that if you hit him in the wallet, somehow things kind of move the needles in the positive direction, right. So that's a good thing to hear. As it's it's shifting the momentum in a positive direction. Thanks so much for joining us, we really appreciate your time.

Parham Eftekhari 23:20
It was a pleasure. Look forward to being here in the future if you need me. All right.

Stan Wisseman 23:24
Thanks, Parham.

Rob Aragao 23:25
Take care.

Parham Eftekhari 23:26
Thank you.

Rob Aragao 23:28
Thanks for listening to the "Reimagining Cyber" podcast. We hope you enjoyed this episode. If you would like to have us cover a specific topic of interest, feel free to reach out to us and you can find out how in the Show Notes, and don't forget to subscribe. This podcast was brought to you by CyberRes, a Micro Focus line of business, where our mission is to deliver cyber resilience by engaging people, process and technology to protect, detect and evolve.