Micro Focus Reimagining Cyber Episode #19 Arvind Seshadri

Fri, 7/30 3:41PM • 22:28

Listen | Blog

SUMMARY KEYWORDS
security, organization, arvind, cyber, customers, cyber resilience, application, cloud, csp, business, stan, paas, conversations, companies, pandemic, device, role, people, area, responsibility

SPEAKERS
Rob Aragao, Stan Wisseman, Arvind Seshadri

Arvind Seshadri 00:03
One thing is for sure, there are companies who have been attacked, and companies who don't know they've been attacked. That's the reality of the situation. And I think it's a question of accepting the reality that you are exposed. It's only a question of time. So when it does really happen, how do I bounce back faster? And as you said, you know, keep the engine running.

Rob Aragao 00:28
Welcome to the Reimagining Cyber podcast where we share short to the point perspectives on the cyber landscape. It's all about engaging in 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 and 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 01:00
Rob, today, our guest is Arvind Seshadri. Arvind is responsible for the security line of business at Cognizant and has over 20 years of experience working with global organizations driving this security strategy, and he has worked both for WiPro as well as HP in a similar capacity. Arvind, it's great to have you here, if you wouldn't mind sharing a little bit more of your background with our listeners today.

Arvind Seshadri 01:21
Yeah, thanks, Stan. Happy to be here with you and Rob. I lead the service strategy offerings and partnerships function for the Cognizant security practice globally. In my role, help define the vision for the offerings for the company, in terms of the security practice, and what we deliver to customers, by delivering value to our products and services.

Stan Wisseman 01:46

Given the numbers of different companies you work with, and you're seeing some trends, as far as some of the things are focused on. Are there specific things you're seeing a lot of your customers like, aligning their priorities to?

Arvind Seshadri 02:03
Yes, Stan. I think we've all seen, you know, digital adoption grew in a significant way. You know, many years ago, Cognizant was the first company to start tracking digital revenues. We used to call them SMACK. At that point in time, that was the industry parlance at that point in time, as well, which is about social, you know, analytics and cloud and things like that. What are you seeing now, especially post the pandemic, obviously, what we call is the 'new normal'. And I think the 'new normal', the adoption has definitely increased significantly. But more than the adoption, it's also about what they're adopting, which has changed. Significantly, I have to point out two things. One, is the adoption of PaaS, which is Platform as a Service. The area of Infrastructure as a Service, kind of has matured and, and, and plateaued as well. And even the likes of the Cloud service providers with AWS, or Azure, or Google, are all moving towards the PaaS storyline. And the customers are also adopting to that. Second significant adoption change that we have seen is the end user experience. You know, with the 'new normal' happening and work from home being a reality, or at least most of the organizations are going to have 50% of work from home. It's a hybrid workforce strategy that they're going to have. The user experience and connectivity becomes a significant portion of the IT investment for the company. Because the data is going to be with the end user, they could be using their own devices. You know, we've we've seen enough of BYOD and CYOD in the market. But I think this is a real challenge and doing it in real time.

Stan Wisseman 03:49
You mentioned the the transformation of the workforce, right? And my daughter just started a job. And I was shocked when she's working working remotely, and I was shocked when the company said just use your personal computer. And I was like No. But you know, that's that's one of the things how do you secure all these endpoints effectively as you made this, you know, digital transformation due to the pandemic is accelerated this whole workforce working in a telework kind of environment?

Rob Aragao 04:25
And Arvind, you know, as you were talking, a lot of the main theme I kind of pulled away from it is the whole embedding security into anything that we're doing with these different initiatives, right? And, and this accelerated move to the cloud is a great example. When you when you think about that, you know, we're still seeing organizations have a bit of confusion as to kind of who is ultimately responsible for security when they're moving to the cloud, right? So they're working with a different CSP, but there's this times thought that, well, they're going to take on the security for us. That's not really the case at all, is it? So I guess my advice to you is, what is it you're seeing in some of these conversations? When it comes down to the security aspects of that shift to the cloud and ultimate responsibility and understanding of you know, ultimately, it's still back on the organization that is using this CSP, that may introduce some security capability. But again, they need to still stay core security responsibility.

Arvind Seshadri 05:19

As you move up the value chain, the responsibility shifts a lot more to the cloud service provider than to the consumer. In cloud consumer who's doing IaaS, for example, you know, pretty much except the platform being provided by the cloud security provider, everything else is the responsibility of the customer, right? You said everything above that the bare bare metal that he gets, everything is the responsibility for the consumer. Once you get to the Stage Two, which is what I talked about as significantly growing post, the pandemic situation, is the PaaS. Now in the PaaS, it's a joint joint ownership. It just can't be one person or the other. Because the platform also has middleware today. But ultimately, what goes on that middleware, and the data which is going on to the application belongs to the customer. So you can't really, you know, move away from either CSP or the consumer of who's responsible. I think what's more important now is that both need to think similarly. I think what we've seen in our conversations with CSP is as well, you know, we have Go To Market with them. They're clearly understanding that we need to do more for security as cloud service providers. Similarly, the consumers are now understanding that my responsibility is still going to be higher, because at the end of the day, they lose their data, they lose their application, they are going to be out of business, not the cloud service provider. I think that understanding is slowly coming into play. And I think it's about joining hands and doing the best from both sides. And I think people like us, which are the system integrator part of the world, we actually play the glue between the two of them, because we understand what the native cloud capabilities can provide from a security standpoint, and what the customer needs to look at. So we clearly look at it from three aspects: governance, second is control, which is the deployment of, of controls, be it cloud-native as the CSP provides, or something that's coming from a third party, which is available in the marketplace, and third, is the continuous compliance. So these three areas is what we help connect the dots between the cloud service provider and the cloud consumer.

Stan Wisseman 07:36
What are you seeing work as far as being able to deploy DevSecOps more effectively in organizations? Are there some lessons learned that you would recommend others take advantage of?

Arvind Seshadri 07:48
Yeah, very, very interesting area that you brought up, Stan. Right. DevSecOps, I think, is really something that that's evolving today. We are able to use our experiences with customers that we are helping transform, and take that value and then deliver it to other customers. I think what is definitely understood by most customers today, is the left centricity that we talk about. You know, starting from the quarter to understand security is more important. And I think the tools and technology available in the market have also have also evolved in terms of, you know, providing that to the to the developer, and what we look at it from an overall framework, you know, the one that you were talking about, used to look at threat modeling builds the security at the design stage of the development itself. Now, that defines what my entire chain will look like. So you build in the design the threat model, then you build in the SAST and DAST tools, which actually defines and tell you what is wrong with the code. You know, with static analysis, and then eventually with dynamic analysis. And what we've also kind of incorporated, which I think is value for customers, is ultimately this is all running underneath an infrastructure. So there is a mechanism needed to also look at the operational efficiency and security risk of the infrastructure. So you kind of kind of blend both the application security and the infrastructure security and bring it into a soc platform. The integrated view of application vulnerability, and the level of patching that's being done there, and the infrastructure level and the potential risks that this platform

has into your soc, which then becomes a single pane of glass view. And then we can bring in technologies like orchestration automation, which helps you to plug and remedy that gap. So, I think it's a it's a whole combination of people, process and technology. It's a cliche statement, but I think it's much more valid today in a DevSecOps arena than ever before.

Stan Wisseman 09:57
So, the advantage of having a threat modeling approach upfront, is you have specific risks and threat vectors, your attack vectors, you're concerned about for that application that can then drive the requirements and the route of rigor. If you have a low risk app, based on the threat model, you may not have as rigorous a set of assurance activities associated with that application versus a financial externally facing application that is going to be more exposed and you worried about your merit, wrap it up. And I think that the, the fact that you have that whole journey sort of laid out as far as not only the upfront in the design, but also post-production linked with the SOC is a great way of sort of completing that circle.

Rob Aragao 10:48
As you said, Arvind, if you if you talked, we had a conversation with you year ago, you probably wouldn't have detailed relative to the Sec portion of DevOps, right? When you think about another area, that I think is starting to make some very positive traction, I think industry, in some different verticals are, are kind of emphasizing the need, and it's around, specifically, product security. And so, you know, the importance of cyber securing a product is, again, having relevance. The key aspect and attribute behind it from a consumer is really about trust and safety at the end of the day. But when you look at that, and you think about you know, medical devices and all these different connected devices, and a lot of things that we're seeing out there now, where I think you know, as an example, a marketplace, you're seeing a lot more open roles, focusing on product security coming to fruition, which is great. But what are you seeing in the different client engagements you have around product security, specific, more so to the IoT side of the equation?

Arvind Seshadri 11:48
It's a conversation which is raging in the manufacturing sector. You know, from our perspective, we typically are in three domains, right? The connected health, connected automobiles and connected factories, and each one has its own uniqueness. Because the protocol, these legacy platforms use is different for different industries. So the technologies that are available in the market also need to evolve to keep pace with the newer ones that are being introduced, as well as the legacy systems that are there. I think, broadly, what we look at from from IoT perspective, right industry 4.0, and IoT, OT security perspective, the fundamental thing is visibility. You can't protect if you can't see. So you've got to have technologies and tools that are able to see what is happening if the systems whether it's a PLC in a factory, or a sensor sitting in an automobile, transmitting something back to a cloud, in a in a car that is there. Now that activity has to be seen. And that's where a lot of tools today are available, which are focused on the activities that are happening. And secondly, you also need to look at the vulnerabilities of those two. So any software intrinsically has vulnerability, fix that vulnerability, and also put controls in place that it has that cyber resilience, even when that fix is clearly happening. And once we have that visibility, if there is an attack that's happening, how do I disconnect only a portion of my OT or an IoT system so that my entire industry does not collapse. And that is where the network

segregation also plays a role. So there is a significant focus on device security, but at the same time, they're all connected pieces. And so the network segregation becomes an important aspect. We look at it from what we call as the edge to the cloud security framework. That device both internally within the device, if I have an application that can run within the device, I can actually secure the device and what can run or what cannot run what we call as the application control mechanisms. Secondly, if they can't run anything in the device, we at least have a mechanism of authenticating that it is a genuine one, we don't want to forfeited, you know, medical equipment connected to a patient. Then the network, which is the connected part, and eventually most of these systems have controllers that are outside. Especially if you look at telematics and an automobiles connected automobiles, they have a controller sitting in the cloud, so I need to protect that as well. Because if I take the controller and mess with that, it's going to you know, destroy 20,000 ELAC devices at the same time. When we look at an IoT IoT security, it's a whole string of things that need to be looked at, but primarily as you said, it is about the device per se to start with what additionally we want to focus on. And I think we are also seeing that in the market today. The SOC has traditionally been focused on only it risk management. Today it is about bringing that bridge bridging the gap between OT and IT and having a single pane of glass view both for your OT systems and IT systems. I think the technology is evolving today. We are at a stage where we have working with some of the technology partners to bring this together and create that value. We are not there as yet. But as you rightly said, this is coming mainstream becoming mainstream in a very, very fast way. And we've got to keep pace with that. And eventually I think we will reach there.

Stan Wisseman 15:16
You bring up an issue as far as again, that fusion within the SOC of IT and OT, and I'm just wondering, organizationally, if you think about organizations that have these different security functions, you have the corporate or physical security, you have the classic IT security responsibilities, that has also morphed down to business information security officers, as they try to get it closer to the business. And then we have this role, Product Security Officer. Are you seeing as far as how they're organizing those different roles emerging and to reporting up to a single individual that has like a CSO title? Or are they are they keeping to their swim lanes?

Arvind Seshadri 16:02
I think, good point, Stan. I think what we are seeing today, customers are also coming up with new roles, right? The Chief Digital Officer is the role that that's evolving in most organizations today. What they're also seeing is a Chief Risk Officer role. You know, it's not really a CISO, or a CSO, it's a Chief Risk Officer role. And that Chief Risk Officer kind of blends or merges all of these together. In terms of minimizing risk for the organization, I think all these teams, Stan, need to work together. In my view, it is not just the boardroom problem. The security guard at the gate, who lets people inside to the CEO of the organization has to think security. And I think they will have to create these kind of cross-functional teams, which understand the importance of security. And you talked about identity management, Stan, that's the fundamental baseline for any organization. I need to know who you are and what you're accessing, for what purpose. If we are able to bring that into the various organization, it's not there as of yet. And I completely agree with you, a lot of the organizations today operate in silos. And I had a conversation with one of the CSOs where identity management offices with the application team. I asked him, you're the CSO of the company, how can identity management be there? He said, I joined later, that's the way the organization was, and I am I'm not supposed to disrupt what's working, right.

So, it scared me when the CISO said, identity management is not with him. Right? So, a tough question to answer. I don't have a straightforward answer to you. How do you bring all that together? I think it's about the vision of the organization top down. And the realization for every individual working in the organization, that securing the organization is their responsibility, and a bottom-up approach, and a constant messaging through the corporate security teams of that enterprise, to the various people on how best to understand the various risks, create awareness so that you minimize the risk for the entire organization.

Rob Aragao 18:02
You know, one of the things is we're talking across multiple different aspects of cyber, and the kind of tie into individual verticals that you've had so much exposure to Arvind is a frame of thinking that we've been discussing and had previous conversations, which is all around cyber resilience, right? It's basically one of the areas that's really again, had this shift from traditional thinking of we need to do all these different things in cybersecurity. Well, sure, yeah. That's kind of the hygiene, right? The basic foundational elements, no question, those don't need to be applied. But this pivot to more of a cyber resilient type of mindset approach doesn't matter necessarily what vertical you're in. It's just ensuring that you keep the business operating, or whatever occurs, is minimized to the best possible. I'm interested to see, you know, from your perspective, and all the different conversations across multiple verticals globally, what you're seeing that theme of cyber resilience is it's something as well, that you're hearing a lot of and conversing a lot of with different clients?

Arvind Seshadri 19:03
One thing is for sure, there are companies who have been attacked, and companies who don't know they've been attacked. That's the reality of the situation. And I think it's a question of accepting the reality that you are exposed. It's only a question of time. So when it does really happen, how do I bounce back faster? And as you said, you know, keep the engine running? I think that's where the real essence of understanding the end-to-end framework of security really comes into play. You fundamentally need to have a BCP plan. You've got to have controls deployed in the right places, identify what investment to make where. I don't want to secure 25 locks for a receptionist SPG which has no value. I need to look at where I need to make that investment, that's the second thing. And third is, creating this integrated, you know, framework of people right cross-functional teams from HR to finance, to all the people. You know, then it's not just a resource problem to solve and get cyber resilience, it has to be everybody. When you go through something, and we as an organization went through it as well. And what was really appreciated by the customers is, you've gone through it and come up. And that shows that you have the ability to bounce back from what you were, what you went through. And that learning is being passed on to all our customers today. And very big names have gone through this. IT service providers, manufacturing companies, everybody has gone through this phase of, especially with a pandemic today, there are medical companies, which is the pharma companies were creating the the drugs, which is the vaccines, they are the targets today, and and it's gone beyond IT and business, right. It's really gone personal today. And I think that is where it's important that the people understand that. But I definitely believe, Rob, over a period of time, I think companies have understood that, I will be at risk, and I will be taken down at some point in time. What measures can I put in place so that I returned back as fast as possible and keep running?

Rob Aragao 21:10
And I think, you know, one of the things that you just responded that really resonated for me is organizational, organizational resiliency. And ultimately, what you're describing is, to me at least, it's a culture, right?

Arvind Seshadri 21:24
Yes, absolutely.

Rob Aragao 21:25
You have to get them to think culturally, here's how we're going to be resilient no matter what function in the business you serve. Let's all get on the same page and ensure that we're focused on how we can actually be resilient to keep the business operating. So very insightful. Arvind, we really appreciate having you on very much across multiple areas of cyber, multiple verticals, very much a wealth of knowledge, and appreciate your time today.

Arvind Seshadri 21:48
Thanks, Rob. Pleasure being with you and Stan.

Stan Wisseman 21:51
Thanks, Arvind.

Rob Aragao 21:53
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.