The Future of ERP Podcast

Cyber Endurance: Zero Trust Strategies to Secure Your Cloud ERP

[00:00:00] **Gaurav:** You gotta make sure you're following zero trust architecture to secure your ERP because the future of ERP is API driven, cloud first, more open a hybrid landscape.

[00:00:11] **Richard:** Welcome to the future of ERP, a podcast where we discuss hot topics, best practices, and the latest innovations in today's global business. In this week's episode, I'm chatting with Gaurav Singh from Under Armour about cybersecurity resilience in ERP and how endurance and agility can help protect brands, boost profits, and secure supply chains.

So Gaurav, it's a pleasure to have you on the podcast. Maybe you could quickly introduce yourself and your role at Under Armour.

[00:00:41] **Gaurav:** Hello everybody. My name is Guarav Singh. I am a cybersecurity professional, specializing in securing the ERP and SAP ecosystem. I work as a senior manager cybersecurity for SAP at Under Armour. And yeah, I'm a book author [00:01:00] as well and I'm a big fan of having a community and having a tribe. Richard, thank you for doing this podcast with me.

[00:01:08] **Richard:** No problem. And you're not only a book author, you are also a podcast host. So you have a podcast, which we'll make sure to include a link to in the show notes, but maybe you can talk a little bit about what you cover in your podcast.

[00:01:20] **Gaurav:** So the podcast name is Cyber Crea. Crea is a Sanskrit word, which means action. The idea for podcast was, for cybersecurity, we need a team, right? And we need to take actions. So the whole idea was to bring in the experts, leaders from our community together on a platform. No sales, no fluff. It's more about hearing from them what has made them who they are, their journey, for the future, for the native generation to inspire and also what they do to protect or to secure their systems, they're responsible for securing. [00:02:00] So I would say the podcast is for my effort to give back to the community,

Richard. I'm learning from the podcast as well, so I would say I'm a little bit selfish as well to learn and become best version of myself as well. But yeah, the podcast name is Cyber Crea and I will share the link, so take actions to secure your SAP ecosystems.

[00:02:17] **Richard:** You're absolutely right. I learn something new every time I do one of these episodes. So, as you say, it's a bit selfish as well learning yourself, but helping that community to learn more as well, which I think is a key enabler. And you mentioned a book that you've also written, and it's specifically around cybersecurity for SAP. So maybe you could talk a little bit about highlights of the book and what are the some of the key learnings and findings from the book.

[00:02:42] **Gaurav:** Yes, I have been in industry for, I would say 20 plus years, being SAP security, GRC, doing whatever we do to secure SAP ecosystem. And the book I have written with my amazing co-author JP, who's a C2 and co-founder of On Appis. The whole reasoning behind the book [00:03:00] was because what I have seen all this 20 years in the SAP world, there was some false sense of security, right? SAP was a close within a firewall on-prem systems. It was a black box for most of the outside SAP, like the InfoSec cyber guys. So the book referred to bringing those two words together, like the, the CISOs org, where they keep seeing SAP's black box. Even though they're responsible for securing it, they may not even understand SAP as they should. So for the book was for the both audiences. Either you are a cybersecurity or InfoSec guy who's trying to understand more about SAP and make sure you're doing everything to secure SAP. And on the other hand, the SAP practitioners, right? Just maybe doing GRC and security more around identity side, but not doing about vulnerability management, threat management, incident response. And we use like the framework, which is like SAP, secure Operations Map, new cybersecurity framework to like how you can build the [00:04:00] cybersecurity program for SAP. So yeah, I would say that the, yeah, this was effort for, from our, and I think it worked pretty well because I, on the other side was more from the practitioner who's living this whole world day to day and figuring. And it's so much to do right. And SAP world has changed. Now it's become a cloud first and it's opening up to the world on the other side, my co-author, JP, he's like a, somebody who was built and thought of about this whole thing, maybe a last decade or even earlier, right? Right. So we kind of compensated each other, right? He was more like a technical guy who's finding vulnerabilities, helping SAP to patch and doing things like that. And I was more on the, on this side of the fence. So the book is, I would say, is a great resource for anybody who's trying to understand what I should be doing to secure my SAP, even in the cloud world with the BTP and S/4. And it was well received. I think the funny part, Richard, was like, we were told, the cybersecurity [00:05:00] books don't

sell well. Um, but we became the number one bestseller I think it maybe two, three months after the launch of the book. So that was a, I would say great moment for both of us as the co-authors.

[00:05:12] **Richard:** That's a pretty cool achievement and also a testament to the quality of the content that you created. Maybe we can draw some parallels between the company that you work for and the business that you are in and cybersecurity. How do endurance and agility matter when we are talking about cybersecurity? Because we know it's important in a sports environment. How can you have those parallels from a business and IT perspective?

[00:05:38] **Gaurav:** That's a really great question, Richard. So in a athletic world, you don't get fit or you don't get good in sports if you just go to gym like once in a month, right? You should be doing that almost every day. That's how the cyber security also. You cannot be secure, just sayING, okay, we just do this, this control or the security [00:06:00] action of the crea, once in a month, right? You gotta be on your toes. Doing what you do. Following your controls, implementing your controls, securing your systems every day. So that endurance, that keep doing every day, even if it's a small action, security is always a layer, right? We call it a layer defense. You need layer, right? The one layer could not be suffice. And you can only do that when you kind of keep doing the good part, as a athlete would be going to the gym or playing his or her sports, or maybe if you're do swimming right, you just gotta build the endurance, keep doing and, be agile. If you're not agile enough, the other side of the fence, the bad guys, right? Because it's a kind of a cat and a mouse game.

[00:06:40] **Richard:** Yeah. Your competition is always improving. Always evolving.

[00:06:44] **Gaurav:** Yeah. And the AI is also kind of adding to it, right? Even the learning part, I think one thing we always miss is the learning part. As you train, learn, you learn new things and you learn more about your competition and how things are changing. And then you, you become better version of yourself. Same way from the cyber [00:07:00] side. If you stop learning, if you stop doing the whole playing that endurance game and not agile, I think you're gonna be behind and then lose to the bad guys on the other side of the world.

[00:07:10] **Richard:** With that mantra of keep improving every day, keep evolving every day, keep learning every day, what are the operational challenges of keeping a global business, a global ERP system that's always on. How do you ensure that it's always available and running?

[00:07:28] **Gaurav:** So cybersecurity is all about securing or protecting us like there's something called CIA tried like confidentiality, integrity, and availability. So the whole CI tried and we all know availability is key, right? You wanna make sure you're always on because you can't stop your business processes like your supply chain, your sales, your purchase, your customers order something, your systems should be able to process it, immediately without any delay. Right? But your security, right, you got ASAP security package every second Tuesday of the month, or you wanna do a support back upgrade, maybe you wanna [00:08:00] have a, some maintenance, right? We are not here for the business of security. Security is here to be enabler for the business, right?

[00:08:07] **Richard:** Yes.

[00:08:08] **Gaurav:** The

[00:08:08] **Richard:** opposite. Yes.

[00:08:09] **Gaurav:** If you can't patch, you can't take that maintenance window, which you want to have. You wanna make sure you just have a mitigation control. You have all the other things to make sure systems are secure. But business is always, I would say, should take a priority, And that's where we, security folks probably has to be a little bit, I would say think more from the business perspective, not just security. uh, Idea is to, okay, zero day or, or critical. I think you should just patch it, and which I would agree as well. But if the business you cannot take the system down for, for whatever, six, eight hours, maybe make sure. You have the compensating and, and mitigating controls and mean, maybe the systems are not even exposed to, uh, internet, right? Maybe we are okay to take that downtime maybe on the next weekend versus saying, no, it has to happen today. So I always try to be the, partner or be the enabler to our business. Then be that, oh no, [00:09:00] okay, you have to do it now. So that's how I take it. And I know it is kind of a middle part, which we have to pick as a cybersecurity professionals, Richard.

[00:09:10] **Richard:** So we, you have tens, if not hundreds of thousands of customers who are also concerned about their security, their private data being leaked and so on. So how do you ensure when you are talking about a business system where lots of users are leveraging it, both internal to the organization and from a customer's perspective, how do you ensure the security and resilience protects both and everybody leveraging the system, both the customers and the organization's brand?

[00:09:41] **Gaurav:** It all start from the whole policies. So you gotta have a policies for organizations. Those policies should define, help you define standards, procedures, and even controls. The security controls you have, which you ensure by people, process, and technology. Those controls are [00:10:00] being done, they're effective, and any gaps, you gotta have an integr ation control remediation plan. You have to secure your critical vision processes and the technology and systems you have are key to secure your sensitive data, whatever data you have in your ecosystem. Richard.

[00:10:19] **Richard:** Okay, I want to go back again to that performance ethos and relate that back to the business side of things. So how can companies use a performance mindset to make their technologies more resilient? I mean, take into account that ever improving, ever evolving, ever learning discussion we had a little earlier.

[00:10:40] **Gaurav:** In sports and in athletes world, you can never win all the times. Right? So even though you prepare for the best and be ready for the worst. And another thing is, it's not matter of if it's matter of. For when?

[00:10:57] **Richard:** Yeah.

[00:10:57] **Gaurav:** So you, you have to prepare for [00:11:00] that worse, like if we get breach, if we get that security incident, how can we respond? If you get the disaster happen, do we have a business continuity and DRDR plan, which is effective, tested, and vetted, not just one time. It should be your BCDR plan should be the stable top exercise. There are other testing which you can do, and even like the true DR test, right? Are we doing a full DR test as a recurring activity, right? So you, if you're not preparing for that worst. That, that when it happens, you're not ready. And I think same, I would say, if I have to again go back to that whole athlete, you have to prepare, right? If you, in that situation, how do you come back? How do you recover, respond, and then, win, right? This is a game, right? This is a game with the bad guys and the good guys. And we are being the good guys on the ethical side. We have to be ahead in [00:12:00] that game from those who are trying to get into your systems. So we have to be ahead in that game. And the same in in the performance world as well, Richard.

[00:12:08] **Richard:** I actually love that concept because it's basically learning from your, mistakes and not making the same mistake twice. I think the saying is, fool me once, shame on you, fool me twice, shame on me. Yeah. So you always have to improve. You're always getting better. You learn from your loss is you learn from your mistakes. Another thing that I wanted to discuss was

many people. We'll be listening to this and they'll consider cybersecurity a necessary evil. It's something I have to do, it's a chore. But how does strong security enhance business profitability and shift it from being that chore, that cost center to a business enabler? How can you take, put it to your advantage?

[00:12:50] **Gaurav:** How do we change from being a cost center to be a enabler to make sure our business, is growing and I always start from people part of it, So at least, [00:13:00] all the years I've been working, I think I changed from saying no. Like if your business is trying to do that project, right? Um, don't be that guy and say, no, you cannot do that. Right. I think listen to them, right? And let them explain you in why that, project they're trying to do, or even the, whatever thing they're trying to do, maybe building a new API or any new functionality understand that, let them explain the business need behind that ask, which you were so eager to say no. And then as a cyber professional find out how you can still enable them to do their project while not compromising on security, right? So be that partner on their journey for the business versus blocking them. Because the more you block them, they wanna see you as a cost center, right? You was always the bad [00:14:00] guy. You always say no, right? Yes. I think when you say no, I think even my, in my podcast there was one podcast episode, which I loved it. One of our like, he's like a ethical hacker, so he told me about one of the example where the process was so bad it was blocking them to do or move changes as frequent as they wanted to. So they find a loophole, they build some custom, whatever program which they let them import, changes that in the production, right. So the users are gonna find ways, right, to bypass the policies and security controls you have. if you keep saying no to them every time, versus

[00:14:37] **Richard:** that the user becomes the hacker at that point.

[00:14:40] **Gaurav:** Yes.

the, the risk today is more from the inside, right? The, the, those, experts, the admins who knows your system From A to Z. So be, be their partner, be their friend, right? Create that team and understand them versus trying to say, okay, you just have to follow this policy, right, because you would [00:15:00] not be there on everything they're doing, right? So I think that's how, at least I try to see it Richard, like, be the enabler, be that teammate, and join them on their journey while it's still making sure you are doing everything to secure the beta processes and then the systems and everything you should be doing to secure your landscape.

[00:15:19] **Richard:** That goes back to a sports analogy as well. I mean, you're stronger as a team. You're stronger working together to a than doing everything as individuals.

[00:15:29] **Gaurav:** Yeah.

[00:15:30] **Richard:** We have one final question that we ask all our guests and I, and, want your perspective from a, cybersecurity perspective. In a few sentences, what do you see the future of ERP?

[00:15:41] **Gaurav:** I think the future of ERP it's more API first more cloud first more open a hybrid landscape. It should not be a black box anymore, which is good and a bad. So the good guys get to know more about it. It's this API first, which the word they live in today to secure it. But [00:16:00] also I would say is something bad where even the bad guys also know more about ERP now, right? So the defender community, have to be ahead learn it because it's all new word for us. And we say identity is the new parameter, right? So make sure you identity has all the, the whole zero trust mythology, we talk about it. You gotta make sure you're following zero trust architecture to secure your ERP because the future of ERP is API driven. Looking forward to the whole AI changes into the ERP world, but I think this is a new word we are not used to before. The API first, just add more responsibility on my shoulder to be ahead to learning every day.

[00:16:41] **Richard:** Good. Thank you. Thank you, thanks for a great conversation. It's been really interesting. I've heard a lot, as you say, you learn things when you do your podcast. I learn things when I do my podcast.

[00:16:51] **Gaurav:** Yeah. Thank you, Richard, for having me.

[00:16:54] **Richard:** Thanks everyone for joining. Please mark us as a favorite. You can get regular updates and information about future [00:17:00] episodes, but until next time, from Guarav and I, thanks for discussing the future of ERP.