The Future of ERP, Episode XX: Staying One Step Ahead: Shared Security Roles in Cloud ERP Threat Prevention

Ryan: [00:00:00] So, future of ERP from a security standpoint is gonna continue to evolve. And back in the day for ERP, we're focused on roles and authorizations and now we're talking cyber. Where it's gonna continue to go is going to be this conversation around artificial intelligence how can we use it to increase productivity, but also what are we doing to put the appropriate governance and secure AI?

Richard: I'm Richard Howells, and this is the future of ERP, a podcast where we discuss hot topics, best practices, and the latest innovations in today's global business. And I'm joined by my wonderful co-host Oyku.

Oyku: Hello everyone. I'm Oyku Ilgar a marketer, blogger, podcaster in the ERP and Digital Supply chain area at SAP. In this week's episode, we will be talking about cybersecurity and the importance of shared security roles in cloud ERP threat prevention. To guide us through this really important and interesting [00:01:00] topic, we are going to be joined by Ryan Throop from IBM. Hi Ryan. Great to have you here today. Could you please introduce yourself and your role at IBM?

Ryan: Certainly, and thank you so much for the opportunity to talk to the two of you and the broader audience. Again, my name is Ryan Throop based in Raleigh, North Carolina, and I'm part of IBM Consulting's Cybersecurity Services Organization. I've been in the SAP security space my entire career from undergrad my very first position was with IBM and specifically on an SAP security team knowing the ins and outs of SAP role management and SAP GRC at the time, that was the Versa product. Needless to say, after all the years I'm still here and loving the continued challenges and everything that we're able to do for our clients in the ERP and SAP security space. Like many [00:02:00] of the SAP security practitioners listening I've gone through that journey of application security, governance, risk and compliance and controls. And now over the past couple of years a strong focus on cloud security and threat management. For SAP at IBM, I'm an executive consultant that is responsible for our global SAP offering. So really all things related to SAP security, GRC, and cybersecurity.

Richard: We've certainly got the right person then on the call to talk cybersecurity. And you mentioned challenges, but what challenges have you seen impacting businesses and their business systems so far in 2025?

Ryan: Well, let's look at this first one, the positive, and then we'll look at some of those more difficult challenges. I like to look at 'em as, as opportunities. But here in 2025, what we're seeing is our organizations and are significantly impacted [00:03:00] by a lot of ongoing digital transformations. And digital transformation for me is normally these large SAPS four HANA transformations, but that's almost not giving it enough justice. The, these. Transformation programs now are inclusive of S4 HANA Cloud, ERP, but also a much broader set of applications and systems. Most of our projects now are including aspects of enterprise CRM solutions like a Salesforce, HR systems like SAP Success Factors and Workday but also in the area of identity governance. And so these digital transformation programs are becoming much broader in terms of their benefits but also overall impact to the organization. One of the other trends should be of no surprise, is [00:04:00] the use of ai and in the security space here, what we're working on is areas for AI assisted threat detection and basically automating with our gen ai, the ability to alleviate a lot of the tier one and tier two triage and response activities. There's an area where both SAP and IBM are leading the charge and making AI in a secure and compliant way with appropriate governance and data models to give our clients that peace of mind that these systems in 2025 are going to be secure and lead to the increased productivity gains they're expected.

Richard: You mentioned the evolution that you'd been through with SAP and SAP solutions and many companies are also going through this evolution and moving to the cloud. So how has the role of cybersecurity increased in [00:05:00] importance? As we are more a cloud centric business systems.

Ryan: Yeah, that's a great question. So these conversations, it's similar to what I was saying earlier. They're not. Purely SAP centric. We're now talking about broader security domains such as Identity and Access Governance. What is the lifecycle of that employee or end user that is part of their day is maybe using SAP, but they're using other applications and so we're working with our clients to have those broader security conversations about how do we integrate this set of ERP solutions to be incorporated into your broader identity lifecycle? On the threat side, we also look at it in terms of many organizations have very mature [00:06:00] security operations centers and SIM solutions where they're able to, in real time, be alerted and respond to incidents and indicators of compromise across their landscape, but they rarely include the SAP landscape. So as organizations are moving to the cloud, we're bringing up these topics and need

for a inclusive cybersecurity solution. What we're also seeing here is this is very refreshing. Is an increased maturity in the overall control space. We're seeing new regulatory and compliance requirements, and as a result of that, organizations are putting a more concerted and focused effort to address these control gaps. A lot of these control gaps were vulnerabilities and areas that were always present. [00:07:00] Now with the support of organizations like IBM and these new frameworks, not all are new many have been around but we're able to look at their enterprise in a more exhaustive manner to highlight their responsibilities and control objectives, but then also those of their third party vendors and support organizations.

Oyku: Right. We hear in the news about accounting, hijacking and denial of service. This DOS and DDOS attacks every other day. Can you explain some of the most common cybersecurity threats targeting cloud ERP?

Ryan: Certainly, well, you nailed it with those three. But the first thing I'll say is ERP environments are susceptible to the same type of attacks you hear about in the news on a weekly and awfully daily basis. It's often [00:08:00] unknown what the underlying systems are, but for my role I will say that these ERP systems are being exploited. And so in years. Many organizations had this unfounded, for lack of a better word, sense of security because their ERPs were being hosted OnPrem and their own managed data centers, or it was even onsite in their headquarters basement. And so that traditional defense and depth model they thought was sufficient. But now that we've got the prevalence of cloud and expectation of being cloud hosted in hybrid environments, those same controls are, need to be modernized to address those internal and external threats. And so what we're seeing, from a current set of threat actors and threat vectors is a lot of this comes from a report that IBM publishes each year. It's called: The Cost of the Data Breach report. [00:09:00] I highly recommend those listening to seek this out. We can provide the link, I believe and give our security practitioners an opportunity to read this. The 2025 edition came out in July and just an incredible. Asset for practitioners to see the trends of new and old attack vectors. And I think you mentioned account hijacking as one of the first ones, that's a true problem. And what we're doing with that is in the event that end user credentials have been released out into the wild or the dark web. Well, it's important for organizations to have a way to.

Identify and have indicators that these privileges are being used. So working with organizations to we have ways of doing patterns of saying there's unusual login attempts from a country you don't even operate in or time of day and other end user analytics to indicate that maybe [00:10:00] this is a, an ongoing breach.

More importantly, automate the ability to stop it and thwart it in its tracks. The other one you mentioned that I wanted to harp on is on around the malicious insider attacks. There's insider threats. I think I mentioned it earlier as well in our report, this was actually a bit of a surprise to me that insider threats was actually the most costly incident per incident. More so than ransomware attacks, denial of service attacks, it was those traditional insider attacks at almost $5 million per incident. And so I think that really resonates that organizations still need to have that balanced approach to protecting the organizations against both internal and external threat actors.

Richard: You mentioned a little earlier the [00:11:00] on-premise implementations, it was normally the role of the IT department to manage the security or they felt they had control of it. And that's changed when you come to supply chain because you've got the software vendors, you've got the companies or may be different to host the data. And then you've got the company using the system. So what is the roles and how do those roles and responsibilities change? What's the role of a software vendor, like SAP to companies that they serve when it comes to cybersecurity and who's responsible for what?

Ryan: Yeah, great question. So you're getting at the the shared security responsibility model and organizations or software vendors like SAP. You're the underlying hyperscalers, be it IBM, cloud AWS, et cetera. They play a crucial role in ensuring the security of those platforms. But one area that we work with our clients with is really making it clear what are they still responsible for. [00:12:00] And so the first and most critical one is gonna be the data. The data is the client's responsibility and how you're securing that. So this can be intellectual property, financial records, HR data. PII like the list of sensitive data that resides in these ERP systems is almost endless. And so what we do with our clients is walk them through very prescriptively what are the cybersecurity, the security, and the control responsibilities across all of these different personas? When I say personas, that could be SAP, that could be the client themselves, could be the hosting provider.

But then if you start thinking through the complexity of your organization, you also realize, oh, I have some contractors. I have a third [00:13:00] party that manages my applications. I have a different third party vendor that is managing the infrastructure. So as you start mapping out all of these different personas, you realize how complex that shared security responsibility model is

Richard: Right.

Ryan: when ultimate responsibility or accountability is gonna roll up to the organization still.

Oyku: And humans are widely considered the weakest link in the cybersecurity right. Studies show that approximately, sadly, 72 - 95% of cyber incidents are linked to human error. This might be because of phishing attacks using weak passwords or this configuring systems. So my question is. How can organizations ensure end users follow the cybersecurity best practices and avoid risky behaviors that might help compromise Cloud IRP data?

Ryan: Well, it's pretty simple. It's security awareness training and I'll say it again. [00:14:00] Security awareness training. Yeah. Organizations can promote a cybersecurity awareness with their end users through these comprehensive training programs. Most of us here today and listening have been going through these for many years.

What I'll say is these programs have just come a long way to become interactive and aspects of gamification. That for me, and maybe I'm biased as a cybersecurity professional, but I no longer see 'em as gimmicky, but rather a platform for employees to walk through real life cyber attacks and examples that resonate. And one thing that I've seen with organizations that has just been a relief or a nice change of pace is that you have your corporate or your enterprise cybersecurity awareness, but then they've gone down another layer so that when [00:15:00] end users are requesting access to an ERP, like SAP they have training that is required before access is even given. They're having to go through a curriculum, and now the primary purpose of this training is so the end user knows how to perform a specific job function. But what I'm seeing is also that opportunity to embed specific ERP and SAP security awareness training to further enforce those enterprise principles, but now making it specific about what are the ramifications or consequences of sharing your SAP credentials or leaving your workstation unlocked as you walk to go to launch or something like that, and walking through these specific ERP examples I think is a, an amazing evolution of security awareness trainings is making it specific to these [00:16:00] applications.

Richard: You've already given some great examples of what I was going to ask next with the cybersecurity awareness training and embedding security and cybersecurity processes into the standard training of implementing a new system, and I know that at SAP we have lots and lots of classes that we're expected to attend on a regular and ongoing basis. But what security considerations and best practices should be prioritized both during the

implementation of a business system and the ongoing management of that system?

Ryan: Great question. Great question. Yes, so that this is going back to my comment about let's make this a conversation, not just about business transformation. Let's not make it just about SAP or any ERP. Let's make it a broader security and cybersecurity conversation, because [00:17:00] the security organizations and the CSOs that I work with over the years, they've built their wishlist of how they want things to work. It's just always been a matter of prioritization and budget constraints, where these large transformation programs are now that opportunity to bring in a interconnected security operations set of tooling and processes. And so the areas that we're focusing a lot with these organizations is, well, where are your big pain points? Be it from automation or audit findings, and let's address those as a part of these large implementations. And so what I'm seeing across all industries is that concerted effort to consolidate security operations and toolings to include the SAP landscape kind of, that leads us to [00:18:00] go through these exercises with our clients to come up with a solution, an approach to say, extend their existing identity solution to include the new ERP systems or to enable their security operations center their SOC in sim solutions to be alerted, triage and respond. SAP, security indicators of compromise. In the past, they had these processes and tooling in place, but SAPs was being managed in a silo. Separate processes, separate tooling. So seeing that consolidation has been incredible and a very fun exercise for myself and my team. The caveat I'll say to that is there's still a strong need for SAP Centric Security Solutions and Cybersecurity Solutions in most of these situations that properly address the [00:19:00] nuances of SAP S4 or the business technology platform, the SaaS applications. So it becomes a matter of leveraging existing enterprise solutions, SAP solutions and then SAP centric solutions from third party vendors to truly maximize an organization's transformation efforts, but also those day-to-day operations.

Richard: I would imagine it's also keeping up with the rate of change because these cybersecurity threats are evolving all of the time. The business systems are evolving all of the time, and there's always new threats on the horizon.

Ryan: Correct. And that's part of our strategy and approach with our services is certainly not looking at yesterday. We're considering what's going on today a little bit, but really our focus is tomorrow [00:20:00] and future proofing these solutions and processes.

Oyku: I have one follow up question. Can AI driven animal detection and real-time monitoring within ERP systems can help businesses also to create other business values rather than just from a cybersecurity perspective?

Ryan: Without a doubt because if you're obtaining optimization of your security operations using AI to more quickly and effectively detect, or those same resources being human capital being dollars, those can be reapplied to other value add in strategic initiatives. So it's not a matter of reducing your team, it's a matter of putting them in positions [00:21:00] of true value add revenue generating, or other areas of risk reduction that will only further protect the company's reputation protect them from financial damage and financial and regulatory, cumulative damages.

Richard: With that in mind, Ryan, most companies are part of other companies supply chains, and we usually find that the weakest link in a supply chain can affect other companies further up or downstream of that in that supply chain. So are companies promoting their cybersecurity when they're trying to win contracts with other companies, for example, to ensure the safety of data throughout a broader supply chain?

Ryan: Well, I wanna go back to some of the facts and figures, so that report the cost of a data breach. I was mentioning earlier [00:22:00] supply chain and third party vendors that was another big highlight here. First off, it was one of the most common attacks and one of the most costly, it was just under those insider malicious attacks.

Richard: Right.

Ryan: And so the way that is being addressed again across all industries is very elaborate third party risk management processes and procedures. And so, when we're looking at contracts and RFPs, those organizations are expecting and looking to IBM to provide evidence that we have appropriate cybersecurity policies, procedures, best practices, to give them that confidence that we will not be involved in a breach that would then directly or indirectly impact that organization. [00:23:00] We also do it on the flip side. If we're working with an organization, we expect that same sort of certifications, that same set of policies and procedures to provide that confidence that IBM will not be on the receiving end of a public or non-public incident.

Richard: Yeah, so you're only as strong as your weakest link.

Ryan: correct.

Oyku: So how can IBM help?

Ryan: Certainly well first off, in the SAP space, we are one of the largest sis and managed service providers of SAP. And the story I like to tell is. SAP was founded by former IBMers.

Richard: That's right.

Ryan: So the five founders there that they were with IBM, they were working on great projects and came up with the idea of a [00:24:00] of ERP and really with that, IBM was one of the first partners of SAP that goes back 50 plus years.

Richard: Yep.

Ryan: As a result we have over 38,000 SAP consultants. We have such a strong set of SAP security and cybersecurity SMEs around the globe. And so, where we can help is we're going to co-create and look at these security challenges collectively with our clients to come up with that right prioritization and improve their overall SAP security risk posture. And so the areas where we're helping is these large digital transformation. A lot in terms of providing a consistent model for threat and vulnerability management for SAP. [00:25:00] This is where the IBMers that I have the pleasure of working with every day are just continue to impress me with all of the client conversations and creating a set of best in class vulnerability and threat management solutions and processes to not just further protect our organizations, but also leveraging their existing investment and tooling to make this a real win-win for our clients. You think about that, like securing the organization while being very cost effective, quick to deliver. What more can organizations ask for?

Richard: Well, it did. It also enables them to focus on their core competencies. Their core competencies aren't necessarily cybersecurity. That's your core competence. They have other business drivers to that they should be focusing on.

Ryan: correct. Their definition of value add shifts.[00:26:00]

Richard: Yeah. Ryan, we're coming to the end of the podcast, and you've certainly given us a lot to think about here around the topic of cybersecurity and shared responsibilities. But I want to ask you the same question we ask all of our guests at the end of the podcast, and I'm assuming you'd give this response from the perspective of cybersecurity, but what is the future of ERP?

Ryan: Yeah. a loaded question. So, future of ERP from a security standpoint is gonna continue to evolve. And back in the day for ERP, we're focused on roles and authorizations and now we're talking cyber. Where it's gonna continue to go is going to be this conversation around artificial intelligence how can we use it to increase productivity, but also what are we doing to put the appropriate governance and secure AI? And then I'll give the audience a little bit [00:27:00] of a taste. The next thing we're gonna be talking a lot more about is my prediction is around quantum safe and quantum resiliency. What parts of the infrastructure and applications will need to be modernized to adapt and be prepared for the next age of crypto? Those are my two cents.

Richard: That's a whole other podcast. I think the whole concept of where quantum computing will take us and are we ready for it? And probably not at the moment, I'm guessing.

Ryan: Ready to have that conversation on a later date.

Richard: Well, we'll certainly invite you back to do that. Hey Ryan, thanks for a great conversation. It's been really interesting.

Ryan: Perfect. Thanks for having me.

Richard: No problem. And thanks everyone for listening. Please mark us as a favorite and you can get regular updates and information about future episodes. But until next time, from Ryan Oyku and I thank you for discussing the future of [00:28:00] ERP.