THE FUTURE OF ERP PODCAST

Staying One Step Ahead: Security Roles in Cloud ERP Threat Prevention with PWC

[00:00:01] **Stewart:** [00:00:00] Security in ERP can no longer be an afterthought. This is ultimately about protecting our critical assets based on the fact that we see ERP still being the backbone of an organization going forward. Think about security in a much more holistic and complete manner upfront, understanding all the various components. But secondly, understand where your most critical assets are as part of your organization, and what would most disrupt you. And finally, make sure that security has an equal footing in the conversation as we do around process, data, and control. Bring it forward, bring it into the conversation, and escalate it to the right level of seniority.

[00:00:39] **Richard:** Hello, 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 as ever, I'm joined by my wonderful co-host, Öykü.

[00:00:53] **Oyku:** Hello, everyone. I'm Oyku Ilgar, a marketer, blogger, and podcaster in the supply chain and ERP area at SAP. In [00:01:00] today's episode, we are joined by PwC's Stewart Light to discuss how to stay one step ahead when defining security roles in the cloud ERP threat prevention. Stewart, it's great to have you here with us today. So let's get started. Can you introduce yourself and tell us a little bit about your role at PwC?

[00:01:17] **Stewart:** So, hey, so Stu Light. So I'm a partner within our technology risk practice. I spent the last, call it over twenty years now, helping organizations think through kinds of security controls, in the face of those external risks, and what they need to do to make sure that, least privilege, make sure people are doing the right things according to their job role, and also that they're compliant with whatever the regulation they're working in. So I was very lucky, day one, joined, and somebody literally said, "Hey, know anything about SAP?" Of course, naturally, we don't. And I was then building security for an energy organization for two years. And then off the back of that, simply speaking, I now lead a team of people, of security control consultants and control consultants who help organizations really tackle these challenges.

[00:01:58] **Oyku:** ERP systems have come a [00:02:00] long way from being purely internal systems of record, right? They're now much more connected, dynamic, and they're more exposed. So how do you see the role of ERP evolving beyond that traditional definition?

[00:02:13] **Stewart:** You know what? It's a really interesting topic of conversation, I find at the moment. I was, I was literally on a call about sort of forty-five minutes ago around this, and I think you're right in the sense of where ERP has come from. So we talk about it being a system of record. My view is that when I first started out, and we are talking twenty-plus years ago, it was a financial system of record. It was just the general ledger. It wasn't really anything more, and we had multiple different ways that interacted with that. Nowadays, where we are is that we went through a phase where ERP was essentially wall-to-wall. So organizations were wall-to-wall SAP. They invested in it heavily, and SAP was doing everything for these organizations. And then there were peripheral systems around the edge. And what that means is that an organization has heavily invested in SAP technology to underpin their business, underpin those [00:03:00] ways of working. Where I think we'll get to, if I take-- I was speaking with a CEO the other day, and she said to me, she said, " SAP is going to be my system of choice going forward. It is that end-to-end system for me, but I don't ever want my people to ever type anything into SAP, again." What they're thinking about is that it will be, you know, either through voice or through sensor data or various other things. It's gonna be very much about that connected ecosystem around SAP that is gonna drive that data capture, that SAP will operate as that process engine, that data layer in the middle. And then that UI, which we see today through Fiori or other things, that UI will be through voice, or it will be through kind of speech, whatever it might be. That's the way she sees it. So if I think about what that means for the ERP itself, it means it still becomes the spine of the organization, connected through those cloud products. But I think the way we touch and use it will feel very different in five or 10 years' time. I think we will see [00:04:00] almost less of SAP visibly, but it will still retain that spine of the organization. And that has huge impacts, both in terms of how the business operates using and is enabled by SAP, but also what does that mean for things like security and controls? How do we ensure the integrity of those transactions flowing through the system, the information that comes out of it? And how do we ensure the right people are interacting with it? Bearing in mind, we're probably gonna have digital agents start to react with it and interact with it. So that for me is about what the vision is for how organizations are gonna use SAP going forward. How do we transition back and forward?

[00:04:35] **Richard:** I want to expand that even more as well, because it's not just how people will interact with the business system, with SAP, the SAPs of

the world moving forward, but there are all sorts of other things touching our ERP system, whether it's third party, partners. It could be supply chain partners, for example, but it could also be technology. AI is gonna play a huge role in [00:05:00] feeding information. Automated devices, the Internet of Things, is gonna be putting information into our business system. So what happens to traditional ERP security models when the users are no longer just human? How should organizations think about automation, AI agents, and the digital workforce of the future when we talk about security?

[00:05:19] **Stewart:** I think you're absolutely right to expand it. So if I sort of reflect back, you know, I spent a lot of my time in energy and utilities. And energy utilities in terms of the Internet of Things, that kind of sensor data, that's been around a long time in that space, so capturing data that then interacts and links into our ERPs. So that initial capture of data and push through, I've seen that for many, many years. We've seen automation try to come through, but now AI and interpretation of that data are really important. So you're right, you have multiple parties now interacting with the system in a very different way. And we have to think about that holistic security model, because if we simply think [00:06:00] about security in the traditional way, and I'm going back to ten, fifteen years ago, and when I used to build security. And as my team would say, we would trust you, Stu, to lead an engagement where we're doing security. I'm not entirely sure we trust you to go and configure and build the security anymore. I think it is quite fair. It's quite a fair piece. But the principles by which we need to think about security now have changed so much. We cannot think that the approach to security and how it's been in SAP is relevant from yesterday as it is now in the future. So for me, that's about let's look at kind of that whole, that holistic landscape. So, to your point, let's think about who is interacting with our system. And by who, we don't just mean the physical people. I mean, technology, the third parties, the devices, all of those kinds of aspects. You have numerous users, and we've got to be really careful about how we think about that user population and in terms of how they interact. Because even when we start to think about AI [00:07:00] and how that is interacting, do we mean native AI? So do we mean Joule and the agentic capability, or just kind of the Joule natural language? Do we mean non-native AI? So I was with an organization recently where we found it really nice and easy to post a financial transaction. An individual couldn't post that financial transaction. But guess what? Their non-native AI tool, which was set up as a communication account within the system, could post that financial transaction because it was clever enough to recognize how to do it. And obviously, it picked up the privileges of the communication user, not the user ID, back to the dialogue accounts. So we really need to holistically think about, firstly, when we're saying security, what population do we mean? So let's be really clear about that. Secondly, we need to think about where we are trying to protect. Where do we

focus our security efforts? Because, as we know, not all aspects of SAP are equal. So we've got to be really careful about, and I think this is where we connect it quite nicely [00:08:00] into an organization needs to think through what are my most critical assets across my organization. So by that I mean, what are the things that are most important to me as a business? If I think about that, then what are the processes that are critical to those most important things? What are the systems and the data that underpin that? And in understanding that, I can start to think about where I really need to focus my security efforts. So I think it's both that take a much more holistic approach, but matrix it with and where are the most important areas I need to focus on. And from that, you start to design a security strategy around SAP that considers both of those things, because we've got to be careful as well that whilst there are a lot more considerations, we do not over-engineer it. And we don't want to over-engineer it for a couple of reasons. Cost, I mean, let's be honest, we've all been there where there's been very, very costly SAP security programs. So how do we make it pragmatic and practical, but also suit the regulatory needs? [00:09:00] But also, if we over-engineer it, we constrain the business if we're not careful as well. So I'm working with one organization right now that has just said the answer is to segregate everything. Now, from a security purist point of view, great answer. I can also say to the regulator, "Hey, nobody can do the same activity, so everybody's reviewing everybody's work. It's all really good." But then the business says, "But realistically, to do that, I now need to double the size of my workload." And guess what? Digital agents aren't quite there so far. So not a practical answer. So I think that's where we're seeing holistic considerations in the most important areas, but knowing you have that complete view from the outset.

[00:09:38] **Richard:** Let's delve into that a little bit because you mentioned that ERP will always remain core to the enterprise because it's that foundational layer. It's the data that all of these businesses need, all of the tools that leverage the business system need. So what future-proof security principles should organizations be thinking about today with all of those [00:10:00] things that you've just talked about in mind, the automation, the different users, the new agents coming in and actually driving things, and that example of where the AI could post that transaction, but the human couldn't because that was probably a loophole that they took advantage of?

[00:10:16] **Stewart:** There are a number of kinds of constraining factors that you need to think about in terms of cost, regulation, operational efficiency, all of those things. I still start with the principle of least privilege. I still think that's a very sensible kind of principle to start with. Because by that, I mean that the agent, the model, the individual, the supply chain contractor, they should only be doing what they are expected and employed to do, whether that be as a third-

party contractor, whether that... Let's be clear, a digital agent will be part of the workforce. As a digital worker, you are employing that agent to do something, so therefore, the least privileged to still say they should only do what they are [00:11:00] required and have been contracted, have been employed to do. So we've got to think about digital workers in the same way we think about physical workers. So that principle for me about least privilege is really important. You then have to overlay, okay, how efficient and how pragmatic is that in the world we operate within? And it'll be really interesting to see what happens when we come around to things like quantum as well. You know, so how does a combination of quantum and some of these kinds of models, such as Mythos, and there are other ones out there, right? It's not the only one. We all know that, and we've seen some of the research papers around that. So how does that come together, and what [00:12:00] impact does that have upon the security models of today? And I was talking to some of my colleagues the other day about what the purpose of the ERP is. How might security look back on that differently in 10 years' time? So if we go back to what we said at the outset, at the start of this, it's the system of record, right? SAP should contain the information that we trust, which tells us how our business is performing and where we need to make adjustments to our business in order to get a greater outcome. That's ultimately why we look at what our ERP is: it's the thing that connects everything we do. Now, through today, through the traditional models, we have a transaction process through the system. It has checks and balances throughout the system, and we have security to ensure that the people who are trained in those areas are transacting those processes. So ultimately, we have integrity over those numbers. Basically, what we're saying is that the actions that are taken within it, what security does and what controls do, are they [00:13:00] validate those actions, and they make sure that we're doing it in a complete and accurate, valid manner with restricted access around it. So you then ask the question, is there a different way to validate on an ongoing basis the integrity of the information? Could I get to a point where I actually open security? Say, for example, I don't create segregation duties, I don't create least privilege because I have an alternative way that validates the integrity of that information flowing through the system, through some of the agentic AI models that are coming out nowadays. So there's also a whole bit about how security looks if we completely re-engineer the way the ERP operates. So what I mean by that is ERP will always be that outcome. As you've rightly said, it will always be the thing that ultimately drives the information we need as an organization to run and perform. But actually, if I can get comfortable with the integrity of that information in a different way [00:14:00] that doesn't require security, doesn't require controls, does that change my stance on security? And I think the answer to that is yes. But again, I'm talking 10 years' time before I think we get to that.

[00:14:14] **Oyku:** With all that in mind, I wonder what the security questions are that organizations aren't asking yet, but they should be about the future of cloud ERP?

[00:14:23] **Stewart:** I think a number of organizations are asking the right questions when it comes to identity management when looking at those cloud products, right? 'Cause I think in reality, what we're saying and I speak with CISOs, CTOs, CIOs all the time, and what we're looking at is we're going, we recognize we're in a different ecosystem today than we were previously. The stance 20 years ago would've been, "Okay, well, got my security role profile sorted in SAP, therefore big tick, security's good." That just is not fit for purpose today. And actually, if you look at the IAM solutions that are out there nowadays, they're taking a much more holistic approach to that cloud ecosystem. So actually, I need to [00:15:00] make sure and understand that the entire ecosystem is secure, both from an external and internal application perspective. I need to make sure that I'm creating least privilege across it. The one thing some of these solutions don't quite do is get to the depth and granularity that SAP does, and we all know that. We all know that building security in SAP is an art form. I would say that 'cause obviously.

[00:15:23] **Richard:** what, you do.

[00:15:23] **Stewart:** That's how I started, right? That's what I do, right? Of course, it's an art. It's more than a science, it's an a- art form, and I know a number of my colleagues would say the same thing, and a number of people no doubt listening would say the same thing. But what we've gotta look at, again, if you take that least privilege notion, I'm not just, what often identity management solutions do nowadays is to say, Stuart's got access to this product, to this product, to this product." What we're not quite doing is going down to that next level of saying, "What do the privileges within the product mean I can and can't do? And therefore, what do I need to restrict within the core S4 system?" So if we [00:16:00] go back again to the outset of this, what we're saying is S4 is our system of record. So all the transactions we operate within that ecosystem that we initiate either through a different cloud product, through an SAP cloud product, ultimately the end result flows through to SAP. That's the system of record. That's where it ends up. So we need to make sure that when we think about where those transactions and that information are being initiated or captured, how do we ensure that it can't be overridden and initiated in S4 itself? So, for example, a really good example of that was I knew one organization that was using a non-native purchasing system and effectively created this beautiful kind of purchase catalog, the purchase order, the requisitions. They've got these stunning workflows through it. They were

hugely, hugely proud of it. They were like, "This is leading edge." And it was. Don't deny that for one minute. It meant that in the way it was set up, you would buy the right goods based on the projects they were [00:17:00] doing. They would really push down the prices because of how they were negotiating. The catalog contained the approved supply base, all of that. Absolutely fabulous. Went through a workflow, and then ultimately that converted workflow went into an approved purchase order in SAP, which obviously, as we know, drives the goods receipt, invoice receipt, and the payment.

Brilliant. What they failed to realize is that when they went live, they gave two hundred and fifty people in the organization access to directly create purchase orders on SAP. And ultimately, as all humans are, and let's be clear, because this is also important for digital agents, as they try to find the easiest way to do things. Humans go, "What is the most efficient way to do my task? What is the most efficient way to get something done?" So these people were not, they're not people who are doing things erroneously. They weren't people who were doing something fraudulently. They just went, "The quickest way to get a purchase order, get my goods in to deliver the project that I am meant to do is just to create that purchase order directly on [00:18:00] SAP, because I don't have to deal with any of that nonsense in the other cloud product." And that effectively completely undermined this way of working. And I think the organization, when they finally discovered it, reckoned it had cost them the best part of twelve million pounds in inflated prices over the course of that quarter. And this is the bit we've got to really, really think about. It's not just about least privilege in SAP. It's thinking about it in this new world, in this more complex world, where do we initiate the capture of that information? Where do we initiate that process? And if we initiate it external to S/4, whether it be a native SAP cloud product or a non-native SAP cloud product, what does that mean then for how we build our security so that we retain the integrity of that transaction? And ultimately, that's what's really important, because we design these ways of working, and we all know organizations spend millions and millions, if not, as we know, some of the leading organizations as well, spending [00:19:00] billions on this stuff, right? In terms of designing new ways of working that are fit for the future, they should underpin their operating model. And then what essentially we do is go, "So we've done all that. It's brilliant. It's aligned with a wonderful benefits case. But what we're now gonna do is just give the keys to the kingdom to people, 'cause we don't build security in the most appropriate way, and we don't think about how that new ecosystem needs to be underpinned by the least privilege concept. So that for me is why I have to be asking those very tough questions and making sure the security build comes off the back of, we really understand our ways of working. We really understand the initiation of those transactions and how they flow through the various systems. And therefore, we really understand when we're thinking about

identity management and governance, what we need to monitor on an ongoing basis to make sure we simply do not give the keys to the kingdom, undermine the millions of pounds we've spent.

[00:19:54] **Oyku:** Can you share an example, like a real-world example of how a seemingly small [00:20:00] authorization gap in ERP can lead to real financial or competitive damage?

[00:20:04] **Stewart:** I've got many, but one of my favorite ones that always remains true was I was working with a service company into the energy industry, obviously will remain nameless because we definitely don't wanna share the stories. And it was through a whistleblowing policy that basically came out and said, when somebody left the organization, they said, "I'm not comfortable with the way we're dealing with our third-party shippers, because effectively, I think our third-party shippers are sharing information with each other, which therefore, what it means is the pricing that we're getting charged is at the higher end, that we've not created that competitive tension. I think it's all these people who are doing this." Now, it was a really interesting claim back into the organization, and they came to me at a certain point, and they said, "Stu, we've exhausted, like we- we're [00:21:00] comfortable with the integrity of our people. We don't think there are any issues. Like, what could it be? We know the authorizations have been built correctly in the SAP system, so that they're clearly restricted down to the relevant kind of shipper, so they can't see each other's information. Like, we just don't know what it can be. Could you do a full check for me?" And I was like, "Sure." So we did a full check. Beautifully designed roles for these third-party contractors. The authorizations are all in place, absolutely fantastic. And I was puzzled, if I'm really honest, at that point. I was like, "Well, what is going on? They've absolutely done it right." And I went, "Oh, do you know what? I'm just gonna make sure that the authorization is, check has actually been enabled in the system." And found that the underlying authorization check for shipping hadn't been enabled, and therefore, when they were validating their access, the reality was that they went, "Maybe I can just see what the other shipper's doing." They could because the authorization check [00:22:00] itself had not been enabled within the system. So as a result, they could literally see each other's commercial information. They could understand what the other was charging the other. And funnily enough, what the other organization simply did in this case is they went, let's put our pricing up." They worked out it'd cost them about 60 million quid in shipping costs because of the inflation over the period of time it had been available.

[00:22:25] **Richard:** So they weren't collaborating with each other. They just had access to each other's

[00:22:29] **Stewart:** They weren't collaborating with each other. They had to have access to each other's information simply because, although the organization felt they had designed segregated roles, they could not see each other's information. And we all know how hard that is to do in SAP. It is difficult because it's very complex, and obviously, you've got to get it down to an activity level, so it's really difficult. And then the reality is, having built this beautiful role design, they didn't switch on the authorization check, and it was really commercial.

[00:22:58] **Richard:** click or lack of one click [00:23:00] was...

[00:23:00] **Stewart:** lack of one click, lack of simply not transporting that change, and that's what it resulted in. And it was, not just a, it's the least privileged thing. It's about making sure that we protect against fraud. There are genuine commercial reasons. It's a great one where third parties can see each other. But, you know, and we know, supply chains are becoming more and more complex, and we know that we need more third parties interacting and engaging with us. You know, we talked about how those third-party products are all working and interacting now. We know it's, we're only gonna see more and more of this. So it's, and this is why we talk about it. It's really important to understand the ecosystem of people that are interacting with their systems, be they physical internal employees, be they contractors, be they digital agents, be they digital workers, be they third-party providers. There's all of that we need to think through properly, where we want them to operate, how they operate, and then how that fits into the security models we need to deploy.

[00:23:53] **Richard:** So let's move on and provide some advice. We've given some great examples of where things have gone wrong and how you've solved [00:24:00] those problems. But looking ahead, what are the key security considerations organizations need to start planning for now, even if it's not a problem today?

[00:24:10] **Stewart:** I think that's great. I lo- I love that, if it's not a problem

[00:24:12] **Richard:** Well, they're not aware of it as a problem

today.

[00:24:15] **Stewart:** Not aware of it as a problem today. Look, the reality is we've gotta look at what would threaten. So again, come back to what the purpose of the ERP is. The purpose of the ERP is to have that kind of integrity of information flowing through it that allows us to record what we do as an

organization, allows us to do our jobs efficiently, effectively, and ultimately give the information to the management board so they can make the right decisions to really drive performance in that organization. So we've gotta think about, so what threatens that? And what threatens that on the old models would be that people have too much access. You know, we all remember the days of SAPL. I dare say I still see some of it today in production environments, which always, always makes me nervous. But we've gotta think about the way that happens today in terms of making [00:25:00] sure that access is only restricted to those that need it and least privilege. I think that's really important, but we've gotta take that holistic approach. So we've gotta think about, number one, when we start any program, and I'm gonna use a transformation program as this illustration here, is that we've all worked in many, many SAP transformation programs. And we know the focus is on the business case. We've signed off on these significant benefits being done, and that ultimately these new ways of working, the automated ways of working by using native SAP functionality, clean core. I can throw all the buzzwords out there, right? But they're gonna save us millions and millions of pounds, and we're gonna see all these benefits, and we're gonna be the most wonderful, intelligent, driven organization in the world going forward. And so we do all of this, we build it, we test it, we do everything. And then, in the last minute, we go, "Oh, probably should do something on security, shouldn't we? Probably should, probably should do that." It cannot be an afterthought. I think what I've seen recently is actually more and more CISOs also realizing the [00:26:00] importance of application-level security, more so than previously. So, you know, the advice would be, as we start to get into these transformation programs, first of all, how do we get security and controls upfront in the agenda, so it's not an afterthought. So we are building it alongside those new ways of working. So for me, that means this is how we're gonna deliver these new ways of working. That needs to be underpinned firstly by good controls, and controls are the checks and balances we put in the system to make sure, as those processes flow through, that it's complete, it's accurate, and valid. And as we know, SAP has numerous flavors of configuration. So let's get that right and get rid of any back doors. But it's again been really clear that as we build processes, we're building controls alongside them. As we build processes and controls, we build security alongside them. Because what we do by bringing all of that upfront and not as an afterthought, we say, "How do we build sustainable resilience and secure processes from the outset?" And those to me are [00:27:00] absolute core principles we should be putting into any transformation program going forward. 'Cause if you build, let's say it's a billion-pound house, 'cause that's what we're doing, right? We're building this billion-pound house, and then we go, "But what we'll do is we'll leave the back door open, and we'll allow people to climb through the window and do what they want." There's gonna be problems there. And I think that's what we really need to think about, is like, let's put that at the

forefront. So bring security, bring controls right to the forefront of what we're doing, and make it as important. Help us realize that that stuff underpins and sustains those processes. So that's how we need to be thinking about the transformation. As we do so, come back to those principles about how we need to be thinking about it in a holistic way. It's not just about the SAP products. It's about this ecosystem that we're entering, this ecosystem of applications, of technology. So what does that mean for security from the outset? And, I can see multiple organizations, examples being Anapsis and Security Bridge as well, [00:28:00] bringing in their applications into the story as well. So, we can't just think about security in isolation. We've got to think about patching and various other things as well. So we've got to make sure that we're kind of building a complete solution here. So first and foremost, think about it upfront. Be clear about getting those foundations in place. And then when we design our processes, we're designing security and controls alongside that. When we're testing, everything is aligned with it. What we're not doing, for example, and I dread to think people do this nowadays, because I'm sure they don't, but we're not doing user acceptance testing with SAP All or, Oh, we'll just give them wider privileges to see how that happens because we just need to accelerate through UAT, and we'll do some security stuff at the end." Don't get me wrong, organizations have matured significantly from when I was doing this stuff 20 years ago. But the reality is, it's probably still not where it needs to be, and we really need to make sure that security forms a fundamental part of any transformation [00:29:00] program, such that very clearly we know that when we go live, those ways of working are absolutely underpinned by very, very robust and sustainable security mechanisms. And I think when we do those considerations, it's not just about, "Well, Stu's gonna have this access. We need to think about him." It's okay, so what agentic capability might we be delivering as part of this? What digital workers might we be using? What third parties might be interacting with our system going forward? And then thinking also about our support partners. I still see the old, our support partners, when we go live, post hypercare, they still need all this access in production because they need to be able to see what's going on. No, they don't. They're not gonna post a transaction. Why would they be posting a financial transaction? They don't need SAPle because they have to have it. It's actually, we've got to think about all of this. It's about protection. [00:30:00] And so for me, that's, the bit about bring it forward, think about it upfront. And for those who've already gone live with S/4 or are gonna stay on ECC 6.0 for a lot longer because of the extension of, you know, when they're going to extended support, let's kind of recognize we are in a different geopolitical world these days. Let's recognize that threat actors are becoming more intelligent and, therefore, applying this least privileged kind of principle now. Let's just try to review what level of risk we think we are carrying as an organization. It doesn't necessitate that we have to do a complete security and role redesign, but it says we might have to think about what our

risk posture is, and therefore what we might need to do differently as an organization, just as a result of that. So two very succinct pieces of advice off that long monologue would be number one, bring security and controls upfront in any transformation program, and make sure it has the right cadence and importance as part of this. And if you're not doing that, do a review to make sure you're clear on what, if any, [00:31:00] risk exposure you have today based on some of those principles.

[00:31:02] **Richard:** Great advice. Hey, Stuart, we're coming to the end of the podcast, and there's a question that we ask all of our guests, and I always find this the most challenging 'cause I'm trying to ask you to summarize what we've talked about in the last 30 minutes in two or three sentences. So, from a security perspective, what's the future of ERP?

Perfect summary. Thank you very much, and thanks for a great conversation. This has been really enlightening.

[00:31:29] **Stewart:** Fantastic. Thank you so much.

[00:31:31] **Richard:** And thanks everyone for listening. Please mark us as a favorite. You can get regular updates and information about future episodes. But until next time, from Stuart, Öykü, and me, thanks for discussing the future of ERP.