Who Owns IAM in Cloud ERP? Navigating Roles, Risks, and Responsibilities

Joe: [00:00:00] ERP has gone from a single system to running your entire HR, finance transformation, supply chain, vendor. So if we're talking about the future of ERP, it's an evolution of that, right? What is going to be the next piece in that ecosystem that we need to be viewing from a cybersecurity perspective and secure? And in my opinion, that's gonna be the AI components and looping that into ERP.

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 as ever, I'm joined by my wonderful co-host, Öykü.

Oyku: Hello, everyone. I'm Öykü Ilgar, a marketer, blogger, and podcaster in the supply chain and ERP area at SAP. Today, diving into one of the most critical and often misunderstood areas of cloud ERP: identity and access management. In this episode, we will unpack what IAM really means in the cloud [00:01:00] context, where organizations tend to struggle, and how to strike the right balance between security, ownership, and usability. And to do so, we are joined by EY's Joe Surmeier.
But before we get started, just a quick disclaimer. The views reflected in this podcast are the views of the speaker and do not necessarily reflect the views of the global EY organization or its member firms. That said, Joe, welcome to the Future of ERP. Could you please introduce yourself and your organization?

Joe: Richard, Oyku, it's great to meet both of you. My name's Joe Surmeier. I'm a senior manager at EY. I have been doing cyber for ERP for a little bit over a decade at this point in my career. And identity is one of the most exciting parts about ERP, especially when it comes to cybersecurity, so I'm super excited to have this conversation today.

Richard: So although you may have a decade in cybersecurity, many people listening may not as much experience. So maybe we can start with the basics, and maybe you can explain the role and importance of [00:02:00] identity and access management, and I'll be calling it IAM from now on. So identity and access management within a cloud-based ERP environment.

Joe: Absolutely. So identity access management, or IAM, is one of the best enablers that you can have from a cybersecurity component for a cloud ERP. Identity access management really focuses on who you are as a user, what authorizations you should have, so what data you should be able to access, and then how you govern that access. So IAM is really the facet of all three of those components, and when done right, you build an enabler for your users, you build a better user experience, and you build better compliance controls that allow for your organization to run more efficiently.

Oyku: As more companies move to the cloud, complexity tends to increase in new ways. So what makes IAM in cloud ERP [00:03:00] particularly complex compared to traditional on systems?

Joe: Yes. It's such a great question, and I'm gonna go back about 10 years. Ten years ago, we were all in the office, right? We were all from a singular location, so you knew who was accessing from where? Now, after COVID or post-COVID, we have really gone into a remote workplace, and that's been compounded by going to cloud ERP. So now we don't know where our users are working from, and we need to make sure that they have the access to the right information within an ERP, because the ERP is the brain of our organization. It is how we run our business. And so if we don't have the right access to the data and we don't have the right people being able to access that data, our operations stop. And that's where identity is the enabler. And I'm gonna keep saying that today, so stop me if you want to but, it's really important for us to change that terminology around.

Richard: It's funny, [00:04:00] my son works for SAP actually, and, he actually got kicked out of our systems yesterday, I spoke to him this morning. He still can't get back into the system, so that security and clearance becomes when you can't do your job. And given your experience working over the last decade with I'm sure lots of different companies of all shapes and sizes, you've likely seen how these challenges show up in practice. So what are some of the most frequent mistakes you see organizations make when setting up IAM responsibilities in a cloud ERP project?

Joe: I wanna dive into a slightly tangential topic of privileged access management. So one of the subcomponents of identity access management is privileged access management. PAM, similarly to IAM, is a core component of a cloud ERP environment. There are, for example, built-in administrator accounts that need to be controlled, locked down. [00:05:00] When we're talking about historical ERPs and then now we get to have a refresh by moving to a cloud ERP environment, locking down those administrator passwords, those administrator accounts, making sure that they have only the right people have access to those and only on a time-based rationale, like for an upgrade, for example. Those are some of the bigger changes that have really helped organizations move toward the future of cybersecurity. So to answer your question directly, one of the biggest mistakes that I see is the over-permissiveness of uh, administrator accounts, making sure that BASIS or our IT administrators of the cloud ERP systems, they usually request more access than they actually need. And being able to reduce that permissiveness is really the foundational concepts to be able to have a [00:06:00] secure environment And this is even more critical now with some of the releases of the new AI products that have been announced especially with some of those vulnerabilities that they're finding today. So that's part one, and I know that was very long-winded. Part two, to answer your question, is really going back to accountability. need to make sure that we are accountable for how our users are accessing the systems. Security is setting the policies, IT provisions access, and then those business approvers, those roles are done once and we move on, right? We don't refresh how those roles are looked at, and that goes back to SOX compliance, SODs, right? It all ties together. But if we're able to go back to the accountability and making sure that we have the right roles and we refresh those roles regularly, we're able to protect our data, [00:07:00] and we're able to provide the right level of access for all of our users, and all of our team members.

Richard: I have a follow on from that, because you said update. What guidance would you give to what regularly means? Is it different company by company, or should they be looking at it at least once a year?

Joe: I would say at least once a year is the best way to do it. The future of cloud ERP and identity in the space is really gonna be utilizing AI and automation to be able to help define those roles. So looking at Richard, you and your peers on your team, like, let's say that there's one peer on your team who doesn't ever access system X. If they don't ever access system X, do they really need to be able to have that role associated with them, or do they need to have a different business role associated with that user? And so if you're able to take into context [00:08:00] HR and the organization, then you're able to define the correct roles for each user, and it becomes a lot more granular, and it becomes easier for visibility and transparency.

Richard: Thank you. Nicely explained.

Oyku: You set the stage perfectly for my next question, mentioning often people tend to ask more permission or access than what they need, So there's always a bit of tension between the security and usability. Yes, one person shouldn't have too much power. Like, you just cannot let someone to create a vendor and approve the payments to that vendor, right? But if you split the roles too strictly, processes can become slow and frustrating for people. So my question is, how can companies design access control in ERP systems so they stay secure but still allow employees to work efficiently, especially when roles have to be carefully separated to prevent fraud or errors?

Joe: There's no great answer for that. And so what I've [00:09:00] seen a lot of organizations do especially going through a migration or a transformation is they want to set the permissions as open as possible, and with the intent to come back in the future and restrict those roles to only what the users need. What happens is that future restriction never comes into play. So those organizations open up all these roles, say that, "Okay, you can go do these 15 things because you are in finance," but you really only need to look at tax information, for example, right? If you have that over-permissiveness now, it is very hard post-transformation or post-migration to go back and look at that role and say, "Hey, what do they actually need to do?" And so it's a challenging concept from the fact that I would suggest or recommend that there's analysis done upfront. And [00:10:00] this is where it's really challenging from a business standpoint, because we don't wanna move slowly, but we wanna do things in the right manner and set the foundation in the right way. If we don't set the foundation, we are gonna have cracks in it, and then those cracks are gonna be evident later on. It may not be part of your SOX reviews or your financial reviews, but it may be in an incident. It's a really challenging concept, and I had a client actually, a few weeks ago. They had an incident within their ERP environment where their ERP environment's been stable for years. They had a developer request built-in administrator access within the cloud ERP. And so that user, they had access for the last year to that built-in administrator because he helped us close the ticket without removing those permissions. So I know we were talking about roles, but that [00:11:00] goes back to making sure that the roles are the right fit and they're monitored in the right manner. And each organization's going to have a different way of monitoring those roles, but it's really important to review them regularly, and to Richard's point, at least once a year. We wanna make sure that it's done at least once a year to be able to review

those roles and those user permissions.

Richard: That preparation and planning at the start of a project is always something that, opinion, is time well spent. Whether it's around the cybersecurity, whether it's around the business processes in general. Because as you say, once you've gone live, it's harder to retrofit things than you start. But because one of the things that we talk a lot about when we talk about cybersecurity in this podcast is the whole concept of shared responsibilities. Because there are multiple players that play a part when we get into the cloud. Whether it's the cloud provider, the ERP vendor, and of course using the system. [00:12:00] So under a shared responsibility model, where does the cloud providers' and ERP vendors' IAM responsibilities end, and where does the customer's responsibilities begin? You took a breath, then.

Joe: That's a really hard question In reality, it's organization dependent, it's cloud ERP dependent. But the rule of thumb for cloud ERPs is that the ERP platform provider is going to be managing the ERP systems and the infrastructure. And there is going to be a lack of administration at the application layer, which is going to be that organization's responsibility. But the shared responsibility model becomes even more complex for identity because we have cybersecurity, which would typically provide single [00:13:00] sign-on or provisioning, deprovisioning of users. You have an ERP security team, which is going to be providing those role definitions. They're typically going to do SOX compliance to some extent, and they're going to be the ones who are looking at the actual ERP systems. Then... That's within the organization. Then you have to have the handoff to the ERP provider And then typically in most organizations, you're gonna have a third party as well, right? An SI or a BI who's going to be involved.

Richard: Yep.

Joe: It's just so important to clearly define the roles and responsibilities of each of those teams, because I cannot tell you how many times I go into a client or an organization asks me if, like, should this be a cybersecurity role? Should this be an ERP security, or is this the ERP provider? So if you're looking at it from application layer, it's typically the organization. [00:14:00] If you're talking about the cloud infrastructure or databases, that is typically going to be the ERP provider. Hopefully that answers your question, Richard.

Richard: No, it does. Thank you. so looking ahead, seeing trends like adaptive authentication, password-less access, and AI-driven detection. And the first time we've mentioned AI in this podcast, so it's probably a bit of a record that we've gone 15 minutes without talking about AI. So how do you see IAM for ERP, I have trouble with acronyms, IAM for ERP evolving over the next few years?

Joe: It's conditional access approvals, it's authorization approvals. It's the ability to detect anomalous behavior quicker than we ever have before. And then within an ERP environment, there's typically AI [00:15:00] related to that ERP. So we have to even think about how are we going to handle those AI non-human identities. And that's where, from a cybersecurity perspective, that's really where we need to start focusing our time, energy, and effort. Because that's kind of the unknown, right? Do we treat them as service accounts or non-human identities, or do we try and focus and treat them as human identities because AI has the ability to make its

own decisions, make changes? And so we're at that crossroads of how do we handle this? And I don't think the verdict is out. I'm personally on the side of always being a little bit more secure. So I think handling AI non-human identities as human identities, having the same monitoring in place as you would for Joe, because AI can make its own decisions. And I read an article a few weeks ago about an executive who had AI delete her [00:16:00] entire mailbox, right? So if you have some of those scenarios where it can make its own decisions, like we need to start focusing on what the future is for protection, but then also how do we enable users? So in the same breath, going back to the conditional access authorization and really reducing the manual oversight that's required from managers is really important. We wanna make and empower our employees without just adding work for work sake.

Richard: I think AI is a double-edged sword as well, because we'll definitely be leveraging AI as a tool when we're talking about cybersecurity. But AI also brings many threats when it comes to cybersecurity both from a bias perspective, but also from a bad players trying to access your business [00:17:00] systems.

Joe: Yes, it's insane where AI is. I read an article yesterday. They used AI to entirely hack an organization. That was the first known attempt and successful attempt was back in November, and we are many months away from November at this point. There's been a lot of talk about the latest models, what they're able to do from an attacker's perspective, identifying vulnerabilities that we have identified as mediums or lows, which organizations have ignored for years. But the new AI models are better than the human security researchers, so they're able to tie together those medium and low vulnerabilities to be able to successfully attack and hack into organizations. So we are at the precipice of kind of a revolution within cybersecurity because it's always been a cat and mouse game, but the cat just got a lot bigger and [00:18:00] scarier.

Oyku: If you were to leave our listeners with some tangible advice on how to get started in moving their ERP to cloud today, what are the first three IAM priorities they should focus on identity-related risks?

Joe: Define the shared responsibility model upfront so that you understand exactly what needs to be done. That's first and foremost. Then second, work with the business and with your security teams to be able to clearly define what the access and authorization model should look like. Many organizations are going for a, quote-unquote, "lift and shift" from on-prem ERP to cloud ERP. The identity access model is implicitly changing, and we need to be able to talk about that. And then third really focus on how do we automate and operationalize the lifecycle governance from day [00:19:00] one. These are the foundational steps where you're able to show to the business from a cybersecurity perspective, we understand that you are the priority, and we want to enable your users, and we want to enable your managers and reduce their workload. And I think it's really important to have those conversations up front so that cybersecurity has a seat at the table. And I would just really focus on those three things, building the foundation, and then you can always build on the foundation later on.

Richard: Joe, I was gonna ask you how can EY help, but I think you've made that very clear in the last twenty minutes or so from th-the examples that you've given from the information that

you've shared, that EY can help companies in this environment. So I'll change my question to where could, where could a listener learn more about how EY can help?

Joe: I'll make sure, Richard and Oyku, have my email address in there as well, so please feel free to reach out to me [00:20:00] directly. I'm always happy to have a conversation, help however I can.

Richard: Okay, we have a final question that we ask all of our guests, and, I usually think it's the hardest question to answer because we want you to summarize everything we've talked about the last twenty-plus minutes in two or three sentences. So in a sentence or two, from a cybersecurity perspective, from an IAM perspective, what's the future of ERP?

Joe: ERP has gone from a single system to running your entire HR, finance transformation, supply chain, vendor. So if we're talking about the future of ERP, it's an evolution of that, right? What is going to be the next piece in that ecosystem that we need to be viewing from a cybersecurity perspective and secure. And in my opinion, that's gonna be the AI components and looping that into ERP.

Richard: Hey, Joe, thanks, thanks for this great conversation. I've certainly learned a lot. I [00:21:00] must admit I came in not knowing a lot, but I've learned a lot the IAM topic. So thanks for sharing your knowledge.

Joe: Yes, absolutely. Thank you guys for having me. It was a pleasure.

Richard: Great. And thanks everyone for listening. Please mark us as a favorite. You can get regular updates and information about future episodes. We'll also share the links that Joe provides in the show notes so that you can get more access to information about the topic and also about EY. But, until next time, from Joe, Oyku and I, thanks for discussing the future of ERP.

Oyku: The views reflected in this podcast are the views of the speaker and do not necessarily reflect the views of the global EY organization or its member firms.