Silent Cyber War

[00:00:00] **Asha:** If we start looking at it more as a crown jewel, we can make ERP less of a back office sort of enterprise, future-proof it by making it more identity native rather than focusing on role legacy.

[00:00:16] **Gabs:** From a security perspective, the future of ERP won't be just about preventing incidents. It's going to be primarily about being resilient by design. ERPs will be able to take a hit, recover fast, and so business can move on.

[00:00:34] **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. I'm Richard Howell, and I'm joined by my wonderful co-host Oyku.

[00:00:45] **Oyku:** Hello, everyone. I'm Oyku Ilgar, a marketer, blogger, and podcaster in the ERP and Supply Chain area at SAP. In this week's episode, we chat with Asha Vartak of Bayer and SAP's Gabriela Fiata, and together we will explore cybersecurity in [00:01:00] our hyperconnected world, diving into escalating cyber threats, often called the silent global war, and the key strategies for building resilience against them. Hi Asha. Hi Gabs. Pleasure to have you here today. Could you please introduce yourselves? Maybe we can start with you, Asha.

[00:01:15] **Asha:** Yes, hi, I am Asha Vartak. I work at Bayer, and I'm responsible for leading the cybersecurity in our whole ERP transformation. We are going from on-prem services to the cloud, RISE in S/4HANA, and I am responsible for leading through cybersecurity end-to-end for this transformation program.

[00:01:38] **Oyku:** Thank you. Gabs?

[00:01:39] **Gabs:** Hi again, everybody. Gabs, Gabriela Fiata, looking after the market strategy for SAP Cloud ERP private operations and support. Nice to be here again.

[00:01:52] **Oyku:** The world today runs on code from phones in our pockets, to the aircraft in the sky, to the infrastructure powering our [00:02:00] communities. Everything is connected and therefore vulnerable. Should we be afraid?

[00:02:05] **Gabs:** I don't think fear is the right reaction. I think that definitely awareness is. So we shouldn't be surprised if systems are vulnerable because they are. I think the real mistake is actually the opposite. One of pretending they're not. Because that's not a problem, that's actually part of our evolution. What definitely needs to be top of mind for. All of us are resilient in everything we do in business, like in everyday life. And resilience starts when we accept that failure is possible. And once we accept that, then we can stop chasing perfection, which applies to security as well. And we can actually start planning for fast recovery and business continuity. So it's a little less focused on, again, perfection. And a lot more focus [00:03:00] on resilience. That's my perspective. I dunno what you think, Asha.

[00:03:04] **Asha:** Yeah. My take on this is: fear? Absolutely no. Concern? Yes. And preparedness is essential. So we need to see cybersecurity from a risk perspective rather than a fear-based one. Yes, everything is connected. That's true. That's never going to go away. But in this, we have to make sure our cybersecurity is less about perfection, but more about moving, as Gabs said, resilience, recovery speed, how do we sort of contain if there is a breach? So, really talking about resilience, anti-fragility. So here I do agree a lot with Gabs, and we should start asking questions. Can we design systems that are more cyber incident survivable? Can it be limited? Can it be reversible? Treat cybersecurity less as just an it [00:04:00] risk, but more as an engineering and business risk. So if we start changing the way we think about it, we can be less about fear and more about preparedness. And of course, the concern never goes away.

[00:04:15] **Richard:** I love some of those examples of its awareness, not fear. It's about resilience, not perfection. Because I think we live in the real world, and we have to respond to things that happen in the real world. And Oyku, you mentioned a little earlier, this idea of the silent global war against cybersecurity. So in this environment, how should CIOs rethink ERP strategy and architectures to ensure that operational resilience that we talked about, against things like ransomware, data theft, and critical system outages?

[00:04:50] **Gabs:** That's a tricky one. Silent global war. okay. okay. I'll go first. Asha. So it's an interesting, um, question you're asking Richard. So, like definitely [00:05:00] living and operating in a world where disruption. It's almost the new normal. It is not exceptional anymore. We have seen a lot of high-profile attacks, and we have probably more attacks in the last couple of years than we have seen in the last 20 years. So it's definitely becoming kind of the new normal, and ERPs are a core part of any business that uses ERP. Because if you think about it, if your core business systems go down, you can

ship, you can bill, you can't pay, you can't comply. And all of that makes cyber resilience a board-level responsibility, a business responsibility. Asha was referring to that in the previous question. It is not just a technical problem anymore. And I think the question really needs to shift from can we prevent to actually, can we continue, can our business continue? And because again, every business really needs to assume that they will be breached. It's [00:06:00] gonna be a big mistake to think otherwise. So to recap, I think companies really need to start measuring themselves on how fast they can. Detect an attack, how well can they contain that incident, and how quickly can they recover? It's all about business continuity, really. And another thing I would say, nationally, I'll leave it to you to share your thoughts. I really believe that you know your customers, your regulators, and your partners. They won't measure you anymore on whether you were attacked or not. They will actually start to measure you on how prepared you were and how transparent you were in responding to an attack. This is what we really count on. I don't know what you think, Asha.

[00:06:50] **Asha:** From my perspective, we should always go with the attitude of we assume a breach, right? And design for resilience. [00:07:00] So going back to the previous question, we should always have in mind that we design for resilience and also accept, and this is what modern security strategy also accepts that no perimeter, if at all, a parameter exists is not perfect, right? Some controls will fail, and we have to accept it. What we can focus on is early detection, containment, and recovery speed. So, success in this scenario is like limited impact and fast restoration. So our strategy should be such that. We should not think about a single event that stops the total business operation, but talk more about what is tolerable. What is the business tolerance? And this is why I always say we have to engage the business upfront, and when we are talking of resilience, we should also make sure that it should be treated as a mission-critical system, ERP, [00:08:00] not an IT back office system. Mission critical, but, and how we survive if there is an attack, if there is a disruption, what we can still have a partial operation going on while we recover, so we have to plan. Change our mindset more into recovery, what we can restore quicker in a very resilient environment, and always engage the business and have the business tolerance in mind, and not about if you're working with third-party promises.

[00:08:37] **Oyku:** And AI premises us to make ERP systems smarter and more autonomous, right? But it's also giving cyber criminals new tools like automation and deepfake-driven attacks. So how can CIOs use AI to boost ERP security without opening up more vulnerabilities?

[00:08:54] **Asha:** I think AI strengthens ERP security [00:09:00], and we should ensure that we use AI more in an observance mode rather than act or execute in a way that we can use AI to translate technical risks to financial exposure. We can also use AI, where we can avoid this control sprawl. We tend to create controls over controls, over controls. At some point, we don't even know which control works or which contradicts the other. So then you are working on an exception rule. So you have more exceptions than necessary. So these are the areas where I feel we can really leverage AI, where we are more using it to simplify rather than multiply. As an example, we can use AI, maybe to reduce access rather than expand access, but we can have AI outside the ERP core, and we have certain principles that we operate on. Zero trust. So there are [00:10:00] ways to use AI, but more from an observation standpoint, more from using that information and translating into business risk rather than using executing AI in lot of other controls and so on. Until we get more familiar with AI, we can mature it more. So that's the way I like to see AI currently.

[00:10:25] **Gabs:** Mm-hmm. This part is about using AI for. Let's call it quantifying cyber is actually a very interesting perspective because when Oyku asked this question, the first thing that my mind went to was, how AI can, and it's actually already being used by many security teams to spot abnormal behaviors, even in ERP systems, of course, faster than any person ever called. It's something that companies are [00:11:00] already using. But I think where we are going, when it comes to using AI for security, it's actually what you were referring to. It's how. AI can actually support organizations and business leaders to suggest where the security budget should be spent. And you are making some very good examples, and I agree with that. If you give AI the right data, it can suggest what risks will impact the strategic business objectives of the company. It could then suggest what the mitigating factors are. Efforts and controls that the company should allocate costs and resources to. But I also know that the devil is in the details. So it will take a while. And sometimes to actually calibrate, AI from a security and risk management perspective, where we need security and risk management experts to ensure that the output [00:12:00] that is provided by AI, it's reliable and can really be trusted and used by business leaders to make decisions on security. I still see the expertise of security people and risk management people key to calibrate this, let's call it an AI engine, until you can really produce results that are meaningful for business leaders, because it's not. That’s easy, right? To really understand where I put my budget? What do you think?

[00:12:29] **Asha:** I think we should use AI more, and this is our opportunity. I also think there's more of an opportunity to enhance the trust. Where we can use AI to increase the explainability of why we are doing cybersecurity in a certain way, we can leverage AI for that. Also, when we are using automation, we can

leverage AI in automation without accountability. No, that doesn't work. But while we are using [00:13:00] automation, we can also increase accountability. So, there are areas where the cyber folks can leverage AI. You still need cybersecurity experts, but these are the areas I think we can leverage AI for our benefit in ensuring the business risks are better explained. We can use it to observe our risks, to translate the risks, and so on.

[00:13:26] **Gabs:** I agree. And also, now that you were talking about this, the second part of your question was also about how CIOs can use AI without increasing risk, which is also a very interesting question because you put AI and you plug AI everywhere without control. Then, now you have a problem because AI agents are like privileged users. You might agree on this, Asha. When you provide AI with the authorization to perform in the system, whatever they need to perform to solve critical situations, then they're like a [00:14:00] privileged user, and like a privileged user, you need to train the user. You need to monitor the user. Otherwise, it just becomes another attack surface for the company, actually an internal attack surface. So it's definitely very important to monitor AI with AI.

[00:14:17] **Asha:** Basically, thinking we can use AI to prioritize the real relevant business impacting risk. And also, we can leverage it to translate the technical risk into a financial exposure. And sometimes we have fatigue with a lot of controls, a lot of alerts, and we can use AI to reduce what I call the alert fatigue. And we can also use it to perhaps collapse some rules, because at one point, we'll have too many rules. But perhaps we can use AI to be much more efficient with these rules and really translate that into real risk signals for business exposure.

[00:14:56] **Richard:** I want to move on to another subject because that whole topic [00:15:00] of reliability and trust. Makes me think about the other rules and regulations that we are mandated to follow and where cybersecurity comes in. Because companies like Bayer have ERP systems that span multiple geographies and jurisdictions, and those different regions have conflicting data protection laws. So in a world where digital sovereignty is becoming a geopolitical issue, how can CIOs ensure compliance and secure cross-border data flows at all times? Because you must be facing this every day at Bayer.

[00:15:36] **Asha:** Good question. I mean, this is a real challenge now. And this is where we are shifting now, from the silo, how we worked in the past, right? So when you talk about cross-border jurisdiction, so on, we always said that was a legal topic, and then we had a privacy topic, but obviously, that's not the case anymore nowadays. [00:16:00] So we need to really move from, is this a

legal topic? Really, from a data standpoint, where does this data live? Where does it move, how it gets processed, and then how we design sound and architecture. So here architecture comes in play. How do we design a robust architecture that takes all this into consideration? So when I say robust, it's really aware of the jurisdictional needs, the localization needs, and builds your ERP architecture according to that. Taking this into consideration, and its two parts, right? It's governance and architecture. And that's again, a change of mindset. Moreover, it's a legal topic. It's not relevant for it, but really, it's not about it. Again, we are talking ERP as a business platform; business backbone data is important. And can we build systems that take this into consideration [00:17:00] upfront? Think about data sovereignty rather than a privacy checklist. Maybe we should also think about classifying data upfront and building it into the system so that it's enforceable by default, rather than start coming up with a list of exceptions for certain things, because then you lose sight of the exceptions as well, and make it more of a by default system taking these data sovereignty into consideration. And also at the same time, make the system more federated, not centralized. And if we are working with a lot of third parties, also make sure that our contracts, many times we forget about it, but these contracts also reflect this, rather than focusing on only the technical part of the contract. Gabs, I'm looking forward to hearing your thoughts.

[00:17:53] **Gabs:** I like the idea of the preventative classifications of data. You know, you're almost giving me an idea [00:18:00] to build an app around that. So, with AI nowadays, we were discussing AI a minute ago. It's not too far from reality, right? To have an immediate classification and an automated classification of data. That will definitely make our lives much easier. The topic of digital serenity and sovereign cloud is becoming for sure one of the CIO's toughest choices to make, or let's call it the balancing act. But it's also, I think, a great opportunity they have to enhance trust for their company. And as you said, some companies will have to get away from the centralized global setup way of structuring ERP infrastructures and architectures, as it has been done for many, many years. That doesn't mean that centralization is not important anymore. Of course, it's important. Global policies are important, but maybe it's gonna be more difficult to have [00:19:00] that one-size-fits-all approach. However, the good news is that there are definitely ways where centralization is still possible, and then there are ways to keep global standards or to localize, let's say, global standards where it makes sense where processes require those localizations, where there are specific security principles and where there are local laws or local controls that needs to be implemented, because sovereignity, requires it. That means you can know exactly where your data is. ERP will allow you to do that. You can see in the ERP environment who can access what information from where, and you can segregate that based on which jurisdiction and in which country you want to do that. So there are ways, of course, of doing it.

And I think again, a positive for [00:20:00] CIOs is that ERP platforms nowadays and cloud ERP platforms allow customers to choose where they want to deploy. A company wants to deploy the ERP on a hyperscaler, on a public cloud, on a private cloud, on a sovereign cloud, or on a private data center. So there are lots of options for CIOs to choose from when it comes to a deployment choice and to choose how they want to organize. Especially multinational companies, how they want to organize their processes so that they can still run centrally for simplicity, but they can still apply local controls to countries that need sovereignty. So, just to close this, we shouldn't really see sovereignty as a compliance tax because if you actually do sovereignty right, it can actually improve resilience and trust for your company. And I believe that going forward. It could [00:21:00] become a strong differentiator. Companies that can do this better will have an edge against competitors.

[00:21:06] **Asha:** We start building our enterprises, taking this data architecture, data sovereignty into consideration, so that this is part of the build, right? Rather than after you build the system, you are going. Checking with the privacy and other colleagues to ask them, " Hey, give us a checklist, and then you are trying to fill the gap. And that's where it becomes very complex. So if we start building with a data architecture mindset, I believe this is not the only way, but at least one of the good ways to be prepared for these new laws that keep popping up. And all the geopolitical issues that make us focus on digital sovereignty. And this is really a challenge for a global company that is operating in so many countries.

[00:21:59] **Oyku:** Great [00:22:00] answer. I was going to ask another question related to digital trust, but I think you have already answered that. But I'm just going to ask it in case you have anything else. Because Gabs, in one of our previous episodes, you said something that really stayed with me. Now I cannot stop bringing it up in every conversation. You said trust is the new currency, and cyber attacks can now hurt not just revenue, but trust among customers, employees, and partners. So how can CIOs position ERP as a core enabler of digital trust, and of course, also transparency and governance within their organizations?

[00:22:36] **Gabs:** Great question. And I'm, uh, happy that that resonated with you. So, yes, ERP has always been the source of truth. If you think about it for companies, ERP is where companies produce their financial annual reports, where they store customer data, bank information, personal data, and more. So there's always [00:23:00] been a. Big trust in ERP systems to secure data. Ensure this data is reliable. It can be audited by auditors. And this will just continue. But, and I'm sorry to say that now, it'll be just under a lot more stress

and pressure as cyber attacks are more frequent and more sophisticated with the usage of AI. But I trust ERP will still provide what companies need to keep their business running, which is ensuring they have clear audit trails. There is real-time visibility, and there is controlled access. And ERPI, I really see ERP still being the foundation for trust for companies. Not just internally within their organization, but also with the partners, regulators, and, of course, their customers. I dunno actually, what perspective you have on this [00:24:00] one.

[00:24:00] **Asha:** I think trust is the foundation, but along with trust comes great accountability also. And then we need to have transparency to it, and you slightly alluded to it, but it's also about traceability, right? So you want to, when you have transparency, you have to have traceability, all with these audits. If there is a breach, what is the traceability of it? So, definitely, if our mission is to make ERP the core enabler, then it should also be the single source of truth. Position it that way with accountability. And I really like that trust is the new currency. We can also make ERP the enterprise truth. If you have this accountability, traceability, you can make this the enterprise truth and embed the governance into the [00:25:00] processes, you know, not just like a list of controls, just embed it into it. And we spoke about AI. I would also say to leverage AI to explain the risks with transparency and accountability. We need to be more articulate about the risk, and when you articulate the risks, you are also not obscuring the accountability that comes with it. So, AI can be leveraged to enhance trust because it also increases the explainability of why we are doing a certain thing. So I would really like to see AI as an enterprise trust platform, if you will.

[00:25:38] **Gabs:** Yeah, absolutely. And um, especially because the data is there, right? Asha, so ERP is where the data is. Everything we need in the ERP system to really leverage AI to suggest next steps, suggest what to do, and even provide more visibility than what we have now.

[00:25:57] **Richard:** You are setting me up perfectly for the [00:26:00] last question that we ask, and I'm going to go to that question now because we've discussed lots of things in this half hour. We've discussed the importance of having resilience, and something was going through my head when we were talking about that. It's not that you get knocked down, it's how you get up and respond. I think that summarizes resilience in my mind. We talked a lot about AI, the role of AI, both as a threat and as an enabler of cybersecurity. But now the hardest question is, because I want you to summarize everything that we've talked about into a few sentences. So in a sentence or two, from a cybersecurity perspective, what's the future of ERP? You've done this a few times before, so maybe you'd like to go first.

[00:26:45] **Gabs:** Yes. I almost need to think about what I say that's new from the, but actually this.

[00:26:51] **Richard:** Consistency is is good as well though!

[00:26:53] **Gabs:** Yes, true. And, I have to say this episode gave me some food for thought. So. From a security [00:27:00] perspective, the future of ERP won't be just about preventing incidents. It's going to be primarily about being resilient by design, and what I mean by that is that ERPs will be able to take a hit, recover fast, and so business can move on. Attacks might happen, but operations won't stop, and security will be maintained. It's not measured by the absence of incidents, but by how well and fast business can recover and keep operating.

[00:27:34] **Richard:** Asha, your perspective on the future of ERP?

[00:27:36] **Asha:** I would position ERP as a crown jewel. If we start looking at it more as a crown jewel, we can make ERP less of a back-office sort of enterprise, future-proof it by making ERP more identity native rather than focusing on role legacy. And also, we need [00:28:00] to start thinking about architecting jurisdictional resilience. If there is a breach, how do we cover quickly and make it also designed for resilience, as Gabs said, and just not keep it as an audit dependency, we wait for an audit after 10, 12 months, and then we start trying to mitigate it. I really feel this is more about building our secure controls, secure by design, data requirements right from the start, and of course, ERP as a core business enabler.

[00:28:31] **Richard:** Great answers. Asha Gabs, thanks for a great conversation. This has been really eye-opening for me.

[00:28:37] **Asha:** Thank you.

[00:28:38] **Richard:** You are welcome, 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 Asha Gabs, Oyku, and me, thanks for discussing the future of ERP.