The Future of Supply Chain

Cybersecurity Talks: From Complexity to Confidence with Private Cloud ERP

[00:00:01] **Gabriele:** [00:00:00] Supply chains are getting faster, more connected, and more complex, and that means more doors for attackers to work through. So today, ERP systems need security at their core. It cannot be added later as a tool or as a plugin. And I'm talking embedded, real-time threat detection, AI that spots weird behaviors before they become a breach, and most importantly, a mindset shift from trusting everything inside the network to the concept of trusting no one and always verifying. And at the end of the day, a secure ERP means a resilient supply chain. And in today's world, resilience is the competitive edge.

[00:00:51] **Richard:** Hello, my name's Richard Howells, and this is the future of ERP, a podcast where we discuss hot topics, best practices, [00:01:00] and the latest innovations in today's global business. And I'm joined by my co-host Oyku.

[00:01:05] **Oyku:** Hello, everyone. I'm Oyku Ilgar marketer, blogger, and podcaster in the ERP and Supply Chain area at SAP. Today, we're going to be discussing the IDC business value paper on cybersecurity with SAP's Gabriela Fiata. Gabs, welcome back. For those of our listeners who do not know you, would you like to introduce yourself?

[00:01:22] **Gabriele:** Yes, thank you. And hi, everyone. Great to be here again. I'm, uh, Gabrielle Fiata, and, uh, most people call me Gabs. I work for SAP and I focus on ERP strategy for cloud and, uh, cybersecurity.

[00:01:35] **Richard:** So Gabs in, in the past decade or so, we've seen some big changes in how companies think about protecting their systems. So with that in mind, what's driving organizations to take security and resiliency more seriously these days, and what has changed over the last few years?

[00:01:51] **Gabriele:** Honestly, it's the reality check from all the high-profile hacks and outages we have seen recently, and 00:02:00] we have seen those in the news. If you think 10 years ago, cybersecurity was an IT checkbox, and today it's on the CEO's agenda because a security issue doesn't just eat your systems, it eats your brand, your customers, your bottom line, and in worst cases, it impacts entire communities and even people's lives. And with editing

accelerating from. Digital apps to global supply chains. Businesses are realizing that resilience is an option, and if you're not resilient, you are vulnerable.

[00:02:39] **Oyku:** So when it comes to moving from on-prem to cloud ERP, what are some of the biggest cybersecurity headaches or biggest security headaches that companies are hoping to leave behind?

[00:02:51] **Gabriele:** Yes. So the biggest one for me is the weight of doing everything alone. For many, many years [00:03:00] on-premise meant that customers were responsible for everything from installing touches to configuring security to handling threats at 3:00 AM in the morning, and with cloud ERP. A lot of that heavy lifting has shifted to experts who do this full time, and for me, it's not just about outsourcing the work; it's primarily about upgrading the way that customers protect the business and when they collaborate with trusted experts who provide different perspectives and views on things and on security. Then, uh, that's a successful, um, collaboration between the customer, the vendors, and the cloud providers. There was actually a recent study done by IDC where they interviewed customers who are using SAP cloud ERP private. [00:04:00] There were some really interesting, uh, results that came out. Amongst all the findings, the one that really caught my attention was that companies reported getting an average of $8.9 million in value each year from security services included in SAP Cloud ERP Private. And this number comes from the quantification that IDC has done on things like spending less time on repetitive work, getting security updates faster, spotting threats more quickly, and reducing the overall business risk. You'll actually find the link to the full report in the episode notes, so I highly recommend that listeners check it out because it's a great read.

[00:04:53] **Richard:** We're seeing increases in cyber attacks, or at least they're in the news more now than ever. [00:05:00] And compared to last year, there's been a 25% increase in cyber attacks, to supply chain. So, how can companies protect themselves against this? What can happen if something goes wrong?

[00:05:11] **Gabriele:** And just to clarify this for our security audience, your question is about the business supply chain rather than the security supply chain, which is a different, different thing, which is another concept you're, yeah. Okay. So you're really asking me about the cyber attacks on the business supply chain, which is moving goods from location to location, from vendors to customers.

[00:05:36] **Richard:** Yes, and the importance of having that visibility across a business network, for example, because a security breach could happen with a supplier or a supplier's supplier that could still become a security risk for you.

[00:05:47] **Gabriele:** Yeah. So the risk is definitely rising. If your supply chain gets hit, your business stops. And, to protect against that, companies need to think [00:06:00] beyond the traditional firewalls and access restrictions. They need a security strategy that includes constant monitoring, regular updates, and clear responsibility across all partners involved. And contributing to the overall security of the business on exactly who does what. The worst case is that customers can lose customers' trust, they can lose data, and data can be sold on the dark web. They can lose revenue. I mean, there are many worse cases and catastrophic results that can result from that. But I always like to finish on a positive note. So there's also best best-case scenario if you are prepared, which is that you can build long-term resilience and protection for your business.

[00:06:53] **Oyku:** Gabs, you mentioned earlier that companies do not really need to do everything alone. So, um, this shared [00:07:00] responsibility or shared fate model in cloud security is getting a lot of attention. Can you break down what this means for companies and how it changes their responsibilities?

[00:07:09] **Gabriele:** Yeah, sure. Imagine rowing a boat. So the customer holds one paddle. SAP holds another one, and our partners hold another one too. So we're basically all rowing together, towards the same objective, the same goal. Now, customers still have responsibilities like who gets access to what business activity, um, in their business applications. But SAP and partners, we take care of the infrastructure, the updates, and a lot of the hard security work. So it's a partnership, and it means that customers are not alone anymore. They can actually collaborate with experts from SAP or from our partners, who share the same goal and the same objective as them.

[00:07:58] **Richard:** In this podcast, [00:08:00] we talk about digital transformation almost every episode. And digital transformation is really happening. It's more than just a buzzword. But if it's done not done securely, it comes with real risk to your business as well. So, how do you see companies balancing this push for innovation with the need to keep their data and operations secure at all times?

[00:08:21] **Gabriele:** Yes, I see it a bit like building a new house or renovating a house. So you want big windows, you want smart features, but you also want solid blocks, security, and you want an alarm system. And you can have all of this, actually, you should absolutely expect all of this when you build a house or

you renovate the house, and the same applies to ERP systems. Companies are realizing that they don't have to choose between speed and safety anymore. With the right setup and the right partner, and the right vendor, they can innovate and stay secure. And it's all about smart planning, [00:09:00] ensuring that security is brought in at the design phase and not later. And also in the cloud, like we mentioned before, understand who does what within the shared responsibility model.

[00:09:13] **Oyku:** And I can imagine culture plays a big part in tech shift. So, implementing an ERP Cloud requires more than just implementing a technology, but also a human component. What changes have you seen in company culture or mindset as organizations embrace cloud ERP for both security and business continuity?

[00:09:33] **Gabriele:** Yes. So the biggest change I've seen is trust. So companies are learning to trust the cloud and their people. And if you look at the IDC research, it actually serves as a solid confirmation of this. There is also a stronger focus on training because, let's be honest, the weakest link in security isn't the tech. It's usually human. It's us, [00:10:00] it's people. But rather than seeing this as a weakness, I like to see this as an opportunity. I always like to say that people are the greatest asset of any organization, so giving them the right security training is key because when people know what to look out for, they can contribute to security, and they can be a strong line of defense. So culture really, really matters. And like I said before, security isn't just an IT issue anymore. It's something everyone needs to care about.

[00:10:32] **Richard:** We've talked about the fact that you need trust in the system. The people need to be trained. We're also seeing new technologies coming into play all the time, and we usually can't go this far into the podcast without mentioning AI, for example, agentic AI. So, looking ahead, what trends or technologies do you think will have the biggest impact on how companies approach security and resiliency in the [00:11:00] ERP and supply chain systems?

[00:11:01] **Gabriele:** Yeah, so AI or agentic AI, as you mentioned, they're going to be huge, not just for catching threats faster, but for helping teams figure out which ones actually matter. There is so much noise in cybersecurity, and AI can really help. To focus on the real dangers instead of looking at millions of false positives. And also at SAP, for example, we are focusing a lot on automation for recovery and response, which means that companies can bounce back quickly when something goes um wrong within their systems.

[00:11:41] **Richard:** do you think they'll be able to sense or identify security risks quicker or before they happen, even?

[00:11:48] **Gabriele:** I will, um, go as far as saying that they already do that. They are the speed that AI can use to [00:12:00] identify potential breaches before any human can. It's incredible. There is still a bit of tuning to be done to ensure that, especially when we ask AI to take an action. You were talking about agentic AI. So, especially when we ask agent AI to take an action and make an important decision, that could be, for example, stopping a payment, or stopping a business process. We still need to ensure that we are not blocking the business if that's a critical business process step. But I don't think we are too far from having, uh, agentic AI really making important decisions, and really being able to stop the attack that second before is too late.

[00:12:49] **Richard:** On the other side, though, we can also see the attackers, the hackers, leveraging AI to be more sophisticated in how they attack businesses moving [00:13:00] forward.

[00:13:01] **Gabriele:** And they already are. Yes, they already are very sophisticated. And defense, it has always been a common scenario in security. Defense has always adapted to the sophistication of attacks. And maybe for the first time in history, we're actually seeing defense trying to take the lead and be proactive in addressing the cyber trust that will be powered by AI in the future, and trying to predict those so that we can defend them before they're actually made in operations.

[00:13:40] **Oyku:** Perfect. And finally, if you had to summarize in a sentence or two from a business process cybersecurity perspective, what is the future of the supply chain?

[00:13:49] **Gabriele:** Supply chains are getting faster, more connected, and more complex, and that means more doors for attackers to work through. So today, ERP systems [00:14:00] need security at their core. It cannot be added later as a tool or as a plugin. And I'm talking embedded, real time threat detection, AI that spots weird behaviors before they become a breach, and most importantly, a mindset shift from trusting everything inside the network to the concept of trusting no one and always verifying. And at the end of the day, a secure ERP means a resilient supply chain. And in today's world, resilience is the competitive edge.

[00:14:41] **Richard:** Great summary. Thanks very much. Gabs, as ever, thanks for a great conversation.

[00:14:46] **Gabriele:** Thank you.

[00:14:46] **Richard:** And thanks, everyone, for listening. Please mark us as a favorite. You can get regular updates and information about future episodes. Also, check out the show notes to download the IDC White Paper. But until next [00:15:00] time, from Gabs, Oyku, and I, thanks for discussing the future of the supply chain.