Capgemini

CRLIVE 20

AWS re:Invent 2023 Guardians and future of trusted cloud with Max Peterson and Gary Meshell, AWS and Anne Saunders, Capgemini

CRLIVE 20

AWS re:Invent 2023 Guardians and future of trusted cloud with Max Peterson and Gary Meshell, AWS and Anne Saunders, Capgemini

Disclaimer: Please be aware that this transcript from the Cloud Realities podcast has been automatically generated, so errors may occur.

[00:00:00] Do you know any Queen songs? Maybe we could do a quick Queen song? I love Queen. Can we do that? We'll add Lib, let's go.

Welcome to Cloud Realities, a conversation show exploring the practical and exciting alternate realities that can be unleashed through cloud driven transformation. I'm David Chapman. I'm Sjoukje Zaal, and I'm Rob Kernahan.

And we're in Vegas still. And I'm delighted to say we're doing another double feature today. We're going to be looking at two areas of very significant importance, not only to re:Invent and AWS and what they're talking about, but actually Generally in the world of cloud and in the world of digital generally, so we're going to look at Sovereign Cloud, talk about that, talk about regulation, talk about AWS [00:01:00] response.

And we're going to talk, later on this afternoon, we're going to talk about cyber and we're going to pull those two things together into a single episode and see if we've got any thread. Gary Meshell, the Global GSI Cyber Security is going to join us later on today. But I'm delighted to say to kick off the day's festivities, we have Max Peterson, the VP of Sovereign Cloud in AWS joining us.

Max, welcome to the show. Hey Dave, thanks very much. Looking forward to an exciting conversation. It's a great capstone opportunity here at the end of re:Invent. We're delighted you could make the time. Why don't you tell everybody a little bit about your day job? How did you get involved in Sovereign Cloud?

And what does every day look like? Talking to customers about such a, not only a critically important subject, but one that's growing in importance, I think. It's been a journey, like so many things, right? For the for the past nearly a dozen years, I've been involved leading our AWS worldwide public sector business.

Working with governments, working with educational institutions, [00:02:00] national healthcare, aerospace and satellite companies, all in very complex regulated environments. And the one thing that we've seen over the last two years, Was the discussion with customers about how they maintain control and digital sovereignty over their operations in the cloud just kept getting bigger.

So it was super exciting that I could make the leap now to vice president of sovereign cloud. Where I get to spend all of my time helping customers and our partners figure out how we drive solutions forward in this in this next phase, frankly, of the cloud transformation journey for so many customers.

Fantastic. I'm very much looking forward to digging into that in a second. But of course, with me, I've got Rob and Sjoukje here. Sjoukje, how's day three in re:Invent for you? It's Sjoukje's first re:Invent. It is. Oh, come on, Sjoukje. Yeah. Will not be my last. Yeah. How's it feeling? Good. Yeah.

Feeling good. You're a little less yesterday, weren't you? Yeah. Feeling a bit sick, but I'm better now. Yeah. Our our [00:03:00] housemate Chris. It's his fault, isn't it? It is his fault. Patient zero. Yeah. Exactly. And Rob, how are you doing? Alright, I am starting to get the, I've been here a while and the curve is slowly working its way down with energy, but yeah, still going.

The punch drunkness starts to come in, I think, at this point. Yes, it does, yeah, but again, the intensity of the conference, it's kept its energy, which is great for day three, isn't it? It is indeed. I tell you what, both of you, Schalke, especially for you you've gotta just pace yourself to re:Invent.

Remember, it is just day after day of new announcements, new capabilities. This keeps coming, doesn't it? It's a crescendo. It doesn't stop. Werner was on this morning doing his keynote. Just more and more. It's a marathon. It's a marathon, not a sprint. It's a marathon, not a sprint. I think people who come here the first time I think it's a sprint, and then get quite surprised halfway through, but it is this it's an onslaught, but in a good way.

Yeah, for sure. So talking about big announcements then, I wonder Max, from [00:04:00] your specific role in your particular your mission at the moment. What's really resonated with you in terms of what you guys have been talking about this week? Sure. Some of the announcements have been specific to the area of Sovereign Cloud for example, we announced 65 new controls as part of the digital package for Sovereignty under Control Tower And so it's continued to respond to customers needs For making sure that they've got the best sovereignty controls the best privacy controls the best security controls so for me Those were some particularly exciting new announcements, but I think if you zoom out a little bit and if you listen to Swami's keynote and Werner's, and certainly if you were there in the morning for Adam's keynote, I just love Amazon Q.

That does seem to be the hot one that everybody's talking about getting excited about. Also my personal highlights. Is it yours too? Yeah. For me, right? 30 plus years delivering, different types of mission enabled solutions for customers almost [00:05:00] 12 years now here at AWS doing the same thing.

And the reason I like Amazon Q is because it makes it really clear and practical and it goes straight to the work that customers do and how they're going to be able to benefit from generative AI, right? In very practical use cases. And the other thing that I think at least to me came through. Is the focus on privacy and security for the enterprise, right?

So this is how are you really going to. Exploit the benefits of all of your data and the power of these large language learning models right in the context of an enterprise, a business, a government, a heavy, heavily regulated industry like health care, right? How are you really going to practically put that to work?

And I think Amazon Q just answered a number of that. It made it clear like it was like, Bing, I got this. So that's a yeah. Good little summary of what resonated this year, but you were saying just before we started that actually you've been to every one of these. [00:06:00] I wonder if you'd like to wind back to year one, what's your take on the whole arc of the thing?

It's been an incredible arc. So Dave, year one, I can remember a re invent where we had Somewhere just over 4, 000 customers, right? And at this year's re invent, past 10 times that. And still there was this air of excitement that we were on the verge of really changing the way people did work.

And, making things. I think that when you talk about the arc, somewhere along the lines, I think I would have expected things to slow down. But I've got to tell you, it just is not the pace of innovation, that customers have been able to take advantage of and that AWS has wound up sustaining right through to this re:Invent.

It's not like any other career, that I've had over the 30 plus careers. We just aren't slowing down the pace of innovation just as accelerating. And that's what's I think [00:07:00] keeps you energized. And, when you look at something like the the pandemic, But actually, for all of the unpleasantness that, that happened around that was an accelerant as well, right?

Because it made it clear back to boards that actually there is something different about this sort of new era of technology. It's not the same as it was like when we were trying to deploy,

big global ERP, for example. Oh yeah I know every one of us here remembers, the day when instantly our kids were back home.

And we were homeschooling, and if we had not had the power of the cloud to deliver distance learning processes, right? If we hadn't been able to on a dime, literally, turn around over a weekend. Yeah. Literally over a weekend. Over a weekend. Yeah. We had the Ministry of Egypt shift all of their state education, online, on AWS, in a flash and, I mean it is, it was terrible for the impact on people and yet it was really an interesting Case study in how fast you can [00:08:00] pivot, on on the cloud.

Nothing, nothing sharpens the mind like an existential crisis. Not that it's represented by A global crisis. Yeah. I'm sure you guys experienced it, right? I mean If you think about the change that we had to our, our just the family unit, imagine what that would have been like without the ability to be, use cloud to video conference, connect, learn.

That would have been a very depressing situation. It was Oh. It was a big impact. For sure. Cloud delivered a little ray of light into your life where you were able to continue to connect, albeit virtually, and people found new ways. Over COVID People found new ways! Yeah, they did. Over COVID, I spoke more to my brother playing a computer game online than I had spoken to him in my entire life.

I'll tell you what, nobody cracked alright, just while we're on this subject. It's a bit of a digression. But you know at the beginning of COVID, everyone was jumping on Zooms, right? Choose your video conferencing platform you want. I'm sure you guys were all on Chime, but like the , which is obviously the world's most favorite [00:09:00] video conference course goes that the same mate, especially when you build ai.

No, it's gonna be, but the where I was going with it though, it was all of them, even the big ones that came to, big prominence during it, nobody cracked, had being able to have a three-way conversation that didn't require two of the people to basically sit back. And allow the other two to talk constantly.

It's surely there's a way with directional mics and directional cameras to allow crosstalk on this thing? Yeah, we think so. Come on! And yet it was so essential, and yet I also will not miss the Zoom happy hours. Oh, yeah. You ended up drinking more on those things than you did if you were in a pub.

What was that about? But you never get the same experience. You're always That was not as fulfilling. A bit lonely. Yeah, still lonely. Probably rather watch TV. Anyway, look, back on the subject. Let's go back to the very serious subject. Oh, you're going to get us back to the subject.

Alright. I'm on my way back around. I'm going to have to do like A big arc. Okay, come on, Dave.[00:10:00] Sovereign Cloud. Tell us about it, Max. What does it mean to you, seriously? What does it mean to you in terms of two things, I think. The first thing in the sense of like Just define it for us in your mind and then secondly, how is it mapping on to The sort of geographies and the politics of the world at the moment and what's your mental model of that?

Yeah, sure. I mean it all starts with customers and what customers are asking for The interesting part of it though is there is no one definition of digital sovereignty means something different based upon your country or regional context. And so what Amazon did starting a year ago was we stepped back and we really started listening and working backward from customer needs.

And in fact, at re:Invent last year, we announced this thing called sovereign by design. We came to have this view. That while no one customer or no one definition existed, the need was really based on four different things. It was [00:11:00] based on the strong need for data data location and data residency and control data control.

Customers wanted. Absolute ability and transparency to understand what was happening with their data in the cloud and how to secure it, right? That was the foundational piece. The second one really was around having the right operational access restrictions. How can I really be certain that I've locked down my applications of my data so that they're solely the provenance of, my business, my government.

My healthcare practice that really became the second pillar as we started diving deep into what customers needed. The third one was really around security and resilience. And so customers beyond the video conferencing calls, beyond the distance learning customers had committed [00:12:00] now after the pandemic.

Mission critical applications. If there's one thing that you talk about silver linings, it was really the pandemic was that inflection point that just. Made it essential that we figure out how to do business in a fully digital channel, right? You couldn't go to the Department of Tax or the Department of Social Services or the typical in person servicing mechanisms that a lot of governments used.

Healthcare was locked down. How many of you did telehealth prior to the pandemic? Yeah, no, it's a thing now though, isn't it? Yeah, but it just didn't exist. It's an absolute thing. It was a fraction of the work done in the medical patient sphere, and yet now it's commonplace. And so as a result of that, the third major theme was really security and resilience.

These are mission critical apps. Now, I got to [00:13:00] have the certainty around those protections. And the fourth one really was about transparency and part of the trust that, and trust and, Auditability and attestation, like the third party confidence, my data is fully under my control, that my security is fully under my control, that privacy is completely under my control, and that others, whether it's bad actors or foreign governments, don't have the ability to get to my applications, my data on the cloud, that's really those, The key four characteristics that we've distilled from literally hundreds and hundreds of customer conversations.

And what I love about that is the way you've thought about it is when you talk to people about what their sovereignty needs are, they don't have the structure, they're confused about it. So what you've done there is nicely map out think of it in these tenants. Here's how we're working with those tenants.

I think regulators are [00:14:00] waking up to cloud, they understand the benefit, they're coming down to meet. As cloud rises as well. And there is this happy point in the middle that we talk about, and it feels like a tipping point is starting to occur where people get it, they understand because of the structure you brought to it, they see the capability, they've seen what the private sector's been able to do in cloud and they want more, don't they?

So they're and I would also tell you that with that, that the AWS ecosystem of partners. Have also started getting a clearer view and a clearer set of service offerings as you all are doing that's going to help all of our customers. And so I think that's, again, that's part of the power of AWS.

No one organization is going to have all of the answers here. And in fact, a critical part of many countries, digital sovereignty goals is to have a certain trusted separation of

responsibilities with local firms and local knowledge, controlling aspects, essentially delivering managed managed sovereign cloud services.

And how have you [00:15:00] managed to square the circle between The idea of the cloud being and I recognize physically it's not like this, but just staying at conceptual level, the idea of the cloud being this sort of universal resource that you can move things around very straightforwardly, and then the sort of the tension between sort of nation state and regulation and, some of the elements you pointed out that, that sort of again almost suggests that the cloud needs to be carved up and walled off.

Have you managed to Balance that tension, do you think? Yeah, I think it's a matter of you've got to dive deep. And so it's easy to say the cloud, but our, clouds are not the same. All clouds are not the same. AWS has been at this for 17 plus years, right? And from day one, we had a design objective of being able to handle the most sensitive workloads on the cloud and the highest volume, highest scale workloads on the cloud.

This is a bit of old history, but if you go back to 2013, 2014, [00:16:00] you'll remember that. Amazon was the first cloud service provider that any defense and national security customer committed their workloads to. Now in 2014 the U. S. National Insurance National Intelligence Community made a move exclusively to the AWS cloud.

And I think that was a big bellwether moment. If the world's national security organizations believe the cloud is secure, then banks followed other highly regulated industry followed him. That was a big one. So all clouds are not the same, I think. And that's where we help customers dive deep.

And that's where we work with our partner community to similarly help them dive deep. It really is about working to the distinct customer requirements. And then helping them architect and implement and operate on the cloud securely. So much as what Capgemini is doing. And how, when you look at the the [00:17:00] different regions of the world, not from a cloud point of view, actual sort of countries and, how are you perceiving different levels of requirement at the moment?

Some areas of the world significantly further on in terms of how they're thinking about regulation versus others. Actually, I would turn it around. And I would tell you that what we see is customers who are thinking about their path to modernization and transformation, particularly right now, because I think with many customers after a year of sort of excitement and perhaps hype around generative AI that we've seen, since it burst on the scene and we all as like individual consumers could like type into a little box and then just see this amazing sort of answer come back.

Now we're starting, which is part of the reason why I'm excited about Amazon Q. Now we're at that point where customers are going, now how am I really going to put this to work? And I think what so many of our customers, whether they're highly regulated industries or government [00:18:00] customers, they're now, it's not the pandemic inducement quite, but it's pretty close because they're looking at their current IT estate and they're saying, Am I going to be able to take advantage of this?

That is so true. Doing AI without cloud, that's just a headache. It's just I can't imagine even where you'd start. Yeah, so you asked about what I was excited about. I was excited about the announcement of the joint partnership with NVIDIA, right? There's not many enterprises that are going to be able to have an enterprise GPU cluster at their fingertips that's that big and therefore you've got to figure out how to get your enterprise in a position where you can take advantage of the next wave of modernization.

And so we sit down and we talk to customers and they're saying, Hey. I have these regulatory, or these policy, or these statutory constraints. How do I get through them so that I can get to the [00:19:00] capability I want to have? And that conversation varies around the world. Because the way people think about digital sovereignty varies by country and region.

That's both the Challenging part, and it's the interesting part that we're all out here working to solve right now. And your role must take you takes you everywhere, meeting all those Different people. That's got to be a fun part for you as well. They're just the different countries, cultures, conversations, different governments you're talking to.

I suspect you probably get quite a lot out of that as well. I do, and it gives me a very interesting perspective that I can share with other customers. We had one of our customers that we recently developed a capability with, so Amazon's classic customer working backward process with the Singapore, Spartanation, and Digital Government Group.

And, And Chow Ho, who's leading that organization, was here at the summit talking about what the Singapore government was trying to achieve. They had started their transformation to the cloud years [00:20:00] ago moving into the commercial cloud on the Singapore region. Well over 50 percent of their work migrated to their government commercial cloud.

Very well structured, control schemes, governance mechanisms, quite comfortable moving on to the commercial cloud. And then they hit a couple of more sensitive workloads, and they needed a different approach to it. And so we sat down with the Singapore GovTech group, and we reimagined how we could deliver some on premise AWS cloud infrastructure that would unlock that next wave of innovation, but still respect The physical security concerns that they had and the further operational security concerns that they had and because the dedicated local zone is a customer specific, customer dedicated AWS infrastructure solution, they get additional operational controls.

Yeah, and maybe just by way of bringing our conversation this morning to a bit of a close, let's do a bit of [00:21:00] crystal ball gazing. And if if you look forward maybe to next year's re invent, what kind of big movements in the world of sovereignty are you expecting to see or anticipating seeing over the next 12 or 18 months?

I think what we're going to see just like with the generative AI, we're going to see people moving to real solutions. Again, super excited about the work that we're doing with Capgemini to give people a clear path. So they can evaluate their digital sovereignty needs, and then they can make clear progress.

So I'm looking forward to next year being able to have many more organizations where they've charted that path to where they want to go in the future, and they've taken these actions like Singapore, like government of Singapore did. I also think that we're continuing to learn about how important resilience and continuity of government is when when Ukraine was attacked we were able to work with the digital minister of Ukraine, back up all of their critical government workloads, more than 40 different government [00:22:00] departments, more than 10 petabytes of data, and Literally, in days, have them up on the cloud and running government in a way that they couldn't in the face of that kind of frankly, it's the worst humanitarian crisis in Europe since World War II.

Nobody wants to find themselves in a position where they haven't laid the found work, laid the foundation, to be able to respond to some of the unpredictable incidents in the world. That's another big driver of governments thinking about how are they going to modernize in this digital world and how are they going to do it in a way that respects the digital sovereignty that's important to these nations and that is, a regulated part of industries like

health or telecommunications or energy.

Thank you for the insight this morning, Max. I think you put it very well in the sense of the next level of maturity of being able to do things like cloud and then, of course, AI is going to have to come with this sort of [00:23:00] solution and good to see you guys leaning into it. So thanks for your insights.

Thanks for the partnership. It takes a lot of people to be able to deliver on the requirements our customers have. And we're just excited about all of the announcements here at re:Invent and looking forward to the year ahead. Let's jump to a couple more announcements. So Sjoukje, what else have we seen?

Yeah, some cool announcements on the AI keynote from yesterday. A couple of new large language models are announced for image generation, but also for multimodality. So explain that stuff for those of us. Say Rob who doesn't understand what that is. Okay, I will. Multimodality that you not only have to generate text or put in text, but you can also use videos or images and then let that larger language model reason over that.

Wow, that is pretty sweet. Yeah, that's really good. There were some SageMaker features announced. For instance where AI decides which trainer data is relevant for you. So the A. I. telling you how to use the A. I. Yeah, that's going [00:24:00] to be good. It's going to be hard, Rob. It's that thing, you could just one day just, Alexa, can you run my life for me?

And go walk off. I'm looking forward to that day. A different reality then. A different reality. There was some announcements around Responsible AI, the AWS AI service cards. Now, Q of course, Max, you already mentioned that. That was also part of the keynote. Lots of cool announcements. Taking another step in the AI.

That's okay. I appreciate you calling out the Responsible AI part. Cause again, from a real practical perspective, customers care about that. Adam talked about being at the at the, announcement in the U S for responsible AI, and then being at the announcement in the UK on AI safety. And I thought that was a super exciting announcement where customers now can pick.

The responsible AR guard whales that they want to implement in Bedrock. We sat there going, how moral am I? Should I slide it to the left or the [00:25:00] right? Don't socially judge me. The morality or immorality slider, as I was saying. That is really a prerequisite for starting using this in your enterprises, right?

It is indeed. Look. Thanks again, Max. Great conversation this morning. And we end every episode of the podcast by asking our guests what they're excited about doing next. That could be going for a nice dinner, or it could be something in your professional life, and of course, we're in Vegas. Max, what are you excited about doing next?

Yeah, Dave, I don't really have a good, I'm excited about being in Vegas next because I'm about ready to hop on a plane and go see some customers in Australia. I am excited about going and seeing customers in Australia. I'm excited about Bondi Beach. I've always wanted to go there and I think I need a reason to go.

So maybe the you never know. Maybe digital sovereignty will take me there next. Yeah. You look like you're a little too big for the baggage. So I'm afraid it'll have to be digital sovereignty. Sneak into your luggage when you're not looking. It's heavier than I thought. So a huge thanks to our guests this week.

Max, thank you so [00:26:00] much for being on the show. Yep. No, it's my pleasure. It's great. Love the conversation, love the love the energy here, and y'all did a great job.

And we are here for the second part of our double feature today, looking at regulation, sovereignty, cyber. And all of the very complex areas that as cloud is maturing, we're needing to get into and understand. And I'm delighted to say we have two guests with us today. We have Gary Meshell, who's the Managing Director of the Global Partner Security Initiative at AWS.

And we also have our very own Anne Saunders, who's Global Cyber Security Partner Director at Capgemini. Guys, welcome. Good to see you. Thank you for having us. Oh, thank you so much for taking time. I'm sure you've got a busy [00:27:00] schedule this week. It's been a non stop rock tour. I bet. And I just don't have anybody to carry my bag, so it's Everyone needs a bag carrier.

Yeah. I've walked 63 miles since I got here. How many steps is 63? That's amazing. I've lost count. That's almost like a triple marathon. 63 miles since Saturday. I think we have a winner. Ding ding. That is good. And I've only done 59 and I thought I was going to win that. There is no way you've done 59.

Just for the avoidance of doubt, the listeners, no way. So Gary, do you just want to, do you just want to tell everybody a little bit about your role and your, and what you do on a day to day basis? My role at AWS is to scale security through partners. If you look at the AWS business model for security, we very much focus on securing the AWS cloud, and we believe security is job zero.

And our model is very much what we call shared responsibility. We work with our partners, we work with our customers, but we [00:28:00] only do that in an AWS environment. And the world has dramatically begun to change when it comes to security over the last couple of years. We're living in a digital state where it's a multi cloud world.

You've got platform as a service on prem, you've got platform as a service off prem. My business is focused in working with partners like CAP to really scale security through joint collaboration, joint innovation, and joint investment. Terrific. And we're going to dig in a lot into some of those subjects in a second.

But Anne, let's come to you. Thanks for making the time. How you doing? I'm good. I'm good. So my role counter to Gary's is, looking at the cybersecurity partners and technologies we should have in the portfolio that support the initiatives that our customers are rolling out with regards to how they're transforming their business, moving to the cloud, becoming, digital world.

As from every aspect to what they do from a business [00:29:00] perspective. So I spent a lot of time reviewing technologies for the different cybersecurity domains and collaborating with Gary. AWS is a very important partner to us. Collaborating with the AWS cybersecurity leadership on what they need, what they see and where they'd like to drive their business.

And with that shaping solutions on how we can jointly support customers together. That's good. . And I wanna pick up actually on, on one of the things that you said there, which was like the, the ever increasing digitalization of customers and organizations across the world.

Of course, what that comes with is ever increasing ta attack surfaces, ever increasing complexity. Gary, maybe we can just, we can kick off by zooming out and just talking about the threat landscape as ex as it exists today. I remember. I was a CISO at at a previous organization of 10 organization, but it was in the days where it was client server, it was perimetered.

It was, it was actually only 10 years into internet era at that point, like [00:30:00] dating

myself terribly . But it was a contained problem in, in, in so many ways now. In that last 20 years, there probably isn't many disciplines that have got more complex, more fast moving and frankly more dangerous than cyber.

So give us your take on that. So there's some sobering numbers that I'll share with you. It's estimated by the end of 2025 That cyber security attacks will have a net impact to GDP in the United States of 10 trillion dollars numbing a numbing number amazing, it's interesting we're here in Vegas and MGM grand was Significantly breached a month ago, right?

Yeah, it was a ransomware attack. There's a ransomware attack It is still not resolved, and we're at 230 million dollars and counting to get that resolved. That's a staggering number for a, like a, just an organization to have to cope with. Off the back of a base. [00:31:00] Shut down a gaming floor, isn't it? Yeah, it's like a, it's total, it's a complete shutdown of the business, isn't it?

So it's that's massive impact. It's not only the cost, it's loss of trust, and it's loss of your brand equity. Absolutely. Yesterday, we had the see saw of Marriott. On stage as part of our keynote and he's a hundred and ninety eight million Elite customers now think about 198 elite customers who can't put their keys in the door The net outcome on your brand and trust Is staggering.

I think a couple of other things that are worth commenting on is This is no longer a CISO problem. It's a board problem. It's a CEO problem. And the level of accountability that boards and CEOs are having placed upon them really makes me nervous. Yeah, I bet. I'm not sure they really know what their accountability is.

I don't think they understand [00:32:00] how they communicate what is their commander's intent when there's a massive breach. When do you call your shareholders? When do you call your board? When do you shut your services down? So my take on cyber is it's inevitable. I talk a lot about it's not a matter of if, definitely a win.

Yeah. It's a matter of when. The winners and losers are gonna be the ones that had to respond. Yeah, and the other point I'll make and I'd like to get Ann's take on that, It's all about data. It's all about threat intelligence. And the problem we've had until recently, there was data from everywhere.

You were a CISO. How many products did you have? From how many different vendors well, yeah, so we had a we had I think we had three different External data services and then probably in the sock at that point And like I said, this is when this is 2001 2001 2003 We probably had at that point like [00:33:00] three or four, it wasn't at that point it was a much less big problem than the sort of Complexity they were about to come on to talk about I suspect particularly then when we're going to step forward and talk about you know What on earth happens when?

Artificial intelligence is in the middle of all this but let's leave that for a little bit longer in the conversation Why didn't you give us a reflection? I've been in the business for a long time as well. I remember the 2003, 2010 era. Those were the days, I think. Those were the good old days. It was super easy.

You set up a VPN, you have access, and you have multi factor access. And, hey, good to go. Yeah, now it's totally different. And in my role, I find myself having to really weed through to figure out which technologies are really relevant and really We'll stand the test of time with regards to how things are changing when they're changing so fast.

I say this because what I've observed and what we've all observed, Gary and I've observed

with our clients, they have had so, they have so many point products that [00:34:00] they've been using for years. And now all of a sudden, there's they're all saying something different and you need a different way.

You need a translator for all of them Yeah, and now we're at the point where there's not the amount of data that's being created by just art The digital reality of what the world we live in those point products don't keep up anymore. No one's around to really trans, no one understands how to translate what it truly means.

And you get caught up in just this mess of just technologies that are there's no consistency and there's no streamline of the security posture within an organization when you have so many point products. And of course, where I sit, looking at all these technologies that come in, it's okay, you're great at doing X, but how do you translate and how do you impact Y and, what does the horizon look like?

What does the overall landscape look like? And how, how do you tie in and create that consistency with other tools?

Cyber trends happen in a matter of days, not a matter of months and years. [00:35:00] And one of the seismic shifts that's occurred is one, the realization that you can't have 60 products from 35 vendors. Absolutely. That's gone. Yeah, that's gone. But what the industry is demanding is a common schema. One of the things that AWS is doing, we're trying to lead the industry to create a common schema through something we call the Open Cyber Security Framework.

Partners like CAP, ISVs like Splunk, CrowdStrike, they're all now saying, you're right, we need a common schema. And just for those that haven't kept up with what that actually is, what does that look like and what are the major components of that schema? So it's an open source framework. AWS and Splunk started it.

It's taken on a life of its own. There's a 120 cyber threat intelligence providers today that all subscribe to [00:36:00] OCSF. Now, the importance of that is it now allows you to aggregate your data using a security like. So one of the things that we're laser focused on with our partners will present almost untapped amounts of threat intelligence, cyber signaling from all different sources, all different technologies, all normalized and yeah, normalized, aggregated, easy to access, clear, and the winners, in my opinion, are going to be ones that build platforms, right?

Platforms that aggregate platforms that integrate. Okay. Single pane of glass. So it's all basically going after the, Unintentional obfuscation and confusion is in and of itself increasing your risk as an organization. It is reducing your ability to move quickly and reducing your ability to to react [00:37:00] to security problems.

And of course that, that has been a truism in security for, the 20, 30 years, and perhaps even longer when it comes to physical security. So it's really it's really going after that and taking that to the next level in an ever more complex landscape. Does that itself though become a target?

So there's this great thing that's stopping more? It has. It has become because you just say straight away, you go, that's the biggest threat to the people who would do us harm from cyber attacks. They've got to be going after it quite hard. The other interesting thing that's happening a year ago, an ISV would never want to work with a G.

S. I. What I describe a triparty motion. Yeah, they wanted to basically implant on prem their security software lock you into a proprietary data schema. One of the things that

I've been almost blown away while I've been here the last six days is the number of ISVs that have come up to me and said, [00:38:00] look, your program, which is co development, co innovation with systems integrators, we realize to survive, we need to be part of that platform.

It's the future. A year ago, they were in ISV denial. Now, they get it. Yeah. They want to partner with you. They do. And that's what's interesting on the Back of that, the conversations I've been having all week with the partners that we have in our portfolio that support AWS. It's all about the marketplace strategy.

And that's the result of that shift happening. That's a part of it, at least. I don't know if you had the opportunity to hear Ruba Vorno's keynote, but on stage, she had a global systems integrator and Palo Alto. And the CISO of Marriott. And with the CISO of Marriott said he wants more than anything, I'm not going to buy any new ISV software.

Second, if you can't [00:39:00] commit to a common data schema, you're not coming into my shop. And third, we need to deal with a platform provider that brings us analytics, data modeling. Because AI, I mean everybody talks about AI as a silver bullet. There's a sort of dichotomy here. The bad guys also realize that AI is a silver bullet for them.

So the more you have upfront understanding of your threat landscape, the more you're not chasing false positives, which we do today. AI now basically will say, go chase this, ignore that. That's what I'm really encouraged by. So let's actually move on to AI. So I think what we've established is like every increase in complexity in the landscape, also what's happened is an increased complexity in the tool set.

That's being now addressed through the framework and the schema [00:40:00] that we've just discussed. What you've just introduced there I think is the big looming. Peace in the in the firmament right in the sense of we've been talking positively about AI all week Amazing stuff coming along but exactly to your point The black hats also see AI as a major tool for them and AI itself when it we you know when AI Systemic AI is established within large organizations and that, and we all think that's going to be a very accelerated adoption period over the next two or three years.

Zooming into the future, you're going to have AI enabled organizations, workforces are going to have been changed, organizations are going to have been reshaped. And sitting at the heart of the decision making process is going to be AI, it's going to be language models, it's going to be data, and it's going to be front ends of various different ways.

That itself creates so many new attack surfaces you would have thought. So how do we pick this? Let's get into it maybe [00:41:00] via the new attack surfaces and then let's come back to AI as a tool to actually combat some of this stuff. So some of the new threats. Frankly, they're more at the end point, they're at the network level, they're at the IT, OT level.

We've been way too focused on the digital estate. If you look at major breaches that take place with airlines, with power companies, with healthcare providers, they're not happening at the core, they're happening at the network level. Manufacturing, IT, OT, we've got to start figuring that space out. And Anne, I don't know if you agree with me.

I still think we're way too focused on the digital estate, as opposed to some of these new endpoints. I agree with you. I think, too, we're still caught up in thinking about security from a control perspective, whereas the security of the future, you're [00:42:00] right, it's, wherever the data is accessed from.

But if we really are going to incorporate AI, it's the data itself and how we protect that and

how we manage the life cycle of that data. So it's doing and we're using it in the proper way for security reasons and for business reasons. I agree at the end point and from the end point in, you need to think about it holistically.

You need to think about from a consistent viewpoint and the security has to follow the asset, wherever that asset is. On the OT side, operational technology, that's what. I think the point you make about data to me is one of the ones I worry about. Yes. We had a guest on the show actually who talked about he gets involved in some of the wargaming that some of the, some of governments do and his point was we win wargames all the time by attacking the data sets but in very subtle ways.

So not attacking them necessarily in a ransomware style way, but slightly corrupting some of the data sets. So the decision making that comes off the back of that data set over time just moves more and [00:43:00] more out of step where it should be, but in an almost an unnoticeable way initially. So that, the data set, particularly when that's sitting underneath AI that's powering organizations and making, having boards, assisting boards in decision making, seems to me to be like one of the biggest new threats when AI comes along.

I'm going to flip the model. Sure. And look at it from a use case point of view, because a threat is a threat, and there's no magic bullet that AI brings. AI is all about data, actionable data, predictive data. Where I'm excited is the amount of what I call autonomous security that can be created.

Most threats are a result of bad human behavior, bad hygiene, insider attacks. Through autonomy. Leveraging the best threat intelligence. You're not leaving it to a person in a sock, [00:44:00] average age, 26 years old to make a decision. Is it a threat? Is it a false positive? That's use case one for AI. I think the more profound use case if you look at, I think, we've not been thinking about cyber the right way.

We've been thinking about manage and detect. What about respond and recover? If you believe it's not a matter of this, it's a matter of when, how many organizations that you talk to have a resilience recovery strategy. That is always a moving target and it's always something that's being worked on because it's constantly changing.

So here's the cool use case. Think about your bank is under attack and Your data is telling you it's time to turn your core banking system down. You've got to alert the FCC. But using AI, [00:45:00] you can create now minimum viable services. Make sure if you go to your ATM, you'll get money. A minimum viable service that my heart defibrillator or my insulin drip doesn't get turned off.

Because I have a backup. I think that's where we're lacking right now is on the response and the recoverability. That's true. Yeah, we're gonna, we're, the incident response practice is definitely going to have to evolve to deal with the information and acting on the accurate information because that's another attack vector.

That's another area where we're going to have to protect against. false information that could impact how you respond. What if it's fake? Is that they actually, are we doing the right thing? Did we turn off your defibrillator on accident because we use the wrong data and the modeling? And we talk a lot in the show about the Kinefin framework, which allows us to manage, it breaks the world into chaos, complicated, complex [00:46:00] and order.

And when a cyber attack occurs, it causes utter chaos. And your response point is getting it back to the complex. And being able to manage it. And so then you can get back to some form of normality. So you bring up a really good point. You mentioned technical war games.

My response would be, so what? Have you run a business response exercise?

Has your CEO, has your board, your key business line stakeholders, been put in a room? And say, okay, we are now under attack. What do you do if CNN calls you? And says, hey, I heard that. X, Y, Z company is under attack. We have missed a whole spectrum here of focusing on security as a technical practice. It's a business practice.

It just so happened. It's a technical problem. And I think what AI is going to do is allow CEOs and [00:47:00] boards when the bullets are flying to not have to wonder what are my critical decisions, it's going to help them. Make those critical decisions. What I was gonna ask, actually, maybe just to bring this part of the conversation to a little bit of a conclusion, is, what should boards be talking about?

You made a point earlier that, the CISO is not a technical role, the CISO is a board level conversation, and I, and I would observe, I don't know whether you observe the same, that The boards probably aren't having that level of conversation and maybe they're trying, they're just not having the right conversation.

What is that board conversation, how has it evolved in your mind and what should they be talking about now? So it's evolved in a number of ways. It's an acceptance of what we talked about, it's not a matter of if, it's a matter of when. Second, I think it's evolved to the reality that when you're punched in the face, What is your response going to [00:48:00] be?

How are you going to communicate it outwardly? How are you going to communicate it internally? And what are you going to tell the regulators? We talk a lot about continuous compliance. We do, yes. I'm just happy to see that we are seeing a shift at the board level where the CISO does have a say.

The CISO is involved in kind of strategic direction and what the board discusses now with the SEC rulings around the response time that puts more responsibility and more, highlights the CISO's role and the importance of having the security at the table in the boardroom at all times to think about the business, the impact to the business.

We're working on a continuous compliance framework with CAP. Here's a great use case. A board, a CEO, a chief compliance officer needs to know in real time what their security posture is, in real time what their regulatory posture is, and what their internal risk management. [00:49:00] And I think what I'm excited about, AI now creates the opportunity, you're not wondering.

What's your posture is you've got your regulatory obligations right in front of your real time snapshot exactly where you stand with your most critical assets and you tie in the response like that's Gary's really wants to focus on and is important for, for the board. How do you respond?

And what is the best response? That's where I could come in to help for sure. Brilliant. On that note, let's pause the conversation for now. Thank you both for your insights and giving us a framework to think about. Thank you. Probably one of the biggest problems that we've that we have ahead as we move through the next few years.

But let's turn our attention to some of the announcements. You, References you went through that Gary Werner Vogel's talk this morning, I think. Schalk, that's where you're going to major now and the other, what announcements we've seen since the last show. Yeah, I also want to focus on that keynote of Werner Vogel's.

He had a couple of, he said a couple of things that I think are worth mentioning here. It was about architecture, some new announcements and also about AI. [00:50:00] And he

said you need to build evolvable architecture, but also need to pay off your technical debt. That's very important. And when you architect your solutions, You should consider cost and sustainability in each and every step of your design.

And the last thing he mentioned was without good data, there is no good AI. And that's totally true, right? It's at the end of the day, cyber is about data. Everything else around it is extraneous. It's the quality of that data and what you can do with that data. Yeah. It's always about data. Yep. Yeah. And one release that I would like to mention, the new AWS Management Console for Applications gives more insights into costs, potential issues going on through your development lifecycle, and Amazon SageMaker is getting a code assistant in the IDE itself.

And what would that, what does that help with? It can make coding smoother and faster for everyone that is using it. So is it, like [00:51:00] AI code generation? It has something to do with code generation. It is an assistant in SageMaker that can help you to make it much easier to build your applications.

Cool. Any big announcements that either from today or across the conference that are particularly exciting you, Gary? wHen you're thinking about some of the problems we've been discussing today one of the things That AWS does when we announce something we make sure we re announce it right and talk about the results So last year we announced AWS security like yesterday.

We announced there's a hundred And 20 security vendors that are now publishing and subscribing to SecurityLake. That's very exciting. Our announcement of cybersecurity insurance, powered by AWS, where, think of a good housekeeping seal of approval from AWS, where we'll go in. And we'll do a security architecture [00:52:00] review.

We'll score it. And you can now come to AWS to get cybersecurity insurance. I think that's the other one. And just this ongoing set of bedrock announcements. Where we're spreading AI in as many information and data sets as possible. Fabulous stuff. Anne, what's resonated with you across the week? The, all the announcements around AI in particular.

And how. A lot of the vendors here and partners here, everyone has an initiative around it. I think it's going to be very interesting to watch how cyber security companies and cyber security practices address the, using it for good and protecting the organization from bad things happening because of it.

It'll be interesting to see how that evolves. Won't it just, I would imagine it's going to evolve quickly like everything else at the moment. I'm sure. lOok, thanks again for your time and [00:53:00] insight this afternoon. Cyber is such an important is such an important bit of the conversation. And it should be, I think, kept a spotlight on.

So thanks a lot for your insights. Now we end every episode of the show by asking our guests what they're excited about doing next, and that could be, I just want to see the faces of my family again. Or it could be something that's exciting in your personal life. Anne, why don't you kick us off?

What are you excited about doing next? I'm excited to get home and not go anywhere for a few weeks. Amen. Yeah. That's a good one. Yes. I'm right up there with that one. A lot of people will support you in that. Yes. 100%. Yeah. So for me I'm excited that when I get home, I'm heading up to New York to see my two new granddaughters.

Oh, beautiful. Congratulations. I've got a four month old granddaughter, and I have a six week old granddaughter. Wow. As much as I care about cyber, I care a little bit more about

my granddaughters. Oh, how beautiful. The last time Gary and I were together was at [00:54:00] Reinforce, and I think we were texting, Is she here?

Is she here? Is she here yet? Yep. Wow. Wow. I've Off the record or on the record, they, my daughter gave birth in the middle of me making a speech at the end of the first. Yep. God, honestly, it's weird how those timings happen, isn't it? Yeah, it's crazy. Yeah, it is absolutely crazy. a Huge thanks to our guest this week, Gary, and thank you so much for being on the show.

Thanks also to our sound and editing wizards, Ben and Louie. Our Jet Lag producer Marcel and of course to all of our listeners. We're on LinkedIn and X, Dave Chapman, Rob Kernahan, and Sjoukje Zaal. Feel free to follow or connect with us and please get in touch if you have any comments or ideas for the show. And of course, if you haven't already done that, rate and subscribe to our podcast.

See you back in the AWS reality soon [00:55:00]

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get The Future You Want | www.capgemini.com