
# CR093

## Role of AI/Gen AI in Cybersecurity with Corence Klop, Rabobank

Capgemini

# CR093

# Role of AI/Gen AI in Cybersecurity with Corence Klop, Rabobank

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

[00:00:00] Sorry. David. That is what it sounds like when you're on mute. I was confusing the hell out of me there, I'm thinking it's my audio gone. As you can see, we're highly professional in all that we do. I wasn't sure why everyone was sort of staring at me.

Welcome to Cloud Realities, an original podcast from Capgemini. And this week we're going to take a look at cyber in the world of financial services, but from the perspective of a leader that's transitioned over from the world of data and analytics. I'm Dave Chapman, I'm Esmee van de Giessen And I'm Rob Kernahan, Rob good to see you. How you doing? I'm all right, David.

I'm all right. You good? Ez, how you doing? Yeah, good. Steady as we go. Steady as we go. I hear, I heard that there's a big sort of celebration in your village. Yeah, we actually have carnival. And I thought, should I wear my jacket or not? Cause I live in, I'm part of [00:01:00] Oeteldonk.

Uh, it's now called Oeteldonk and it's actually s'Hertogenbosch, Den Bosch. Uh, but we have different names for the cities during this time of year. Uh, so yeah, it's, it's amazing. It's such a huge event. It's compelling. It's, it's everything. It's a lot of. Drinking, to be honest, uh, weird music, but mostly it's just spending time with each and everyone and everyone's equal.

That's the idea behind Carnival. You know, so people living in the village, rich people, poor people, we're all equal in these days. So that's what I really like. So I'm trying to behave for one day. That's what I say every year. I'm going to go one day. Does it work? Is that the classic, I'm going to be good.And then at the end you go next year, I'm going to be good. And then next year I'm going to be good. Yeah. It's work in progress. I 56 hours at this point, but I'm still going strong. Yeah. Well, you're going to see me on Monday. So, uh. Yeah, that's right. You'll see the result. Now, what does a carnival jacket look like?

Well, you have different, well, every town has different rituals actually. [00:02:00] And then Den Bosch has a black jacket and you have like, uh, we called it emblems. I don't know what it's called. Badges. Badges. Yes, indeed. That you can put on there and that showcase. We, I'm actually part of Sontagsdorp, which is Rosmalen, which is actually a small town that is now officially part of Den Bosch, which is a huge, that, that's something, you know, you can imagine different colors.

We're not part of Den Bosch. Yes, we are. So now, you know, it took us years, but I can actually now showcase them both, both colors. Uh, so I have some kind f elevated position. It sounds like you've got there. Well, I don't know, but, and I'm also import, right? I, I, I'm from above the rivers actually. And since the year of 20, below.Yeah, it is hugely political. There's a huge story behind it, but in the end it's just people drinking together, uh, dancing and that's it.

He's, he's the big question though, is would you let Marcel in? No, he's from the big city, you know, [00:03:00] wasn't a fast response on that. Was that very, I was just trying to picture how that would look like. I don't know if he's actually would enjoy that. Um, but I think you all are very good in celebrating carnival. Cause we're talking a lot about, I think I'm a natural. Yeah. Yeah. o. I think it's something that you should experience. I think that sounds like quite good fun. All the factions and everything trying to come together to say we are one.

It's quite nice. But yeah, unless there's a huge fist fight in the middle of it, but you know, doesn't feel like it would be in the spirit of it, does it? No, it doesn't feel like it's in the spirit. Yeah. No fighting. Anyway, look on with the show. I'm delighted to say that joining us today, we have the CISO of Rabobank, Corence Klop.

Corence , lovely to see you today. How are you? I'm good. Thank you. And. Uh, you are also, I believe, in the great country of the Netherlands. Yeah, I'm very happy that I moved out of this part of the Netherlands where we celebrate Chronicle. I lived there for [00:04:00] 25 years. What, uh, what outfit did you used to wear? Did you have a jacket? I'm originally from a smaller village, so we don't have the official jackets and stuff there. So you have to be in, so the impression I'm getting is you have to be. This is elitist. We're learning about the elitist culture here, aren't we? Where I'm covering it. It is complex.

It's about equality as may explain, but still there's a lot of difference. Yeah. I mean, it's ironic some would say. It's the same as equality. We're all equal, as long as you're not from that village, and then you're definitely not allowed in.

It's just like companies. You know, we're all equal, but if you're from that department, So, Rob, is there anything more confusing than this this week?

No, I think that's taken the biscuit. I mean, I thought I had, you know, it was like, what? Anyway, that's, yeah. Well there there is one thing in my world, Dave, which is ai, straight up, lied to me this week, like proper lied. Were you

asking it to do inappropriate things again? [00:05:00] No. , no. This was a really simple question, which is, um, we're away next week.

Um, remote potting and Marcel's booked the hotel, you know, being an organized producer. So I asked AI, which hotel has Marcel booked for me next week? And it came back with absolute confidence and told me, Marcel has booked you this hotel. And it was completely the wrong hotel. And I mean, not, it was like miles away from the one that we're actually staying in.

And the only thing Twiggy made was, that doesn't sound right. Because it came back with this lovely little boutique, you know, trendy hotel. I thought, there's no way our producer would have booked us in there. I'm like, all right, nice. And so I went away and checked it complete. I mean, like miles. away. And the confusion was if I turn up, believe in that and go to the wrong hotel, like banging on the desk, going, I definitely have a room in this hotel.

Um, who's at fault and where does that go? And as a society, we ready for, you know, humans make mistakes and we're used to it. Yeah. Okay. We got that. But now AI, [00:06:00] but it's the, with the confidence, it came out, it says, Marcel has booked you this hotel. So I think Rob, you know what I, you

know what I think it's done.What's it done. It's, this is your co pilot, presumably. Yes. I think it's picked up on your travel anxiety, . Oh, it's like playing with me. Oh my God. God. I tow, I'm gonna tow you with him I think what's going on?

Exposure. Yeah. It's like, is this the rise of the ai? They're just gonna, you know, slowly start denting it, chip, then eventually, yeah, it's gonna chip away at you and they're gonna bring you down through your. Each of our individual weaknesses, in your case, is travel anxiety, is your kryptonite.

But it was, it was this, it was just the way, if you took it on face value, it looked like a really compelling good answer, and you're like, oh, it's just because, you know, the spidey senses tingled hooktail exist? Because that's why my question was, is it a real hotel? Because it could be like an imaginary thing, right?

Oh no, it actually gave me a link to the hotel I could click. [00:07:00] And uh, it was all there. It was like, this is a thing that exists. So if I'd not been paying much attention, or I only had a couple of seconds, or I just arrived in, in, in, in the place, I'd be in a taxi to the wrong location.

This isn't good. Was it the right Marcel? Maybe it was the wrong Marcel. Are you saying another Marcel has booked me into a hotel? Yeah, yeah, yeah. This would be, this would be odd, but okay. I mean, look, stranger things have happened, Rob. But, yeah, I just, I just, um, maybe that's it. Maybe there's a duplicate Marcel, which is quite scary if you think about it.

Two people like Marcel in the world, but yeah, okay. Sliding door sort of situation. Yeah, yeah. Well, there you go. Well, I think what's happened, it can only be one of two things. Your co pilot has become self aware and decided to try and take you down via travel anxiety, or it's just got the data wrong.

Uh, I'm gonna I reckon it is. I'm gonna go for one. This is, this is the That's the better answer. AGI has happened. It's keeping it a secret and it's slowly going [00:08:00] to take us down in various ways. The rise of the robot, much

more mundane than I thought it was going to be.

Yeah, oh yeah, sent me to the wrong hotel. It's like, it's lacking, if AGI is there and it has happened, it's lacking imagination, isn't it?

On that note. Let's start with just examining your background, Collins. I understand you haven't got a typical profile for a chief security officer. What was your journey to it?

I started with working in digital transformations for many years and in data analytics. So I'm really a big fan of seeing what new technologies can do for a bigger organization and actually exploring how you could use that.

I think these are also for a big bank, for example, very important to follow and actually to see the opportunity side of it. And from, from this background, I moved into being responsible for information security, uh, for the Rabobank. So I, I was switching from this. Well, a group of [00:09:00] innovative, explorative people, uh, always looking at the opportunities into a way more risk, well, risk management kind of culture.

Um, but I do believe it's a really nice step and it's also, in the end also security is about balancing innovations and risks as well, so. And there's an interesting duality there because data people want to exploit the data and get access to it and create new data and aggregate and security people kind of sometimes come from the corner that says, I don't want you to have access to any data and you can't see it and you shouldn't create new data. And so there's a, there's an interesting two worlds coming together there.

Yeah. And I think I also see there's really a friction, of course, because I think it's also my personality. I'm way more opportunistic. So I always think about what you could do with data or with certain technologies. And it is what you're saying is, um, Being in security, it's, there's also a lot of attention, of course, for the privacy of the people [00:10:00] behind the data. It's also about preventing that data goes to people who shouldn't say it, that it doesn't leave the organization. And that it's really looking at, at a different perspective, actually, I think of, of the same topic.

But both of them are important. It's the same. And sometimes you feel like security is like, Oh no, they're stopping us. They're preventing us. So how can we get around them? To be honest, I sometimes also think that by myself, but on the other hand, it is very strong that they do it from a sense of feeling responsible. And I think if you can highlight that and actually applaud for that and understand their ways of thinking, you get the best of both worlds.

It's the empathetic thing, isn't it? Somebody's trying to create value out of data, so they need access to it. And the other is fundamentally trying to protect the organization and the

people.

And so you have two very different worldviews coming together there.

Yeah, and I think that's also how you should look at these kind of topics as an organization. And that's, I think, the decisions you should take. It's security is not [00:11:00] only about preventing risk. It's also about finding most value for your organization.

And I think that's exactly the discussion that I also try to have. So it's. It's not just about preventing anything and taking a lot of measures so that all data is safe. Of course, that's my job, but it's also being, it's also about being able to actually run your business and to create value to deliver services for customers actually to do business.

Maybe, for example, in countries that might be a bit higher risk from a security perspective. But you could still earn money there and it's about taking the right decisions and that's what I really like about it.

So do you see a tension in the world of security between this, you know, the notion of protection and the notion of value creation?

I don't think there's not a lot of. People and decisions that take both perspectives into account. So I think a lot of [00:12:00] security experts that they're very, very good at risk management and having controls in place to prevent a lot of stuff. And I think it's, it really is shifting a bit also towards. Okay, how do we keep still create value with what we're doing as an organization?

And sometimes you might accept a certain risk if it really delivers something. And that's actually what I hope that I can change. So, and I think it's also all about the mix of people, of course. So I'm very happy to be surrounded by a lot of experts. And they know exactly what they're doing. They know exactly what the risks are, what the measures are that we have in place.

But I also think it requires a bit of a stretch to also see the other perspective and to also challenge that a bit, because we also have to move forward as an organization. We have to create value, but we also have to be ready for the future.

Can you match that with agile ways of working? Because it also sounds like, you know, you do have [00:13:00] to know what you're going to do and you have, you know, you have to be very aware of what type of risk are we getting there.

But before you know it, you're waterfall and you're making a lot of plans and what ifs, What do you see happening there?

Well, I personally really try actually to get focus also for the like the non standard topic by having a proper strategy and by setting the right priorities for the organization. So as an example, in our security strategy, we do have a what we call a foundation and there we have all the basic measures in place that we should have.

But on top of that, we also build, like, in preparation for newer technologies, like AI, indeed, or quantum technologies, these kind of things. And we do the same in the priorities that we set each year. So, of course, we have some basic priorities that you need to have as an organization, like the basic security stuff that you need to have in place.

But we also try to explore how we prepare for [00:14:00] topics that might come up in two or three years, um, and also start working on that actually. And I really try to have a bit of balance in there. So not only have the technology in there that we need now, but also make sure that we build it for the future.

And a nice example of that is, for example, of course, post post quantum crypto, what's happening there, it might not be a real risk. At the moment, but we know it's coming and I really try to push a topic like that. For example, that we already have it on in our priorities that we start working on it. Um, at least by creating like an inventory of what we have in the organization by also starting to build more expertise on these topics and by pushing it into the organization as well.

And the post quantum crypto one's really interesting. I was watching a presentation on the other day and he was um, from one of the organizations trying to create effective quantum [00:15:00] computing and the qubits are rising, right? So it's going to arrive pretty soon and we've seen some pretty big announcements about it in 2025.

Quantum safe crypto is available. There's open source libraries you can implement it, but the timeline for organizations to get that right through their systems is quite long. So you must start now because it's a 5 10 year journey to get everything sorted. So there is an answer to it, non factorial based encryption.

But you have to start now. And I think sometimes how do you, how do you convince people that the long range vision is required? Cause you're storing up the problem. Cause they're always in the here and now we'll fix the problem today. But actually this is big thing over the hill. It's about to come and hit us.

Yeah, I think it's, it's, it's a tough discussion, of course, but I really believe it's. How you tell your story and how you how you actually formulate your vision and your priorities for the organization and I really try to have focus on the new developments as well because I also see that people get really [00:16:00] motivated by it.

Because there's no one who doesn't want to work on Gen AI, for example, or post quantum crypto topics. Everyone wants to learn that. So I really also try to make sure that if we talk about security, it's not only about like the measures that you have to have, but also that we look a bit forward and people also start learning about these newer topics that get relevant.

Have you, um, started to update all your keychains yet, Rob, to be quantum safe?

Quantum safe. Our family's quantum safe, Dave. We're all right. It's just everything we interact with isn't quantum safe, so it doesn't matter. Because anywhere our data leaves the house, we're nobbled.

Yes, look at that. You'd be very proud of, uh, of Rob's password.

Password philosophy, Corence . It's quite impressive. It's not even that complicated. It's a different password for everything and it's like 12 plus characters. I mean, it sounds complicated. Unlike the rest of the pod team that uses the same 6 to 8 character [00:17:00] password for everything they use. I mean, I'm not saying I might be a bit more secure, but you know.

Are you saying Marcel's password of capital P podcast, 12345 exclamation mark is not secure? I don't know. That's over 12 characters. That isn't it. So you might get to a safe level. It's probably better than yours, Dave. More by luck than judgement, I think. Okay, let's move on then to the future of the world of cyber.

We've touched a little bit on quantum then, of course. The other big hill that's in the distance is AI. It wouldn't be a conversation these days without it. In fact, our brilliant sound wizard who makes us all sound good afterwards, literally sent a previous recording of us again. I think I've got the wrong recording here.

Cause you didn't mention AI once in it, but unfortunately we are going to talk AI in this. So, so, so tell me your view on AI and cyber current. So what are you seeing at the moment and how would you get started with something like that?

Well, [00:18:00] I'm trying to actually follow, you know, two things here. So. I'm trying to stimulate in the organization that we, uh, we work on it because the research shows there's a lot of potential for AI engineering and security as well.

And it could really save us billions. Uh, is that's really the expectation. And I, I strongly believe in that as well, because if you're looking at security for a large organization, we really get, well, millions of potential attacks. In a year, of course, and we have to decide of all these millions, what is real, what we should look into and whatnot.

So in order to be able to do that, you simply need this technology. That's what I believe, because you, yeah, you need to evolve there as well, because yeah, your analysts, they cannot keep up with that. So I really believe you need it there. But I also follow what's happening in the outside world. So I also follow a lot, but for example, hackers are doing with it.

And that's really [00:19:00] interesting to see as well, because you also see them evolving. So you also see them picking up new technology. So you can. You can really buy like deep fake technologies on the dark web, for example, it's just for sale there. So if you want to attack a bank, you can just buy these kinds of solutions for it now.

So I'm also very curious all of how that develops and how actually the people who I have to actually defend my organization against, how they change their approach and their tactics. So it's twofold and it, it needs. Yeah, it needs to be in balance. So I, I need to follow them. I need to step up myself and then hopefully I will still not be worse.

And what, what I love about, well, not love, it's not a good thing, but they've, um, the hackers, the defarious, um, actors in our world. Yeah, you know, I've, yeah, I've got a dark side. And the, um, uh, they've, they've basically Followed capitalism and monetize the hacking. Now [00:20:00] they used to do the old I'll ransomware you and get money out of you.

And now they're just flogging their solution to people who can do that themselves. So they've kind of like productized their thing and it's the level of maturity that's rising in that world, but it does show you the sophistication. We need to track it closely because you know, they're just behind or maybe just ahead.

And it's a, it is an arms race from that perspective.

They really have created some very interesting business models. That's what fascinates me. So it's for ransomware, for example, that there are really good business models behind it. That's if they ask for a ransom and you pay and they're so professional and actually trustworthy.

Yeah. And indeed also for, yeah. If you want to become a hacker, there's a lot of solutions available, but you can just buy and it, yeah.

I mean, it's so professional how they actually approach that. Yeah. It's almost like a hacker marketplace. Yeah, there is. Yeah. Okay. I mean, that is amazing. Isn't it?

Maybe we're [00:21:00] in the wrong business, Dave.

Maybe this is the new thing because we're, we're, we're professionals. We create, you know, professional interactions. We just have to do it for hacking as opposed to, you know. Yeah.

But the thing is,

so I'm constantly trying to think of, okay, so what's, what's happening in the outside world and how is this developing and what does that actually then mean for me and for being a bank in, in this kind of environments?

And that's why I think. I want to move, of course, because I really believe that there's a lot of potential in it, but we also have to move because we don't want to be the slowest organization here. And then that actually could make you very vulnerable.

As you've transitioned from the world of data and analytics into the world of.

Cyber. Obviously there is something in common here and you've already touched on it, which is like masses and masses and massive masses of potentially unstructured data that you have to wean through. So I wonder what your personal view of that is having a background in data when you look at the challenges of cyber [00:22:00] and whether you, whether you observe any differences between some like a traditional CISO who's come up the infrastructural and security route.

Whether that kind of manifests itself in a, in a, in a different way around decision making and use of data and things like that,

I think I will leave different as a leader because. I strongly believe in collaboration and that you really need the mix of skills to succeed. And of course, I lean a lot on the security experts that I have in my teams, but I also still lean, of course, on my former analytics colleagues, because we also need them.

And I still need them to be successful, actually, as a, um, as a CISO for a bank as well, because the basic security experts, they're really good at their job, but it's also a different skill to be able to handle these amounts of data and actually to build models on that and to, to work with it. And that's what I [00:23:00] really like, because if these worlds really come together.

Then, yeah, you can take massive steps there and then you can really actually see what's happening in your organization and how to respond to that.

Has that act of collaboration and the different way of executing security leadership felt different for the rest of the organization, do you think?

I really believe so.

So what I hear from my own teams is that they get more respect because we really focus on collaboration and not on only saying, okay, this is what you need to do, but we really also built a relation and explain why certain topics are important. So that it's also about the relation and the collaboration actually to do it together because yeah, we can also not do it on our own.

And because of that, you get respected and people listen to you. And I think that makes a big difference if you have to keep a bank secure, because imagine this, I, [00:24:00] there's over a thousand spots that need to implement security measures. Yeah, if they respect you, and if they listen to you, the job is much easier than if you just try to force your, your, your work into their backlogs.

Yeah, it's a very, it's a very different way of, of executing it, isn't it? And I suspect there are other upsides to that. Like one of the things that security I think this is still true, but you know, correct me if I'm wrong here, there is often a frustration from the security communities and organizations because they're left out of the decision making process and the go live conversation.

But perhaps if you're kind of more open and collaborative, does that help ease that issue? I wonder.

I strongly believe that. And I think at the moment by just being there and telling a good story, why certain things are important and making sure that you do it, of course, in the proper language, I think our board members and our CEO, they really [00:25:00] understand the importance of security.

They, they always mention it in their top priority. So next to having business priorities, the security is always there. And. I think it really feels different in how you get things done because people just respect it and it's kind of normal that teams spent about 10 percent of their backlogs on security measures because they, they know it's important.

Everyone agrees to that. I think it's a lot from years ago, right? That's, that's a huge difference compared to five or 10 years ago.

And there's still a thing I'm still surprised when we go into sessions around major change and I often ask where security and then there's always this sort of shuffling of, you know, noise in the background and they go, well, we didn't invite them and you go the first people you invite to anything where you're doing major changes, get security people in the room.

So they're there day one. And rather than tell you, Okay. Uh, you know, get surprised by it. They're steering you correctly in the right way from the very [00:26:00] beginning. So you don't have any regret associated with what you're trying to do, but it's still this thing. People forget to invite security. And then when you say it, they sort of, you know, go, okay, then the type thing.

And then, but it's that learning experience that when they're in the camp day one, it gets a lot easier. Like you say, Rob, I also learned to invite myself. That's the thing. Ah, you just turn up and go, it's me, I'm here. Yeah.

But people just, They respect that. And that's the good thing, of course. So, yeah, it doesn't matter actually that who in the organization, but they always take you serious.

And that's, of course, what I have to be very good at explaining them to everyone. Okay. Why is this important? And what am I expecting from you?

I like the way you're expressing the sort of the different stance of security. I wonder what kind of journey the rest of your team had to go on. Like, were they, were they used to working in a slightly more authoritarian version of security previously, like a, an enforcement and [00:27:00] checking type environment versus what you're now trying to establish?

Well, to be, to be, to be honest about that. We had to get used to each other. So when I stepped in, people were also looking at me like, okay, so you are the new CISO. Um, but tell me what you know about security.

The thing is that that's actually that, that, that did happen. And, um. Of course, I really, I studied a lot as well to actually get certain certifications and to really prove that I have the right knowledge to do this as well.

But I also stress that my skills are different than the basic security skills, and I really believe that you need both. So what we talk about, like a focus on collaboration and how to get things done in a big organization, I strongly believe in the mix. But it took a while before people really felt that, of course, in their work as well.[00:28:00]

So it's really about getting to know each other and giving it time actually to evolve in that. Because I do, yeah, I'm, I'm a very different leader, I think, than, than different CISOs or also

how the Rabobank has been steered before. Because I know where I'm going to, and I also know how I want to get there, but I also really steer on a lot of autonomy in all the teams.

So it's also up to them to actually, yeah, they have the expertise to take the decisions.

I wonder what it was like for you personally. to go on that journey. I was also fortunate enough in my dim and distant past to be a sea surfer a relatively short period of time, about 18 months in a, in an FMCG. The world is hugely different to the experience I had, but I know when I went on that journey.

There's a tangibly different culture attached to it and at the time, I'm sure you have the same thing, like digital security was connected to, [00:29:00] uh, sort of physical security and I sort of had the opportunity to sort of delve into the world of physical security for a period of time and that's a wholly different game.

So I wonder what that personal journey has been like for you.

Well, there have always also been moments that I was, well, I really didn't know what to do, of course, because it also took me a while to get up to speed. So it definitely has been, it has been tough as well, because I also had to learn a lot of the technology behind it and the contents.

And what scared me most is when the first incident happens, because as soon as you get called as a CISO, then of course, that's the point where all your people say, okay, we don't know anymore. So there have been some especially scary moments. Uh, in my first months, because there's a few things that it's just the first time then, and then, then you have to decide.

But I think by now, after doing [00:30:00] it for about one and a half year, yeah, I'm, I'm much more comfortable and it's not that I know all the details, but I really, I think I know how to take decisions. I know what the expertise is that I have. in the teams. And that's, that's the point of comfort. I think that you have to grow towards, of course, that's, yeah, you know, what's possible.

What's not possible. You know, when you have to take a certain decision because the teams might simply not know, or when the organization needs something. But it took me quite some time because when I was working in data analytics and I was working with data scientists, for example, I thought that I learned how to work with experts.

But then I became a CISO. And then I realized there's a whole different world of experts.

Yeah. And experts come in lots of different shapes and sizes.

Yeah. And yeah, I really had to get into that as well. And it's not just only, of course, the content and the knowledge, but it's also about just how people behave, you know, [00:31:00] in the office or yeah, how things are done and.

Uh, that also took a lot of time, of course, to, yeah, to build relations again, to get into, uh, really in the dynamics of the teams, et cetera. So, yeah, I've definitely been scared, uh, yeah, because there's times where I really didn't know what was happening or what was the best thing. But now I think it's, it's such a relevant job and it gets more and more difficult and there's definitely a lot of challenges in it.

But I can also explain. For the first time, for example, to my daughter, what I'm actually doing for a job and I don't have any fake job in a bank. And yeah, you know, my daughter's, yeah, she does things. Okay. A bank is like a couch. Yeah. So there's something where you sit on, but now, you know, yeah, it's also relevant what you do and people really understand it.

And it's also, yeah, the news these days, it's very exciting. So it's a very [00:32:00] exciting role to work in as well.

Maybe just to bring our conversation to a bit of a close, what reflections you've got on it and maybe thinking about how your. measuring success and whether, whether you've brought anything new in terms of how you're measuring cyber success.

I think we, we have a very solid set of KPIs, of course, but what I would say really works for me now. And what I'm proud of is that we're looking into these topics for the full. So that means that we, we have a lot of different labels, so we have a lot of subsidiary or for example, as well, we really do as well for everyone and not just only like a part of the organization in the Netherlands or so we really have a focus on the full organization.

So that all the security topics there and that really goes back to also collaborating with this part of the [00:33:00] organization that might need your help. The most because they're smaller and they might not be that mature. And what I also really learned is the topic about collaboration. And that's, of course, not what you really measure.

But I do believe that in the basic security measures that you have in an organization, we see a constant growth now. And that is because of this. So a lot of our metrics, they, they, yeah, they steadily move up and yeah, behind that is of course, that people understand why they're doing it, that they know what to do, why it's relevant and they commit to it.

This week, I want to talk about user adoption in a multi change environment. Because, uh, we know all those teams that create beautiful products. They do have UXers in teams. Well, that that's already [00:34:00] a level of maturity that at least you see increasing, but then they all look at that same and one application or product that they're responsible for.

But as an end user, I usually have to, you know, Work my way around with all these different applications. So how do you actually get into a flow as an end user with all these different applications? That's still something that fascinates me very much. And I think it's the same with cybersecurity, right?

We have these security tests. We have simulation phishing emails. You know, that our security team is trying to, uh, to provide us a test in a real life situation, just to see if in the pace of everyday life, are you able to pinpoint that phishing email? I think that's a great example, at least, um, for me as an end user, if you get into that flow and you also have different types of security tools and programs, and we have all these different types of, [00:35:00] uh, technologies.

How do we make sure that you do not get fatigue in all these tools? Because that also influences, I think, your level of being aware. Is this actually some, is this phishing, is this et cetera? So if it's very overwhelming, how do you make sure that you get that level of, uh, awareness for end users as well?

And I was very curious about the thoughts of Corentz on this topic.

Oh, that's a tough question. That's why she gets her own segment. Yeah.

To ask the most difficult question at the end. Well, for my role, what I try to focus on is really integrates getting attention where these topics into like the daily activities of users or in my case, colleagues in the organization. Um, so we tried to focus on not making it really like feeling like an extra or a lot of trainings, but it's really about all these very small moments [00:36:00] where we try to focus on these topics and try to, to learn our colleagues something.

And this, this fishing, I think is a very nice example, of course. So. We send them phishing emails on a continuous basis and we monitor and then we help colleagues with how they respond to that and not by giving them like an extensive training of day, but it could be like a five or 10 minutes where you can just pinpoint.

Okay, this is what you could have checked or this is what you could have done differently. And you might also be interested in this. So to me, it's really about you. Yeah, making sure that it's a small thing, how they can actually participate and try to find a creative approach for this.

There's a wider societal issue here, which is as a society, if you look at the education system, we don't actually educate people about digital or cyber.

And it's not, it's not even like. I'm not saying you have this massive curriculum you have to take, but it's just those little nudges throughout your life, from your [00:37:00] early days, where you just have those moments and those interventions where you can say, oh yeah, okay, I get that, I understand that. And it slowly builds over time, doesn't it?

This awareness. Whereas actually, we tend to take cyber security training very transactionally, and then you get a big star at the end saying, you've completed your cyber security training! You are secure! Tick, audit, you know, audit complete, checkbox, uh, achieve. And it's not that, is it? It's this constant awareness that has to build up in you all.

Your mind's eye about what to click, what not to click, what to be aware of, because it will come from the, you know, the most unassuming places at times. I do think as a society, we need to reboot the way we think about this stuff, especially education and digital. It's just not there yet. And I'm thinking we're going to fall foul eventually and have to sort of retrofit a load of stuff.

But yeah, there's, I think there's a big bit there that we need to think about more as a You know, a collective, the thing within all of that, which I agree with that I, I mean, it is genuinely difficult is to spot the different types of attack, like [00:38:00] embedded links, for example, in your Twitter feed that may well be as dangerous as an embedded link on a phishing email, but may appear relatively innocuous because it just looks like a photograph on a pretty standard.

you know, tweet, for example, it's that aspect of the awareness is something that I think just changes so fast.

Yeah. There's loads on Twitter where they mock up reputable news organizations and put some massively sort of salacious story that you think, you know, and you go, Oh, that story's not true, you know, but then they want you to click it and it takes you off.So some literally the example I was thinking of that is literally the example of thinking it's like, it's something like Holly Willoughby's career collapses in because of off the cuff comment on, you know, good morning Britain or something ike that. Something like that. And it's the, uh, um, and I think, I think there, um, you get, and it's that you can be weak, you can be tired, you know, you could have had a hard day and your thumb accidentally lands on it and that's it.

You're done. Becoming so realistic. It's not that, [00:39:00] it's not that like, Oh, you've won a hundred thousand euros somewhere in another part of the country. And then that was the first, you know, attempt of luring us all in. But now it's so real. It's harder and harder to really grasp

the bad ones. It looks perfect nowadays.That's the difficulty because of technology. It looks perfect. Yeah.

I have, I have rose tinted glasses for the past where a rich prince from some far flung nation needs my bank details to transfer 50 million pounds in. So, and then he wants to share it with me. I miss that. Those days, those were fun days of security.

You know what I do enjoy now though, is when you get one of those calls that tells you you owe tax or something like that. Oh yeah. Oh yeah. It's so patently. Not HMRC. And I just enjoy talking to them. I try and keep them on for as long as possible.

I actually know an example of a boardroom member that also got the email that your camera was on when you were [00:40:00] watching, uh, certain types of videos.

And then they opened up the entire conversation in the boardroom. Like, guys, I have to admit this. I actually did it. And then. Well, two days later, then they, yeah, that was so painful. That's embarrassing. But it's also, you know, created a bond because they all shared like, Oh, that could have been me.

That's bad life choices right there isn't it? I mean, there's lots of questions in that example that we don't have time to explore. It's a whole different podcast.

Well, look, uh, Corence , thank you so much for spending some time with us this Friday morning. It's been a real pleasure to get your different and very refreshing perspective on cyber.

Thank you.

Now, we end every episode of this podcast by asking our guests what they're excited about doing next. And that could be, you have got a restaurant book that you're looking forward to at the weekend, or it could be something in your professional life.

So, Corence . What are you excited about doing next?

Well, I'm gonna head off to pick up my daughter with my [00:41:00] parents because she had a holiday the whole week and she was staying with my parents. So I'm really looking forward to that. So we, at least we have like a half day to enter a holiday together.

Oh, how nice. How nice. Have you got any plans? Are you just going to chill out? We're going to the swimming pool and it's disco night. So, um, Oh, great

memories. Yeah. In the UK. This is not connected to, unfortunately, anything as cool as a, as a disco swimming pool, but it is still good in the UK. There's a restaurant called the Hawksmo, a steak, steak restaurant.

And they have created the 20 pound big Mac. What's there like a gourmet version of the big Mac. That's what I'm looking forward to at the weekend. I just thought going to try. Yeah, I'm going to try it. And you're on your own. Yeah.

Looking forward to that. You'll have to, you'll have to send a picture of that Dave, I'm, I'm now, I didn't know about this and I'm now extremely interested in this experience.

You've, you've drawn me in. You've, I've, I've been seeing it. See, I thought it was [00:42:00] worth mentioning. We don't normally do our own, but this one is so powerful that I thought I'd share it. What motivates us, eh? But the, uh, yeah, no, that sounds, that sounds nice.

It sounds like high potential, doesn't it? I will send a picture.

I will send a picture. Don't build it up too much in your mind, just in case there is a little bit of disappointment in it, and then it'll ruin the experience. I did

see like, um, food influencer type person on Insta trying an actual Big Mac against it. And all I'm gonna say is, it was high prez. It was high prez.

Yeah. And there weren't paid advertisement. That's the other thing, isn't it? Influences now paid. And then they go, this is amazing. And you go, how much did they give you? It's a scam. It's a scam.

That's what I was thinking, what we just spoke about. You know what happens online, right?

Yeah, Dave's just fallen foul of the entire, have you listened? Did you listen? Were you involved in the podcast we just had, Dave? I'm sorry, I'm just a bit confused. It's just a prince covered in meat. Oh, on [00:43:00] that note, dig us out as if you would like to discuss any of the issues on this week's show and how they might impact you and your business, please get in touch with us at cloudrealities@capgemini.com. We're all on LinkedIn. We'd love to hear from you. So feel free to connect and DM if you have any questions for the show to tackle. And of course, please rate and subscribe to our podcast. It really helps us improve the show. A huge thanks to Corence, our sound and editing wizards, Ben and Louie, our producer, Marcel.

Thank you for not making any weird sounds this episode. And of course, Of course, to all our listeners, see you in another reality next [00:44:00] week.

## About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the future you want | www.capgemini.com



Capgemini