Capgemini

CR046

The Cyber conversation Boards should be having, but probably aren't with Simon Hodgkinson

CR046

The Cyber conversation Boards should be having, but probably aren't with Simon Hodgkinson

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

[00:00:00] Describe the problem in the security industry, Dave, everybody's worrying about AI and securing AI at the moment when the, the back door is wide open because they're not doing the kind of basics.

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 this week we're going to be. Talking about the ever important conversation that goes on around the world of cyber.

It's got more and more complex over the last few years, but maybe the basics are still the important thing that we need to focus on. So this week we're going to talk about the conversation that boards are having around cyber and maybe some suggestions on. A wider conversation that they could have if they're not already having it, [00:01:00] but before we get to that,

I was walking into the office the other day and Rob was just finishing a human beat box, heavy version of Hark! The Herald Angels Sing in the foyer, caroling away and he was waving madly trying to get my attention and I was walking past trying not to make eye contact with him, but eventually he managed to drag me over and of course I was like, Rob, what's confusing you this week?

I must say, Dave, you've You've raised the bar with that one. Well done. as I was singing, I was confused about Bluetooth and where it's going to go next. I'll tell you why it is remaining. It's almost 30 years old. Bluetooth 1994. It got created. So it's been going for a long old time, right? It's still one of the most frustrating and unreliable things you have to suffer in your life.

Okay. And also you see Apple and Samsung and Google put in proprietary logic into their Bluetooth system. So if you buy. Their phone and get their Bluetooth earbuds. They pair really well. However, if you try and cross pair them, it all goes [00:02:00] horribly wrong. And we've lived with Bluetooth for far too long.

So I'm confused about what's going to happen next. So we've seen proprietary divergence when normally you want convergence of that. And it remains, one earbud connected, but not the other. Oh, it's not connecting. Turn it off and on again. This 30 years we've been doing this and it's not got better.

Maybe I've under thought this important subject that you raised this morning, but it seems to work okay for me. Maybe though, Rob, maybe the issue is I've chosen. a closed mobile system to use, which just works. And you've maybe gone for a open, slightly a buggier system that maybe doesn't just work every time.

If you get into the Android, Apple, iPhone type debate, David, I'm going to just no, don't do it. But it is, we've been going 19, I checked it 1999. The first time Bluetooth headphones came out 24 years later, they still don't work properly. And I'm like what next? Is it even secure? I know.

I don't even get started on that. But yeah, it's like this [00:03:00] panacea. When it came, it launched. Massive fanfare. This is going to, revolutionize your tech experience. 30 years later, I'm still swearing at Bluetooth headsets. I, this is one like normally when you do your confusion subject. This is more rage.

I'm more, more frustrated. This is the sky stuff. I reckon like Bluetooth works pretty well. That's where I'm going with this. Yes, there's the odd, there's the odd little quirk. Sometimes

when you get a renter car and you're trying to connect your phone to play music, that can be a little bit of a mess about, but that's generally because of the interface in the car.

Hang on. You actually materially failed to be able to connect to your phone in Vegas. So that's a perfect example of where that's a Bluetooth fail. I would say that was more the the car's interface than the, and my ability to work. Blame everything else other than your Apple ecosystem.

Well done you. Let's leave it there, shall we? I'm not sure we're ever going to resolve that one because I think most of the world think Bluetooth is broadly all right. I think you should go back to your caroling, Rob. [00:04:00] Probably a good idea. So look, let's move on to today's major subject then.

Joining us this week, I'm delighted to say is Simon Hodgkinson, the former CISO at BP and now strategic advisor to a number of boards. And also old friend of mine, we worked together back in the days of BP. Simon, great to see you. Thanks so much for joining us today. Do you want to tell us a little bit about yourself?

Yeah, thanks, Dave. Really appreciate the invite, actually looking forward to the conversation. Yeah, so 30, 38 years now in technology, been doing cyber and cyber security predominantly for the last eight to 10 years. And prior to that, worked for various different industries, including software and financial services before joining oil and gas.

So Simon, why don't we start by just getting a sense of your history? Tell us where you started off in your career and then how you ended up in the world of the CISO. Yeah, perfect. So interestingly enough, I do talks for schools trying to encourage people [00:05:00] into sort of STEM careers and what have you.

And I always start by saying I started my career in the cloud. And that was in 1985 because what we were doing was selling compute on mainframes to companies. And it was just like exactly like the cloud is today. So I started out on mainframes. I used to be the guy that was trying to debug programs on punch cards.

I know I don't look that old, but I am, I was just in the late sixties, maybe 68, 69, I'm I'm envisaging, like those old videos of the moon launch and stuff like that. Yeah. Did you wear a white coat with pens in the top? No, we didn't have to punch cards was a thing and you'd get like a thousand punch cards and put them through the processor and one would be wrong.

And you then have to try and debug and actually get a little clipper and and amend it and get little sticky tape to put over the holes that were wrong. Did you ever witness massive comedy moment in computing when the punch cards [00:06:00] go in the air and all fall out of order? That's because that's just like the ultimate what moments.

Yeah, absolutely. But the other thing I say to them is actually I showed them a picture of the computer room. It actually wasn't our computer room, but it was a very similar one. And say that, your phone has got 18, 000 times the compute power. That entire room had in it, which was like the size of a football pitch.

So yeah, I started back then Dave and it was in the very early days of open systems. So we had this little they had this box turn up into the, in, in the computer room and everyone looked at it and I thought let's just open it up and and have a play. And it was Unix. And it was BSD 4. 2 Unix in the really early days.

So I got into Unix then and into early versions of relational database. So Ingress for, if people can remember that the name Ingress and I joined Ingress in early nineties. [00:07:00] And got into big time into relational databases. That sounds quite sad actually. But yeah Dinner party

conversation 101.

Let's talk about acid principles and then i'll move to cybase, Went on from Sybase to Lehman Brothers and worked for Lehman for four years doing database and Unix. And got into leading the team at that point. In 2000 uh, I got tempted out of Lehman, probably a good thing in the long run.

Yeah. Got a lot of that. Exactly. To do a dot com and we built a fixed income electronic brokerage platform. And it was it was a really elegant solution in very early days of Java and that. It was a really lovely solution. The trouble was nobody wanted it. Was it ahead of its time?

It was. So fixed income brokers always did their deals over several bottles of wine and a really expensive lunch. What they didn't want was the the electronic. [00:08:00] Exactly. Yeah. So I think we got that a little bit wrong and the financial markets in 2002 were horrible. So shut that down.

And then I joined BP. And I always remember when it was an old boss of mine that encouraged me to go over and I said, I don't want to go to an oil and gas company, like dirty industry. I've been in tech. I've been in financial services, done a. com, failed by the way, but I've done a. com and he said no, come on, come and have a look.

And I didn't realize BP at that point had the largest commodities trading function in the world. So it was just like walking in. To an investment bank, except that they hadn't invested much in technology at that point. They wanted somebody to come in and run infrastructure for them, build their first data center, which was the, you would lovingly remember as a southeast hall in in global switch.

Yeah, I've had, I had nine jobs at [00:09:00] BP and the last two I ran Global Infrastructure and Ops. We called it INIS then. And then when Daniel Barriuso who was the CISO, great guy, resigned, I had a, almost a sort of guttural reaction to, I want to do that job. So I went to, went and asked if I could do the job on the expectation, I would take it on as well as doing the infrastructure role.

And they said no, you can go for it, but you'd have to give up the infrastructure role. So I went down the CISO route and absolutely loved it. for four years, but it's exhausting. That maybe brings us onto the, over that same time period, perhaps like the evolution of cyber itself. Like I was actually, I'm not sure we ever talked about this in the past.

I was a CISO for BAT back in the early 2000s, like 2001, 2002 sort of period of time. And at the time you, I was double tracking that role with with a head of infrastructure role and. It was very parameterized and we spent a lot of time, working with group security and we thought about it in much [00:10:00] more controlled and physical terms.

And I think it's fair to say over the course of the last 20 years, your ability to manage it security in that way is completely vanished. You got the. When cloud didn't exist, everything could be in a walled garden estate and you could always sort of a lot of people focused on the perimeter.

We've learned that perimeter defenses aren't always the best. They're a good thing in your bailiwick. That whole big walled garden getting smashed open by cloud completely changed it all, didn't it? So you used to be able to put your arms around it, touch it, feel it, see it. Excellent. I can quantify the problem easily versus the new world, which is compute is everywhere and highly distributed.

How do you manage that? Then your edge and everything else has made the problem

dramatically worse or harder. I should say, I agree with you. And I think like most things in life, it's a people problem as well. So if you go back to those early days when you were see, so Dave, actually, there was a lot of control points in the system and actually the volume of change [00:11:00] in I.

T. Was dramatically lower. So you could actually be involved and put sort of human controls around things. Now, the sort of pace of delivery is so quick that model no longer works. You can't have somebody at the end of a project with a checklist going, Oh, hang on, you haven't done this or you've got this medium vulnerability that we're saying you can't go live with.

Those days are gone. And yet there's still a lot of people in the industry and a lot of companies that are still making money off that kind of old school security model. Yeah, so, so I think that it's one of the biggest changes. It's a technology change, but it's also just the way everybody does digital now.

It's, everybody does right. In your mind, if the old model is this perimeter controlled checkpoint at the end framework for security, how are you conceptualizing what the current environment looks like in terms of if you're a [00:12:00] CSO today, how would you be envisaging how you would get your arms around what's going on?

So a couple of things. I think first you have to completely change the thought process to, we use the whole castle and moat, that terminology is used quite a lot about the old world. Okay. But actually now it's about identity and data. So that's what you've got to protect ultimately is the identity and data.

And people talk about zero trust and too many people talk about zero trust being a product. It's not as a design principle, but at the very heart of zero trust, you can have all the segmentation you want in the world, but if you have got, have you got no integrity or availability of your identity.

Nothing works. So I think you've got to really focus on those things that are really important to protecting those core assets, which is like I said, identity and protecting the data. I also think that automation is absolutely critical. So now if you think about those. [00:13:00] Waterfall days when people would run a project and you get security to come in at the end and do their bits and bobs and then tell you couldn't go live and then you'd have an argument and then somebody would make a sensible decision or a pragmatic decision on when you could go live if you did X, Y and Z.

You're doing drops multiple times a day now. So that has got to be completely instrumented through the software delivery life cycle. Completely instrumented on having control points in that along the way. And part of that is also embedding security in everything that you do. As a business.

Everything that you do as a business. So it's not this thing that sits on the side ticking boxes. It's embedded in the decision making on mergers and acquisitions, the decision making on things like new country entry, your developers become security experts as well. So you embed, knowledge and capability in the development community, because frankly, there's not enough security [00:14:00] people now to, add to every single products that you're delivering.

So you've got to find ways of embedding security in every aspect of the business, in my view. And what's your view on the scale of the risk change as well? So hacking continues to grow. You heard yesterday, nation states calling out other nation states for saying you're hacking us. Stop. We know what you do in type thing.

There's this ever increasing. Threat seems to be more pervasive everywhere. Everybody's having a go. That appears to have piled on a lot of pressure as well. Never have you have we ever been so intensely thinking about securing our systems and the dodgy actors out there trying to get control of the data?

Yeah, I think that the attack surface just rose and it grows because Digital world is getting bigger, right? What business do you know can [00:15:00] survive without their technology platforms for a month?

It's just it's beyond comprehension that will be the end of most businesses as we know no bcp plans in my view can last for a month without the digital platforms that underpin them so i think companies need to really reflect on the sort of geopolitical challenges that you brought up there rob and i know when i'll give you an example when there were trade sanctions turned up in the middle east guess what.

The attacks increased and the attacks often come from proxies for government that are criminal gangs. They're frankly funded by the state. I think everybody would would say that's true of things like Russia. If nothing else they're prepared to harbor those people in there.

So I think that, that's an example where why are they, why do you see that increase? Frankly, if you. If you cut off the flow of money through one route, guess what, they're going to go to [00:16:00] the criminal world to try and fund those economies. And so you can see there's that sort of state and criminal sort of activity that's driven by the whole geopolitical world.

I think the other thing that's occurring as well is there is more nation state activity because you can hide behind it. And a nation state activity, uh, you've seen some recently, the attack on the power stations in Ukraine, for instance, is that an act of war? thEre's no Geneva Convention for cyber.

There is in the physical world, but there isn't for cyber, but actually one might argue an attack on critical national infrastructure is is a war, is a trigger for a kinetic effect. The one I always remember was Stuxnet in the enrichment facilities, incredibly sophisticated, took offline enrichment.

Very effectively and destroyed some very complicated engineering and, they [00:17:00] didn't really recover properly, but that was an example of one nation state going another to take something that they didn't like the other nation found extremely critical and was, progressing a very intense geopolitical conversation about.

Yeah, absolutely. Stuxnet there's a great book on Stuxnet as well. It's really, it's a really fascinating fascinating case. And it just shows that the, how, that was a brilliant piece of malicious software. You've got to take your hat off to the people that know that whoever did it was very talented.

Yes. Very talented blackhead off. You mean they didn't destroy it. That, that was the interesting thing is they didn't destroy it. What they wanted to do is just slow down the centrifuges. So actually it it reduced the pace at which they could enrich. And actually if things just shut down, people would do a root cause analysis and try and figure out what it was, but actually it's much smarter.

To do things over a long time at a slow pace. Isn't there [00:18:00] also another pernicious attack surface, particularly with things like Gen AI, which is in the data itself? Exactly the same philosophy. Yeah. Which is just slightly tweak the data to drive the decision making just mildly off course. It doesn't have to be radically off course, does it?

No. And it's interesting those models as you train the data. It was that classic example is it

Microsoft released something in in, I think they released it initially somewhere in the far East and and the model worked really well and then they released it in the Americas and, people deliberately poisoned.

Yeah. It's like, how can we corrupt this? There's somebody always having to go, isn't there? Yeah. And it became racist at that point, but it wasn't because culturally people didn't do that in one area in the U S it did. And this model became became racist in the end. And it's just so there was a very early days example of.

how you can manipulate the data to change the change the outcomes. So it sounds like there's a number of different [00:19:00] things that are changing the game here very radically and it's accelerating. So obviously you've got the increasing sophistication and volume of attack. You have got.

a radically different technology landscape with, wholly automated processes being built into it. That's changing the game in terms of the day to day security process. And then you've got the ever increasing reliance of organizations on technology. To your point, most organizations could not withstand these days, extended periods of being cut off from their technology.

So radically different set of dynamics. Tell us a little bit then about the day to day change in the CISO role itself. So when I did my role, I reported to the CIO, the CISO conversation and the security conversation was almost like an AOB on the ITLT conversation. And it was like, security is all good then Dave?

We're like yep. We're all good. We've just patched, we've patched again. It's all fine. Thanks very much, [00:20:00] lads. Quite a different conversation today, I'm guessing. Absolutely. And there's just a couple of other areas just to flesh out the totality of it. Before I get into that question, Dave, the whole geopolitical situation that we were just, Rob and I were just talking about actually manifests itself in regulatory changes as well.

So if you look at the world in the early 2000s was all about creating this massive global economy with no. boundaries. Today, it's all balkanization. It's all countries described, declaring sort of an isolationism position on, you can only store our data in our country.

And that's making the digital world that much more difficult and the CISO job that much more difficult as well. And the final bit is the operational technology. People often forget about the fact that all of your rigs, your refineries, your manufacturing plants, they're all run by technology. And and there's this sort of, [00:21:00] there's this almost this cultural divide between the engineering community and the cyber community.

And they need to come together to secure those critical assets. And the reason I link that into the geopolitics side is because very recently there's been a number of breaches of water treatment plans. Now, if you want to create. Civil unrest in the country, the thing to go after is drinking water, so you know, you've got to be thinking about all aspects from a security perspective as well.

And the final bit then would be actually this notion of like we talk about physical and logical security. The two things are interlinked with things like insider threat. And with terrorism and what have you. So the, CISO is so broad. So that, my, and I'm, I've been at the corporate role now for three years at the end of December, which is remarkable, but I do get, I do have the privilege of working [00:22:00] with some brilliant people in the security industry still, and.

The conversations that happen now are so broad. Like I said, everything from sitting around

the CEO's table talking about mergers and acquisitions to new country entry you've got to be really thoughtful about the security implications based on the geopolitical situation of Going into new countries.

So you're talking about from talking at very high level business strategy, you've got to understand the regulatory implications of the different environments you're going in, or, from a say China perspective, China's still a massive growth opportunity for most organizations, but.

You've got to be really thoughtful about how you position yourself from a cyber perspective as you go into that country. So that's really interesting. Then you get all the way down to, actually, have you patched everything? Microsoft we've just [00:23:00] seen, yeah, and you'll be going.

And so CISO now is just just so broad. And I think that's where Again, this is where technology can really help by just assimilating all of this data that you've got across the organization and producing meaningful insights into what you need to go after next, which is the next mold you've got to whack.

Is the role now, has it evolved to routinely be at least organizational? Leadership team or CEO report role, or are you still seeing it being typically being a CIO report role? Unfortunately, I think it's never a simple answer to this, but most of the time it's still into the technology function.

I see one of my leaving gifts at BP was to get it raised as a peer of the the CDO, the chief digital officers and the CIOs, et cetera, because I think it should be at that level. [00:24:00] What I do see, however, is a lot of the people that certainly in the bigger FTSE 100 or S& P, top S& P and what have you, the CISO gets a direct line to the CFO, CEO and the board.

There's, most organizations don't, the CIO. Doesn't put himself in the middle of that. And I was blessed at BP that, I had a direct line into the CFO. I had a direct line into the CEO and and the board, and it was never, even though I reported to the CIO at that point, it never got in the way.

So I think there's that human behavior thing. And there's also the positive side of being part of the CIO organization is you get to see everything that's happening from a digital perspective. maYbe you get less visibility from the business side, and I think the CSO role is more about kind of business and operational risk now than just the technology role.

I think it's much broader than just technology. You can't disconnect again your business. You got the merger of IT and OT, and I [00:25:00] absolutely agree with the engineering thought pattern around OT is very different from security perspective to IT. So you got that. Merger and coming together. And then you've got the business inextricably linked to technology.

Your business is technology over that. And so all the factors that affect all those three things come together in one big melee in the middle, isn't it? So you've got this increased complexity and then you've got to apply technology to the problem. Otherwise, you're just gonna top out, aren't you? With just too much to deal with.

Yeah. Yeah. And that that's situation reporting that almost real time sit situation reporting is so important now. I don't know a single person. I certainly could never have put my hand on my heart and say we've got everything landed in BP. And I don't think there's a CSO in the world that could say At any point in time, have they patched every vulnerability that's out there?

Is there any internet facing assets that they don't know about? Do they know everything

that's going on in their organization? With the democratization of digital [00:26:00] now, I think that's almost nigh on impossible. You're always gonna be behind the curve. Yeah. It also sounds like a very huge responsibility.

This role. It is a huge responsibility and it comes into that that the issues that have come up recently around the Joe Sullivans of the world. So Joe was CISO at at Uber and was indicted and convicted actually of allegedly. I guess it's not allegedly given he was convicted, but of actually, covering up a data breach.

But what was your interest in there was the CEO not indicted at all. And yet as all the reports I've read, whether they're accurate or not, you have to take everything with a pinch of salt, but everything I've read suggests that. The ceo knew what was going on. So so, so on top of that broad church of Accountabilities you've now got the regulators stepping in And taking criminal cases you then had tim timothy brown from [00:27:00] solarwinds at the end of october Again indicted and what's really interesting about timothy brown's is they've gone back to say that, frankly He wasn't doing enough about, he was overstating the security position of the company, um, misrepresenting their ability to deal with cyber attacks.

And that's a really difficult thing to do. Failing to apply adequate security controls was that misrepresenting the security stance of an organization to say investors and is that what the situation that I mean, that's an amazing microcosm example of the magnitude of change of accountability around the sea.

Isn't it? It absolutely is. And it makes a job pretty pretty concerning if you were a CISO now, people talk about, you've got to have directors and officers insurance and it's great, but that doesn't protect you from criminal liability. That will cover your legal [00:28:00] expenses.

But frankly, I would be less worried about my legal expenses and being banged up in a prison for getting something wrong. So there's that thing though, which they do with pilots in the airline industry that if you declare something in time in the right way after it's happened, the pilots protected as long as they haven't had gross.

misconduct. And what that's allowed to do is the aviation industry has become open and transparent. So it's an open solution and they constantly improve off the back of those learnings as opposed to closed systems, which is where, medical is a good example where things might be covered up in that industry.

There's good cases of that and a different approach to how the CSO role can be discharged legally because. Who's going to want to do the job if you sat on top of an organization, you may not have complete control over a lot of politics in play. You may not have the funding that you need, and yet you can go to jail for something your organization does.

So it's like a maybe there's a regulatory and legislative position that needs to change to allow the see so to be able to discharge the role. [00:29:00] But as long as they do the right thing, they are Protected. Imagine that as an interview question if you're interviewing for a job at CESA. You'd be like, how would you deal with that situation?

I was, Rob I couldn't agree with you more. I was on a panel with and this guy who was an ex district attorney from New York. And we get on really well, but we disagree on the whole role of the regulator. And I always use the analogy of the airline industry. The only reason safety performance improved in the airline industry is they created an open, transparent reporting environment, not just within their own companies, but shared that across all the airline industries.

So everybody learns and it's straight and oil and gas was exactly the same. Really sadly, we

used to kill loads of people in the oil and gas industry decades ago, but actually adopting that it's called black box thinking, it be adopting that sort of mentality of, encouraging people to speak up [00:30:00] when there's near misses.

You want people to say, Oh God, blind me. Maybe I shouldn't have done X, Y, and Z. Let's report that. Just in case, and that model seems to me a lot better if the regulators could incentivize people to report and then share those learnings across the industry, we would collectively become better.

But I think that these recent cases, and let's be honest, security CISOs don't sit in an island, right? They sit in an organization and the tone of that organization comes from the CEO. Shadow of leadership and all of that. So you might be a CISO who wants to report something, but actually the organization dynamics says no, cover it up.

God forbid any gets put in that that situation. But, I know people who will. As a result of just the company cultures that you see, but I think if the regulators were really encouraging people to report and celebrating the fact that people had issues, but they were [00:31:00] open and transparent and shared those learnings that would drive a much healthier culture in cyber.

It's like you don't train a dog by. Kicking it. Do you chain a dog by rewarding it? Let's continue that thread actually and talk about the board conversation. So in your view at the moment, and maybe we do this, let's pull a few threads together and and bring today's conversation to a bit of a head.

Is what do you perceive the board conversation is at the moment in most organizations and then of course, really what should it be? So I think the larger organizations and things like financial services and critical, more of the CNM and that's not true actually, but some of the bigger providers in CNI, I think there's a fairly robust conversation that happens at the top level.

I think people have to remember that the board is there to help manage manage risk. It's not there to do the job. So I would say over my, Tenure at a at ciso. The maturity of the conversation at the board dramatically [00:32:00] improved as their understanding that cyber wasn't special.

Cyber is just another operational risk. It's just a trigger for a business impact and event. So they're. They're as capable of managing the conversation around cyber risk as they are about any other operational risk. And so that, that encouraged them to start asking the right, right questions and the right questions, about are we doing enough around things like mergers and acquisitions and what lessons we learned from from that situation alongside the usual.

I don't know how we doing around getting the foundations, right? I hate a lot of people talk about getting the basics, right? Nothing is basic in cyber. So getting those foundational controls in place and operating, and that's where you've got to have real time information. And I see so many people patting themselves on the back that, yeah, we're great at patching 95 percent of our estate.

And it's okay, what about the 5 percent that's that's [00:33:00] vulnerable? Because that's not good. So having that data to hand that says, actually my controls are implemented and they are effective and being able to report that up to the board is really important. And also then to take them on that journey of maturity, because frankly you have to justify Investment to stand still not and try and that's a really difficult conversation to be able to say, you've got to give me X amount a million dollars.

What do I get back for it? Just about the same. You got today and it's tough, right? It's but that therefore you've got to take them on that journey of why. Of why that is an important investment to maintain the security posture. The other thing I'd say as well is they need to be involved in agreeing the risk appetite.

So what is the right risk appetite for the company? A bit like market or credit risk or liquidity risk, which they would happily step into. They need to be immersed in what is [00:34:00] the right cybersecurity posture we need for our company. Cause frankly, most people, in fact, nobody needs a CMM level five in cybersecurity.

Maybe that's one way of actually getting into that conversation is your maturity against things like NIST or your framework of choice of which there are. Ludicrous amount you can choose from, but actually get them into that journey about where do you want to be in terms of this risk to the company in a way that they can normalize it against other risks the companies are engaging with.

Sjoukje, what have you been looking at this week? So each week I do some research on related ideas and transformation in tech. And This week I thought we should take a look at the biggest cyber security trends for 2024. So by the end of 2024, the cost [00:35:00] of cyber attacks on the global economy is expected to exceed 10.

5 trillion, which highlights the need for cyber security as a strategic priority. So what are then the biggest threats? AI will play a huge role in both attack and defense strategies. Also, the shortage of skilled security professionals continues to be a big challenge. But also the rise of generative AI in cyber attacks, vulnerability of IT devices.

Also, the integration of cybersecurity in boardrooms is going to be a big focus point next year. And lastly, the emergence of cybersecurity regulations. So I have a question for you. What do you think will be the biggest trend for next year? So all of that no, it's all of the above trillion, 10 trillion, that should wake somebody up and go, it's costing us a bit.

Yeah I'm probably just so old and tired in this world now, but but my view [00:36:00] is yes, all of that. But actually what's still missing is good foundational hygiene. The attackers don't need, they're lazy. It's a bit like a physical burglar. If they walk around your estate and they see a alarm box on the front of your house, whether there's an alarm or not, the chances are they're going to go next door or if there's a door open, they're going to go through that.

Most cyber criminals are lazy, they'll fire and forget and hopefully they'll breach somebody and then, through their business model in the dark web, give that access to some seller access to somebody else, you'll take advantage of it, deploy ransomware. It's the basic foundations of the foundational hygiene that people keep forgetting.

They talk about generative AI, and yes, it's going to enhance the capability of the attackers, but it's also going to enhance the capability of the defenders. But the reality is credential theft is at the heart of nine out of 10 breaches still. [00:37:00] Phishing attacks and that phishing attacks will get better as a result of things like gen AI, you're going to get more and more deep fakes and things like that.

That is a way, but at the end of the day, what they're going to try and do is get out of credentials. And use those credentials to do what they've always done, which is to sit there, do some reconnaissance, laterally move, escalate privileges, get control of your domain, and then extort money from you really amusingly.

I've got to bring this up because I found this was quite ironic. So we talked about, ransomware was. The first level extortion, the second level was actually because people are

not paying ransomware anymore, necessary or paying ransoms necessary, less, less exfiltrate data, and then try extort money on two dimensions.

So double extortion. Now there's triple. The third one is they actually report you to the SEC. They dob you in. I love it. They dob you in, you get arrested. Yeah, so there's now [00:38:00] a threat to dob you into the regulator because they obviously know you've been breached. That's like the snake's eating its tail.

They have inside information, yeah. Without wishing to be flippant, I think all of what you've said is true, but actually what the security Community and that, the whole way. It's not just the security community, the business community and the security community just need to get those foundations in place and operating effectively.

Do you think there's a risk that the board will chase the shiny thing? So get all entrenched in the conversation about Gen AI security and forget all the stuff you just said, which is, you know what the threats actually over there mainly that bit. Yeah, it's important, but this one's the thing you need to think about.

So I think yes, but I think the CSOS job now, especially on the good thing about the not for Joe clearly and Tim, but the good thing about those things is, I think the response from the CSOS to that environment now has to be good. Ultra transparent with the executive [00:39:00] team in the board so if you know there is issues in your environment you got to actually report them up so through that kind of board reporting you've got to put everything out there and most organizations you know got massive technical debt so they can't patch a lot of that stuff they've got to start reporting that up to the board about the state of you.

Those foundational controls that you need to have to protect you against 90 percent of the tax good business case and going to the cloud. I'd say Simon yeah, interesting though. Dave, people are pulling back a little bit now as well. We could have another debate on that one. That's a whole, that's a whole other podcast for another day.

Yeah. But but I think that. So the CISO's got to pull that conversation back on track, which is, you can talk, we can worry about all that stuff, but actually we just got to get this foundational stuff sorted. In my view, we should create a new law that if the CISO does get arrested, the CEO has to share the cell with them.

Yeah. That might change the [00:40:00] conversation dynamic. You should be in regulation, Rob, with that kind of laughter. On that note, then let's wrap up today's conversation. So Simon, thanks so much for your time and insight. What an important subject and still some ways to go, I think in the whole discipline, but we end every episode of this podcast by asking our guests what they're excited about doing next.

And that could be going out to look at the Christmas lights this weekend, or it could be something exciting in your professional life. So Simon, what are you excited about doing next? I'm excited about getting some sun, Dave some winter sun. So not till mid January, but it's already on the kind of horizon now.

So looking forward to Christmas. But frankly it's been so bloody miserable in the weather in this this country, albeit the sun's out this morning I just want some sun, some vitamin D, bit of vitamin D injection. Absolutely. Where you heading to? We're going to Lanzarote to a nice sporting hotel, so get lots of [00:41:00] activity done as well.

Look, enjoy that and have a lovely Christmas in the meantime. Thank you. It's been an absolute pleasure. Thanks for the invite and love the conversation. So a huge thanks to our guest this week, Simon, thank you so much for being on the show.

Thanks to our producer Marcel, our sound and editing wizards, Ben and Louis, 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 in another reality next week. [00:42:00]

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 every day by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of nearly 350,000 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