Episode 17: Redefining data security with GenAI imperatives

0:06
Hi, I'm Andy Packham, Chief Architect for the Microsoft ecosystem at HCLTech.

0:11
And I'm here today talking about something that is, you know, super important.

0:14
We've all been talking about AI, how AI is impacting our business, all of the value that people are seeing in AI, but how we're securing AI is super important and how we're making sure that we are trusted.

0:24
What we do is trusted both by, you know, the businesses, by our customers, by the users of the AI and by society, as you know, on a broader level.

0:36
So kick off, introduce yourselves first, and then we'll dig into some questions I'm dying to ask.

0:43
Do you wanna go?

0:45
Yeah, sure.

0:45
So, yeah, my name is Vijay and I'm from Microsoft and my role in Microsoft is it's like a specialist in a specific area.

0:53
So I'm a data security global black belt, which means it's just specifically on data security and data governance that we focus on mainly on the areas around compliance and in the in M365.

1:07
And that's kind of my focus to work with product teams or with customers.

1:11
We understand what's driving the requirements for, for a product to feed that back to product, the product teams as well.

1:17
And also, you know, get that out to customers, let them know what we're doing with the product as well.

1:26
So, hi, I'm Vivek Rai, I takes care of GRC and cybersecurity practice.

1:33
So that's here for your region.

1:36
Looking forward to a good discussion on AI, especially how we can secure plus the change in the regulations happening and what is how it is impacting the various aspects of AI.

1:48
So looking forward for this discussion.

1:51
Yeah, Thanks, Vivek.

1:53
My name is Piyush Bedi and I'm part of the cybersecurity team at HCLTech.

1:57
I look at all of the financial services clients in Europe.

1:59
And like all the gentlemen here, AI has been a topic of discussion for all our customers, which is which is quite hard.

2:04
So very happy to be a part of this conversation.

2:07
I think where I'd like to start is this this big, this challenge the, you know, we've always had insecurity between enabling the business and protecting the business.

2:15
At one hand we've got the business wanting to forge ahead and the other hand, you know, there's a, there's a responsibility that CSO has to make sure that's done with the appropriate level of risk.

2:25
So Piers, why don't you just talk a bit about the challenges, you know, the conversations you're having with customers and how you're thinking about balancing those two sides of the equation?

2:33
Yeah, sure, Andy.

2:33

So I think AI in general is being looked at both as a weapon and as a shield for by our customers, right, Because it's an equal tool for attackers and defenders.

2:44
In fact, the attackers are kind of up in this race as compared to defense side.

2:50
And that's where our thesis are quite confirmed because with the scale of AI now and the sophistication, right, the defense has to catch up.

2:59
And you know, just take an example of phishing attacks, right?

3:02
I mean, the kind of sophistication with phishing now, Yeah, it sounds as a legit e-mail has come to you, right.

3:07
And how do you combat all that sophisticated malware which is being just built by writing a simple query on, let's say, a ChatGPT.

3:15
So I think most of our customers are concerned that how do we kind of manage the speed of response now?

3:21
And that's where I think the defence is adopting AI from a prevention and detection standpoint.

3:26
Yeah, that's awesome.

3:27
And but Joe, I just want to pick up one thing I've shared in your introduction I think is really important is AI and data.

3:33
So kind of what do you, you know, you can't have AI without data and you know, you get the value of data from AI, but you know, from a Microsoft perspective, how are you seeing those challenges you're seeing with customers?

3:45
How are you seeing those play out?

3:47
And that's a really good point because it's about data quality as well.

3:52
You know, AI is completely dependent on data.

3:55
Really, we all know it's dependent on massive data to give you good quality answers.

4:00
And the way we should be looking at it is, you know, use AI, use it as I use it on a daily basis, use it as my kind of best friend.

4:07
Now I'll ask you questions about work and other stuff as well on a regular basis.

4:12
And it's a bit trust of trust, but verify.

4:15
So you, you need to make sure that you know, you, you get a good answer, but you need to still verify as well to an extent that your answer is it's legitimate.

4:23
And the way that you can do that really is internally to an extent you can help trust, but verify is to have a good data quality, you know, platform effectively.

4:34
I mean, recently, a few weeks ago, I saw this IM tech summit.

4:37
It's like an information management tech summit.

4:38
It's one of the 1st that they've done actually.

4:40
And it's specifically around managing of data, life cycle, records management.

4:46
And previously, I think up until really, you know, where Gen.

4:51
AI has really made AI more of a consumable product, things like records management, data loss, soccer management, retention.

4:59
It was many, many driven by regulation.

5:02
You know, that there was a need to do it, but it was based on regulation.

5:07
Not the most exciting thing really, you know, but now actually, and this is, I heard this from people at the conference who are in this space, they said now that they believe this is now their time to shine because they can actually be a business enabler by now making, you know, retention part of the business and like putting in policies around not having data because bad data will pollute your, your AI responses.

5:29
So yeah, that's what I'm seeing now is like things that have been traditionally thought of as something that just has to be done for regulation is now switching to becoming like a business enabler for, for Gen.

5:38
AI.

5:38
That's one thing I've definitely seen where there's an onus on people thinking actually now we can be part of the business now enabling them to do things with the data.

5:48
So you, you know, from the compliance perspective on one hand, you know, as we just said, you know, it's about data, it's about the things that are actually haven't changed, but it's radically how are you seeing things change in that space?

6:02
You know, what are you again, you've seen those customer challenges changing or, or are they just the same as we've always seen?

6:08
Yeah.

6:08
So, so with coming of AI, there are there are always a traditional controls which will remain, which is going to keep, you know, the base security of the AI engine.

6:19
If you say the, the layer like a computer and a below layer, you always have to follow the, the traditional controls with respect to your data security like encryption, access management or you know, keeping data anomalization, data minimization.

6:36
So those controls will always remain either it is AI or not AI, right?

6:40
Other, other element, what is adding as a part of coming of AI is your algorithm layer, right, where you have your NLP and then the base.

6:50
Now how to protect that part of data is now important cybersecurity or you know the GRC or the compliance what they have to secure.

6:58
One part from HCLTech's perspective as service sector, what we see that one part is definitely we need a products like from the Microsoft that we have product to see the data security, data monitoring.

7:10
Another part is that how your base product of an LP algorithms to be secure.

7:15
And for that level of security, what we are trying to do that we are trying to map the different set of new regulations controls like how you can protect the model AI models, right?

7:30
How to protect that that theft to the AI model where you can do a watermarking or some other aspects where that particular IP of organization what we have created should not be lost.

7:42
So 1 is that part and second comes and the third one mainly comes as a governance as a top layer that one is to securing.

7:50
Then second part is the architecture part where you're monitoring then how you are governing from start of this transformation journey to end and then regular monitoring.

8:01
So governance is the top layer which has to be adopted as per AI.

8:04
So Piers, just, I'm coming back to that and just trying to build on that theme.

8:09
There's so there's so many layers there, right, that you're supposed to do, you're supposed to do everything.

8:13
And, and yeah, that's what the C cell has to do that, you know, they only need to leave 1 hole somewhere.

8:17

Yes, but yeah, from your customers, what are you seeing as the most important priority that they're looking at?

8:23
Yeah.

8:24
So I think, Andy, I think the trust factor, which we just spoke about, right, is very key that do you trust the AI model today, right?

8:30
How much information should I feed to this?

8:33
Am I giving him something priority, proprietary, which is very key for me?

8:37
Is that information going to get leaked when I actually use the data model today?

8:40
You know, am I, am I vulnerable by actually giving a lot of data to the AI models, right?

8:45
I think that's the the trust factor which which our customers are all concerned about because any application can be vulnerable.

8:51
You know, hackers are out there actually just trying to extract that particular point.

8:54
I think that's one a key area which I've seen like our customers kind of, you know, asking us questions again, and how do you test, you know, that the AI model is, is, is secure, right?

9:05
And the other thing is that, you know, how do you monitor these these AI models, right?

9:10
I mean, they can't follow the conventional monitoring process.

9:13
I mean, this is a new way of monitoring.

9:14
So I think most of our customers are currently figuring out and you know, we are kind of helping them device a way of looking at these particular problem statements.

9:22
So, Vijay, I mean, look, Microsoft, you, you're, you're doing a fantastic job and you're making it really hard for us.

9:30
The speed at which Microsoft is innovating is, is unbelievable, right.

9:34
But again, that same, you know, the same question.

9:35
What's that one big thing that customers need to be thinking about when they're, you know, they look at all of these challenges and the, you know, the CEO is pushing hard.

9:44
Well, what would you recommend is the one most important thing to focus on?

9:49
I think from what I'm seeing is people want to adopt Gen.

9:52
AI.

9:53
Yeah.

9:53
So we, we have different Co pilots in Microsoft.

9:56
We have loads of different Co pilots.

9:58
We have the M365 copilot, which means that people want to access all the different data across all the different 365 workloads like Exchange and SharePoint and other workloads as well.

10:10
What we've seen sometimes is customers are concerned about overexposure of data and that's something that's the key.

10:19
That's the key thing I'll say is it's these controls that around, you know, protecting data, prevent the overexposure.

10:26
They've been around for quite some time now.

10:28
It's just the drivers potentially haven't been there up until now that now there's a stronger driver to secure that data within your estate to make sure that you don't have overexposure issues.

10:41
And that's, I'll say that's the key thing is start thinking more about securing your data as a business enabler rather than just because you're doing it for security purposes or regulatory purposes.

10:52
That's the key thing is that you, you're enabling the business by securing the data, because then you're not, you're taking away, you're de risking that element of overexposure.

11:01
So that's the one thing to really focus on, I'd say.

11:04
OK, thanks.

11:05
And Vivek, you know, I mean, you spoke about regulations, right?

11:08
But I'd like to get your perspective then about what's what are the regulatory positives thinking about this, you know, yeah, yeah.

11:16
And you know, we're hearing a lot about, you know, governance, thinking about stuff, you know, whether or not market's going to become more protective or, or less.

11:24
But, you know, I'd kind of like to get your thing If we talk about customers, we talked about that, you know, where do you see the regulations going?

11:31
So, so based on, you know, the upcoming regulations, what is coming, like what is in the market and it's still there are few regulations which are about to come.

11:40
What we what the people, how the people who are afraid of basically the one aspects of biasing that how to reduce the biasing, right?

11:51
So for that, the regulators are trying to bring the more stringent control that is one second is again, you know, the controls which they're already in place, like with respect to like we just said that with respect to data security, data privacy.

12:07
So depends on that, that the your AI system is what is the classification of the AI system and it depends on not only the system classification, but the type of data which is ingesting into your AI system.

12:21
So that will also, you know, both collaboratively, you have to see that what outputs will come right and accordingly and seeing all these aspects of data, that is what the regulators were trying to, you know, bring more controls on how you secure the data.

12:39
And that is where we that is where organization has to think of again going to the previous principle of data classification, bringing the more control or additional control based on the classification and the data security.

12:53
Yeah, I think that's there's, there's a significant change here, isn't there?

12:57
The whole, you know, the whole role of what we do is changing from this way of protecting you, you mentioned it from protecting to enabling.

13:06
So kind of, you know, looking a little bit into the future, then, you know, if we've spoken about the challenges, you know, where does the CSO, how does the CSO become the hero?

13:17
You know, how, how do they start an organization, move from, you know, just be seen as, you know, security to somebody who's been seen as actually leaving, you know, truly driving business, business value.

13:29
So I don't know if Piyush, if you want to you dig in there.

13:32
Yeah, I think.

13:33
And one thing is very short, right?

13:34
I mean, AI is imminent, right?

13:36
I mean, there is there's no going this is this is the next revolution.

13:39
So everybody needs to think of ways.

13:41
I think the practical things where the CSO's really demonstrating or are kind of experimenting with these pilots is they're able to kind of, you know, bridge the the talent gap now because a lot of talent which was scarce and from a junior analyst standpoint, a lot of that work AI is able to do very, very efficiently now.

13:58
So with a smaller workforce, less trained workforce, they're able to achieve more using AI.

14:04
And there are enough examples with Microsoft Copilot how people are doing.

14:08
And I think that's one clear value which CIO's are demonstrating now that, you know, we can actually get this work done.

14:13
So I think that's one point from my side.

14:15
Yeah, I think another one is from what I'm saying is, so for instance, within Microsoft, we have the E5 platform, OK.

14:22
And I won't talk about product more than that effectively.

14:24
But within that, there's a huge amount of capability and that includes data security and data governance capability.

14:29
But quite often these areas, they're not when I speak to customers and I speak to people in the office of the CISO, data security, data governance is not necessarily areas driven by the office of the CISO.

14:42
And when I go to, I've been to this year, Microsoft, we've gone to other conferences which are not necessarily just security, but they're governance risk.

14:50
You know, these summits around record management, because we're trying to get in front of the people that to let them know at least that, you know, you've got these capabilities already within your existing, you know, you've already paid for this stuff, you know, you've got it already, you can use it.

15:03
So that's I think so empowerment.

15:05
So if maybe if seats goes to think about how they can utilize the existing capabilities and empower other teams to be able to help with security of that data, the gate day governance, that's maybe another area that we can that they can consider as well.

15:18
OK, that's interesting.

15:19
And Vivek, that's the same thing in from the, you know, the regulatory.

15:24
We so we often see the regulations as the ones that hold us back.

15:27
How do we start changing that?

15:28
You know that story to say actually this is what builds trust and in building the trust with society or with our customers, that's a positive.

15:39
So how do you see that?

15:41
How do you see how the regulations need to change to become more enabling What we do and what I say in other words, look, regulations are important especially for for a type of sectors.

15:52
There are two types of organizations.

15:54
Normally one which is starts proactively, like the organizations which start working on change, you know, bringing the change in the culture framework start adopting proactively.

16:04
There are some organizations who start adopting the technology, but they don't adopt, they don't want to adopt the controls of the security.

16:12
They wait for.

16:13
There is some implications come from the regulator and then they will do some changes.

16:18
So that is where you know the regulate, the regulatory requirement are important.

16:23
You know if I if you see the the changes happen especially in Europe, UK, we see a lot of regulations change from last couple of years like if the sector we see in this to Dora a lot of new regulation came.

16:36
But when we studied these regulations, these are not new as a complete new as a regulations, what they did that these are already the existing controls, which is which every organization has what they said that they want to just change a little bit so that you can bring the harmonizations between the different organization with AI also the same thing is going to happen.

17:00
They just want to add the additional layer that how to secure your, you know, the base layer and what all the changes you have to bring as a part of framework, as a part of, you know, governance, trainings, assessments, risk and all those things.

17:15
So that is what the changes need to bring.

17:19
But The thing is, once regulation comes, it's always a human cry.

17:23
I can tell you that how to comply.

17:25
But when we start studying that, OK, let's see how to comply, it's quite easy.

17:30
It's just a mapping of regulations toward the control and then let's go for it.

17:34
Yeah, I think that's really, that's really important.

17:36
And then, you know, to, you know, to wrap up then where are this, where are this sort of juncture, this, this pivot point?

17:43
But there's a lot of, I think there's a lot of optimism and there's a lot that we can very quickly move forward.

17:48
Yeah, you're right.

17:49
If you look at the if you look at the policies and you use those policies as guides rather than as, as hindrance, that's a huge accelerator.

17:57
Yeah, the Microsoft platform, you're right.

17:59
It's, it's all there today.

18:01
You know, we don't need to, we need to see how we do that and we implement that responsibly and, and you know, without bias, but you know, we don't need to worry about the underlying platform.

18:12
I think where we do need to worry, and I think it's the right thing to do is thinking about, the quality of data, how we look after our customers data.

18:18
Data has now become the, you know, the PSU you go to mention this, how this, this, this data is now everything is, everything is, is around data.

18:28
Last week I had a conversation and it was kind of the opposite.

18:31
It was about data.

18:33
And funny enough, it all ends up talking about security as well.

18:37
So I think, I think security, the data governance and the data architecture and the security are now coming together once.

18:45
So look, thank you.

18:46
I think this has been a fantastic conversation.

18:48
Really appreciate all of your time.

18:49
Thanks very much.

18:50
Thank you.

18:50
Thank you, Andy.