Podcast Episode 16: Data security and responsible AI

Host and Moderator:

- Dr. Andy Packham, Chief Architect and Senior Vice President, Microsoft Ecosystem Unit, HCLTech

Speakers:

- Lester Thomas, Head of Digital and IT Technologies and Innovation, Vodafone
- Mondweep Charkraworty, Head of Cloud and Cyber, Group Lotus
- Vijay Punja, Data Security Global Black Belt, Microsoft

0:04
Hi, I'm Andy Packham, Chief Architect for the Microsoft ecosystem at HCLTech

0:09
And I've been involved in so many conversations recently about AI, and those conversations have changed.

0:16
They've changed from what is it, what's the impact going to be to how do we scale?

0:20
How do we think about the challenges and how do we think we, you know, how do we think about doing that responsibly at scale?

0:27
So I'm joined today by three thought leaders from the industry.

0:30
I'm going to ask them to introduce themselves in a in a moment and we'll dig into some questions about how everybody's seeing AI scale for business value.

0:41
So Lester, would you like to go first?

0:43
Hi there.

0:44
Yeah, my name is Lester Thomas.

0:45
I work for Vodafone.

0:47
I'm part of the global strategy and architecture function, and my role is head of new technologies and innovation, which clearly, at the moment, is all about AI and generative AI.

0:57
Hi, I'm Mondweep Charkraworty, I'm part of Lotus Technology.

1:03
So my role is as part of a team called Digital Innovation Tech Centre and we're trying to bring to life new products and services cantered around the car, which should enhance experiences that our customers can enjoy.

1:17
Hi, yeah, my name is Vijay Punja, and I work for Microsoft. my role is effectively Global Black Belt for data security.

1:25
But what that means though, and it was a reason I was just given the title because some, some people know what that means is it's, it's to sit kind of with product teams, listen to what they're telling us about the products are happening and let inform customers and but also more importantly, actually listen to customers and figure out where we can drive the product in in line with customer requirements.

1:46
So, you know, these kinds of conversations with customers are so invaluable.

1:50
So let's start, you know, innovation; yeah, you must be very busy at the moment.

1:56
What are you kind of seeing as the biggest trends?

1:59
Clearly, like the last 18 months ago, when this really hit, we could see straight away that it would have a big impact on our business.

2:08
And I think the interesting thing is we've moved from like data and AI being something done in one department in Vodafone to it being something where we're literally asking every function, you know, show me what your AI strategy is.

2:23
So you work in HR; show me what your AI strategy for HR is.

2:26
Or in supply chain, what's your AI strategy for, for supply chain?

2:30
So it's going to have a big impact on virtually every function of the business.

2:35
And the use cases go beyond, well beyond, just chatbots.

2:38
Like people think of AI and Gen.

2:39
AI thinks we'll have automation in chatbots.

2:42
But actually, there are far more use cases.

2:44
It's almost like whenever you're interacting with human language, there's, there's use cases, there's use cases to derive insight in some way from natural language.

2:55
There are lots of use cases for generating content marketing content, which could even be code content, like we're using GitHub Copilot as part of our software engineering.

3:06
So there's, there's many, many use cases beyond what you might first think.

3:11
Yeah, I think, I mean for me, so I think it comes down to two things.

3:15
It's can we do what we do today better and can we do what we've never been able to do in the past now.

3:22
And I think that's where the real innovation, you know, in Lotus, are you seeing the same everywhere kind of it impacts everywhere or was it in one specific area you see the value.

3:32
So at Lotus, we hold a kind of customer.

3:35
I mean, we've been as we've been a niche producer of automobiles, right?

3:39
I mean, performance is our heritage.

3:41
We are going into should I say segments which are new as part of our Vision 80, which is when we turn 80, we want to have one of our pillars being the ecosystem related group.

3:51
Like what when someone probably buys a car nice car, I mean there are expectations around the digital nature of the car and we want to do provide those innovation, those experiences innovatively leveraging new technology.

4:04
But with data privacy and security, the crux of our proposition we want to respect individuals rights and expectations what the so we want to do that in a very responsible manner.

4:15
So, so we are seeing, we are, we've started ramping up in terms of our car sales, productions, etcetera.

4:22
And we are probably very much starting off this journey where we want to work with open ecosystems and ecosystems.

4:29
So, we want to reinvent the wheel but do so in a manner that reflects our brand identity and our brand heritage in a right manner.

4:36
So yeah, the short answer to that is that we're being led by a customer.

4:40
We're trying to be very customer-centric about what customers want and walk backward from there.

4:46
So I mean, both of your industries have changed dramatically, you know, over the years, Microsoft from the, you know, Microsoft in a way that has always been about the platform, the code, and the tools.

5:01
But I think that's changing.

5:03
How are you seeing what Microsoft does in terms of being a business enabler rather than just rather than just selling technology, if you will?

5:11
I think it's the culture actually is kind of driving that to an extent.

5:14
It was really interesting as to what you said now is that you're asking your business units effectively to drive the AI strategy, and, you know, you said data and AI are no longer just the kind of recluse of the technology teams.

5:26
You know, you, you, it's about empowering teams with data and AI as well.

5:31
And so, so things like products that we've been producing for some time now are now starting to become more prominent.

5:38
So things, because some of the concerns around generative AI, it's about data governance, security overexposure, all those kind of concerns that they're just kind of more prominent now because there's additional tooling now, additional copilots to use that data.

5:58

So, yeah, I'm seeing that things that have been around for some time anyway are just becoming more prominent.

6:05
There's, there's a, there's a real kind of drive to, to empower the business by enabling them to, you know, define the security around data.

6:14
And then, you know, also divine sort of standards around governance around data as well.

6:18
And people are actually starting to become more interested in that because they realize that if they can secure or govern that data, then that is really going to help them enable these general Gen.

6:30
AI apps across the environment.

6:31
So yeah, that's one big change we're seeing.

6:34
Can I just, yeah, yeah, build on what you mentioned, I think the benefit of the last year in which we have seen if I may limit myself to Gen.

6:42
AI, as in the fact that there have been certain industries where people have to, they have to be risk more aggressive decision making.

6:50
Although they were awareness of risk like I would say they have been implementations where there are critical in, in some parts of the industry.

6:58
I mean probably the first time critical vulnerable exposures with that, you know the big players have gone ahead probably including yourselves.

7:05
I do not know in, in, in, in customer facing applications and critical industries and that in retrospective attempt to kind of I think mitigate those risks or fix those.

7:15
But I think with the learnings now learnings from those industries from the big players including yourselves.

7:22
And I think we therefore should form a kind of best practices guardrail based approach to anyone new starting off.

7:32
I'm sure there, there.

7:33
I mean that's the approach we are taking.

7:34
So, as you say in the business, I mean, I answered your first question from a customer point of view, but within the business, whether it's legal, whether it is marketing, whether it is HRI means there's an immense benefit in being able to interpret the unstructured data that is all out there in simplistic manner, right?

7:50
But how do we do so in a manner security is given right?

7:54
But in a responsible way, explainability of the whole thing, right?

7:59
And I think it has to be approached like McKinsey.

8:01
I mean, I provide a lot of thought leadership on this topic.

8:04
Is that how do you start small like start understand what is that incoming risk?

8:09
What risk already exists with no Gen.

8:11
AI?

8:12
What said?

8:12
What is a new risk from Gen.

8:14
AI?

8:14
What is your risk appetite as an organization, right.

8:17
IP infringement as a topic or maybe you know, data allocations, the other topic.

8:22
And then what are what are you willing to make a conscious choice about it and then identify a few use cases.

8:28

And probably this is nothing new I'm saying here, but I'm, I'm quite pleasantly surprised, like in some of my discussions around colleagues here, including from the legal industry, right?

8:37
They're like, we want to just write policies for the sake of policies.

8:41
You know, why don't we work together to identify one or two use cases?

8:45
You know, we work together, identify a risk, measure our risk appetite, and then take an incremental step to it.

8:52
Because I think there is no perfect answer to how we're going to do it.

8:56
We all agree this is game changing.

8:59
This is an attack from under.

9:01
Like in a strategy you've got attack from over, which is fine, but if it's an attack from under then you got to really rethink like how you bet the next opportunity against risk.

9:11
I think that risk based approach is really important because as you say, we we've been democratising the access to these AO tools and platforms.

9:20
There's been a huge number of use cases and traditionally you might have looked at just like what's the business value versus the cost?

9:26
But we've been taking very much a risk based approach because you have to learn by doing the only and, and doing means doing it with, with real data, like doing it in purely POC environment, you don't actually learn anything.

9:41
But if you do it on a like, what is the lowest risk use cases we can pursue and to learn by doing.

9:48
So typically that means like doing use cases where you're the consumer of the data.

9:53
So driving insight from data, there is no risk.

9:55

Like we're not exporting any, any risk doing it for like for chat bots, doing it on an employee chat bot first, you know, to actually learn, you know, how do you build a check bot experience around it?

10:06
So we've, we've got a model whereby we start with the lowest risk use cases and learn by doing on a on a risk basis and also lead you to do some slightly different use cases.

10:17
So there's the whole augmentation versus automation.

10:21
So there's like a, there's a road map of saying the first use cases aren't trying to like replace employees with AI and they're trying to, or setting out to give them superpowers, give, you know, augment them with which is the whole copilot branding, which I which I really like.

10:36
And I thought that's the right approach because you can do that in a much lower risk way.

10:41
You can continuously improve that augmentation.

10:45
And clearly if you're giving people super powers, you do have the business benefits from delivering that.

10:51
Yeah, I totally agree.

10:52
Yeah, yeah, yeah, I think so.

10:55
I think, you know, that the conversation about risk, but I, I think the way that we are talking about risk has changed.

11:04
It's now not a sort of a technology or an IT.

11:06
It's an actually, it's a much broader conversation.

11:09
And I think, you know, you use the word democratised and I kind of find it really interesting now that we're all having this conversation.

11:16
It's a, it's not ACIO, it's not an IT conversation, it's a business conversation.

11:20
We're all learning in that.

11:22
So you know, in in that, you know, Vijay, you've got the whole Microsoft platform.

11:27
For me, one of the one of the important things is the cloud removes the barriers to innovation.

11:33
I don't need to buy thousands of servers.

11:35
I don't need to make massive I, you know, even as a small start up could spin up what I need in the afternoon and be doing cool stuff.

11:42
Exactly.

11:43
So, you know, just talk a little bit about how how the cloud drives innovation and how it just makes it easier to to do good stuff now.

11:50
Yeah, I think, I mean, I've been in IT for a long time and I did a lot of operational stuff.

11:55
So I was in that space where we had to to build an application, you know, you'd have to buy servers in network equipment and there really was a barrier to entry, you know, to to spin up new applications or business capability with technology.

12:11
And then we saw that evolve with cloud technology that it just enabled that ability to do that.

12:16
And now we're seeing that, you know, with AI now there is that.

12:21
And then at the same time, there was risks associated with shadow IT where people would just, you know, realise that asking their IT department to buy 10 servers for an application, they can just go to a SAS provider and then, you know, build, get a SAS service.

12:33
So what we're seeing is, you know, with there is a risk of shadow AI as well now.

12:39
So there is the risk around a lot of Gen.

12:42
AI apps are getting built.

12:43
There's more Gen.

12:44
AI apps.

12:44
I mean, we have a like a catalogue of over 400 Gen.

12:46
AI apps in in definitive cat apps, for instance.

12:48
So, you know, that just shows that probably more than I more than I realised when I heard that stat.

12:53
You know, there's so many Gen.

12:54
AI apps out there.

12:55
So I think that it's always going to, there's always going to be some risk for new, new technology and innovation.

13:02
But I think it's, it's using combination of the different, you know, within so within, you know, Microsoft, we have the E5 platform.

13:09
There's a whole load of capability within the platform and it's using the different capabilities within the, you know, all the different products to secure yourself against those kind of risks associated to Gen.

13:19
I.

13:20
When there's potential for data leak, when if there's information that's being shared into public Gen.

13:26
AI apps, then the nature of a public Gen.

13:29
AI app is that will reuse that to and we'll learn from that.

13:31
So, you know, there's a big risk of that kind of thing happening where you might some or put some information that's a confidential internal information.

13:39
If it's putting it to a public AI app, then it could, you know, be reused and exfiltrated effectively.

13:45
So, yeah, we're seeing that you usually have to use these solutions available to you and really think of innovative ways to secure yourself against those different risks as well around shadow AI AI.

13:58
This is where probably the whole point about like I think those would be successful in the in the next three, five years.

14:06
I mean, I would suggest to say those who use who don't as an interview rocket scientist to understand AI, but those who can effectively use Gen.

14:13
AI or AI tooling, right?

14:15
So there's this whole intrinsic point about motivation, right?

14:19
If you are in an organization, you know, if you're constrained, unable to effectively use Gen.

14:24
AI tooling or to AI tooling in general, you know, you're going to be left behind.

14:27
So how the organization therefore has a responsibility to introduce a mechanism by which the staffing itself could use for their day-to-day jobs, right?

14:37
What are the guardrails?

14:38
What how do we some of the themes that you mentioned about, you know, data, data exfiltration or like in the hundreds of these open source models out there, you know, how do you avoid someone not using something that they're supposed to, what models they should use potentially for image generation and for, you know, text generation?

14:56
How could you improve productivity?

14:57
So how do we therefore create some kind of a mechanism through a platform or and empower employees to start making use of it?

15:07
So I think that is all I will compliment to integration.

15:09
Yeah.

15:10
Yeah.

15:10
I think there's a great point about empowering training, developing the skills across the holding organization.

15:15
It's, you know, it's not rolling at all though anymore, is it?

15:18
It's because people are going to use it regardless.

15:21
Yeah, exactly.

15:21
They're going to use it regardless because everyone's seeing it's so useful.

15:25
Yeah, you've seen that same in telephone, that same, you know in that democratisation, it's more than just providing a platform.

15:33
And we like we have done a company wide education programme because like you, the only way to counter the some of the risks is through education.

15:42
Yeah.

15:44
And so literally every employee in Vodafone will have a, a baseline of education on the the GNA tools, what they're good for, what are the risks, what are the like the things you have to be cautious about using them.

15:56
And that's part of our foundational sort of education that we do.

16:00
So where are you both in kind of in, in your own journeys?

16:03
Are you proof of concept MVP production that you're seeing, you're seeing real use cases kind of starting to scale now or are we still sort of in the experiment phase?

16:14
No, no, we haven't.

16:15
We've for over a year we've had Gen.

16:17
AI use cases in production on the Azure Open AI models.

16:23
So I think we were probably quite early in adoption.

16:26
Again, we started with the ones which were like, I think the first one we did live was transcribing and then using the generator first to understand why our customers were interacting with us.

16:38
So it was like we were the consumers of it.

16:39
So it was like a very low risk.

16:41
And it's our ability to then say you have, you know, you know, we have, you know, 20 markets around the world and customers calling us with issues.

16:50
Our metric is reduced the number of times they call like reduce the issues at source and to be able to use generator, summarise and categorise.

16:59
So literally now we have, we have like a database where every single call is categorized and summarized and there's a team doing root cause analysis of Go and fix it root cause with a target of customers.

17:13
Never call with that issue again.

17:15
And of course you're getting great data and you can run that, you know, constantly and and measure for all that reason, it's gone down like the team looks at the next reason.

17:24
So we've been doing that in production for more than a year, but now we've started to do it even in our customer facing chat bots.

17:31
So, but again, we we've taken this risk based approach.

17:35
Most of our customer facing chat bots still use the traditional cognitive services AI from Microsoft.

17:43

But what we're doing is particularly in tents where we consider that intent to be a low risk that then gets farmed to an open AI model to get a more natural response.

17:55
So again, you have to do that in a sort of responsible way, learn by doing.

18:01
But you, you know, you don't want to swap from, from today it's running on cognitive services to traditional AI and tomorrow it's running and you're in the newspaper because what your chat bot is committed, which you've seen from our companies.

18:14
But it's for those things they're running at scale.

18:15
I think we do 14,000,000 chat interactions a month to our to our what we call our Toby customer check box.

18:23
It's in production at scale.

18:26
That's I think that you've just that from that use case.

18:29
It just, it's really interesting to see that the, the there's like you can so easy to see the value you're empowering your own employees to do a better job with giving them more information that's being pulled in from different sources and helping them understand the problem.

18:43
And then you're also helping your customers to have a better experience as well.

18:46
So it's just, there's so many points of value there because even just empowering your own workforce, it it's makes them feel, you know, if you can do a better job.

18:53
Generally, most people, you know, they want to do a better job if they can do a better job because they're getting more information, better information, quality information, they can help their customers as well.

19:01
So yeah, that's just, there's so much points of value there, isn't there?

19:04
Yeah, I think it's yeah, we we're saying it every right.

19:07
It always comes back to the data, doesn't it?

19:09

Yeah, we, you know, every industry has this ability to create for normal amounts, you know, data, you know, you know, the car must produce massive amounts of data, especially with the soft.

19:20
I mean, the whole prediction is like between 20 thirty, 95% of the cars sold will be connected.

19:26
Cars are connected with your connection.

19:29
And you can imagine what that means, right?

19:30
Yeah.

19:32
Now I'm going to touch on three things here.

19:34
First, this is in is agnostic of any OEM and it can go to Mozilla Foundations dissipation privacy, which is different answers privacy not included.

19:45
That's a Mozilla study of and look up at some of the noted I guess players out there.

19:52
Privacy policies would say if you don't share the data, you can't my malfunction may not purpose.

19:58
Consumers don't really have a choice.

19:59
That's one thing.

20:01
Now back to your point, I'm going back to the software definement.

20:04
You could effectively like.

20:08
We you could diagnose anything, right?

20:10
There's a lot of information and there's the industry is put in regulations like there are things like, you know, WP, you know, there are some group groupings like 155 and 166, which proves how do you protect people from cybersecure cybercrime and software updates and all of that stuff.

20:26
But the point is that how do you make sure that that data is more responsibly used to provide end user.

20:34
Now what we have done, I mean as you say the advanced driver assistance systems and our systems or you know we have our own proprietary stuff there, right.

20:43
I mean, yeah, we're not new to that.

20:45
So it's being used there.

20:47
However, we've tried to use point control environments to test the effectiveness of like customer receptiveness etcetera of Jenny High and other stuff.

20:56
But overall, from a corporate point of view, I think we are kind of very nascent because going back to my first point is we want to responsibly make use of this data to provide the right digital services and experiences across not just automotive, but insurance, you know, effectively bringing mobility, energy needs, financial services together, but do so in a responsible way, keeping a customer at the heart of it.

21:22
So Jenny, I will play a part because, you know, if we understand the customer one their profile to be understood, you know, they might want an opinion from the car to give me, I'm going there.

21:32
You know, what should I do?

21:34
You know, personalized intelligent journey planning, for example, I would love to have the customer because that is the future, because if autonomous cars become the reality and like even in London, I was pleasantly surprised.

21:45
So they like in near Stratford, you could have smart mobility.

21:49
They're using the Olympic cars part to actually test out real life, right set up.

21:54
So autonomous car.

21:56
I mean, we the US way more is already there right when it rolls out.

21:59
I mean, we want more from the it's a third space, right?

22:02
What do you want to watch a movie?

22:03
You want to explore something.

22:04
So it is a real space.

22:06
And I think that's where the data will be very valuable.

22:10
But we have to do it responsibly, respecting people's opinions and expectations.

22:15
Like someone's bar on privacy may be high, someone's maybe low, but we must be able to evidence that we must be able to explain why certain things are doing particularly.

22:24
That's my personal opinion.

22:25
No, I think look, as we wrap up from each of you, just, you know, you, you're very advanced in the journey.

22:33
It it just in terms of one piece of advice you give, you know, somebody who's kind of starting this, you know, you know, in their, in the organization.

22:41
What's the one bit of advice you would each give to, you know, someone signing off?

22:46
Yes, I, I do think you need to have this cultural change because you need to have this like with all this based around the data, you need to have this culture of experimentation because you only learn by by doing things with dual data.

23:01
And you have to have this culture of, you know, being responsible with the use of, of that data in the eye.

23:07
So it's not just, I used to be just cybersecurity and privacy, but now there's a whole ethical aspect of, is it like, even if it's secure and private, is it something which your customers would be happy with you doing?

23:19
Like you want to do things which are for the good of society, to improve people's health, to improve the environment like this.

23:27
So you need to have that, but that it requires its whole cultural change, I think.

23:31
I think so, yeah.

23:32
I mean, I think every organization should assess its own appetite like what is its brand identity?

23:38
What does it want to do?

23:39
And at the end of the day, technology just a means, right?

23:42
What we use for it should reflect what its core values are and how, what it the way it wants to use technology helps achieve those core values, which could be commercial objectives as well.

23:53
Nothing wrong with that, but I think it's being really conscious about what are the guard rails.

23:58
Yeah, I mean from my point of view, the key thing will be to make sure that there are thinking about what is their brand identity.

24:05
So every organization is own value set and technology is just a means to achieve.

24:10
So remind ourselves what are we here for?

24:12
What's what do we want to do?

24:14
What are is our vision and how do we use Geneva or any technology to achieve that right.

24:19
So some of that could be commercial objectives as well.

24:22
Nothing wrong with that, but being conscious about and doing so with that understanding, yeah, I think we have to embrace it.

24:29
I think we don't have a choice.

24:30
And I think I like your point about the culture.

24:32
I think you're right there.

24:33
We the culture, we have to change the culture a little bit in the respect that there's still some fear around Gen.

24:39
AII think people are still a bit feared of Gen.

24:42
AI and what it can do to their jobs.

24:44
But, you know, we saw this with other technologies in the past where actually it's actually create many more opportunities.

24:51
So I think culture, we have to embrace it and embrace it responsibly as well.

24:55
I think that's the key thing that we're, you know, from a cultural perspective that we need to look at.

24:59
Yeah, Look, the three of you.

25:00
I mean, thanks.

25:01
It's, it's a fantastic conversation.

25:03
We could, we could go on and go on.

25:04
For me, I think the most exciting thing is, you know, we're now talking about ethics, we're talking about responsibility.

25:11
We're talking about, you know, we're not talking about IT conversations.

25:15
We're talking about some really, really important things.

25:17
And I think that's a great.

25:18

I think that we're starting in the right place by doing that rather than just kind of talking tech, talking how we're going to deploy.

25:25
Yeah, I'm, I'm, you know, very optimistic that we're going to get this trust built because of that focus that everybody has in kind of thinking about these things that are seriously important.

25:34
So all of you, thank you very much.

25:35
It's been a great conversation.

25:37
Thank you.

25:37
Thank you.