

Podcast Episode 25 Transcript

Moderator: Dr Andy Packham

0:05

Good day and welcome to another Elevate podcast series.

In every conversation about AI today, one truth keeps resurfacing and that is that innovation only scales at the speed of governance and trust is becoming a defining competitive advantage in AI. Governance doesn't slow down innovation, it accelerates.

It enables it. We've explored people, infrastructure and data in previous episodes and today and we're turning to the fourth pillar in the new playbook and that's the quality of governance.

I'm really excited.

I'm joined by two expert practitioners.

People have not only been talking about responsible AI, but making those principles a practice.

Firstly, we'd like to welcome **Dr Heather Domin**, Vice President and Head of the Office of Responsible AI and Governance at HCLTech and **Jenni Rantakari**, the Leader of Cloud solutions across EMEA.

Both of you, thank you very much and I do appreciate your time.

So to pick off the last 18 months have just been amazing, you know, it's been like everything's accelerated at the speed of light and that's a long time.

I'd like to get a view from both of you about what you've seen in the way the conversation with leaders has changed.

So, I mean, Jenni, if you could kick us off, how have you seen the conversation change in the last 18 months?

Speaker: Jenni Rantakari

1:34

Yeah, thank you for having me.

It's really great to be in this conversation today.

If I look back at the past 18 months, I see couple of main themes and one is certainly related to how companies are thinking about AI.

So we started to journey with people thinking about like personal productivity and now we are talking about like end to end enterprise-level transformation and we typically talk about the transformation towards frontier firms.

So that means that companies are thinking about how to build secure AI driven organization across the different functions.

And when we think about this, there are of course multiple questions coming into play.

And we typically try to think about it in three stages.

So starting with the personal productivity, then moving to the organisations where agents are operating in the same organisations as humans.

Then finally going into those agentic organisations like dark factories.

And in the past 18 months, I have seen accelerated innovation, accelerated focus on the journey towards the frontier firm.

And it's starting from the customer engagement, employee experience driving the business processes and of course, depending the curve of the innovation.

And at the same time, we have seen some of the regulations come to play. So this has been very

interesting, very much accelerated journey.

So what do you think, Heather?

Speaker: Heather Domin

3:18

Yeah, thank you, Jenny.

I think it's a fantastic reflection.

And you know, I'm seeing many of the same things essentially.

What I'm hearing about our clients that are really looking to take the next step, right.

So I think prior to the, 18 month period that we're, we've just been through, there was of course a recognition of AI and the importance of AI.

That's not necessarily new, but this, this acceleration in adoption, I think it was, you know, prior to this, it was sort of a people becoming familiar trying to wrap their head around, as you say, around productivity use cases and many of the, the early use cases.

And now what I'm seeing over the last 18 months is more of a maturing, so moving beyond proofs of concept into more scaled deployments where it's fully integrated into their enterprise operations and really transforming the business.

And I think that's exciting.

And it's a period where we're also seeing tremendous benefits and return on investment from AI that finally, you know, when you go to that scale, you can see.

And I think it's important to note that these benefits are not just on the productivity side, but also on the business side.

We're seeing tremendous improvement, for example, when deployed in healthcare and the quality of care that you know, we're able to bring to patients and improving the quality of customer care that's provided in a variety of contexts.

And I think that is, you know, when you, when you think about it, when we move beyond just that, you know, initial focus on productivity and efficiency to moving towards really bringing a more holistic value, that's what I'm seeing and people are excited about.

And at the same time, you know, as we do that of course, it introduces potentially more risk, right.

So bigger broader engagements can introduce new risk.

We're seeing a lot of movement over the last 18 months and we're continuing to see this on the regulatory front and the policy side.

And so that is all part of the picture and looking forward to discussing that in more detail in this conversation.

Moderator: Dr Andy Packham

5:42

Yeah, thanks, Heather and Jenni,, I think Heather, you mentioned one thing about ROI and I think that's the, you know, for me, that's the shift.

If you go back 18 months, we were, we were kind of talking about what it could be.

You know, it was a massive amount of excitement of what might be now 18 months later, we've seen real or, you know, real benefits.

But we're also beginning to understand actually it's really quite hard.

There's a lot of complexity in that as well.

And that need to create that governance suddenly now have gone from being.

Yeah, yes, We know it's important to.

We need it. We need it to build trust.

So thank you, Jenni, if I come to you, does Yeah, as Azure is just this full stack solution that has responsible AI built in as core and I think that's really key.

But that do the features in Azure provide sufficient assurance on their own or do organisations still

benefit from, you know, the additional values and customisation that come through partnerships with HCLTech?

Speaker: Jenni Rantakari

6:59

Yeah, no, absolutely.

So that's a really great question.

And maybe I'll start with saying a few things about what we have built in into Azure.

And of course there are tons of capabilities that are inbuilt, but at the same time, I think that the customers still need to think about couple of other things in addition to that, especially when we go to the sector specifics.

And if I may give you a couple of things to start with from Azure, what we have done, we actually have built some pre-built metrics for quality, for example, crown crowdedness, relevance, fluency, things like that.

And we also have some pre-built metrics for security and risk.

And then also metrics that are looking at, for example, some problematic content that potentially might be emerging in some of the models, but we also want to give customers an opportunity to build and define their own custom metrics, so they will be much more tailored for their own use cases. So we have all that available in the platform.

And what I would say as well is that thinking about going beyond these kind of platform build metrics, they're starting to think about how do you tailor the governance frameworks to your unique challenges in your own sectors.

And thinking about like what are those custom governance policies and how do you think about those to address what is required in your sector?

Also building risk assessment, independent risk assessments, which will be really key as well.

And then, of course, building those critical human oversight so that we can look at the high-stakes and sensitive applications and integrating that human in the loop.

So I think there's a lot of things that the platforms will provide, but then combining that with governance, risk assessments and human oversights will be really, really critical when I think about it.

Moderator: Dr Andy Packham

9:08

Yeah, Thanks.

Heather, in your experience then from, you know, the native platforms, how do they need to be complemented?

I mean, one thing that Jenny said is around metrics and providing the metrics.

I mean that that is, that's incredible.

Speaker: Heather Domin

Yeah, you're right.

So and this goes to, you know, that transformation that we were just talking about.

So people, organizations that the employees who are working with these systems expect these inbuilt controls.

So that's a ship that we've seen.

And now, of course, there are these inbuilt controls and metrics.

Part of that though, is how you use that, how you then integrate that into your overall organizational governance structure, right?

So you do need to think about those broader, broader aspects.

And also, even if we think about the training aspects, so many employees, if you're introducing metrics that you know are in the platform, how do you train the employees to make sure that they're reviewing them and integrating them into their governance cycles?

That is an important aspect of this. When we think about broader governance controls as well, we're thinking about the use case itself.

So, how are you using the AI and in what context?

Is it a high-risk contact context? In which case you're going to need perhaps some more controls built in even outside of the platform, as well as some process based controls which relate to decisions in the business about, you know, what types of uses are actually allowed, what decisions you're making with it.

And you know, because the system output, of course is an output.

And then what you do with that is, is especially where it becomes a critical next step.

And that's where the governance has to come in.

So I think, you know, in organizations, we're seeing more and more companies deploying specific AI risk management policies.

And as part of these policies, they'll have assigned, you know, roles and responsibilities to different individuals that may include the developers or data scientists who are working in Azure and working with these metrics.

And it's going to also include some, you know, risk and compliance individuals, some AI governance professionals and other focals throughout the business that will support critical decisions and implement the controls.

So all of that is happening today.

We're seeing that and that is what is really helping maximize the benefit that organizations are finding from these systems is they're actually taking the inbuilt controls, pairing them with organizational governance controls and getting that reassurance and you know, the right checks in place to feel confident to move forward, right.

So that's where, you know, sometimes we hear this debate of, you know, will, will the governance, will the compliance slow us down?

But what organizations are seeing is that it's speeding them up when it's inbuilt like that, when it's part of the process and they feel confident to move forward, they can give the the green light essentially to keep getting the benefits from these systems.

Moderator: Dr Andy Packham

12:52

So Heather, in in that you talked a lot about what needs to happen across across the organization.

So it's not a, it's not at all thing.

It's not an IT thing.

It's across the organization. Yeah.

Where do you think organisations are then struggling in, in that movement away from, you know, the principles to, to the practice, the practical implementation, Responsible AI?

If there's any examples you can give, then that would be brilliant.

Speaker: Heather Domin

13:18

Yeah, sure.

So one of the biggest challenges right now and I've spoken to many, many leaders recently working in the AI governance space who have expressed and this is like real time.

I'm bringing it, Andy.

What professionals today from leading organizations are finding is that there is basically too much demand on an AI governance professional for what needs to be done.

So, for example, contracts.

So one of the big things that's happening recently is a ton of third party AI integration.

And this is something that many companies are dealing with.

They wanna, you know, their vendors are integrating AI, They wanna, integrate it. And but how do you manage that, right?

So now, now it's and so what's happening is like the business doesn't know.

So they're going to their, their AI governance professionals and they're saying, OK, give me, give me a solution, right? Give me a solution. And it's partly a legal thing.

It's partly A procurement thing.

It's partly is an AI governance thing, right?

So what you're finding and what becomes the challenge in putting this into practice many times is these are cross-functional issues and cross-functional challenges that require collaboration across the business from various functional units.

And that's, so, you know, in my case in HCLTech, that's a big part of my role is to help bring that cross-functional collaboration.

And this is also, you know, what I'm seeing and hearing from the teams and other companies and in our clients as well, is that, you know, getting this organizational oversight to function properly.

And in some cases they're implementing, for example, an AI, an AI office, OK.

And so where they're essentially managing the AI use cases and deciding on what's going to be prioritized from an AIU standpoint, but then also the governance controls as part of that having governance functions.

And this helps to more formally establish those connected points.

So that's something that I'm seeing.

Moderator: Dr Andy Packham

15:51

Yeah, I think so.

I think there's something profound happening there.

Then the you're kind of, you know, moving from maybe governance been something that was at the wrap around.

It was at the edge. We dealt, we did everything.

Then we checked it was all OK to do it to actually the role of that the person driving that responsible AI is now actually central is actually kind of almost the hub around which that that cross functional team is beginning to work.

So Jenni, do you see similar patterns?

You see similar areas of friction in your conversations?

Is it something else?

Speaker: Jenni Rantakari

16:26

Yeah, no, absolutely.

So building on what Heather was talking about, I think there's a couple of things that are emerging in most of the conversation that I have with the our customers and partners.

One is the speed of change, speed of innovation.

How do you go with that complexity?

How do you start to break it down to the, to the stages that your organization is is ready to take?

And then on the other hand, you, need to skill your organization that you can also run your business

and innovate, build those future experiences for employees and customers within that new AI driven organization.

And of course, big questions everyone has is that how do, how do I go with this killing and and making sure that I don't have 5 year old organization when I, when I'm innovating and moving very fast.

The other thing is, of course, thinking about those aspects of bias and fairness and when companies are thinking about different applications with AI, how do you make sure that this doesn't really undermine the trust that you have with your clients, you have with your employees?

And of course, it can have reputational regulatory risks and then how to manage that.

So that's definitely one thing that will be factored in.

I also think that for example, the uncertainty and maybe the compliancy with the new regulation sometimes is, is something that the customers are asking, but how do we navigate this and how do we how do we go when we don't exactly know how it looks like from five years from now.

And then finally, the operational side, change management adoption.

So when something has been built, so do we have the right model or is the model potentially drifting, is it reliable?

Is there change management program so that we see the benefit and get that business value that Heather mentioned earlier as well.

So when you start building all this, it kind of leads to that sort of clarity on what's the road map, what's the framework, what are the tool kits, what's your training programs, what's the innovation that you want to take when you go forward.

So it's certainly is multifaceted journey.

And, this is where HCLTech and Microsoft, everything we can offer and support our clients is absolutely critical,

Moderator: Dr Andy Packham

Jenni, in that you mentioned speed of change and speed of innovation.

19:13

And yeah, we're going through another kind of innovation phase now around agentic AI and moving on from where we were just thinking about GenAI.

How do you think accountability and oversight changes when you start to have environments that are more agentic and less manually supervised?

Does that change dramatically the way that we look at responsible AI or is it something that is an evolving story?

Speaker: Jenni Rantakari

19:36

Yeah, no, absolutely.

I think personally that it is actually changing quite, quite a lot.

So in a way thinking about in, in the past we used to have pretty static compliance approach and now that we move with autonomous agents, it will be, it will require much more dynamic approach.

So continuously monitoring are we progressing to the right direction.

And there are of course certain things that I would recommend is, is thinking about this transparency. So how do you know what kind of algorithms or AI driven interactions are ongoing there, what your agents might be performing, what they are doing on behalf of the organization, thinking about that traceability, auditability.

The aspects as well and of course it goes back to that, what we said many times already is that what's your clear governance structure so that you can have roles and responsibilities, you can have that oversight, you know, when do you need to do the ethical reviews and then how do you build organizational structures so that that's all possible.

And then of course proactively, continuously monitor what they might be from the regulation perspective as well.

So it certainly will change the landscape when the organisations will get the agents and part of the organisations will become quite autonomous as well.

And this is something that is very much evolving fast as we go.

And of course, it's really important so that you keep that trust and you will be serving your customers and obviously keeping your organization's thriving.

So having that everything built on the transparency, auditability, traceability, having that clarity on the governance structures will be really, really critical.

Moderator: Dr Andy Packham

There is this continual change in this evolution and I think we're all seeing and dealing with.

21:36

Heather come back to you then, how, how do you see organisations redefining accountability and especially kind of building that trust with key stakeholders, the board, regulators and and you know, obviously critically customers.

How's that evolve? How's that conversation evolving?

Speaker: Heather Domin

21:55

Yeah, so it is definitely evolving and a hot topic within policy scenes today, right, Policy discussions. I think policy makers are certainly this is on their mind in many cases currently today, you know, it's being the policy around, you know, the AI agents and autonomous systems is being handled under existing laws.

That may change in the future.

You know, we'll see right how the accountability mechanisms play out from a legal context right now, you know, organizations should assume that the existing laws that surround it apply and how organizations are dealing with that today is of course adjusting to the speed.

So that's one thing.

So thinking about actually having agents that govern other agents, right?

So that's their role and their job per say, right, is to actually help, help in the governance of other agents.

Because of the speed and autonomy that these systems are operating out, that's becoming necessary.

They're thinking about the workflows and how to establish the workflows for the autonomous processes, the agents, such that the right level of human involvement happens, right?

So sometimes it's escalations.

You may set thresholds for certain decisions or certain types of decisions may get flagged for human review.

So all of that is, you know, what people are thinking about today and of course, having to set the right roles and responsibilities around that and making sure that you have the data points to back it up.

So when you do kick it to a human to get involved, do you have the right logs, the right information, the ability to verify the agent's identity, you know, which agent, where in the process did it happen?

All of that becomes extremely important. And we're seeing organizations and leaders think about those things and start to implement them.

Moderator: Dr Andy Packham

24:15

Yeah.

The one thing you mentioned about, you know, regulators saying that the existing, you know, there's existing laws and they apply, but very few have kind of issued, you know, explicit AI guidance.

How should organisations be kind of interpreting that regulatory gap?

And what does that look like?

You also talked about being proactive.
What does proactive actually look like?

Speaker: Heather Domin

24:37

Yeah, Yeah.

So this is something and actually I've, I've been in conversations recently where people are saying, well, you know, can we be thinking about almost like a, a, a rethink on, you know, returning to like principles based self governance mechanisms in the midst of some of this gap.

So I think what we saw maybe in like the 2018-2019 time frame where there was a lot of talk of principles, many companies were coming out and publishing, you know, AI ethics types type of principles and then a lot of focus on the regulatory aspects.

But now as you point out, I think there's some gap because there is a discussion about the enforcement.

Of course, even when we have the laws, there's often a period until when certain parts of that become, you know, applicable and actually enter into force and organizations that are held accountable.

So there's that, that gap between when the AI law is passed and when we actually see the accountability enforcement happen.

And then also because, you know, the technology is moving so quickly that the like with with agents, we don't yet see that in the laws.

We don't yet see specific requirements.

So organizations are still needing to turn to and relying on their principles and their values.

So this means, so for example, the way you can operationalize that of course is your own internal

policies and which may be stricter or put more requirements on your teams than are seen in the laws.

So for example, on like bias assessments or certain checks that you may have internal compliance reviews that are required and they check for various aspects and accountability.

And that is something that may not necessarily be required by law in all jurisdictions that you operate, but it's good practice.

And so organizations are adopting that because they know the value that that can help bring to their business, to their clients and to the wider society.

And so they're doing that right and they're aligning their practices.

And that's one way, you know, we're seeing is actually, you know, setting your own higher standard essentially.

27:02

Yeah.

Moderator: Dr Andy Packham

27:03

Thanks, Heather.

I think, Jenni, then just to wrap the list, I'd like to get a kind of what Microsoft's view on this and where are they?

What are the principles that shape, you know, the forward-looking approach of Microsoft's responsible AI practice?

Speaker: Jenni Rantakari

27:17

Yeah, absolutely.

So we've been on this journey actually quite a while since 2018 when we started already thinking about some of the principles.

And when I look at it, I would call out maybe four key things that we typically think about on anything when we build the systems.

And one is externally starting with that governance, thinking about then mapping the different risks and, the impacts and then measuring, measuring the potential impact of identified risk and then obviously keeping the continuous insight. And if I go a little bit deeper on some of these and our learnings, first of all, the governance like we discussed a lot already.

So it's really having that clarity on roles and responsibility documenting, to Heather's point as well. So not always thinking about what comes from the regulation, but also thinking about at the team level what and how do you do that with cross-functional teams so that you bring different parts of the organization together as well to think about if you have a sufficient approach.

And also thinking about like when you are going into the deployment, having those pre deployment reviews, thinking about privacy, security and potentially even using red teaming.

So that's what we do a lot as well.

And then moving to the mapping the risks proactively.

So we talked about proactiveness, so thinking about the technical vulnerabilities, but also like ethical societal impact as well.

And then thinking about like the different stakeholders, what those scenarios could be and planning for the safeguards.

And then of course, thinking about going forward, is that what are those metrics that we discussed already?

So do you need something that is more than we already have a part of the solution or do you have something more that is required in your specific use case, for example, for accuracy or reliability?

So some of those things are really, really critical.

And then going into when things go into the deployment, you start using the different solutions is like that ongoing monitoring so that you have feedback loops, incident response processes so that you can address, for example, new and emergent risks.

But also basically taking this defence in depth space, building those layered approaches so that you have safety and you have the user experience, you have the transparency.

So it's really like building those four, four things into your system and then proactively starting to manage what does it mean for you versus waiting for everything being laid out in, for example, in the regulation.

Moderator: Dr Andy Packham

30:14

Jenni, thanks.

I think, you know, 2018 till now, things have evolved.

Yeah, dramatically and not just in the way that we spend, you know, we think about responsible AI, but the way that AI is, it's become more autonomous, more deeply embedded.

And I think from what I've heard and you know, I'm now pretty sure, you know, governance is going to be the capability that separates organisations that really thrive here from one they're going to store. You know, the organisations that have not put responsible AI and governance at the centre of that cross functional team and then to move forward and accelerate will have a real problem.

It's clear, you know, organisations, they want clarity, confidence and control customers.

They want systems they can trust, they can understand and rely upon.

And those that's where the governance becomes, you know, hugely important and that becomes, I think a strategic asset.

I want to thank you both.

It's been a fantastic conversation.

I've really enjoyed it, you know and everyone listening, thank you as well.

If you want to explore more about how HCLTech and Microsoft can help build that next generation responsible AI governance, resilience, transparency ready for tomorrow.

Delighted to continue this conversation.

31:35

Thank you very much.

Speaker: Heather Domin

31:37

Thank you.

Speaker: Jenni Rantakari

31:38

Thank you.