Caitlin McDonald:

For this episode, I'm joined by Mark Hughes, DXC's senior vice president of offerings and strategic partners. Mark is responsible for DXC's technology strategy by driving innovation in DXC's core offerings. Before stepping into this role, Mark led DXC's security organization and offerings, and he previously served as BT's chief executive of security. Mark is a Royal Military Academy graduate and a British Army veteran, and he serves on the World Economic Forum's Global Cybersecurity board. Welcome, Mark.

Mark Hughes:

Well, thank you, Caitlin.

Caitlin McDonald:

It's a real delight to have you.

Mark Hughes:

And thank you for having me.

Caitlin McDonald:

Yeah, absolutely. And what I wanted to kick us off with was a few of my prior guests on the podcast have spoken about how digital ethics is currently mirroring the development of cybersecurity as a discipline, moving from a kind of important but little understood set of ideas to a recognized business function. And I'm wondering what your ideas are on that. How has security evolved as a discipline and what parallels might the field of digital ethics might go through?

Mark Hughes:

Yeah, it's a really good question, Caitlin, and thank you. Well, the way I see the way the security piece has evolved is it's gone in quite a few distinct stages. Firstly, I think that there was the realization that there was a need for some level of control on the basis that the reports of malicious activity towards organizations began to kick off. And I suppose there is a fairly important thing about cyber that makes it quite unique. Generally, it gets done to you, as opposed to necessarily you having to consider it in its own right, as something that comes from within. Now, that's not entirely true because there's obviously the category of threat that we call the insider threat, but not withstanding that, I think the genesis really came from organizations suffering the type of attacks and then obviously, that began to start hitting thresholds.

Mark Hughes:

Here we saw then the rising up of the subject matter on the agenda. However, I think the core thing that I've seen in cyber, to a certain extent in privacy as well, is the nature of the risk. And I'm going to contextualize this within risk because the nature of the risk is that there is a risk that when you aggregate it, has potentially very far reaching consequences. And the notion in this world of where risk is taken disproportionately by one part of the digital ecosystem, which has a disproportionate impact on another part, potentially a much bigger part is I think really characteristic of cyber. That concept I think has taken quite a while to be understood.

Mark Hughes:

In the early days through some of the work that I did in my prior organization, working for example with UK, US governments, is that the real challenge there was how to manage that notion of disaggregated risk, where there was an aggregated risk impact, when most of that disaggregated risk sits outside the government department, though all the government machinery, if you want to call it that in most countries, where the ability of the government to then control and manage and mitigate those risks was quite limited.

Mark Hughes:

I think the first stage was a realization that there was a risk and that aggregated risk had potentially really severe consequences. Then I think there was a sort of standoff point where the public-private sector didn't quite understand who is responsible for what. And it's actually only fairly recently in the last five years or so, that governments have really mobilized with that core founding principle in mind. The prior activity and there's a lot of talk of cybersecurity, was much more about information sharing and raising awareness, which is all very well and good, but it wasn't addressing the core ability to manage and mitigate the risks associated with cyber.

Mark Hughes:

Once that step was made, then the cyber management framework and governance framework really began to build up some steam and, and began to be measured and managed I think in a much more comprehensive way, where the root of this is being able to understand what the potential risks are, and then a mechanism for aggregating those risks so the appropriate mitigation can be taken. That is, I think, how the whole ecosystem has evolved.

Mark Hughes:

Governance is at the heart of this and it's this sort of funny word to use. Funny, not funny, but funny in the sense of a strange word to use, in the context of when we talk about everything digital, because it all sounds quite stuffy and yesterday, and all those sorts of things, not really working at the pace. But it's really fundamentally important because without frameworks and the which we can manage and assess risk, then you won't ever get to that point where, as I've said already, one part of the system can have a disproportionate impact on another part. Getting those governance frameworks in place was pretty key.

Mark Hughes:

Then I'd say that the next thing that began to happen is then of course, at that point, once that became clearer, then roles and responsibilities began to be able to be assigned. So then what you see is regulatory frameworks emerging in the cyber area, where often organizations, especially in the private sector have pushed back and said, "Look, why should we be doing these things?" But I come back to my previous point, well, they're potentially quite important because of the knock-on impact across other parts of the ecosystem. So regulation began to appear, and to a certain extent, reputational pressure also had a huge part to play. I think that's a really important factor as well, where organizations, even though in the main, most organizations are victims.

Mark Hughes:

This is the sort of slightly peculiar thing about cyber is that there is a need to be able to put the checks in the mitigations in place, when actually it's the criminals who are perpetrating these types of crimes, who are the ones you really want to go after, but actually the victims are the only ones where the control is able to be put in place to try and thwart the intentions of the criminals in the first place. I think with

that, there's governance frameworks, then came control frameworks and stipulation of controls through regulation. But even before regulation appeared and many organizations realized that reputationally, there was a huge amount of stake, which gave an impetus to then putting more controls and putting the framework in place. So I see that's how the cyber landscape has evolved.

Mark Hughes:

What I would say though, is that there is still a reluctance, and it's not a reluctance born out of one where people maliciously don't want to do something or don't want to do it for the wrong reasons, "Oh, it's too costly. It's too." This there's always, of course, there's a consideration around that in terms of the security triumvirate, if you want to, security cost and the impact of the working individual and digital ecosystem.

Mark Hughes:

What the cyber lessons I think are borne out for me is just the complexity of how we manage and run the IT ecosystems that I'm certainly in the middle of DXC, is very much in the middle of. Where we as a organization, for example, are part of a custom's ecosystem and there are other third parties in that ecosystem, as well as the customer, and then obviously their customers themselves all have a part to play. That is very complex. So the whole notion of, "Oh, yes, let's do cyber and let's do it better," the read across that perhaps to others for me is, it's enormously complex, and even if there is tremendous wealth and there's regulation, and people have quantified and understand the risk, both reputationally and financially to their organization, actually getting the controls in place to be able to then effectively mitigate those risks is extremely hard. It is ever more complex in terms of the ecosystems that we continue to build.

Caitlin McDonald:

Yeah. There are so many great points to pick up on in that answer. One of them is, so when I think about digital ethics, there's the reputation angle, there's the regulation angle, and there's also a revenue angle as well. That's not just from the perspective of your customers might walk away from you if they start seeing you put out what they consider to be unethical services or using unethical business practices, and actually the other way around as well. If you can show that you are behaving more ethically, people will pay a premium for that as well. So if you look at something like the development of Kitemarks around fair trade, for example, you might start to see similar things with algorithmic auditing for instance, and saying, "We actually have had independent checking and verification of these things," and that might be something consumers really want.

Caitlin McDonald:

But also the other revenue side of things really is attracting the best talent of course, is a huge, huge issue for businesses, to try and make sure that they're doing the best that they can. Many different studies have shown that especially people who are working at kind of the pointy end of the most technologically advanced pieces of AI and what we really consider to be the real innovative pieces of digital technologies, they really want to work for organizations that they feel match their values, and that they feel are doing good things for the world. From that angle, being able to position yourself as a differentiator is really important also.

Mark Hughes:

I couldn't agree more with that. The whole world notion of ethics is nothing new. Ethics exists and has existed in business in our daily lives forever. And it's now, how you translate that into the digital world. I think the comparison I would draw there with my experience in the cyber world, is so I would come back to that point around the aggregated risk versus the distributed risk.

Mark Hughes:

Decisions that are made with ethical considerations can have quite far reaching consequences, especially most importantly, when we get into the world of data sharing and how data processing happens with distributed datasets. I think the sort of fairly simplistic view, to quote, do no harm, and things like that are often overused and quite short-sighted. It's a lot more than just doing that. As we know, ethics as a [inaudible 00:11:12] outside, digital is something that is studied and being studied for millennia and will continue to be, because it's not straightforward and there are different decisions and different considerations that need to be made.

Mark Hughes:

But there is now, as you rightly point out, within the digital ethics space, clearly that point about the fact that one particular organization, maybe let's just take an example, managing a particular data set and how that is accessed and made available to others, and do the users themselves, or the people who are depositing that data actually understand how that will be used? There is a really important ethical questions, not on the basis of that particular dataset, but on how that could be used and the consequences of how that then in the broader digital ecosystem, that data could be exploited. That's not easy, but I think there's a lot of parallels there with the cyber piece about how you deal with the aggregate.

Mark Hughes:

I think there are, like with many of these, ethical questions. There's a sense that comes into play. I'm not going to say common sense because it's not as straightforward as that, but there is a sense, sort of the creepy versus cool, if I can put it in those terms. A good example would be a few years ago, not that many years ago, but one of the airlines, I think promoted the idea of being able to select your seating based upon finding a like-minded seatmate, where a bit of social media type information was harvested and all the rest of it. I think that's quite creepy, right?

Mark Hughes:

Some may see that as cool, but there's that sort of boundary. But what was that data, when being made available to that airline, for example, and the airline being able to access that data, did the user ever think that that's how it could be used, and was that an ethical decision to be made? There was a fine line between it, but that doesn't feel right. That doesn't feel ethical in that sense, and indeed, most of the airlines have abandoned any ideas of doing those types of things.

Mark Hughes:

I suppose it always comes back to just because you can, doesn't mean you should. I think that that therefore takes us into the world of, "Well, okay, so if we draw the parallels back to the cyber world, how do you get after this? How do you create a construct that enables you to make those decisions? And even if you make the decision, an ethical decision on how you do it, you don't have the ability to be able to revisit because it's not necessarily obvious at the outset when designing a new tool and new

algorithm, for example, in AI, that it might have consequences, which you don't foresee at the beginning."

Caitlin McDonald:

I think you really nicely drew that parallel between the development of governance mechanisms over time, which essentially is what we see through the model that my colleague Simon Wardley has developed around worldly mapping, where you're essentially saying that as you go from something being in a genesis phase, where it's very, very new, and you don't really know what the possible consequences of that thing are, through to industrialization where essentially the harms of benefits are extremely well known. That's when you can start to develop those governance mechanisms, because you have a much clearer idea of the possible outcomes. And essentially, you can kind of foresee the development of this. You've seen in cybersecurity, that's exactly what happened. It moved from, we have some ideas about this, to we now have governance mechanisms and everything's a lot more structured.

Caitlin McDonald:

I can see ethics going in very much the same way, where you might see regulation beginning, and you're starting to see it happen, but it's going to start to coalesce more. And I foresee a future many more kind of institutional structures around this as well, which might parallel your experience with cybersecurity.

Mark Hughes:

I think that we have to think practically, although again, the whole ethical dynamism questions are quite hard to wrap your head around, but at an abstract level, that is always going to be the case. And even with security, just like there is with another field, which we often talk about, privacy, as well. But then you can take that down from the abstract into the actual doing. But there are some considerations I think, with this, which makes things slightly different.

Mark Hughes:

But to be more in my view, systematic with the type of governance that we've seen emerging in cyberland, that I think has been helpful, they are things like this is an important consideration. When I mean important consideration, from a business, I stand here looking at it from a business point of view, that we have constructs, we have defined parameters of who's responsible for what, so there's a lot that we can borrow on from privacy security areas about having already established the concept of data and how data is managed, for example. The same thing can apply to IoT, AI, and other tools as well. Who's responsible for what? There are some things that we can take from that.

Mark Hughes:

Then having established those principles, then again, we can learn from some of the mechanisms that already exist. So, how do you risk assess, and what does an ethical risk assessment process look like? Well, good news is, as I said, we've done that with privacy. We've had much regulation, for example, with GDPR and stuff, and we've looked at data flows and the like. So it's clearly not the same subject area, but the mechanisms of being able to consider the risks are now much more developed, I think, than they perhaps would have been a few years ago. So there's a lot there that I think that this area can take from there, to then establish ethics by design.

Mark Hughes:

Let's now get down into the work that many thousands of our coworkers do in DXC every day, which is that doing development activity, for example, they're putting new tools in place, and there are therefore mechanisms that they can follow through, which allows considerations to be made during that work, that puts that ethical lens on top of it, just like they do with security, just like they do with privacy. Then we can create some control mechanisms around that, about how then certain considerations can be escalated, and then considered within that risk context. And within a context of risk, that yes, starts with our business and what the work we do on behalf of our customers as well. But then into broader frameworks, back to my point about that disaggregated versus the aggregated risk.

Mark Hughes:

Therefore, I think that there are absolutely the way in which those digital interactions happen, there are clearly defined ways in which businesses and people and individuals interact with tools and data. And so therefore, you have a fairly good starting point where you can then build that risk assessment process and create an environment where the relevant consideration controls... I keep on using the word controls. That's probably my security background coming through Because we do apply controls to there. In this world, it might not be specifically about putting a control in place per se. The control might be less technical, might be much more about a consideration about whether or not that happens or not. But there are equity still controls; opt-in, opt-out questions, understanding, making it clear to users the types of privacy considerations, which then lead to the ethical outcome, but are baked into certain products and services.

Caitlin McDonald:

I really like that. At LEF, we like to look at not only from a risk angle, but also from other kinds of opportunities. I actually want to take this conversation into the idea of resilience also. I know you've written about the importance of developing cyber resiliency before. It's not just about how do we stop things from happening, but also when a bad thing does happen, what do you do next? Because it simply isn't possible to avoid every single ethical risk. Sometimes it's just about accepting the best of a bad set of options and saying, "We did everything that we could to make this the best possible thing that it could be." What do you think in terms of could organizations develop some kind of ethics resiliency? What might that look like?

Mark Hughes:

That's again, a great question. I think about the resiliency as being way down the ecosystem of how you start with, let's be specific, ethics by design. So how do you make that risk assessment consideration about what the ethical lens is about what you're doing? And you have to have some things that you hang your hat on in terms of what is the system of values, and moral principles in terms of the types of digital business and interactions that we're conducting and building. So there's a framework against which you can then create a risk assessment and then a design to design. I think one of the things that I would say, and this is an area which leads to resiliency, I think is about it isn't necessarily as cut and dry.

Mark Hughes:

In the security world, you've either lost the information or you haven't or there's been an attack and something's gone down or it hasn't. Here, this may be more subtle and therefore, I think one of the things in terms of what I consider to be in the beginnings of what is an ethically resilient organization, it's about how you get staff and customers to be able to speak up. And that is so that they have the freedom to speak up about, "I'm doing something. I think I can see the consequences." That has to be

factored in. It's probably one of your best ways of factoring in to that ethics by design, through that risk assessment process. And not just speaking up, but listening up as well. I often think we forget about people can speak up, but you need to listen up as well.

Mark Hughes:

The design piece, and again, the resiliency, I think, comes from understanding what the trade offs are, and understanding and making those assessments. In security that is much, much better understood than it used to be. I think there's a lot to learn there from both the privacy and security area, that can be baked into, as I said, the ethics piece. But then you get into, right, so we've made some decisions, as you right said about, what our appetite there's going to be, risk acceptance and the like. Then we then build governance frameworks with tangible things that we do and we create some lines against which the risk assessment says dictates that we design, we develop in these ways, we make data available in these ways, and there are the controls that we put in.

Mark Hughes:

Then we have to test those controls, so test that they're operating in the right way, so when developers and people who are running the infrastructure, actually are doing this, that they are taking these considerations seriously and making those decisions. That's all very well and good. So you can say, "Well, there's a risk, there's a set of ways in which we operate that make sure that we can underpin our statements that really aligned with our risk in the way in which we do digital ethics." But then you get into, I think, well, as you rightly said, "Well, what happens when something does get wrong?" And people often forget about this and they forget about the fact that often the best mitigation, certainly when it comes to security, is about how you respond when something unforeseen happens or something happens which shouldn't have happened because there should've been a check-in place that didn't operate effectively. As you say, things do go wrong.

Mark Hughes:

What I've learned through my experience with security is that that resilient piece of being able to respond is often the thing that makes the biggest difference with a lot, because things do go wrong, regardless of where you set your appetite to, your risk appetite that is.

Mark Hughes:

Then having the ability to move quickly, the ability to have a framework for response within the overarching way in which you manage incidents. Yeah, we're a technology company, stuff happens all the time. There are very tried and tested ways of managing infrastructure resilience. You can use those methods to be able to escalate, get the right people involved. In terms of the framework for how you do it, clearly they're very different considerations. But then get the incident, if we call it that, into a place where then the individuals who have made the considerations about how you manage the risk and therefore, can be alerted to it and then can decide what they do. I think in that respect, you then have a fairly comprehensive ecosystem there of thinking about the security paradigm of the insecurity, we call it. One of the frameworks we often talk about as a NIST framework, which includes your ability to respond and that's a very important element of it.

Mark Hughes:

I see the same thing in the ethics space. One mustn't forget that that is going to be an important consideration. We're not going to get it right all the time and there will be unforeseen consequences of

doing things in a certain way. So then being able to respond, understanding what part that we, as a business, our customers and their businesses play in that ecosystem is going to be really important, and will continue to be important, and then you can respond effectively. I think that's one area where I would say a direct read across from what I described as cyber resilient to ethical resilience.

Mark Hughes:

However, I come back to what I said earlier on, which is in the concept of cyber resilient, I will go on and often people will look at me, and I spent many years in the security space, and they'll say, There's all these fantastic new tools, and especially in security, there's a lot of technology there." And often I look at it and say, "But it seems that the things that most organizations get tripped up with when they are a victim of a cyber attack are fairly basic things, that aren't implemented or done in the right way." And I often will say that there's only a handful of things, that if organizations get them right and get them right consistently, then they you'll be able to mitigate most of the threats that exist out there.

Mark Hughes:

I think the same thing applies, that resiliency then goes down, not just being able to have the risk assessment, not just being able to put the relevant right controls in place, having speak up and listen up processes and a response process, but it's also about getting people to consistently do the things that you've elected to do across these complex ecosystems. I think for that, especially within this space, cyber used to be not very well understood and now as much better understood. I think ethics, people will think about it as being a, "Oh, it's a conceptual idea," when it's not.

Mark Hughes:

It is on one hand, but it's not when you actually get down to some of the things that I've been talking about today, so therefore, affords us an opportunity to be able to get into that detail with individuals who can then have guidance and things that they need to do consistently. That's how we then create resiliency, by communicating tangible things in ways in which people don't understand, that then changes their behavior, ultimately the culture of the organization. That's how I think you also build resiliency as well.

Mark Hughes:

In security, it's taken a long time to be able to get that, and we're not there yet. In the ethical space, that's going to, I think, require the same sort of approach, keep it tangible, make it very specific to communities of interest within our organization and how we interact with our customers as well, and then ensure that those things are done, and done consistently well across the entire ecosystem we operate in.

Caitlin McDonald:

I think that really takes me nicely onto my next question, which is really about developing the balance between a culture of ethics or a culture of cybersecurity and developing governance mechanisms for these things, because I think they're interrelated, but I think that they both play really important, but different roles in creating the governance that you need.

Mark Hughes:

Yeah, and I think it always comes down to exactly, as you say, which is if I take my experience from security, I would far rather not have a whole plethora of controls lined up where we're all about

checking and monitoring, or actually the developer who's doing an application transformation is thinking about the controls on that particular container or whatever it is that they're doing, that they think, "I better do that because I know now, that it's the right thing to do at this stage in terms of application testing." Or let's think about the other end of the infrastructure spectrum around building configs on servers, for example, that just having a sense that if you're technically capable of building the conflict, you'll be technically capable of understanding that there are certain choices to be made from a security point of view. So I think that there is-

Caitlin McDonald:

And it's a natural part of the development process that you've actually think about those things.

Mark Hughes:

Exactly. And if we take the very, very tangible example, which most of our listeners will be very familiar with, is patching. The world of patching is pushing patches out. Why not have a patching process where now everyone understands that things have to be patched very regularly, and there's going to be vulnerabilities that are discovered. The ability for any software provider to release software that doesn't have potential vulnerabilities in it, that they don't know about it at the onset, it's just not how it works. It would thwart our ability to progress if we decided that nothing would ever be released until it was 100% absolutely perfect. In many cases, you don't know that before you actually put it into operation in any case.

Mark Hughes:

And so the ability then to be able to deal with that uncertainty, live in a world where we understand that now patching is a regular thing that has to be addressed, where we still offer the way in which the process works is, "Here's these patches. Please implement them." What about where people know that patches are coming, they choose how they take the patches down, how they apply them inside their own development life cycles. We're moving towards that now. There's a bit of creating the conditions and the tools to be able to do that. And as you say, a realization that there's a cultural awareness around the fact that that is something that we now do. It's part of our everyday thing.

Mark Hughes:

Of course, I would love that to be accelerated so that we had less around governance and controls and checking and more about, "Well, of course, I know this thing has to be patched and configured in such a way that ensures that we understand that we're not making it more vulnerable than it needs to be for the task that it's there to do." I think there's a lot to learn there. I think in the digital ethics space, that hopefully is something that we could learn a lot from and try and circumnavigate, if you want the fairly tricky governance, heavy governance type of approach and appeal much more culturally.

Mark Hughes:

I think perhaps the ethics world lends itself a bit more to that because there are moral questions that people I think are more intrinsically in tune with, perhaps than some of the security thing. In the security space, I think that people often are surprised and shocked by the willingness of some peoples do to others harm, to do bad things. Perhaps in the ethical space, there are people, we're all making ethically-based decisions all day, everyday.

Mark Hughes:

I think the question is that everyone has their different opinion about where they see that risk. And so being able to communicate that risk in a structured way, but perhaps there's greater hope in this field that people will be able to act more independently with a set of guardrails and guidelines, if you want, that are implemented, not through onerous checking and governance processes, but more through it's the right thing to do and that's the way we behave around here.

Caitlin McDonald:

I'm now picturing this whole world of ethical patches, whatever that might look like, which could be an interesting future. But the other thing that occurs to me, Mark, is other guests who've spoken to me about essentially the development of the health and safety culture and processes, where you never get on a plane without seeing people run through the checklist and do the crosscheck of the doors. Right? You never have a surgeon that doesn't go through the checklist. There's set things that the World Health Organization tells you to do before you do surgery on someone, just to make sure that you're not doing the wrong thing. And so I could see a world like that, where actually it does come down to a fairly simple set of checklists, but you just always do that because that's part of essentially the ritual of making the lifecycle of software of what you're doing. So I think that's an interesting approach as well.

Mark Hughes:

It is, Caitlin and I agree with you. I think the only caveat I put on that is the nature of... And let's think about medical science. Millennial in the making, AI is what... Decades, even would be generous in terms of the length of AI that science has been around. Very few years, relatively, very, very few and it's astonishing what we've managed to achieve in those few years. And so that's one consideration, so just the cultural basis under which those processes operate.

Mark Hughes:

But I think secondly is the system. And the system that is the surgeon doing the operation, it's quite a closed system. There's a patient, there's a surgeon, there's a procedure that needs to be done. I'm not trying to diminish it into something that is in any way, shape or form trivial. It's extremely complex and obviously, there's a huge risk where there's people's lives at stake, but it is a relatively more closed system. Whereas I think a lot of the considerations that we're thinking about and talking about today are things which is a much more interconnected system, almost by definition in its nature, in terms of being digital, where how do we deal with that consideration and checklist in a world where that checklist might've been okay when you were using that particular tool in that way. But then now, you've looked at in another way.

Mark Hughes:

That said, I am a fan, but we've got to grind it out into something and it's the old 80/20 approach, which is a checklist approach that will get us most of the way. Certainly, my experience from security is, get yourself to most of the way, will have a big disproportionate impact in terms of the overall risk posture that you're carrying. And when I say disproportionate, I mean, you get a lot of bang for you fairly simple bucks, if that makes sense. I therefore do agree that there is potentially a way of doing that, with a couple of those caveats, that we haven't had a lot of experience at this, and secondly, the systems are much broader.

Mark Hughes:

Again, a plane, again, I certainly don't want to trivialize the enormously complex ecosystem that airlines and aircraft, and everything else operate under, but once those tools are shot, the thing is the thing operates in the main, in a closed system in the main. There's no [inaudible 00:34:32] connectivity. But whereas what we're talking about is things, it is actually about designing things that are permanently interconnected and those connections are changing all the time.

Caitlin McDonald:

That systemic view is a really important point because you might be designing a very tiny component of an enormous system, and you might actually have no idea what other components are involved in that system. As we grow ever more complex digital ecosystems, these questions do become ever more nuanced because you have to think not only about what you're doing in your day-to-day work, but also about where that fits in, how that might react in a system of other components and other considerations.

Mark Hughes:

But the good news there, Caitlin, and I say this that in security similar consideration, but there are useful definitions and governance and guidance now, which like, as I said, through the privacy space, that allows those delineations to happen. It's not perfect, but at least who owns what, who owns which risk is really important. Otherwise, you can sort of mistakenly assume that I have to take on all the consideration, for all of the risks in any way in which the thing could be redeployed. I think that usefully, there are things we can put on, it's not perfect. We're going to have to think harder in the ethical framework about how those considerations are put together, on the basis that, back to your point about who's got to do what intervention, at what point? Who or what, let's be clear because obviously machine is really important here as well.

Caitlin McDonald:

Yeah, very important. And as much as I would love to talk about this all day, and I'm sure we could talk about this for hours, we do have to finish up, so last words, any final thoughts or key takeaway messages that you want to make sure our audience definitely takes away with them today?

Mark Hughes:

Most certainly, keep it simple. I think the thing is that these are big considerations, but ultimately there are a few things, and you can do those few things extremely well, through proper risk assessment and making sure that then the distributed nature of the people doing the work actually abide by those principles and things that you set in place. Just keep that fairly straightforward and simple and I think that an organization will go a long way to be able to manage that. And then secondly, have an incident process so that if there are unintended consequences and things do go wrong, that you can respond effectively.

Caitlin McDonald:

Super amazing points and thank you so much for joining us today.

Mark Hughes:

Thank you, Caitlin. Nice to speak to you.

Caitlin McDonald:

My pleasure.

Caitlin McDonald:

Thanks for listening to the Growing Digital Ethics and Practice podcast. You can find out more about the Leading Edge Forum perspective on digital ethics by searching for the phrase stemming sinister tides, where the first link should be our position paper, Stemming Sinister Tides: Sustainable Digital Ethics Through Evolution.