IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with Dr Megha Kumar

Carol Baker

As new research reveals that more than a third of UK businesses are dangerously unprepared for AI risks, we talk to Dr Megha Kumar, Chief Product Officer and Head of Geopolitical Risk at CyXcel about the research findings and how CyXcel's Digital Risk Management platform is the first of its kind in helping companies become digitally resilient.

Dr Megha Kumar
Chief Product Officer and Head of Geopolitical Risk
CyXcel (https://www.cyxcel.com/)

Megha is CyXcel's Chief Product Officer and Head of Geopolitical Risk. She brings over 14 years' experience in product innovation, service delivery and client development in the geostrategic intelligence and country risk industry.

She has been a long-standing, trusted advisor to C-Suite decision-makers in Fortune 500 and FTSE 100 companies, across the technology, energy, mining, finance and infrastructure sectors. Within the public sector, she has worked extensively with major governments on national policy and regulations, and various international bodies, including the United Nations, IMF, NATO and the World Bank.

She is a well-known expert on global digital and technology policy, emerging technologies such as AI, and digital market regulations, and on developing Asian economies.

A renowned researcher and writer on technology and gender rights, she has co-authored 'Global Perspectives on Women, Work and Digital Labour Platforms' and authored 'Communalism and Sexual Violence in India: The Politics of Gender, Ethnicity and Conflict'.

Prior to joining CyXcel, Megha held senior leadership positions at Oxford Analytica, where she established and led the firm's Cybersecurity and Technology Practice for over seven years. She has lectured in history and politics at the University of Oxford and was a journalist at two major Indian broadsheets. She holds a doctorate from the University of Oxford as a Rhodes Scholar.

Please tell our readers a little about yourself and your interest in geopolitical and cyber risks

I have always been fundamentally interested in the interconnectivity between things, and how the dots between diverse trends, different disciplines, and different topics connect. I have been fortunate to have a career where I have been able to pursue this core interest of mine.

I was a journalist in India for a couple of years with two Indian broadsheets and then trained as an academic specializing in the political economy, ethnic conflict and gender trends in India.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

I got my Masters and doctorate from Oxford and taught at Oxford for a few years, but I found that even within academia the desire to connect more and more dots wasn't quite panning out as I had thought. So, I turned to the world of geopolitical risk where I advised companies, including Fortune 500 companies, multilateral institutions, and the biggest governments on the political economy of Asia-Pacific, focusing on South Asia and Southeast Asia.

For me, that led to the transition to technology and cybersecurity because increasingly my work in the mid-2010s was touching on issues of technology and cybersecurity. I needed to focus on this because it was becoming apparent that digital interconnectivity was going to be the thing that ties us all together – and potentially – the thing that divides many of us too.

You were at Oxford Analytica for over 13 years, so what attracted you to work at CyXcel?

Oxford Analytica is a terrific company with a fantastic team doing fabulous work, and through that work I got to advise over 500 top companies which are household names, nearly all G20 governments, and nearly all multilateral institutions. I got to work with an extraordinary client base on Asia-Pacific technology and cybersecurity.

What drew me to CyXcel were two big things. First, is the even deeper interdisciplinarity that CyXcel brings to its clients – we combine our capabilities in tech, cyber, law, geopolitics, supply chain – so we can actually solve an organization's difficulties, challenges, headaches with a more seamless and diverse toolkit.

Secondly, is CyXcel's incident response and technological transformation and legal abilities. We can, and do, a lot of responsive on the ground work with our clients, which is not something I had the opportunity to do at Oxford Analytica.

So, CyXcel meets my professional and personal goals.

CyXcel's core team is around 30 people, and we are spread across Europe and the USA. We work very closely with the broader Weightmans team giving us access to about 1,600 legal professionals spread over multiple offices across the UK. Then through both CyXcel and Weightmans we work through an even larger ecosystem of technical and legal partners.

The trust, credibility, integrity that people associate with Weightmans they have come to expect from CyXcel, and rightly so, because we are not just any cybersecurity shop. We are part of a regulated business with a 197-year-old pedigree, and it takes some doing to maintain the kind of reputation we have achieved over those many years for our clients both big and small around the world.

It's been a fantastic journey for us, and in any given year across Weightmans we serve around 5,000 companies – it certainly keeps us busy.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Given that CyXcel is part of Weightmans (a law firm), how would you define CyXcel's independency, and has distinguishing it for potential clients been challenging?

In the UK, I think the traction has been much easier to gain because we offer a full 'boardroom to the courtroom' offering as we are able to do all aspects of technical, cyber and advisory work coupled with all kinds of legal litigation issues. And with this clients can benefit from all the regulatory things that they would expect such as legal privilege, technical excellence, integrity, and the trust that they can rely on.

In the USA, we work through trusted local partner network and across 55 countries through our Global Legal Service.

We are the only the second law firm to be accredited by the National Cyber Security Centre. All those accreditations and credibility have been hard won, but that is what gives clients quality assurance.

Sometimes it does happen that companies, and new clients, take time to wrap their head around this end-to-end service because it is so new, innovative and fresh. But we are delighted by that because it's the right solution for a problem that we face.

What sets CyXcel apart from its main competitors?

This is an interesting one because we have many competitors and in other respects, we have none. We integrate legal, cyber, strategic and technical expertise to provide wholistic solutions for securing digital operations. There are many companies that operate in these silos, and they could be considered our competitors. But in terms of the whole integration piece, there are some large professional companies for example the Big Four could come close to matching what we have. But what sets us apart is our highly competitive offering and our focus not just on big companies and big organizations in the public and private sector, but also mid-sized companies because they are often the ones which have the most constraints on their resources, and therefore we can also have the most outsized impact on their digital resilience.

And what else sets us apart? Well, our world class team – but I would say that, wouldn't I?

Tell our readers more about the research you have undertaken into AI risk and its impact on businesses. Did you undercover any particular issues which firms are facing that surprised you?

I've been advising companies on AI since at least 2016 and at the time when I talked about machine learning (ML) to even very senior executives, they kind of looked at me as if they were waiting for me to speak in English!

Obviously, the world has changed since the arrival of ChatGPT, and we've been innovating over the last year quite intensively and wanted to understand where companies are at regarding their AI. Such as, AI adoption, how they think about AI risk, and the opportunities and impact that they could face within their own


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

businesses, as well as their industry sector or community. So, we set out to find out what was going on.

We surveyed around 400 cybersecurity professionals across the UK and the USA asking them whether they had amended their risk strategy in light of the AI related cyber risks. We also asked whether they were thinking about creating an AI use policy for their organization, and if so, was that policy being kept up to date.

The results were very interesting.

Around one third of respondents (32%) said that they had amended their strategy for adopting AI quickly and safely.

But for me, the interesting number is the other part of that. If 32% have done so, it means two thirds haven't done it. Around 70% said that they have an AI governance policy in place. Well, what's the other 30% doing?

So that seems to me to be very valuable insight in terms of where companies are at, what they see as their priorities, and what they're able to address quickly and effectively if resources are to be optimized effectively given that technology is moving so rapidly.

Was there anything in the research findings that surprised you?

What really surprised me is that about over 60% of the respondents said that they have not amended their AI strategy for cyber incidents or ransomware attacks.

In light of the number and the increasing damage of cyber incidents and breaches, I would have expected the overwhelming majority of respondents to have amended their AI strategy, particularly as cyber breaches have become ever more frequent, more damaging, with ransomware attacks becoming sophisticated and now target all sectors, not just large enterprises. And the other major AI-related risk to cybersecurity is from phishing - freely available AI tools can now create and circulate highly convincing images, videos, voice messages and texts that can result in identity theft, and in turn result in a massive cyber breach.

So why is it something so obvious is not being addressed by the majority? That's what I found striking and a little bit worrying.

What are the biggest stumbling blocks for companies looking to become digital resilient?

First, a lot of companies still don't understand the extent of their technological dependency. They assume that because they are an agricultural or kitchen company for instance, that they are not a technology company. This misperception can result in complacency where businesses think that their digital operations need not be as secure or regulatory compliant as they need to be. The failure to understand that interconnectivity, I think becomes the stumbling block because if you don't appreciate the extent of the problem, you are not going to invest the appropriate resources to address it.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The common misunderstanding which I would encourage companies to rethink is an age old saying, which is “prevention is better than cure”.

If we look at some of the statistics, cybercrime is forecast to cost businesses over $1.5 trillion in the next two years. The numbers are staggering.

However, prevention, at both a global and an individual company level would be much more effective and would lower post-incident costs because the more prepared you are, the stronger the chance of recovering from a cyber incident more swiftly and more effectively. Plus, regulators and customers are more willing to give you a wide berth if you can confidently show and communicate to them that you did the best you could. Things can still go wrong, and you can still experience a breach but if you were prepared and ready to act and could jump into remedial and containment action, then everybody is more willing to be understanding. Whereas if you’ve allowed your systems to operate without basic protections such as multifactor authentication, then you can see regulators and a company’s customers and shareholders would be less sympathetic.

Which emerging cyberattacks can we expect to see in the cybersecurity domain this year, and will CyXcel’s technology need to take any new direction to deal with these?

We are seeing multiple trends emerging this year and next. At CyXcel, we will stay ahead of the curve because if we don’t, then our clients won’t either.

There are two key trends that are worth highlighting. First, sector-focused attacks will continue to rise with social engineering tactics being used to exploit human error, human gullibility, and human trust – all these will become a very common threat vector hitting companies across different sectors who don’t understand their dependency. These companies open themselves up to a greater risk and if companies across different regions, sectors and sizes don’t cultivate an actively enterprise-level culture of cyber safety and cyber responsibility, then the human error factor will always be our weakest point.

The second major trend is supply chain breaches. Sophisticated hackers are only in the business to make money and steal valuable data, and we have seen greater sophistication within the cybercrime market where very targeted social engineering attempts are made to gain unauthorized access to the weakest point in the supply chain. We recently saw this with Qantas where it was a customer service platform used by a call centre, and that person was duped into giving the hackers access[1].

Cybersecurity is only as robust as its weakest link and very often people or small or insecure suppliers.

So those two factors will need to be taken seriously by any company looking at digital resilience, and CyXcel is leading the pack advising our clients. You’ve got to really stay ahead on defensive solutions at all times not least due to the rapid pace of innovation in dual-use technology.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Have you found that companies who have cybersecurity insurance are more, or less, prepared when it comes to digital risks?

In the ecosystem of insurance, cyber policies are still a relatively small category. It has only been around for a couple of decades and over the years it has gained traction establishing its utility. There are all kinds of things which are covered in cybersecurity insurance, such as business continuity, breach work and litigation. Overall, cyber insurance is one way to transfer cyber risk, making it a tool in the toolkit of digital resilience, so appropriate cyber insurance cover is a wise investment for businesses.

However, the risk is that companies become complacent and assume that just because they have cyber insurance, they don't need to take proactive resilience seriously. They assume that if something goes wrong, the insurance will cover it. Much will depend on the policy wording of the insurance policy of course, and some companies can come unstuck when it comes to what is, and what is not covered, and whether the damage exceeds the claim they can make.

Cyber and digital resilience is not something that you can simply buy your way out. If social engineering attacks are putting a company's people at risk of hacking activity, then no amount of cyber insurance is going to fix that problem. That requires a cultural change where everybody from boardroom leadership to the person who manages access to a building, must take resilience and security seriously. So while cyber insurance is valuable, it is no excuse for poor cyber security.

CyXcel has only recently launched its Digital Risk Management (DRM) platform – what sort of organizations were involved in beta testing the system, and which industry sectors are now showing the greatest interest?

In developing DRM we collated feedback, input, insight from multiple sectors - from agriculture, public sector, manufacturing, through to retail, financial, and beyond - and also across multiple regions, especially UK, EU, USA.

We looked at different kinds of risk owners, not just CISOs or Data Protection Officers, but also sourced input from General Counsels, Heads of Technology, Board members and CEOs so that we could make sure that our platform took into account all the various types of sectors which are affected, and support all types of risk owners who are responsible for managing this risk.

As I said earlier, it's not the Head of IT alone who can ensure the security or continuity of any company's digital operations. It's a collective responsibility. People are accountable for different parts of the security framework and to varying levels within this but it's a collective responsibility. So, it was important to us to get the point of view of different risk owners so that our DRM platform could support everyone.

Essentially for me, the guiding principle was that if I can crack the expertise-driven and department-focused language of all these various risk owners in a seamless,


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

simple to use platform, then hopefully companies can spend the resources and the time fixing the problems rather than learning each other's language.

What is CyXcel's vision, direction and priorities over the coming year and how do you see these defining the evolving digital landscape within your clients' businesses?

Our core priority always has been, and will always be, to deliver excellence for our clients – whoever they are and wherever they may be. We take our engagements to cultivate a greater understanding within the economy by taking a holistic approach to resilience – just like physical health cannot alone be managed by food we eat, all kinds of other inputs need to be considered. The same is true for digital health and cyber.

As a company, we also take our thought leadership very seriously and are very active contributing to policy debates that are happening, for example within the UK on the ransomware bill and the Cyber Security Resilience Bill, and CyXcel has taken an active part in establishing the UK non-profit the Cyber Monitoring Centre in collaboration with public and private sector enterprises. Organizations can use the CMC's insights to evaluate and prepare for systemically important cyberattacks.

We also take very seriously the work we do within our community, especially with smaller charities that do important work with vulnerable communities. We want to make sure that our capabilities, our skills and our tools benefit them as well on a pro bono basis, so that they can spend their very precious funds on helping vulnerable people. We have the ability and the commitment to make sure that they are as safe as possible.

All those things matter to us enormously.

All businesses need to do prioritize client excellence, be profitable and deliver for its staff and investors. But we are not a run-of-the-mill business. We take our duty to contribute to policy debates, our wider economy and to our social community very seriously and are a purposeful business.

How do you see tech firms and vendors responding to the geopolitical risks in a light of things like the Trump administration?

We have seen these changes happen over the last decade. The first big shakeup of this was during bidding for 5G networks when we saw all kinds of telecoms providers in Japan, South Korea, United States and India, trying to figure out how their alignment was going to work given the hostility or opposition of several Western governments – especially the United States when it came to Chinese Huawei's 5G technology. At that time, a lot of shifting of the market happened.

We now see a spillover of that trend into other areas of technology. There are all kinds of cybersecurity firms, Russian firms for example, who are not allowed to operate their services in the West. Chinese AI companies are not allowed to sell their AI tools in this market, and equally Western technology is barred from Russia, and from China.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

So, companies in the pure tech sector, as well as the ancillary sectors which surround technology, whether that's customer service or inputs or HR support, have all had to realign themselves and be more alert to geopolitical risk right now.

How are technology supply chains fragmenting?

In terms of the rerouting of global supply chains, there have been two key drivers. First, have been natural events or freak accidents. For example, the Fukushima disaster in Japan, and the COVID-19 pandemic more recently. Factors which are beyond the control of an unexpected incident. These led to rerouting of a lot of supply chains.

Secondly, what has happened more recently, is the geopolitically minded rerouting of supply chains and this essentially, takes three forms. The first, is that you 'friend shore', which means that you oblige your companies to locate their operations in a country that is friendly to the host government. For example, the USA having some Apple fabrication facilities in India because India is a friend of the USA.

Secondly, you can reshore entirely, bringing operations back entirely to the host government.

Thirdly, you can reshore and near shore whereby you relocate your operations closer to your host country so that it broadly falls within your sphere of influence.

We have seen this in multiple areas already and more will happen. For example, when it comes to 5G technology, most of the Western world has gone with European technology from Nokia and Ericsson, because the EU and US are our friends. Likewise, a lot of production from Apple, which used to be in China, has been relocated to parts of Thailand, Vietnam, and India.

The same will continue happening as governments take more active roles in determining their digital sense, but also as they take greater control of their national economic activity, so we expect to see supply chain decoupling to intensify.

Do you think the EU's AI Act goes far enough or is there more you would have liked to have seen in the Act?

I think the law will need to evolve as AI technology develops and as more good and bad use cases emerge. So, what I would have liked to have seen in the EU AI Act is greater definition for the Act to be constantly updated as law processes will need to change if the Act is to deal with emerging AI risks facing businesses.

How do you feel that AI risks can impact on business continuity and the solvency of firms? In short, can we expect to see firms collapse due to AI risks?

AI is inherently a wide lens issue that has the potential to collapse organizations and businesses due to the cybersecurity risks it presents. AI can also inadvertently result in the leakage of sensitive commercial personal data because all AI models


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

constantly retrain and if you accidentally add personal data or commercial data into it then that will be trained in future. Equally, any company that is reliant on using AI services for internal use, customer service or product innovation will also need to be careful about the supply chain of AI which, as we've talked about before, is deeply affected by geopolitical risks.

Depending on the intensity of risks that AI could pose would depend on the exposure that a company has to that. If, for example, a company was not prepared enough to manage cybersecurity risks related to AI and they were to fall prey deep fake attack that impersonates the CEO and if somebody transfers a sizable amount of money to a fake account, then obviously that puts the bottom-line at risk, and the business could collapse as a result.

In terms of business continuity, that can arise from both cyber disruptions, as well as possibly regulatory action. For example, if a company is using AI to screen applicants for a job or to grant tenancy to different people looking for a property credit access. If that AI model is found to be biased or disproportionately turning down the applications of marginalized communities, then obviously the regulators are going to look at it and that could put a company's business at huge risk – not just reputational, but from a regulatory standpoint.

AI has a wide lens risk. It can affect both your cybersecurity through AI generated malware impacting on data protection but also your ability to maintain customer trust. It also can strain your corporate responsibility targets because AI is very water and energy intensive.

Much will depend on the dependency and the exposure of a company to AI risks and what kind of controls and mitigations a company has in place.

How can CyXcel help safeguard executives against personal liability and protect them against action by regulators?

Regulatory compliance – even when we're speaking specifically about data protection – is not transactional episodic activity where it is done once. It's a continuous journey because regulations change, businesses' operations change, so in a way the approach that we take in helping executives manage both personal liability and regulatory liability, is to guide them through the entire life cycle of data. From where it is generated, how it's generated, how it's stored, how it's processed, how it's deleted, and how it's reused.

So, in a way, the journey that we want to take our clients follows the journey of data itself. If at every point our clients can be mindful of their regulatory, reputational, judiciary responsibility, then we can guide them to using their data very effectively.

This kind of holistic and end-to-end approach is what we believe to be the responsible way of managing data protection and making sure that executives who may have different obligations under different sectoral rules or different jurisdictions, can always be on the right side.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Are there any other closing thoughts you would like to get over to our readers?

Digital connectivity is here to stay and is going to intensify and more and more companies, people, individuals, processes, operations will get digitally interconnected over the internet.

But we are also living in a time of deep geopolitical divisions, there are all kinds of criminal activity and huge rifts the nature of regulations – whether it's of new tech like AI or old tech like telecommunications.

Companies will need to manage 'junction of time' very carefully because we are connected and disconnected at the same time. Organizations who look at the problem in a holistic way and how technology, cybersecurity, laws, threats and geopolitics intersect, will be the ones to have most effective, sustainable, robust and responsible approach to digital resilience.

Reference

1 Qantas Cyber Incident (2 July 2025). Qantas. Available at: https://www.qantasnewsroom.com.au/media-releases/qantas-cyber-incident/