CYXCEL®

The 4 Trends Shaping the Future of Cyber Risk

CyXcel Executive Interview With **Dr. Megha Kumar** and **Jack Horlock**

UK-headquartered CyXcel is the world's first cyber consultancy to integrate technology, law, security and geopolitics expertise. Combining proactive legal and technical expertise, CyXcel knows that digital threats evolve by the hour and that organizational success isn't just about innovation—it's about resilience.

Zywave recently spoke to two thought leaders from CyXcel—Partner, Chief Product Officer and Head of Geopolitical Risk Dr. Megha Kumar and Principal Associate Jack Horlock—about the nature of these evolving threats and how businesses can navigate an ever-changing digital landscape.

Dr. Megha Kumar
CyXcel
Partner, Chief Product Officer and Head of Geopolitical Risk

Jack Horlock
CyXcel
Principal Associate

Trend 1:
Given the amount of data organizations process, nearly all companies (regardless of industry) are tech companies now. What does that mean for compliance and cyber risk?

Dr. Kumar: From the top down, technology is deeply integrated in nearly every organization's processes. Regardless of the industry they operate in, the widespread collection and reliance on customer data essentially make every company a tech company in some way, shape or form. Whether it's health care, banking or social media, businesses handle sensitive, personal identifiable information in tandem with data related to customer behavior and personal choices. The same applies to governments, especially since the COVID-19 pandemic: a whole range of essential public services from healthcare to passport renewal are now delivered digitally.

As a result, it's more crucial than ever for companies to have robust contingency plans that cover cybersecurity, operations and legal exposure. The emphasis must be on ensuring strong technological resilience, even for companies who believe they operate outside the tech space.

Horlock: Yeah, as Megha noted, everything is being digitized. Even things you might not think about. Take, for instance, our political lives. Most of us working in advanced economies receive electronic voting IDs through digital means, maybe by mail as well. We often cast our ballots on electronic machines—the votes are counted electronically, and the results are declared the same way.

In the social world, everything is increasingly digitized. If I want to travel to a festival, I can book the tickets online, reserve my train ticket online or order an Uber online. It's all interconnected, and this is true for all aspects of business as well—especially since the pandemic. Remote and hybrid work has accelerated the shift to digital services, which we've realized democratizes access, reduces costs and improves efficiency. So, everything that used to be considered part of our analog lives is now going digital, whether socially, commercially or in terms of how we work.

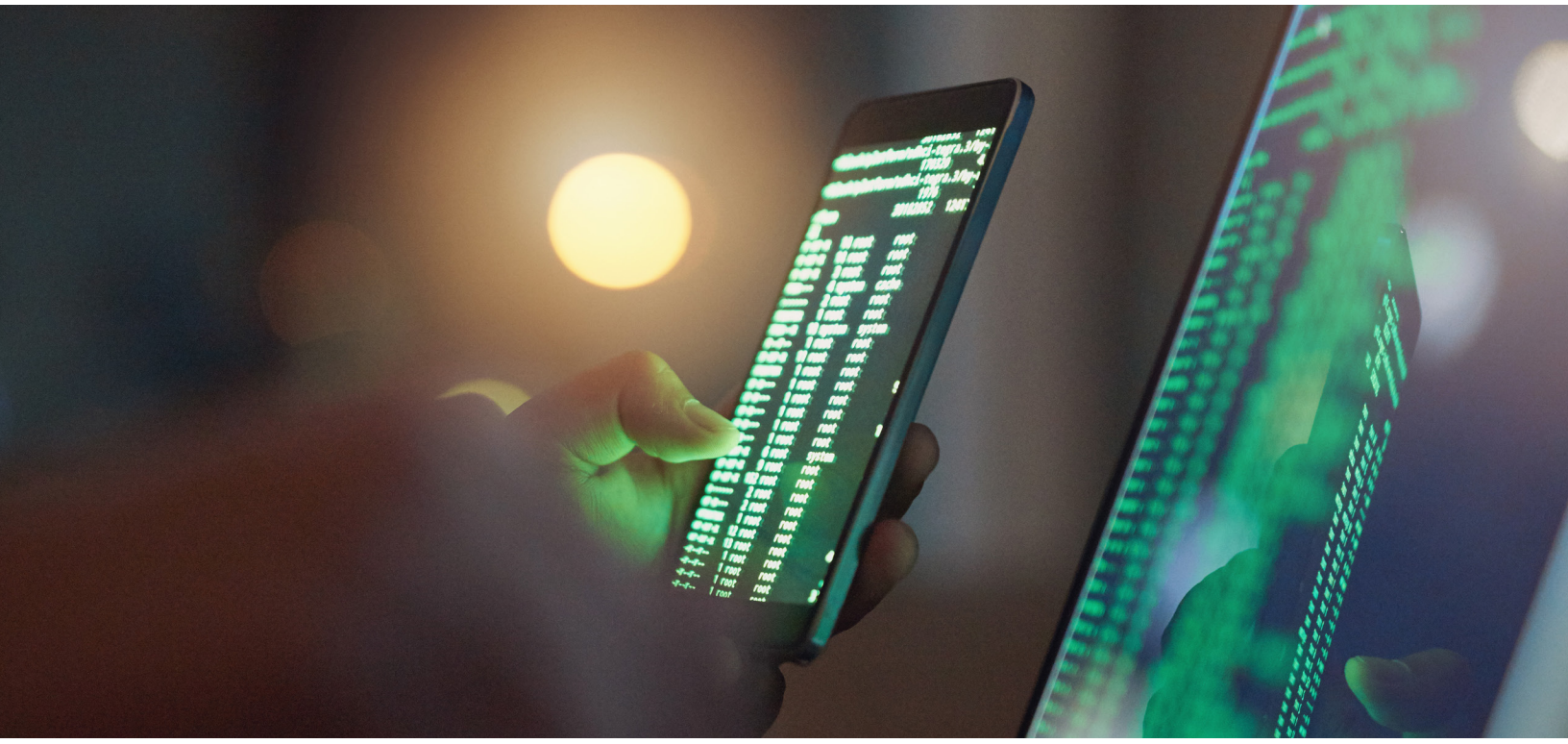
Dr. Kumar: The way I like to think about it is that technology is like electricity—it's not just a tool. Twenty to 30 years ago, technology was mostly just computers,

printers or fax machines. But now, we can't do anything without relying on some form of technological tool, whether it's hardware like a phone or computer, software like Microsoft Teams or tech services like cloud platforms.

And yet, there are many companies, especially those outside the traditional tech space, that believe they aren't tech companies. A dairy manufacturer might think, "We don't produce tech, so we're not a tech company." However, if the machines that process your milk, handle storage, packaging and hygiene checks are heavily reliant on robots or electronic tracking tools, then you are indeed a tech company, and your operations need to be resilient to hacking.

A lot of companies remain stuck in the mindset that they are "analog" businesses because they're not Facebook, Amazon or Google and, as a result, fail to take cybersecurity seriously enough. And I think people take for granted how much infrastructure and daily conveniences rely on technology.

We've seen it in past cyberattacks: A vendor gets hacked, and then seemingly unrelated areas of society (e.g., railways, airlines and airport systems) are severely impacted. It just shows how interconnected everything really is.



Trend 2:
Artificial intelligence (AI) is not merely a new technology; it's a paradigm shift. How does the advent and usage of this technology alter today's cybersecurity landscape?

Dr. Kumar: AI is a very good example of how one piece of technology can be used in multiple functions of a company's operations—on the sales side, the finance side, the HR side, the business workflow management side, and for finding faster, cleaner and cheaper processes in sectors, ranging from agriculture to shipping.

While AI can provide endless benefits in these areas, the risks also become spread out. It's not just one team using AI within a silo, which means that you are opening multiple doors of vulnerability. Some of those vulnerabilities have to do with the data used for training AI models (internal or purchased and customized); companies need to actively prevent leakage of their own IP and inadvertently infringing on someone else's copyright.

Another important consideration is environmental sustainability. AI is both water- and energy-intensive, and ill-considered use of AI can undo corporate progress on environmental, social and governance (ESG) initiatives. These are key and important risks to manage as part of our effort to harness the transformative potential of this tech.

Horlock: And AI use is only getting more pervasive. Many companies worldwide are racing to adopt various generative AI tools, whether they are off-the-shelf models or built custom by in-house teams. As Megha mentioned, different parts of a company are using these tools to find efficiencies. But, the responsibility for managing any resultant AI risks is often too narrowly placed on the chief information security officer or chief technology officer.

Legal counsel must understand the potential risks of using AI, whether that be exposure to copyright breaches when generating images or the possibility of intellectual property leaks if an organization's research and development teams use models that interact with external systems.

HR departments also need to understand the risks of using AI for tasks like application screening. While AI can streamline processes and make them more objective, it needs to be stress-tested to ensure it isn't biased against certain protected classes, such as women or people of color.

Understanding AI from all these different perspectives is critical, and I don't think that's happening enough. It needs to become far more nuanced and comprehensive.

Dr. Kumar: This is even more important given the pace of AI. We've had remarkable breakthroughs in such a short time, especially since ChatGPT emerged. The advances have been rapid, are ongoing and continue at a fast pace. It often feels like by the time we label the latest AI tool "emerging technology," it is already old technology. That's how fast things are moving.

What makes AI particularly fascinating, especially the type we see now with large language models, is that it's multiuse. In a broader sense, many technologies still only have a singular function, which isn't necessarily bad. For example, a computer monitor can serve as both a computer screen and a TV, but that's about it.

AI, however, is different. It can be customized to perform multiple functions. For example, the head of HR can use AI to screen applicants, the head of finance can use it to track financial trends and big data, the head of marketing can use it to generate content, and the head of sales can use it to create effective pitches. Its multipurpose nature means everyone will use AI in many different ways—some of which we haven't even discovered yet. The best and worst uses of AI are still to come. So, while AI is powerful and versatile, we need to take its risks, flaws and regulatory challenges seriously.

Notably, in terms of risk, AI has the potential to supplement existing cyberattack strategies. We've seen instances where AI-powered tools have been used to spread disinformation, develop new malware and generate fraudulent biometric data. At the same time, AI may accelerate cyber vulnerabilities, particularly given the depth and breadth of its integration into organizational systems.

People often don't realize how far AI can reach within their own networks, which means they open numerous doors they don't even know exist. This accelerates the rate at which hackers can exploit system weaknesses.

AI truly is advancing rapidly. Some companies work hard to prevent the misuse of their tools and invest considerable resources to address concerns. However, now that we live in a world where AI is used so prevalently, it's increasingly difficult to close Pandora's box.

We are now seeing the emergence of AI-native crime, which refers to crimes that are facilitated or directly carried out using AI. Essentially, AI-native crime is crime that could not have been committed without the availability of AI.

As an example of this, over the last five to 10 years, biometric certification—like iris scans, facial recognition, voice recognition and thumbprints—has become the norm in banking given how difficult it is to replicate. It was seen as a breakthrough technology, offering strong protection for bank accounts, military secrets and more. But now, AI has been successfully used in experimental settings to clone voices and break into banks, undermining this relatively recent security measure. In essence, AI is poised to disrupt what we thought was the "Holy Grail" of identity verification: biometric identification.

Overall, risks evolve quickly, and perceived solutions to emerging risks, like AI-powered cyberattacks, are rarely future-proof.

Trend 3:
The lines between state-sponsored and nonstate-sponsored threat actors have blurred. How will that impact cyber risk?

Dr. Kumar: In terms of state-sponsored and financially motivated criminal threat actors, the landscape is changing. For the longest time, the one state that was considered rogue in a sense was North Korea. North Korea, by and large, remains the only state in the world whose hackers compromise private companies and public-sector institutions, not only for strategic information, intel and trade information but for ransom as well.

This is partly because the ransom that North Korean state-linked hackers generate through criminal activity finances the weapons program of Pyongyang. In North Korea, there hasn't really been much distinction between a state-linked hacker and a criminal hacker—they are the same people.

Where the blurring between state-sponsored and nonstate-sponsored threat actors has happened elsewhere in the world is Russia, which is home to some of the most notorious criminal gangs of hackers in the world.

The Russian state, especially its various intelligence services, has opaque relationships with criminal hackers. Exactly what the nature of that relationship is has never been clear for obvious reasons: That is simply not the kind of information that would be out in the public domain.

However, it's apparent that Russia leverages its criminal threat actors to advance its strategic interests abroad and to prevent these actors from undermining Russia's foreign policy goals. Since the Ukraine invasion—and, in fact, ever since the Crimean annexation in 2014—criminal Russia-based hackers have compromised Western companies for ransom (such as the U.S. Colonial Pipeline) but have been careful to avoid targeting Russia's foreign friends and allies, such as India.

Horlock: The other component here is the birth of patriotic hackers, which has happened since the Russia-Ukraine war.

Ukraine has a whole army of so-called patriotic hackers whose job is to compromise Russian assets and prevent Russian attacks. By the same token,

Russian patriotic hackers will try to target Ukrainian entities and get information about the war through various channels. So here, these are not state-linked hackers. They just look to the state to orient their approach.

So together, what you get is a mix of traditional state hackers (i.e., those whose only job is to compromise the enemy's ministry of health, for example), patriotic hackers (i.e., rouge actors who choose their political affiliation depending on the moment and act maliciously) and everybody in between (i.e., fully criminal actors who have some kind of a relationship with the state and others who are more hand in glove).

Dr. Kumar: Given their similarities, the strategies and goals of these different players are also difficult to parse. We are in an environment where criminal groups are increasingly adopting sophisticated hacking techniques that were developed by hostile foreign governments. These techniques, which are driven by geopolitical aims, are being used to steal data, spread propaganda and undermine democratic governance. Complicating matters, the prevalence of AI and social engineering can make it even more difficult for a business to distinguish between a state or criminal actor.

In some cases, both state-sponsored and nonstate-sponsored cybercriminals have the same target and goals in mind. Increasingly, both these groups set their sights on organizations with high-level access to sensitive data.

Trend 4:
Why is it critical to look forward and prepare for the threats of tomorrow, not the threats of today?

Dr. Kumar: There is no other option but to prepare for the future, and organizations must be ready for the threats of today **and** tomorrow.

The cyber landscape—specifically in terms of who's hacking who, where and why—is constantly changing. More concerning still, as organizations' defenses get stronger and stronger, cyber actors' strategies and techniques have evolved in tow.

What we've seen in the cyber landscape over the last 10 years is that criminals have become almost corporatized. That is to say that threat actors now seek out other specialist teams and individuals within the broad ecosystem of the criminal marketplace. They then partner with each other on an ad hoc basis to carry out cyberattacks. It's almost like a contractor model where cybercriminals are effectively banding together and spending money to hire one another to exploit a system. This increases the cost of executing a cyberattack, which means criminals are becoming more judicious about who they target to maximize their return on investment. Data, money, system compromise—whatever it is they are after, cybercriminals are looking for the biggest payouts possible.

Given these factors, the need for preparation is almost an existential need.

Horlock: I would say, too, that the overall point in discussing the various kinds of actors and technologies that make us vulnerable is, first and foremost, to remind every business, company and organization that cybersecurity only works if you're proactive. You have to act in defense and adopt cybersecurity best practices. If you only react after being hit, you're not doing cybersecurity—you're doing damage control, and those are very different things.

For different actors and technologies, the risks vary.

Dr. Kumar: Exactly. Every company needs a stress-tested strategy to determine the key steps they would take if, for instance, they were hit by a state actor. In those cases, insurance is unlikely to cover the damage. For example, if intellectual property or sensitive data is compromised, it's difficult to insure against that kind of loss. You may even end up having to involve your host government in discussions.

You need to think about what actions to take depending on who attacked you, what they compromised (e.g., data, money, credentials) and who your stakeholders are. What is the immediate damage?

If you're a hospital and people's lives are at risk, that's a completely different situation than if credit card details from your client base were released. While the latter is serious, it's not the same level of impact as lives being in danger. These situations require different responses and preparations.

And in each of the cases, the damage is not just to IT systems; reputational loss, regulatory penalties and loss of customer trust are all serious fallouts.

Horlock: Agreed. I think companies need to develop a much more nuanced understanding of what to do if a particular kind of actor targets specific assets. Instead of thinking, "It's all just cybersecurity," companies need to recognize that because the world is so complex, they must approach the issue in multiple layers. This type of preparation serves a company well because, after a breach, you don't want to be asking yourself, "Who do I need to call again?"

If you don't take a 360-degree view of your digital resilience, it's only a matter of time before you find yourself in a tricky situation, given the current threat landscape. However, a lot of digital resilience is actually attainable and simple. It's neither too complicated nor too expensive. There's a myth that tech is for "techy" people and full of confusing jargon. But, in reality, it's much simpler than that. Some cybersecurity vendors have not helped themselves by overcomplicating things when the goal should be to educate and empower people.

Dr. Kumar: One challenge to all of this is that organizational and corporate silos are still very much the norm. Companies have a finance department, an HR department and a tech department. At the C-suite level, there's a shared pool of knowledge that is meant to align the whole enterprise on risks and opportunities. However, there's an insufficient understanding of how cybersecurity impacts each department, especially when they adopt new technologies like AI. This lack of understanding is present at the board level, the C-suite level and even at lower levels of the organization.

That's where I think CyXcel can really step in and help organizations align across silos. CyXcel aims to be the one-stop vendor that brings together legal, technological, geopolitical and cybersecurity expertise. This allows us to address the concerns of various functions across an organization, whether it's the general counsel, the head of ESG issues, HR or the CEO. The core of our approach is that digital opportunity, digital risk, cyber opportunity and cyber risk are business strategy issues—not tech, IT or supply chain problems.

Horlock: What's more, because business strategy involves multiple components, we've seamlessly integrated these components within our team. This way, we can offer clients a holistic, seamless solution under one contract.

For example, if your company is hit by a cyberattack, you don't need to hire separate vendors for incident management, legal counsel and government relations. We handle it all—investigating the incident, negotiating with attackers, cleaning up your system, liaising with stakeholders and regulators, and managing government relations if international assets are affected.

If you rely on multiple vendors, something is bound to slip through the cracks. The approach won't be cohesive or joined up in a meaningful way. So, we decided to solve this problem by bringing everything together.

Dr. Kumar: This isn't just a response to client demand—although many companies have told us they don't want to work with 10 different vendors. We also see ourselves leading the way, showing companies the value and critical need for a multidisciplinary approach. We're saying, "Fine, we'll show you what better looks like."

About CyXcel

Our Mission

At CyXcel, we believe the future is built on the foundations we secure today. In a world where digital threats evolve by the hour, success isn't just about innovation—it's also about resilience. Our mission, "Tomorrow's success, secured today," reflects our commitment to empowering everyone to thrive in an ever-changing landscape.

By staying one step ahead of the risks, we protect not only your systems but your vision for the future. We're more than just a cybersecurity consultancy—we're the guardians of progress, ensuring that the breakthroughs of tomorrow are never compromised by the challenges of today.

Our Values

At the heart of CyXcel are our core values: radical transparency, teamwork and respect, and enterprise.

We believe in openness and honesty with our clients and each other always, fostering a culture of collaboration and approaching every challenge with an enterprising mindset that drives us to innovate.

What Makes Us Different

Our integrated approach sets us apart. With experts from cybersecurity, law, regulatory and geopolitical fields, we offer solutions that address every facet of your business challenges.

Whether you're responding to data privacy laws, preparing for digital transformation, battling ransomware or navigating international sanctions, we deliver seamless strategies that make sense in the real world.

CyXcel is committed to long-term client relationships that are rooted in trust, empowering businesses to face the future with confidence. We believe that success isn't just about avoiding risks; it's about using those risks as stepping stones for growth.

With CyXcel, you're not just protected—you're positioned to lead. Together, we're redefining security and resilience for businesses in a fast-changing world.

We'd love for your business to choose CyXcel as its partner as we build a future that's not only secure but full of possibility.

To learn more, visit www.cyxcel.com.