Deloitte.

User Friendly: Season 8, Episode 4
February 2025

Cyber trends shaping the TMT industry

Host: Hanish Patel, Managing Director, Deloitte Consulting LLP

Guests: Phil Malatras, Chief Information Security Officer, Western Digital
Arun Perinkolam, TMT Industry Cyber Leader, Deloitte

Hanish Patel: I'm Hanish Patel, and this is *User Friendly*, the show where we explore emerging trends in tech, media and telecom, and how they impact business operations and the world around you.

As we continue to witness rapid technological advancements, the technology, media and telecommunications, or should I just say TMT industry, is a part of a dynamic landscape shaped by evolving cyber trends.

Understanding these trends is crucial for organizations aiming to protect their assets and maintain a competitive edge. But what are the key cyber trends currently shaping the TMT sector? And how can organizations effectively navigate some of the challenges and leverage cybersecurity as a strategic advantage?

In this episode of *User Friendly* podcast, we will delve into the pressing cyber trends influencing the industry today and steps TMT companies should take to stay ahead of emerging cyberthreats. Joining me today to shed light on these critical developments are Phil Malatras, chief information security officer at Western Digital, and Arun Perinkolam, TMT Industry Cyber leader at Deloitte. Phil, Arun, welcome to the show.

Phil Malatras: Thank you. I'm glad to be here.

Arun Perinkolam: Thank you, Hanish. Appreciate it.

Hanish Patel: So, to ground our listeners, I'm actually going to open up with a bit of a two-part question and the first bit is, can you help define what "cybersecurity" means today and describe the sheer impact it has had on organizations across industries?

And the second part of it is, what does the current cybersecurity landscape really look like for TMT industry overall? And maybe Arun, I'll kick it to you to start with and then hand over to you, Phil.

Arun Perinkolam: Yeah, once again, Hanish, thank you so much for having us. Cybersecurity has truly become one of the primary underpinnings of a successful and resilient enterprise in today's world. With the constant evolution of the threat landscape and the associated business risks, what used to be treated as a cost center within IT over a decade ago does have the focus of the C-suite and the board in today's world.

The role of the CISO [chief information security officer] has also evolved and matured into one that has a seat at the table and is seen as being responsible for safeguarding the brand and reputation of the enterprise and its customers all while supporting innovation and building for the future. In the recent annual *Future of Cyber Survey* that Deloitte concluded, 88% of our CISO participants mentioned at least quarterly engagement with their boards to address cyber priorities if not more often.[1]

To answer the second part of your question, when I look at the global cyber market today, it's roughly a $200 billion market with the US being around $130 billion across both cyber software and services. And this market is growing at a pretty brisk 10% to 12% CAGR[2] [compound annual growth rate]. Nearly all the security technology vendors, in what is a pretty fragmented market actually, sit within TMT.

And over the years, we have benefited from the security innovation and research these technology players have embarked on internally, which they have then eventually productized and brought to market. So, I continue to see TMT shaping the future of cyber, not just within the TMT industry but across industries.

Phil Malatras: I'll dovetail on what Arun just mentioned—some of the same thought processes. In today's extremely complex environment, first and foremost, every CISO needs healthy and positive relationships with leaders across the company, including senior executive leadership team members and the members of the company's board of directors. As Arun mentioned, I'm in front of our audit committee every quarter and I go to our full board at least once, sometimes twice, a year. And establishing and maintaining those relationships is key to be successful in this current landscape.

One of the things that we must do is truly learn the business. It's not just about security; it's about understanding the technology and all the moving parts of the business. We need to understand what's important to each of those stakeholders and enable—primarily to be an enabler, while you're protecting the company—its systems and its data from threat actors. That's a never-ending balancing act between workforce productivity and the appropriate security program.

From a visibility perspective, cybersecurity has emerged to be a core component of ERM, or enterprise risk management. Regardless of team size, technologies deployed, or perceived program maturity, cybersecurity risk will always be present and must be proactively managed. Regarding the current landscape, I think we'll be addressing that in the topics as we continue this conversation.

Hanish Patel: I definitely want to go there as we think about the landscape, but as I considered a backdrop that both of you just said—and firstly, thank you for that. It kind of gives me a really good bridging off point. I do want to dig in around how digital transformation overall has affected, say cybersecurity—the needs, the challenges, and particularly at Western Digital, Phil.

Phil Malatras: Digital transformation at its core is using technology in new ways to potentially improve all aspects of how our business operates. Now often that involves combining data from many different sources and applications, both proprietary on-premise or cloud applications and from the general public domain, to then surface new insights and new capabilities that didn't exist before. So, that dynamic makes it even more challenging to protect company information from unauthorized access because now that data is spread all over the place. GenAI, or generative artificial intelligence, has emerged and is a big driver for pervasive broad spectrum data access needs.

Even though it's still in its infancy, it seems like every business leader is convinced they need it right now to do a variety of things that may or may not be fully understood. Protecting information that is now much more spread around can be extremely challenging.

Hanish Patel: Going back to that backdrop that both of you painted earlier, and actually Arun, as you talked about some of those stats, I was taking a read into the recent article that was published. Can you walk us through some of those key cyber trends or imperatives for the TMT industry that we, as a firm, have identified in that recent article that was put together, which was called "Unlocking cyber excellence: Chief information security officer strategies for the TMT industry," which I think will be really valuable to our listeners.[3]

Arun Perinkolam: For sure, Hanish. As I had mentioned previously, TMT in many aspects is leading the broader marketplace on cyber. And if we look at our Fortune 500 TMT clients, they have prioritized and made significant investments on cyber over the last decade and more.

And a fair number of these investments, if I may, have been on homegrown security technologies and processes supporting them. And while these technologies and processes are doing the job well across prevention, detection, and response—which are the three primary pillars from a cyber perspective, programmatically—there is an element of what I call calcification and tech debt that clients are now grappling with.

The average large enterprise today has well over 40-plus security technology tools and technologies deployed.[4] And at the most macro level, this is at the heart of what we are having our clients in TMT rethink when it comes to refreshing their cyber strategy, which is aimed at driving more cohesion and consolidation across their tech stack, improving operational efficiency and effectiveness, and deriving a lot more ROI from their tech and their talent.

Phil Malatras: Yeah, Arun, I agree. Many of us deployed best-of-breed applications and best-of-breed capabilities. That has, to some degree, gotten out of control.

So, I think currently some of the major players are getting much better and their solution set is either at or close to being acceptable, replacing a lot of those individual best-of-breed applications. I think we will continue to see a shift in that direction to have fewer tools, fewer capabilities that are all adequate, but give us a great[er] deal of visibility across the spectrum than we had with the individual spot solutions.

Hanish Patel: If I may stick with that kind of train of somewhat of an evolution, in terms of where they were, best-of-breed spot solutions. A two-part question for the both of you is what are those biggest maturity opportunities in cyber for TMT companies today? And maybe the second part of it, what are some of the roadblocks that actually exist today in scaling up that maturity score as companies think about cyber as an overall perspective?

Arun Perinkolam: From my perspective, with the backdrop that we just set, a few areas rise to the top where we see, I see, material opportunities for maturity improvement and those are around security operations, third-party risk management, identity access management, and compliance.

Looking at security operations of the SOC [Security Operations Center] and IAM [Identity Access Management] across several of our TMT clients, both the SOC and IAM programs have been historically managed in-house over the years. And what we are seeing is a shift from homegrown technologies to more commercial off-the-shelf solutions, which several vendors have worked on over the years and matured; and to full or partial outsourcing of these capabilities from a process and operation standpoint to better align with in-house talent expectations, so employees can actually focus on higher ROI activities.

And the ability to leverage continuous maturity and scaling capabilities that a lot of these outsourced managed service providers are able to readily support. So, that's on the SOC and IAM side.

Moving on to third party, third-party risk management has been dealt with in an extremely federated manner across our TMT clients. In most enterprises, different views work with different sets of third parties and the nature of the third-party engagement, the data that is shared and collected, etc. are all markedly different.

And over the years, what's happened is these views have stood up their own satellite third-party programs to handle and mitigate security risks. And our clients are starting to realize that this is untenable in the long run as it leads to a very disjointed view of third-party risk across the enterprise, not to mention both scaling and cost efficiencies.

And the last area that I'll touch on in terms of a significant opportunity to mature is compliance. Over the last decade, TMT clients increasingly have had to deal with security compliance obligations, be it regulatory and legal, privacy, FTC-related, or other internal directives.

And not too dissimilar from the third-party point that I just articulated, compliance programs have organically mushroomed to handle these varying directives usually in silos. And this has caused immense inefficiencies on employees supporting what I call *line-one security control activities* as they end up having to support each of these compliance programs separately in a non-standardized manner, all while doing their daily jobs.

As a result, we have been seeing a major shift to compliance program rationalization while leveraging things like offshoring, nearshoring, automation. And Phil alluded to use of AI/GenAI capabilities to drive both efficiency and cost takeout in compliance programs.

Phil Malatras: I'll double tap a little bit on the whole risk management world. Quite frankly, we struggle with it quite a bit. We obviously do a fair amount of risk assessments of third parties we engage with at different sizes, scopes, and scales and purposes.

We've adopted a qualitative risk assessment process, which is pretty unique from everything else we've seen. We don't go after metrics, we don't go after numbers, we don't have scores. We actually try to figure out what the third party's risk program looks like and whether they're truly prepared to protect and detect anything that might be associated with a connection with us or with data we share with them.

Now I'm also on the other end of that; I receive a lot of self-assessment or self-questionnaires on the effectiveness of our program, and it's always almost based on some industry standard. And typically it's numeric-based.

There's an ultimate score, and the process is really to get us to some number. That doesn't necessarily mean we have an effective program; we're just measuring ourselves against their questionnaire in an adequate way.

While maturity is nice, it doesn't necessarily move the needle for a security program. Depending on the business you're in, you

may have no choice. It may be mandatory to achieve various certificates to demonstrate the maturity against some associated frameworks. That requirement could come from your customers, it could come from a government regulated because you're in a regulated industry.

But regardless of whether it's mandatory or not, it's good to understand all those frameworks that are particularly commonly used around the world. They could and should influence your security program. However, I do want to stress, that should not be the only focus. And I've talked to many CISOs that really do solely focus on those frameworks.

To me, the effectiveness of your program are how well you're protecting your environment, your ability to detect suspicious activities, your readiness to respond and resolve to those issues. To me, those areas are far more important than framework maturity. I know from experience, just because you're rated really well in a framework item doesn't mean you're effectively protecting your enterprise.

Every business is different, but I do think that each CISO needs to determine where to focus, to elevate that effectiveness within their program, to address the proverbial "bad things" from happening or those bad things from getting out of control. And don't necessarily just consider that whole maturity aspect of whatever framework your third-party partners are asking you to go through.

Hanish Patel: So, as I think about what you just said there around kind of where to focus, how important then is leadership and culture in building that robust cybersecurity program within an organization?

Phil Malatras: Critically important. I mentioned earlier on our conversation about building and nurturing the right relationships, and that's a key part of establishing the right security culture. Without that, you can't have the right level of influence and the right mindshare throughout the enterprise.

You don't want to be an island on the cybersecurity program. I constantly push the fact that everybody on enterprise is a partner with me and the rest of the cybersecurity team to keep us secure. It's not just one group. And unless you've developed that kind of culture and you get buy-in from the rest of the executives and the collective workforce, you're constantly swimming upstream.

For Western Digital, I can tell you that pretty much everyone knows who we are collectively as a team. Most—not all, but most—are comfortable coming to us to collaborate on something where they have a need that may have some kind of security impact.

We have a very close relationship with our procurement team, so nothing gets procured without running through us. We also have an extremely positive and robust relationship with our legal team. Typically, if we're going to buy anything, it's going to hit one or both of those organizations, and they are very diligent about making sure we are in that conversation. Very few things sneak by us.

That's the kind of relationship building you want to have across an enterprise. So, you've got those checks and balances and you're not just running it on your own. But in a nutshell, relationships and culture? Incredibly important part and an important aspect of building a truly effective security program.

Arun Perinkolam: And I cannot agree more with you, Phil, on that, in terms of that being an exceptionally strong underpinning for any enterprise. And very simply, an enterprise where cyber is everyone's responsibility and not just the responsibility of the CISO and his or her team is a culture that will succeed.

Hanish Patel: I want to stay with that train, when we think about culture, thinking about relationships and leadership, and somewhat going to ask the two of you to get your crystal ball out, so to speak, is what are your predictions for the future of cybersecurity in the TMT industry?

And given what you said about culture, the leadership, their relationships, what steps should leaders in TMT companies take to frankly stay ahead of emerging cyberthreats?

Phil Malatras: I'll go back to my earlier comments about GenAI. Not only is that impacting our ability to protect our data, it's also creating a new dynamic in the proverbial cat-and-mouse game between threat actors and cybersecurity teams.

Now, threat actors of course don't have a procurement department. They don't have to worry about figuring out how long it takes to buy something; they can just go off and get whatever they'd like. So, the speed and the veracity with which they can move, leveraging some of these new GenAI capabilities, certainly gives them more power than they had in the past.

The cybersecurity GenAI tools for companies to protect themselves, from my perspective, are still relatively immature. Now we're hoping that evolves quickly, so we can actually get a little more horsepower on the defense side as well.

I know there's a lot of activity in the marketplace overall. There's a lot of GenAI startups with a lot of venture capitalists funding, but at the moment we haven't seen anything emerge that's a game changer—at least not for a relatively mature group with seasoned professionals.

At the end of the day though, I really do think that even with all that new capability, the way threat actors typically get in is because of mistakes. So, that basic security hygiene needs to continue to be the primary focus for everybody. That's how they're really going to get in to begin with.

GenAI will launch them off, it'll make them faster, it'll make them possibly more destructive, but they need to get in. I don't think GenAI is going to really change the game on how they get in initially.

That's hygiene's place of making sure you have all your vulnerabilities patched, you don't have misconfigurations, don't give them an opportunity to get a foot in, and that's not going to change no matter where the technology goes.

Arun Perinkolam: Phil, I cannot agree more in terms of foundational security hygiene, always the need for that to be a constant in any enterprise. But sticking with the theme of AI for good, I do see a lot of promise, when it comes to cyber in that regard. All the areas I touched on previously—security operations, IAM, third-party risk compliance, in addition to other cyber domains in my mind—will all see material application of AI use cases.

And you're right: Today we see more of a POC [proof of concept] pilot focus with a lot of security vendors being in their initial infancy stages in terms of embedding those capabilities. But I do anticipate a move to actual deployment and implementation of AI agents in the cyber world.

The other trend that I anticipate TMT clients paying attention to is what Phil brought up—is the move towards platformization by some of the largest security technology vendors.

There is no denying the advantage of a best-of-breed security technology architecture. But in the same vein, TMT enterprise security and technology leaders cannot ignore the upside of a platform-based strategy given the tech debt, talent, lack of cohesion, and ROI issues we discussed earlier. So, we should fully expect enterprises to have a healthy internal debate on this topic and the potential shift from the status quo.

Phil Malatras: Yeah, and Arun, I want to echo what you said. I do think the trajectory for GenAI tools, and again with that consolidated top-line uniform tool set, I think the opportunities are amazing. I just don't think we're there yet, and I'm very much looking forward to those products emerging with GenAI capabilities. That's going to really change the game for us.

Hanish Patel: As I reflect upon what you both have just said and just the overall conversation, it's certainly eye-opening to me just how rapidly cybersecurity has evolved, is evolving, and is very much going to evolve. And clearly, it's critical to always stay one, two, three steps ahead or the consequences could certainly be significant for any organization. And by leveraging advanced security technologies and proactive risk management, TMT companies can better navigate the shift in cyber landscape and protect their digital assets.

And I do look forward to kind of seeing those ongoing innovations and continuous improvement in the spaces cybersecurity continues to play a vital role in safeguarding all of our futures individually and across organizations.

So, I do want to thank you both, Phil and Arun, for joining me today and sharing your valuable insights. And to all our listeners, until next time, happy listening.

Endnotes

1. Deloitte, *Global Future of Cyber Survey, 4th Edition*, 2024.
2. Grand View Research, *Cyber security market size and trends report, 2025–2030*, accessed February 2025.
3. Arun Perinkolam, "Unlocking cyber excellence: CISO strategies for the TMT industry," Deloitte, accessed February 2025.
4. Gartner, *2023 Gartner technology adoption roadmap for large enterprises survey*, 2023.

Explore more episodes of *User Friendly* at:

userfriendly.deloitte.com

Deloitte.