Cybersecurity considerations for TMT companies

Trends and attack vectors that technology, media, and telecommunications (TMT) companies should be addressing

CISOs continue to evolve their role and security strategies

The role of the Chief Information Security Officer (CISO) within the TMT sector has become quite complex and demanding. New technologies and the proliferation of smart, connected devices have expanded the attack surface. CISOs are at the forefront of addressing these constantly emerging threats and evolving regulatory compliance requirements while safeguarding critical data and staying ahead of cyber attackers.

Many recognize the importance of positioning their work as a matter of building and maintaining trust, rather than satisfying regulatory compliance obligations. Cybersecurity is a critical element in the products and services offered by the TMT sector and can be a competitive differentiator. This has a direct impact on an organization's revenue, profits, and reputation. CISOs must now speak the language of business and engage more directly with C-suite colleagues to secure ongoing funding and resources.

TMT subsectors have similar business drivers and multiple synergies which have led to boundaries becoming blurred. However, each of the subsectors have unique security challenges. For example, technology services priorities include product release (speed to market), regulatory compliance, supply chain risk management, and mitigating human harm.

On the other hand, software as a service (SaaS) providers are focusing on platform resilience and artificial intelligence (AI) security to protect global operations and reputation.

To enhance their defensive posture, many CISOs across TMT are increasingly relying on automation and AI to help bridge gaps left by traditional manual processes and bolster overall security frameworks. Utilizing a centralized platform to consolidate multiple tools and processes into a cohesive system is a key strategy for managing alert fatigue, improving decision-making, and mitigating risks more effectively. Ensuring resilience is another key area that CISOs are focused on and newer strategies around data security (specifically with heavy adoption of AI), cloud-based recovery environments, and newer innovative methods are gaining traction as well.

This article explores **six cybersecurity trends** that US TMT companies should be following and four attack vectors they should be addressing.

Six cybersecurity trends US TMT companies should be following

Industry convergence

More products and delivery channels require cybersecurity to scale accordingly

Diversification of revenue models

New revenue streams increase the number of attack surfaces

Regulation and compliance

Accelerating regulation presents compliance challenges

Data is the new currency

Fragmented platforms and data sources create plentiful attack surfaces

Basic security measures

Getting the basics right is imperative, including layers of defense, consistent code practices, and visibility

Investment in AI security and data center infrastructure

Considering centralizing the AI security function

Industry convergence

More products and delivery channels require cybersecurity to scale accordingly

Media companies are becoming entrenched in the DTC space and competing with streaming platforms. Telecoms are entering the technology space. Technology companies provide other industries with foundational operating systems, tech stacks, cloud platforms, and DevOps tools. This convergence is increasing the scope and scale that TMT companies operate at.

The emerging space ecosystem-including satellites and control networks that all industries are starting to leverage provides additional territory for disruption, surveillance, and extortion.

Securing the space ecosystem will be critical as space-to-ground data flows grow. Ultimately, more products and delivery channels require cybersecurity to scale accordingly, all while still providing visibility, trust, and control coverage.

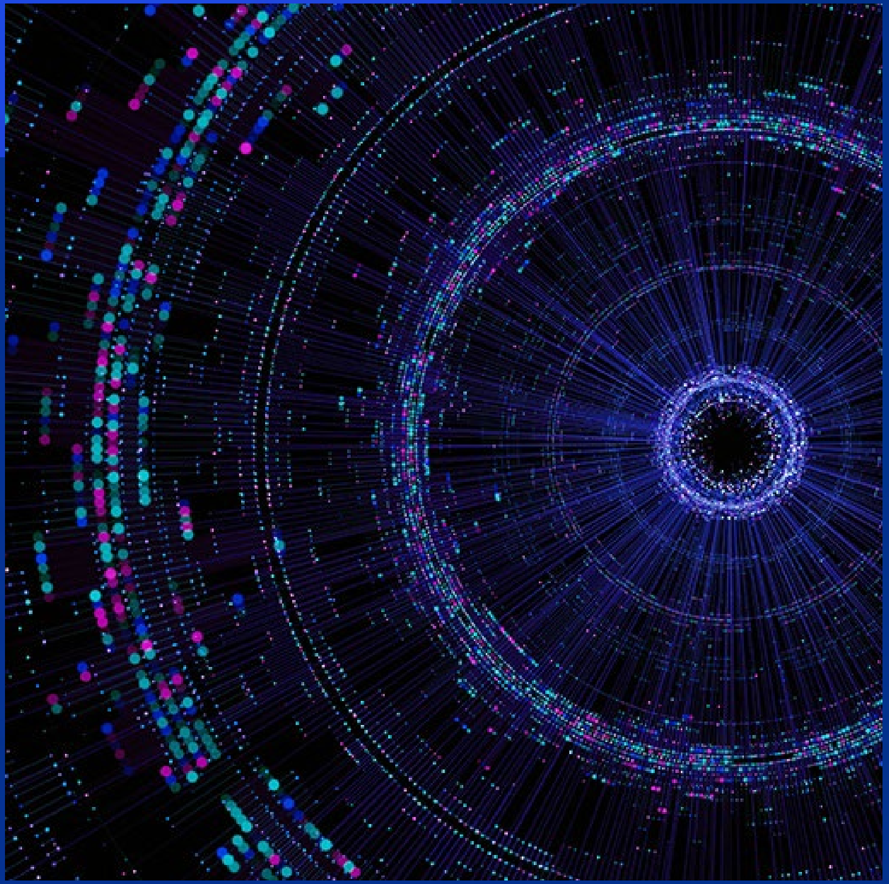
Diversification of revenue models

New revenue streams increase the number of attack surfaces

Accelerated industry convergence is also driving an evolution in revenue models.

Companies that previously had more focused revenue sources may now be managing new revenue streams encompassing customer acquisition, subscription-based models, and advertisement business models, resulting in an increased number of attack surfaces.

M&A activity is blurring the traditional industry lines as well, bringing with it the challenges of pre-close security due diligence and post-close integration within the acquirer's tech stack and cybersecurity protections.



Regulation and compliance

Accelerating regulation presents compliance challenges

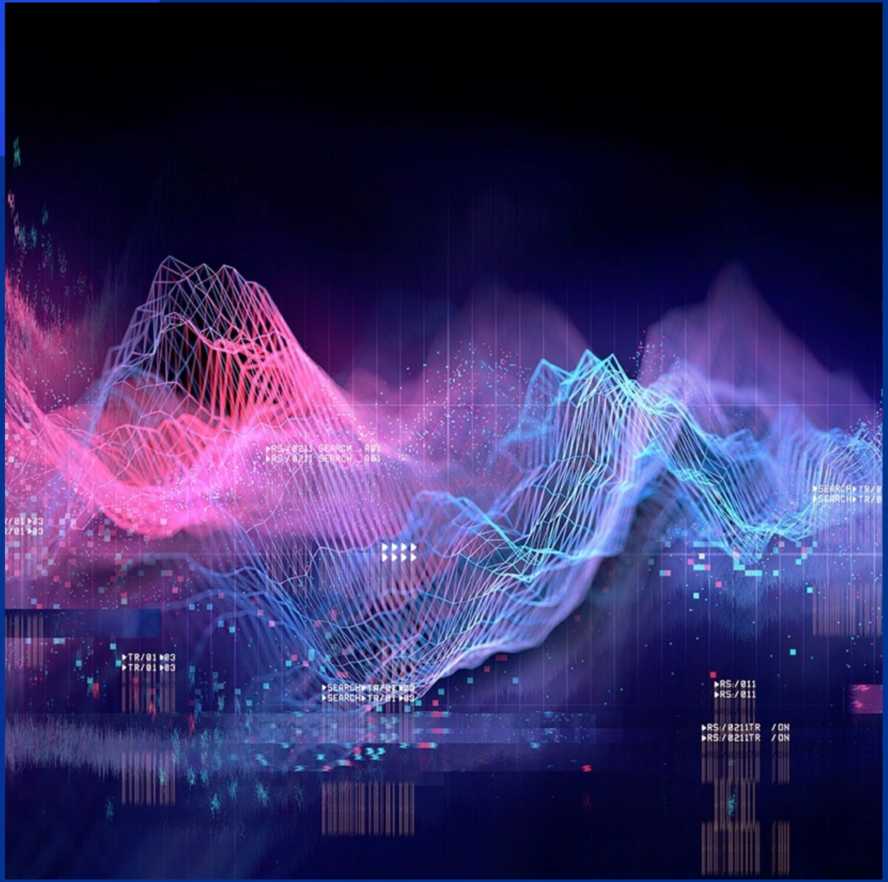
Increasing TMT regulation, especially around online safety and consumer protection, is creating tension between product development and regulatory teams as companies prepare to ensure compliance with the numerous bills and proposals that companies need to navigate.

The regulatory environment in the US is particularly challenging, with over 800 proposed bills related to AI alone. Some TMT companies that operate globally, however, are adopting even higher regulatory standards, such as the EU AI Act, to ensure compliance across multiple jurisdictions.

Geopolitical tensions are also now influencing cyber strategies, particularly around data sovereignty and nation-state threats.

Data is the new currency

Fragmented platforms and data sources create plentiful attack surfaces



The TMT sector is leading the charge in leveraging customer and their own data to drive insights, enhance productivity, and improve margins. Yet significant challenges remain.

There is often ambiguity in data ownership and the complex ecosystem of numerous platforms and data sources often results in fragmented and unsynchronized data environments, creating plentiful attack surfaces that must be secured.

Boards and investors will start demanding clearer ROI on cybersecurity. Cyber risk quantification will become the norm.

Basic security measures

Getting the basics right is imperative, including layers of defense, consistent code practices, and visibility

TMT companies need to focus on these basics while also preparing for the challenges posed by emergent technologies like AI and quantum computing.

- **Layers of defense**: Some TMT companies are making it difficult for attackers to penetrate their systems by implementing multiple layers of defense to protect core assets. The first layer of defense focuses on engineering and product security, while the second provides oversight and ensures compliance with security standards. TMT companies are increasingly focusing on incorporating Zero Trust principles, ensuring identity verification, device compliance, and least privilege (context aware) access. Human-centric security & behavioral threat modelling is also increasing. Concerns about job loss, radicalization, insider threat, and cultural fatigue are mounting. Human-centric security awareness must evolve beyond phishing training.

- **Consistent code practices**: Consistent code building and testing practices are needed to ensure that vulnerabilities are identified and addressed early in the development process. This is crucial for maintaining secure software. Due to the scale at which TMT companies operate, secure-by-design and privacy-by-design principles are essential.

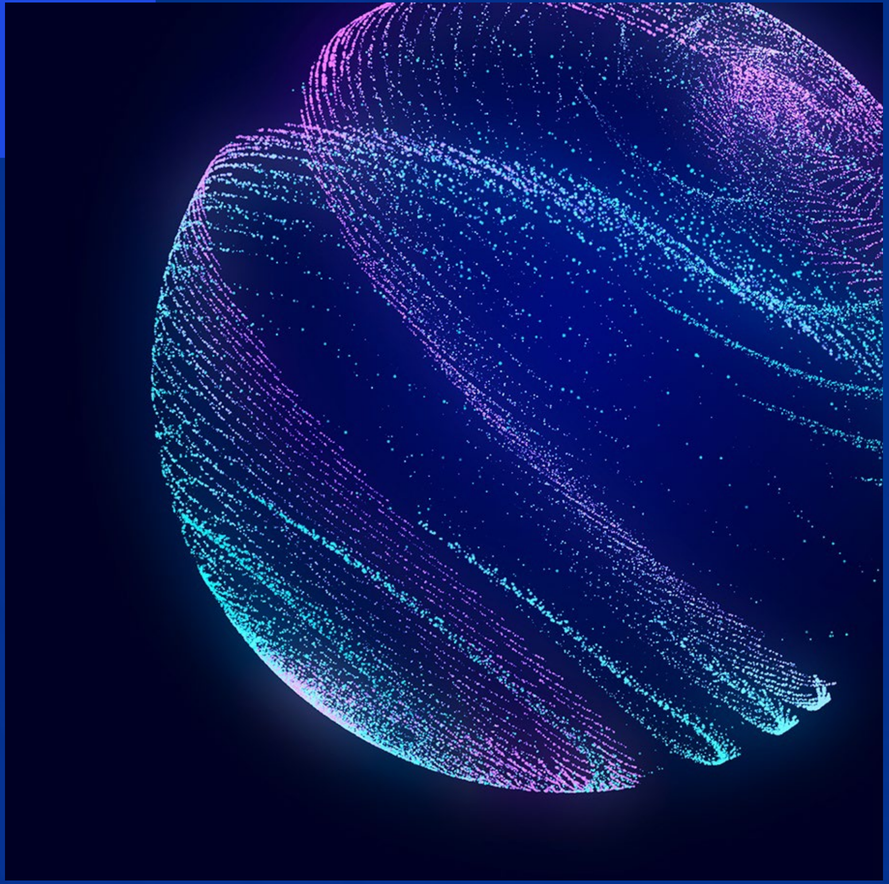
- **Visibility and telemetry**: It is important to have comprehensive visibility and telemetry across all environments. Many TMT companies are investing in automation and telemetry to enhance their ability to monitor and respond to security threats effectively.

Investment in AI security and data center infrastructure

Considering centralizing the AI security function

AI security: We are in the early days of TMT companies integrating AI tools with their enterprise systems and adopting AI-enabled security tools for engineering / code testing, threat and fraud detection, alerts triage, anti-phishing, and identity proofing. Too often, separate teams are tasked with securing AI infrastructure and applications when a central AI security function that also manages data privacy across AI systems and address privacy requests would serve the organization better. And while AI tools are expanding enterprise security capabilities, AI is also being used by bad actors to exploit vulnerabilities and for other activities like deepfake extortion.

Data center infrastructure: TMT companies are making significant investments in energy and data center infrastructure for AI advancement. These new physical facilities, along with the systems and software that maintain them, add to the attack surfaces that TMT companies must contend with. Automated, secure, and privacy-compliant AI solutions are needed from the outset to protect this foundational infrastructure.



Four attack vectors US TMT companies should be addressing

AI software vulnerabilities

The rapid pace of AI-generated code has created more exposures:

Automated software generation:
The rapid pace of AI-generated code has led to an increase in software vulnerabilities. This is a significant challenge as the volume of code generated by AI tools is substantial, and ensuring its security is critical. It needs to be secured from the outset.

Privacy concerns:
The use of AI in handling personal data, prompt logs, and data usage raises significant privacy issues. Organizations need to ensure that AI systems comply with various global regulations, such as GDPR and CCPA, to manage and protect personal data responsibly. Some companies are implementing centralized systems to track and manage AI systems handling private data to ensure compliance with regulations.

Dynamic libraries and SBOMs:
The use of dynamic libraries and software bill of materials (SBOMs) in AI increases the threat exposure of software. This dynamic nature makes it challenging to maintain security and track vulnerabilities effectively.

Authentication, authorization privileges, account takeover, and credential replay attacks

These include social engineering, phishing, and stolen credentials, which are exploited by bad actors both within enterprises and through hacking products sold by TMT companies. Modern authentication platforms and procedures are required to enhance security.

Identity will move from access control to trust brokerage. With distributed work and partner ecosystems prevalent at TMT companies, identity threat detection & response will become critical.

Non-human identities:
Address the management of non-human and machine identities in the cybersecurity considerations.

Anti-ransomware controls:
There are a plethora of proactive and reactive measures TMT companies should be employing to protect against ransomware attacks. Many of these are standard components of a robust cybersecurity program.

- Proactive measures include endpoint detection, response, and protection platforms; secure email and web gateways; multi-factor authentication; and strengthening the human element via strong password practices and awareness training.
- Reactive measures include ransomware detection tools, network segmentation, and having data recovery and incident response plans.

KPMG

Four attack vectors US TMT companies should be addressing

Quantum computing

2026 may mark the transition to tactical post-quantum cryptography.

Encryption challenges:
Quantum computing poses challenges to current encryption mechanisms. TMT companies will have to prepare and implement new encryption keys and certificates that can withstand the computational power of quantum computers. Implementing post-quantum cryptography (PQC) will require careful consideration of algorithm selection, integration with existing systems, and potential performance trade-offs. 2026 may mark the transition from theoretical to tactical PQC.

Preparation for quantum:
By 2030, legacy algorithms like RSA-2048 and ECC-256 will be officially deprecated, and companies are expected to transition to PQC. By 2035, these algorithms will be completely disallowed, according to the NIST standards published in Aug 20241. TMT companies will have to switch to quantum-safe certificates using NIST-approved PQC standards for general encryption and digital signatures and should start to inventory their systems and plan migration strategies using Public Key Infrastructure standards.

Third-party risk

Global procurement and supply chains increase the points of vulnerability.

Third-party risk has become a significant concern due to the global nature of the supply chain and procurement for many TMT companies. Third party/vendor vulnerability and software supply chain attacks are consistent top risks, emphasizing TPRM and scalable trust models. This attack vector highlights the importance of securing the extended network of third-party relationships to protect against potential vulnerabilities and threats.

- Global ecosystem and M&A activities: TMT companies involved in global M&A increase their exposure to third-party risks due to differing cybersecurity regulations and standards across jurisdictions.
- Prime providers to other industries: TMT companies, as providers of foundational products and services to other industries, are attractive targets for attackers due to the scope of access a vulnerability could afford. By maintaining transparency and trust, TMT organizations can further the responsible adoption of their products and services.
- Compromised third parties: Attackers are increasingly targeting third parties through methods like ransomware and malware, which can then impact the primary TMT company's ability to deliver service.

[1] "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." NIST. August 13, 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Real-world cybersecurity in TMT

Case study: Global technology company

Client challenge

The client was seeking to unify the security program that supports all their core products and infrastructure (including AI) under one security portfolio

Additional goals included engraining security into all offerings and increasing the online safety of their products with enhanced security and privacy controls

KPMG approach

KPMG assessed global cyber security requirements, privacy and data protection controls, and leading online product safety features.

We leveraged specialized skills across various domains to stand up a vulnerability management program, operationalize identity access management tools and processes, build a GRC framework, and automate the client’s 3rd party security risk.

Client benefits

The client received several benefits that helped support trust their products:

- A GRC program that included automation tools, and AI-enabled risk and quantification
- Identity and Access Management and Vulnerability Management support
- Improved threat detection and management capabilities
- Increase third-party security with predictive risk recommendations
- Effective risk control of data center infrastructure to enable secure information exchange and resilience

Real-world cybersecurity in TMT

Case study: Telecommunications provider

Client challenge

The client was preparing for a merger and post-close integration and migration activities, including with the cybersecurity systems.

Major technology debt, redundant processes, gaps in operations and tools for holistic cyber integration

Strong need for workforce to maintain day-to-day business operations

KPMG approach

KPMG was engaged to support the development of a multi-faceted cyber integration strategy and roadmap, re-engineer business processes to drive alignment with target standards, establish a technology inventory to support new asset operations; identify, migrate, and integrate data across the two organizations, and provide human capital support to mitigate the impact to day-to-day operations

Specifically, KPMG provided cybersecurity integration assistance across identity and access management, governance, risk and compliance (GRC), security operations, secure DevOps, and data security

Client benefits

- Received a broad strategy and roadmap to support the business and technology integration
- On-boarding procedures were harmonized for people, processes, and technology for scalability and standardization
- Secured coverage and support across multiple cyber functions including IAM, GRC, SecOps, SecDevOps, and data security
- Effective migration to the new identity manager tool and consolidation of GRC platforms

Lets talk

Vijay Jajoo

Principal
Cyber Security Services
KPMG US
E: vjajoo@kpmg.com

Adam White

Managing Director
Cyber Security Services
KPMG US
E: arwhite@kpmg.com

Caleb Queern

Managing Director
Cyber Security Services
KPMG US
E: cqueern@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: in | **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.