KPMG

Mitigating cyber threats in TMT M&A

kpmg.com

Technology, media, and telecommunications (TMT) companies are accelerating dealmaking as they race to keep pace with disruptors and unlock growth. Global M&A value cleared the one trillion dollar mark in the third quarter of 2025—only the second time on record—reflecting pent-up demand for large, strategic combinations and a renewed willingness to act amid regulatory and geopolitical uncertainty.[1]

But as the deal pipeline swells, so do the risks. Historically, legal and operational reviews managed most threats tied to data and technology. That era is over: Attackers are using AI to automate reconnaissance, launch convincing phishing campaigns, and exploit zero-day vulnerabilities at scale. Digitalization and rapid product cycles have created boundaryless ecosystems that span clouds, APIs, open-source components, contractors, and edge devices. Every connection adds another potential entry point, and even sophisticated TMT acquirers struggle to map what they are buying and secure it with confidence, especially in systems they don't directly see or control.

Evaluating the cybersecurity posture of an unfamiliar acquisition target while under deal pressure adds fresh complexity to technical risk assessment. Acquirers in the heat of the moment risk rationalizing away cyber risk, opting for contractual protections instead of a thorough technical investigation. This can leave acquirers with hidden vulnerabilities, unexpected costs, and reputational risk.

Although sellers can help by declaring their cybersecurity posture before a deal, acquirers are ultimately responsible for vetting the systems, practices, and compliance of the assets they are purchasing. Here, we explore the cybersecurity risks inherent in TMT dealmaking, how they affect due diligence, and what acquirers can do to avoid breaches and costly surprises.

Although sellers can help by declaring their cybersecurity posture before a deal, acquirers are ultimately responsible for vetting the systems, practices, and compliance of the assets they are purchasing.

[1] "Dealmakers Defy Stubborn M&A Market With Rare $1 Trillion Haul," Bloomberg.com, September 29, 2025.

The evolving cyber risk landscape in TMT

Cybersecurity too often enters the deal process as an afterthought rather than a foundational pillar of deal review. Yet the financial consequences of cyber threats can be especially significant: Penalties and fines can exceed $1 billion, and that doesn't include the financial impact of lost sales or customer trust.[2] Making matters even more complex is the increase in AI adoption, where all it takes is one bad actor and poor governance to unleash a costly cybersecurity breach.[3]

Six cybersecurity trends US TMT companies should be following

Industry convergence
More products and delivery channels require cybersecurity to scale accordingly.

Diversification or 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
Establishing layers of defense, consistent code practices, and visibility are strategic imperatives.

Investment in AI security and data center infrastructure
A centralized AI security function unifies threat detection, enforces consistent policies, and accelerates incident response across the enterprise.

[2] "The True Cost of Cybersecurity Incidents: A Strategic Guide to Incident Response Financial Planning," Breached Company, May 24, 2025.

[3] "How AI helps—and hurts—cybersecurity," The NAU Review, Northern Arizona University, August 11, 2025.

In TMT, companies face distinct cybersecurity challenges that threaten their most intricate and valuable assets.

Intellectual property (IP) protection is a predominant concern, since critical patents, unique technologies, and extensive content catalogues could be attractive theft and exploitation targets. The theft of personally identifiable information presents another grave risk, as the compromise of customer or employee data can lead to dire ethical dilemmas, substantial financial losses, and irreparable damage to an acquirer's reputation.

Another pressing issue is the security surrounding back-office access and third-party credentialing. Many TMT companies outsource their back-office functions globally, granting extensive access to various entities. This creates potential security threats as attackers can target decentralized systems not overseen or protected by existing cybersecurity tooling, exploiting weaknesses to gain unauthorized access.

Relocating intellectual property to different jurisdictions also poses regulatory compliance challenges. For instance, adding entities that have IP or technology stacks to the European Union necessitates a deep understanding of new legal obligations, such as the European Network and Information Security Directive (NIS2), which enforces strict network and information security risk assessments. An acquisition can also expand the scope of regulatory governance, potentially opening US portions of the business to foreign scrutiny. But even in domestic acquisitions, publicly traded companies must also navigate the requirements of the Securities and Exchange Commission's cyber rule, further complicating their regulatory landscape. These unforeseen compliance costs could significantly affect the financial evaluations that take place during acquisitions.

Moreover, in this code-heavy industry, many businesses inadvertently overlook the security and quality of their software code during due diligence. This negligence allows vulnerabilities to creep into systems, particularly from third-party or external developers and repositories, thereby exposing the acquirer to significant security risks. Operational technology, too, is frequently misunderstood and underestimated, yet it now faces new regulatory scrutiny due to annex 1/NIS2 directives in Europe. This scrutiny renders operational technology auditable and subjects it to hefty fines for noncompliance.

The TMT industry's reliance on third-party vendors and complex software supply chains presents another vulnerability, as these external parties can accidentally introduce risks that permeate the companies they serve. Adherence to technology standards is crucial, particularly for consumer-facing entities whose products must meet industry benchmarks such as the Web Content Accessibility Guidelines (WCAG), ensuring compliance with the Americans with Disabilities Act. Unfortunately, many companies ignore these standards until legal action forces them to rectify their shortcomings, underscoring the necessity of proactive compliance and risk management.

Key recommendations

Early compromise assessments are especially vital in TMT. Dormant attack malware, also known as a sleeper, sometimes lurks unnoticed in target-company systems, waiting until postintegration to spring a trap and gain access to a much bigger cyber prize.

Leveraging real-time insights from advanced security technologies provides a comprehensive view of potential exposures, enabling a more informed and resilient integration process. This intelligence supports strategic decision-making and strengthens postacquisition security posture. While it is not always possible to deploy these tools prior to an acquisition, rapid deployment during clawback evaluation periods helps ensure that the representations made during the acquisition match the target's actual cyber risk posture.

1 Appoint a cybersecurity tiger team

Assemble a dedicated cybersecurity task force to identify industry-specific endemic cybersecurity and regulatory risks and set objectives for the deal. This team can provide guidance on information collection and help ensure seller documentation explicitly ties costs to potential impact.

Priorities during this phase include considering industry-specific risk factors that tailor cybersecurity assessment strategies to industry and acquisition goals. Next, examine regulatory and compliance requirements, especially those that are inherited in cross-border deals. Finally, weigh the costs of assessment and prevention versus the potential cost and complexity of a breach response.

2 Include cybersecurity in your due diligence

In the 30- to 60-day window before a deal is signed, gather preliminary information about the target company's cybersecurity posture, policies, and procedures. This high-level assessment involves reviewing documents, conducting interviews, distributing questionnaires, identifying critical risks, and performing an initial assessment of compromise exposure, breach risk, and threat intelligence. Ask the seller to provide representations of its security posture by completing a questionnaire that details key cybersecurity information, requesting a follow-up for greater specificity, as needed.

3 Conduct a postclose maturity assessment and contract review

After the transaction closes, identify the cyber risks involved in the new enterprise and match it to statements and assurances provided during the due diligence assessment—before integration and the end of clawback period. Determine whether any mismatches produce incremental costs. If necessary, trigger clawback provisions that were agreed to earlier in the deal.

4 Monitor and strengthen cybersecurity

After the transaction closes, teams must conduct ongoing assessments to detect and prevent new vulnerabilities from emerging. Continuous evaluation and enhancement of security measures help ensure the integration process does not introduce new weaknesses.

This phase emphasizes implementing enhanced security controls, such as using EDR and XDR to provide near-real-time alerting. Integrate the new entity into existing incident response planning and connect key stakeholders with the acquiror's Security, Information Technology (IT), and SecOps teams.

Each of these phases is crucial for successfully managing cybersecurity risks throughout the merger and acquisition process and ensuring the protection of sensitive data and IT assets. They are key to identifying potential vulnerabilities that might compromise the target and ultimately the deal itself. With a clear understanding of the target's cybersecurity posture, the acquirer can more accurately negotiate deal protections, budget for remediation, and assess whether the assets justify the cybersecurity risk.

How KPMG can help

KPMG assists organizations with cybersecurity acquisition and divestiture services by providing knowledgeable guidance on due diligence, risk assessment, and regulatory compliance. We help acquirers and divestors adhere to necessary data protection standards like the General Data Protection Regulation and the Health Insurance Portability and Accountability Act.

KPMG helps identify and mitigate cybersecurity risks, develop integration plans for aligning security measures across entities, and establish robust data governance frameworks to protect sensitive information. We support incident response planning and evaluate IT and security architectures for resilience. Additionally, KPMG offers continuous monitoring and improvement services as well as training and awareness workshops. We help stakeholders understand cybersecurity risks and leading practices, thereby safeguarding assets and helping ensure successful, secure outcomes in M&A transactions.

Authors

Anuj Bahal

Global Lead Principal and US TMT Sector Lead for Deal Advisory and Strategy

Anuj is a results-driven KPMG principal combining business savvy and strategic insight with technical proficiency. He has 30 years of transformation, complex M&A, and business consulting experience in US and international markets. Anuj is the National US Deal Advisory & Strategy sector leader for TMT and the global lead partner on two of the firm's priority Fortune 250 clients. He is characterized as a results-driven leader with high integrity and excellent strategic and tactical experience who performs well in all environments. Anuj works smart, communicates well, makes tough decisions, and builds quality teams to help scale operations that consistently achieve growth and profitability. He started his career in London before moving to New York. Anuj lives in Short Hills, New Jersey, with his wife and three children.

Kevin M. Coleman

Partner, Advisory

Kevin has worked at KPMG for more than 20 years, spending five years in Audit and 15 years in Advisory, focusing mostly on IT advisory. He has worked in various industries, including financial services, high tech, dot-com, and state and local government. More recently, Kevin has worked on various projects to improve companies' risk management programs. In particular, he has developed and deployed an overall IT risk management program addressing information security, operational risk, and continuity risk. Additionally, Kevin has deployed a governance, risk, and compliance platform to support compliance, operations, and financial control risk management. His specialties are IT governance, IT risk management, process reengineering, and cloud computing.

Jonathan Fairtlough

Principal, Advisory

A principal in the KPMG Cyber Threat Management practice, Jonathan has more than 20 years of experience in investigating and responding to digital data incidents, cyberattacks, and theft. Jonathan works with a diverse client base to help manage complex data and intrusion incidents, including ransomware, data extortion, theft of intellectual property, and insider theft. Jonathan specializes in working at the direction of counsel to integrate IR response and management services. He has assisted hundreds of clients in response to active data incidents. Jonathan is a Certified Information Systems Security Professional, holding CISSP license number 513407 since 2017. Jonathan also holds the GIAC Strategic Planning, Policy, and Leadership certification. He is an active member of the California Bar Association, number 175496.

We would like to thank our contributors:

Michael Bender, Lisa Bigelow, Sarah McEwen, Brennan Morris, Vijay Subramanyam, and Lara Volpe

For more information, contact us:

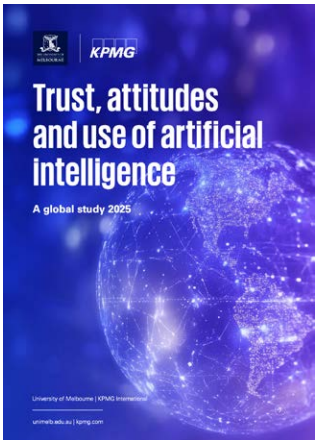
Anuj Bahal
Global Lead Principal and
US TMT Sector Lead for
Deal Advisory and Strategy
abahal@kpmg.com

Kevin M. Coleman
Partner, Advisory
kmcoleman@kpmg.com

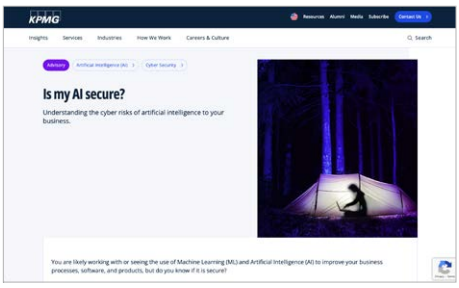
Jonathan Fairtlough
Principal, Advisory
jfairtlough@kpmg.com

Related thought leadership:

Transforming technology risk



Trust, attitudes and use of artificial intelligence



Is my AI secure?

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

Please visit us: **kpmg.com** **Subscribe**

DASD-2025-18782