Markets in Focus

Q4 2025

TECHNOLOGY

Economic Overview & Market Update

IMA

INTRODUCTION

The landscape for the technology industry in 2025 has been defined by two intertwined themes: technological acceleration and a rapidly changing risk landscape. Technology sectors moved decisively from pilot initiatives to full-scale implementation, with artificial intelligence (AI) a dominant technology deployed across operations. The rapid integration of AI has introduced a complex risk environment, where anticipation of innovation often outpaces infrastructure readiness, such as security, and emerging threats demand proactive risk management to safeguard competitiveness and operational resilience.

ECONOMIC OUTLOOK

Several strong tailwinds are helping the tech sector, and they suggest the industry is not just coasting but actively entering a new phase of growth.

The technology industry sector is well-positioned for growth in 2025, albeit not without caveats. The fundamentals—strong tech trends, AI/automation, cloud/data-center expansion—are in place. But growth is not guaranteed to be smooth. Macroeconomic headwinds, regulatory/supply risks, and the need for companies to transition from optimization to innovation all imply a more selective growth environment.

SOLID SPENDING GROWTH

+ Global IT spending is expected to grow by about 9.8% in 2025, with software and data-center segments–in particular–seeing double-digit growth.[1]

+ IT spending in the U.S. is expected to grow 6.1% in 2025, to roughly U.S. $2.7 trillion, despite macroeconomic headwinds.[2]

STRONG STRUCTURAL THEMES

+ In the semiconductor space, even as PC/mobile demand is soft, data-center / AI-compute demand is expected to drive a rebound.

+ The sector is shifting from its recent cost-cutting focus toward strategic growth and investment.

RESILIENCE AMID TURBULENCE

+ Tech spending is showing meaningful resilience, despite slowing global economic growth. Companies continue to invest in digital transformation, automation, and productivity enhancement.

+ Even in more challenging macro conditions, the relative value of technology—software, cloud, AI, automation—remains high.

MACRO SLOWDOWN & EXTERNAL UNCERTAINTY

+ The Organization for Economic Co operation and Development (OECD) notes that trade barriers, policy uncertainty, and tighter financial conditions will weigh on growth.[3]

+ Global GDP growth forecasts remain modest, with an expected 2.9% growth in 2025, which means tech does not operate in a vacuum.[4]

EARNINGS / VALUATION RISKS

+ While spending is growing, earnings growth for tech companies has been revised downward, with 2025 earnings growth estimates down due to macroeconomic and competitive pressures.[5]

+ Some mature segments such as consumer hardware and telecoms are seeing price compression, margin pressure, and slower growth.

LABOR & TALENT, COST PRESSURES

+ The industry has undergone large layoffs/focused on productivity rather than headcount growth.

+ Recruiting/retaining high-skill talent (AI/ML engineers, edge-compute specialists) is more competitive and expensive.

+ Inflation, interest-rate pressure, and supply-chain constraints still exist and can increase cost of goods sold or delay investments.

+ Tech is increasingly subject to regulatory, export-control, data-sovereignty, and national-security pressures (e.g., semiconductors, AI chips).

REGULATORY/GEOPOLITICAL & SUPPLY-CHAIN RISK

+ Tech is increasingly subject to regulatory, export-control, data-sovereignty, and national-security pressures (e.g., semiconductors, AI chips).

LEGISLATIVE AND POLICY UPDATES

RECENT COURT RULINGS AND REGULATORY CHANGES

The Loper Bright decision has shifted how regulators operate. They're now less likely to create new rules, since those rules are more easily challenged in court. Instead, they're focusing on enforcing existing rules that have strong legal backing. For your compliance teams, this means documenting your reasoning clearly. Show exactly how you interpret regulations and make decisions. The Sixth Circuit recently struck down the FCC's attempt to restore net neutrality, creating more uncertainty. With federal power shifting to states, businesses need to prepare for different rules in different places. The Supreme Court's Corner Post decision also allows companies to challenge older regulations for longer periods, potentially leading to more lawsuits in the future.

LAWS ENACTED

The Take It Down Act, enacted in May 2025, criminalizes the non-consensual sharing of intimate images—including AI-generated deepfakes. Platforms are required to remove infringing content within 48 hours of receiving a notification. The FTC leads enforcement, imposing severe penalties where minors are affected. Prompt removal provides liability protection for platforms.

California's SB 53, signed in September 2023, is the first U.S. law targeting frontier AI safety. It requires large AI companies (those with over $500 million in annual revenue) to publish governance frameworks, transparency reports, and incident reports. It also protects whistleblowers. This applies to foundation models trained with over 10^26 computational operations.

PENDING LEGISLATION

The No FAKES Act, introduced in April 2025, targets digital replicas and deepfakes. Stakeholder concerns center on perceived favoritism toward major tech and entertainment interests. The bill does not establish clear federal digital replica rights and could conflict with state provisions.

The Kids Online Safety Act (KOSA) directs tech companies to shield children from harmful online content like posts about eating disorders or bullying. Although reintroduced in May 2025, it has not passed the federal level. States such as California, Utah, and Florida have enacted their own child safety laws, which differ greatly and face legal challenges.

The SANDBOX Act proposes an AI innovation environment, granting companies regulatory waivers of up to 10 years contingent on risk-benefit analyses and periodic progress reports. The objective is to advance U.S. AI capabilities and gather evidence to inform policymaking.

Unveiled in April 2024 with bipartisan support, the American Privacy Rights Act would provide enforceable privacy rights under a single national standard, replacing varied state laws.

CHIPS ACT UPDATE

The CHIPS Act is driving U.S. semiconductor manufacturing growth. As of August 2024, $30 billion allocated to 23 projects across 15 states had created 115,000 new jobs. Major companies—including Intel, TSMC, Samsung, and Micron—secured an additional $33 billion. The Act may face revisions as stakeholders express concern about firms accepting subsidies while continuing investment abroad, particularly in China; limited foreign spending is still permitted under the Act.

ARTIFICIAL INTELLIGENCE

2025 marked a definitive shift in how businesses approached AI. Companies moved from experimentation to demanding demonstrable value, though many struggle to measure an effective ROI. A key development is the emergence of agentic AI—autonomous systems or 'agents,' that can independently plan and execute complex, multi-step tasks. These virtual coworkers are capable of making decisions and adapting to environments with minimal human input. Some tech executives see the eventual creation of networks where AI agents perform specific tasks, with the possibility of an "uber agent" for oversight.

The current reality about AI remains more nuanced. Concerns over AI causing mass job displacement are being balanced by evidence that AI is proving to be a powerful co-pilot that automates mundane tasks and helps workers be more productive. Industries more exposed to AI show higher growth in revenue per worker and higher wages for those with AI skills. While multimodal AI has evolved to enable richer interactions and better contextual understanding, human oversight remains critical.

AI reasoning has improved significantly, yet models still struggle with certain complex reasoning tasks, an issue in industries such as finance and healthcare, making human review a necessity.

Physical limitations—like energy availability and access to specialized chips—continue to challenge network scalability. The rapid growth in AI demand reveals stress points across global infrastructure, from constrained data center power to supply chain bottlenecks and regulatory hurdles around grid access.

As AI becomes more deeply embedded in core business operations, ethical concerns—particularly around bias, privacy, and security—are moving to the forefront. In the absence of comprehensive federal AI regulations in the U.S., companies are taking the lead in establishing responsible AI practices to earn stakeholder trust and mitigate risk. Globally, governments are accelerating regulatory efforts, like the EU's structured AI Act. The result is a fragmented and evolving landscape that organizations must carefully navigate

CYBER

Third-party risk is a growing concern for enterprise security strategies. Threat actors are adjusting attacks toward strategic operational vulnerabilities—focusing on supply chains and vendors that serve critical customer bases and exploiting vulnerabilities in interconnected networks. This strategy has become increasingly effective, as the disruption of services and supplies creates a rippling effect, producing significant disruptions and losses for customers.

Ransomware remained dominant throughout 2025. In the second quarter alone, the average ransom paid increased by more than 100% to $1.13 million.[6] Small and mid-sized organizations bore significant impact, with a third of all attacks targeting organizations with fewer than 100 employees and another third against those with less than 1,000. Data theft accompanied 74% of all attacks, though only 26% of ransomware incidents in Q2 2025 resulted in actual ransom payments—reflecting growing organizational resilience.

The role of third parties in high-profile attacks proved significant. In May 2025, threat actors compromised a well-known cryptocurrency exchange not through digital social engineering tactics, but by bribing employees of the exchange's overseas IT vendors to obtain customer information, which was then used to trick customers into transferring funds. Supply chain attacks continued producing cascading disruptions: a June cyberattack on a large food wholesale distributor left grocery store shelves empty throughout July and into August, impacting sales upstream and downstream while increasing the distributor’s operational costs and significant breach remediation expenses.

New attack vectors are emerging beyond traditional IT systems. GPS spoofing disrupts navigation systems, misdirects vehicles, and even manipulates location-based applications.[7] In May 2025, attackers used spoofing to broadcast fake GPS signals to receivers of MSC Antonia in the Red Sea, which disrupted navigation systems and misdirected the vessel.[8]

AI is amplifying cyber threats. Threat actors are using generative AI to create convincing phishing emails that mirror the tone and style of colleagues and eliminate the grammatical errors that made attacks easy to spot. These sophisticated messages are being translated across languages and deployed at scale. Threat actors also use AI to mine for organizational data, such as financial and, operational data, that they can use in demands against victims. Most concerning is AI's role in lowering the entry barriers for less-technical threat actors, writing code and automating ransomware-as-a-service model, democratizing sophisticated attack capabilities across the threat actor ecosystem.

DATA CENTERS

Driven by AI's voracious appetite for computing power, the race is also on to construct the data center at scale. Training and deploying AI models requires vast resources. The numbers are staggering: the global data center market is projected to grow at a compound annual growth rate of more than 10% through 2030. AI demand alone could drive a 165% increase in computing requirements for hyperscalers by 2028. By 2030, data centers globally are expected to consume 945 terawatt-hours of electricity—more than double their 2024 consumption.[9]

This explosive growth is creating both opportunities and pressures. Governments are investing in AI infrastructure, easing regulations, and passing supportive legislation. Major tech firms are pouring capital into infrastructure to support AI-ready facilities, which require specialized construction. Yet scaling challenges persist: data center power constraints, physical network vulnerabilities, and rising computer demands are exposing infrastructure gaps. The challenge extends beyond technical architecture to talent shortages, policy constraints, and execution difficulties.

SURVEILLANCE TECHNOLOGIES

The proliferation of commercially available surveillance applications has created significant legal and operational exposures for businesses. More and more companies are using monitoring technology to track employee activities, but it carries significant legal, ethical, and operational risks. If not handled carefully, this practice can erode trust, damage company culture, and lead to serious financial and reputational fallout. As organizations look to balance oversight with transparency, it's critical to ensure monitoring practices are thoughtful, compliant, and aligned with core values.

Legal risks are substantial. Employees may sue for invasion of privacy if monitoring is excessively invasive, particularly when recording them remotely in their homes. The Electronic Communications Privacy Act allows employers to monitor communications for "legitimate business reasons" or with employee consent, but companies risk civil and criminal penalties for illegally intercepting private communications. Data privacy regulations like GDPR, the California Consumer Privacy Act, and Illinois' Biometric Information Privacy Act impose strict compliance requirements.

Beyond legal exposure, surveillance creates operational risks. Secret or excessive monitoring erodes trust and morale, signaling a lack of confidence that can make employees stressed, disengaged, and resentful. High-performing talent may be the first to leave if they feel their autonomy is compromised, while companies known for aggressive surveillance practices struggle to attract quality candidates. There are technical vulnerabilities too: monitoring systems that collect sensitive behavioral and personal data become prime targets for hackers if poorly secured, while AI-driven monitoring tools may use algorithms that unfairly target certain groups or misinterpret activities.

KEY COVERAGES TO WATCH

TECHNOLOGY ERRORS & OMISSIONS (E&O)

+ Technology E&O protects organizations from the financial impact of third-party lawsuits. This coverage protects against costly legal defense fees, settlements, or judgments stemming from allegations of software bugs, misrepresentations, failed integrations, or product malfunctions that lead to client financial loss.

+ Rapid innovation and evolving regulation are complicating insurer risk assessment. As technologies—particularly AI—advance quickly and regulations strive to catch up, insurers face difficulties in defining coverage boundaries and avoiding unintended exposures. This dynamic landscape challenges underwriters to constantly reassess what losses are within scope versus those they inadvertently insure.

+ Warranty and guarantee exclusions should be refined to preserve coverage for liabilities assumed under standard SaaS contractual terms.

+ Insurers are increasingly deploying broad AI and model-error exclusions; affirmative model-risk endorsements are emerging. Many E&O policies now include sweeping provisions excluding any claim related to the use, development, or deployment of AI—encompassing model errors, hallucinations, biased outputs, and training data risks. Conversely, some carriers are offering limited affirmative endorsements specifically covering generative AI failures—such as hallucinations and inaccurate data—underscoring the necessity of actively negotiating clear policy language to secure intended coverage of model risks.

+ Regulatory sandbox programs are introducing heightened E&O exposure due to mandatory incident reporting. Pilot programs that fall under recent regulatory frameworks (e.g., those in bills like the Sandboxing Act) mandate the disclosure of serious incidents within tight timelines (often 72 hours). This rapid reporting requirement—whether under S.2750 or similar statutes—could increase the volume of E&O claims by spotlighting failures in early-stage deployments and triggering insurer action.

CYBER

+ Cyber insurance capacity remained strong throughout the first half of 2025.[10]
+ Cyber continues to be a profitable insurance line, prompting insurers to expand their portfolios.
+ Insurers are increasingly supporting cyber MGAs that focus on small and mid-sized market organizations.
+ Policy language around third-party risk exposures is tightening, especially when it comes to vendor responsibilities, data handling, and breach response.
+ Technology manufacturers adopting smart technologies should look to cyber insurance policies that address emerging operational and strategic vulnerabilities.
+ Cyber risks now extend beyond IT to include operational technologies (OT), IoT devices, cloud-connected assets, and supply chains. All of which demand more precise policy endorsements, conditions, and exclusions.
+ Where necessary, cyber policies should be tailored to include contingent business interruption and OT/IoT coverage.

DIRECTORS LIABILITY

+ Directors' and Officers' (D&O) litigation remains elevated compared to historical levels, but overall market conditions remain favorable.
+ The downward trend in pricing has begun to stabilize.
+ Capacity remains abundant, driven by competition among established carriers and new entrants seeking to grow their market share.
+ Underwriters are placing greater emphasis on pricing discipline rather than growth.
+ Mid-market companies may be purchasing more D&O coverage than they need, by as much as $15 to $20 million, with total claims settlements averaging nearly half of their total coverage.[11]
+ Carriers remain cautious towards companies with near-term capital needs or a high likelihood of M&A.
+ Legacy policies may offer a foundation of coverage against AI claims, but new exclusions may narrow protections just as AI-related liabilities increase in frequency and complexity.[12]

GLOBAL LIABILITY COVERAGES

+ The liability insurance market is experiencing significant challenges, with double-digit rate increases.
+ Securing coverage for the primary layer is becoming increasingly difficult.
+ Terms and conditions are becoming more flexible as reinsurers become more willing to protect programs, including lower attachment points and more frequent return periods.[13]
+ Competition remains limited for clients with higher-risk profiles.
+ Social inflation continues to drive up litigation costs, jury awards, and settlement values.

WORKERS' COMPENSATION

+ Hybrid work environments are increasing ergonomic and mental-health exposures, with a noticeable rise in remote-work-related ergonomic claims.
+ The use of AI-driven HR tools has led to employment discrimination claims arising from algorithmic bias, potentially reinforcing Employment Practices Liability (EPL) definitions related to employment decision-making.

IN SUMMARY

While global IT spending is set to grow significantly, the sector faces a complex risk landscape shaped by macroeconomic pressures, regulatory uncertainties, supply chain challenges, and talent shortages. Companies must shift their focus from cost optimization to strategic growth and innovation to remain competitive.

AI continues to redefine business operations, offering opportunities for enhanced productivity and efficiency while introducing new ethical, security, and infrastructure challenges. The emergence of agentic AI and the increasing reliance on data centers highlight the need for robust investment in infrastructure and responsible AI practices. At the same time, the rise of generative AI and advanced cyber threats underscores the importance of proactive cybersecurity measures.

Legislative and regulatory developments, including the CHIPS Act, Take It Down Act, and pending bills like the SANDBOX Act, are reshaping the industry's compliance requirements. Businesses must adapt to this evolving landscape, balancing innovation with risk management and regulatory adherence.

The insurance market is evolving to address the unique risks posed by technological advancements, offering tailored solutions for cyber threats, AI-related liabilities, and operational vulnerabilities. As the industry continues to grow, organizations must prioritize resilience, adaptability, and strategic planning to navigate challenges and capitalize on opportunities in this dynamic environment.

The road ahead is promising but requires careful navigation. By embracing innovation, addressing risks proactively, and aligning with regulatory and ethical standards, businesses can position themselves for sustainable growth and success in the rapidly evolving technology landscape of 2025 and beyond.

Sources

1 LoDolce, Matt, and Moran, Meghan. (2025, January 21). Gartner Forecasts Worldwide IT Spending to Grow 9.8% in 2025. Gartner. https://www.gartner.com/en/newsroom/press-releases/2025-01-21-gartner-forecasts-worldwide-it-spending-to-grow-9-point-8-percent-in-2025

2 O'Grady, Michael. (2025, February 11). US Tech Spending Defies The Economic Slowdown To Hit $2.7 Trillion In 2025. Forrester. https://www.forrester.com/blogs/us-tech-spending-defies-the-economic-slowdown-to-hit-2-7-trillion-in-2025/#:~:text=Despite%20persistent%20inflation%2C%20US%20real,enhance%20customer%20and%20patient%20experiences.

3 Organisation for Economic Co operation and Development. (2025, June 3). OECD Economic Outlook, Volume 2025 Issue 1. OECD. https://www.oecd.org/en/publications/oecd-economic-outlook-volume-2025-issue-1_83363382-en.html

4 Organisation for Economic Co operation and Development. (2025)

5 Bogdanova, Kelly. (2025, August 7). Tech steals the Q2 earnings show. RBC Wealth Management. https://www.rbcwealthmanagement.com/en-eu/insights/tech-steals-the-q2-earnings-show#:~:text=Tech%20and%20non%2Dtech%20earnings,are%20Bloomberg%20consensus%20estimates%20(E)

6 Burke, Tim., and Boeck, William. (2025, August 27). Cyber Market Update Q3 2025. IMA Financial Group. https://imacorp.com/insights/cyber-markets-in-focus-q3-2025

7 Burke, et al. (2025).

8 Burke, et al. (2025).

9 International Energy Agency. (2025, April 10). AI is set to drive surging electricity demand from data centres while offering the potential to transform how the energy sector works. IEA. https://www.iea.org/news/ai-is-set-to-drive-surging-electricity-demand-from-data-centres-while-offering-the-potential-to-transform-how-the-energy-sector-works

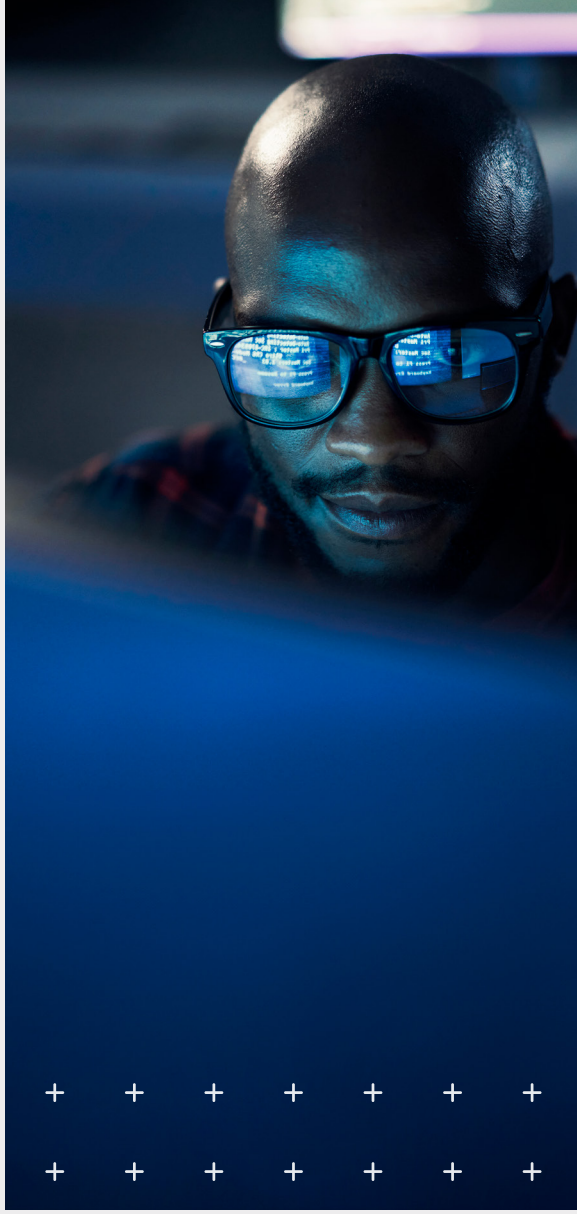
10 Burke. (2025)

11 Dilworth, Shane. (2025, May 29). Companies might have too much D&O coverage: Report. Business Insurance. https://www.businessinsurance.com/companies-might-have-too-much-do-coverage-report/

12 Bracken, Lawrence; Fehling, Geoffrey B.; Levine, Michael S.; Moore, Madalyn; and Pappas, Alex D. (2025, July 2). How Insurance Policies Are Adapting To AI Risk, Law360. Hunton. https://www.hunton.com/insights/publications/how-insurance-policies-are-adapting-to-ai-risk

13 Wells, Kane. (2025, July 16). Capacity & competition put further pressure on prices after 2024 peak: Fitch. ReInsurance News. https://www.reinsurancene.ws/capacity-competition-put-further-pressure-on-prices-after-2024-peak-fitch/

GUIDANCE



START EARLY

Partner with your broker early to prepare for any changes to increase renewal success.

PARTNER WITH INDUSTRY EXPERTS

It is important to collaborate with your broker's industry experts who understand the business and the market for placing the specific risk. Collaborating with a team that can best represent your risk and partner with your operations is more important than ever during this disciplined market we are experiencing.

HIGHLIGHT CYBER SECURITY & PROACTIVE RISK MANAGEMENT

IMA has a team solely dedicated to managing cyber risks. They offer expert assistance, including coverage analysis, monetary loss exposure benchmarking, contract language review, in-depth cyber threat analysis, and strategic development of comprehensive, high-value cyber insurance programs.

CONTRACT REVIEW

Our contract review teams add value to our clients' overall risk management program by ensuring the indemnity language is market standard and does not expose our clients to unforeseen losses that may not be insurable.

ENGAGE ESG

IMA invests heavily to deploy specialty niche teams concentrating on innovative technology, green energy initiatives, and advanced manufacturing. As every client is different, our Sustainability Advisory team provides clients with education, advice, and access to tools and best practices to advance their sustainability resilience and showcase their ESG performance for insurance underwriters.

MARKETS IN FOCUS CONTRIBUTORS

JEN SHERIDAN | *Vice President, Manufacturing Practice Leader, Advanced Industries Specialty*

ANGELA THOMPSON | *Marketing Strategist, Market Intelligence & Insights*

BRIAN SPINNER | *Senior Marketing Coordinator, Market Intelligence & Insights*

KEEP READING

MARKETS IN FOCUS

INSURANCE INSIGHTS

HR INSIGHTS

FOR ANY QUESTIONS, PLEASE REACH OUT TO:

JEN SHERIDAN
Vice President and Manufacturing Practice Leader, Advanced Industries Specialty
jen.sheridan@imacorp.com