# Technology sector faces critical turning point amid AI scrutiny and rising cyber threats



The technology sector faces a critical turning point in 2025 as businesses and stakeholders increasingly scrutinise the return on investments in artificial intelligence (AI), while simultaneously grappling with rising cyber threats and growing vulnerabilities in IT infrastructure.

The momentum behind AI growth, spurred notably by the launch of OpenAI’s ChatGPT in November 2022, has accelerated sharply, with industry leaders such as Microsoft, Google, and OpenAI channeling billions into the development of advanced AI systems. However, as Tom Kidwell, Co-Founder of Ecliptic Dynamics, outlined in an analysis for TechRadar, the conversation is shifting from AI’s vast potential to its measurable performance. He noted that despite projections of AI-related spending exceeding $1 trillion, many organisations are yet to see clear evidence of tangible returns.

In a recent comment highlighted by Kidwell, Glenn Fogel, CEO of Booking Holdings — which owns travel platforms including Booking.com — remarked that, while AI tools offer helpful assistance, only a small fraction of customers engage with the company’s AI services. He observed, “responses and recommendations are inconsistent,” indicating that AI still requires refinement before large-scale deployment can be confidently pursued. This points to a broader industry dilemma: the challenge of balancing high implementation costs against unpredictable outcomes, alongside ethical considerations surrounding AI technology. The uncertainty around AI’s optimal business applications has led to growing scepticism among investors and company boards about the viability of continued extensive funding.

Alongside AI developments, the cyber threat landscape has grown markedly more volatile amid ongoing geopolitical conflicts. The surge in state-sponsored cyber-attacks, particularly linked to the war in Ukraine, is notable. Data reveals that Russian cyber-attacks targeting Ukraine surged by nearly 70 per cent in 2024, with over 4,300 incidents aimed at critical infrastructure. Analysts anticipate an escalation in these hostile activities, especially throughout Asia. One significant concern is supply chain infiltration, especially given China's deep integration within the global technology supply chain. There is apprehension that malicious code, backdoors, or hardware vulnerabilities may have been embedded well before deployment, posing a stealthy and persistent threat.

Australia has also been identified as a potential hotspot for state-sponsored cyber aggression. Its strategic alliances with the United States and increasing tension with China mean that any emerging cyber-attacks within Australia could potentially signal wider Chinese cyber strategies.

Interconnectivity, a core feature of modern IT environments, presents its own risks. The global reliance on interconnected devices and software means that single points of failure can trigger widespread operational disruption. The high-profile CrowdStrike outage experienced last year served as an alarming example, exposing how a solitary IT failure can ripple across industries worldwide. Kidwell highlights that many organisations lack comprehensive backup plans and are unprepared for incidents such as prolonged cloud service outages or critical software failures. He emphasises the importance of developing robust contingency strategies to ensure operational continuity under adverse conditions.

Data residency and sovereignty concerns have also come to the fore in 2025, intensified by geopolitical friction and incidents of undersea cable sabotage. Much of the world’s internet traffic relies on these undersea cables, which increasingly face risks of disruption. Sweden, for example, has suffered multiple instances of damage to its undersea cables, with the latest incident occurring after a similar event in November of the previous year. Such attacks can severely impact global connectivity, financial markets, and other essential systems, potentially leading to sluggish or absent data transmission across whole regions.

Emerging technologies like satellite internet services, including Starlink, show promise as alternatives to traditional undersea cables but introduce their own security vulnerabilities. As Kidwell points out, “with these systems becoming integral to global communication, they present lucrative targets for cybercriminals and state-sponsored actors.” He advises companies to maintain clear knowledge of where their data is stored and under which jurisdiction, ensuring they have robust response plans to mitigate associated risks.

The landscape of cyber and IT security is evolving rapidly in response to new technological breakthroughs and the intensification of threats. As observers look to 2025, it is shaping up to be one of the most transformative years in IT history. According to Kidwell, firms that prioritise resilience, take proactive measures on AI integration, cybersecurity, and infrastructure management, and anticipate emerging risks will be best positioned to navigate the uncertainties and lead their sectors.

This analysis was originally presented in TechRadar’s Expert Insights channel, which features commentary from leading voices in the technology industry.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://am.jpmorgan.com/se/en/asset-management/per/insights/market-insights/investment-outlook/ai-investment/> - Discusses the scrutiny of AI investment returns and the gap between revenue expectations and actual growth in the AI ecosystem, aligning with concerns about tangible returns and investor skepticism.
2. <https://news.microsoft.com/source/features/ai/6-ai-trends-youll-see-more-of-in-2025/> - Highlights AI's evolution into an integral part of daily life and business by 2025, supporting claims about AI's growing adoption despite implementation challenges and inconsistent customer engagement.
3. <https://dws.com/en-us/insights/dws-research-institute/artificial-intelligence-what-to-expect-in-2025/> - Predicts a shift to industry-specific AI solutions in 2025, correlating with the article's focus on balancing high costs and unpredictable outcomes in AI implementation.
4. <https://hai.stanford.edu/news/ai-index-2025-state-of-ai-in-10-charts> - Reports on AI's maturing field and growing saturation in 2025, reinforcing the discussion of AI adoption rates and the need for measurable performance.
5. <https://www.noahwire.com> - The original source cited in the article, though specific content could not be verified (placeholder for completeness).
6. <https://hai.stanford.edu/ai-index/2025-ai-index-report> - Provides broader context on AI trends and challenges in 2025, supporting the article's analysis of industry-wide skepticism and infrastructure vulnerabilities.
7. <https://www.techradar.com/pro/ai-to-state-sponsored-attacks-how-tech-will-evolve-in-2025> - Please view link - unable to able to access data