AI-Driven Software Pressure vs. Cybersecurity Strength

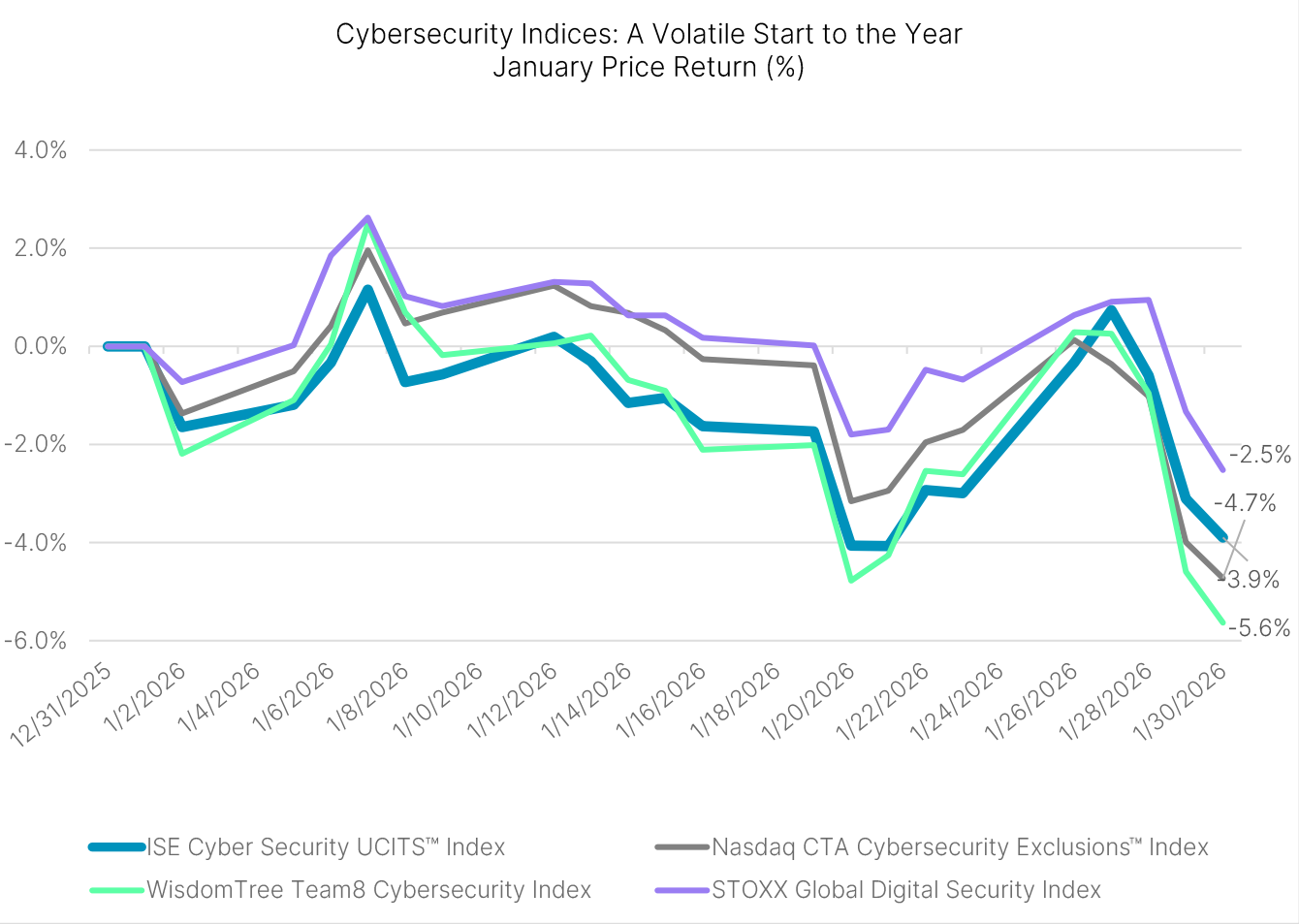
Monthly Cybersecurity Update

January 2026

Ilaria Sangalli, Head of Index Insights, EMEA

Cybersecurity indices start the year with heightened volatility

January was a volatile month for major cybersecurity indexes, with sharp swings across the broader space reflected similarly in the ISE Cyber Security UCITS™ Index (HUR™).



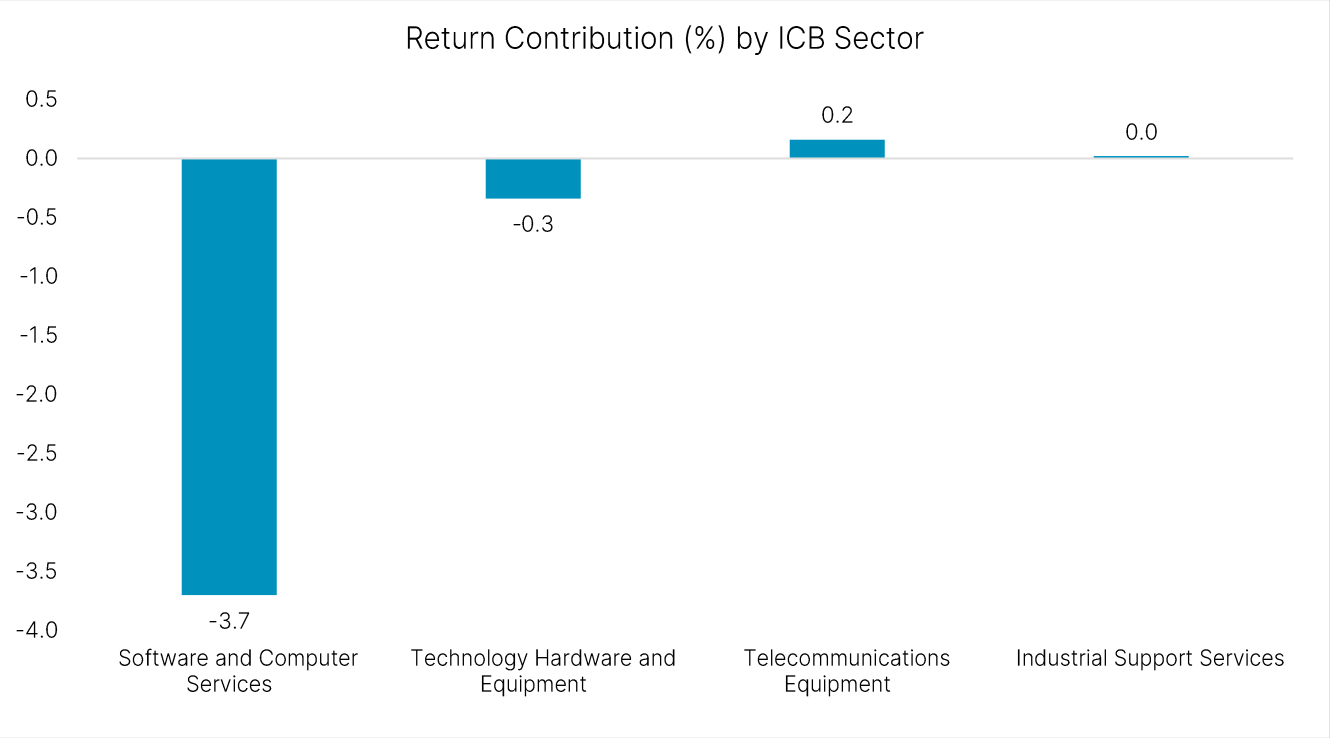
Source: Bloomberg, Nasdaq. Data as of January 30, 2026

The index gained 1.2% through January 7 before reversing into a steady mid-month decline, falling 5.2% between January 7 and 20. A short-lived rebound of 5.0% followed (January 20-27), but the move quickly faded, and the index ended the month sharply lower, dropping 4.6% from January 27 to 30.

Overall, the month was characterized by two short-lived rallies bookended by sustained declines, resulting in a negative monthly performance of -3.9%.

Sector performance deep dive – January 2026

The Software & Computer Services sector remained the dominant driver of overall performance. With an average weight of roughly 85%, it contributed -3.70% to the index's total return for the month.



Source: Bloomberg. Data as of January 30, 2026

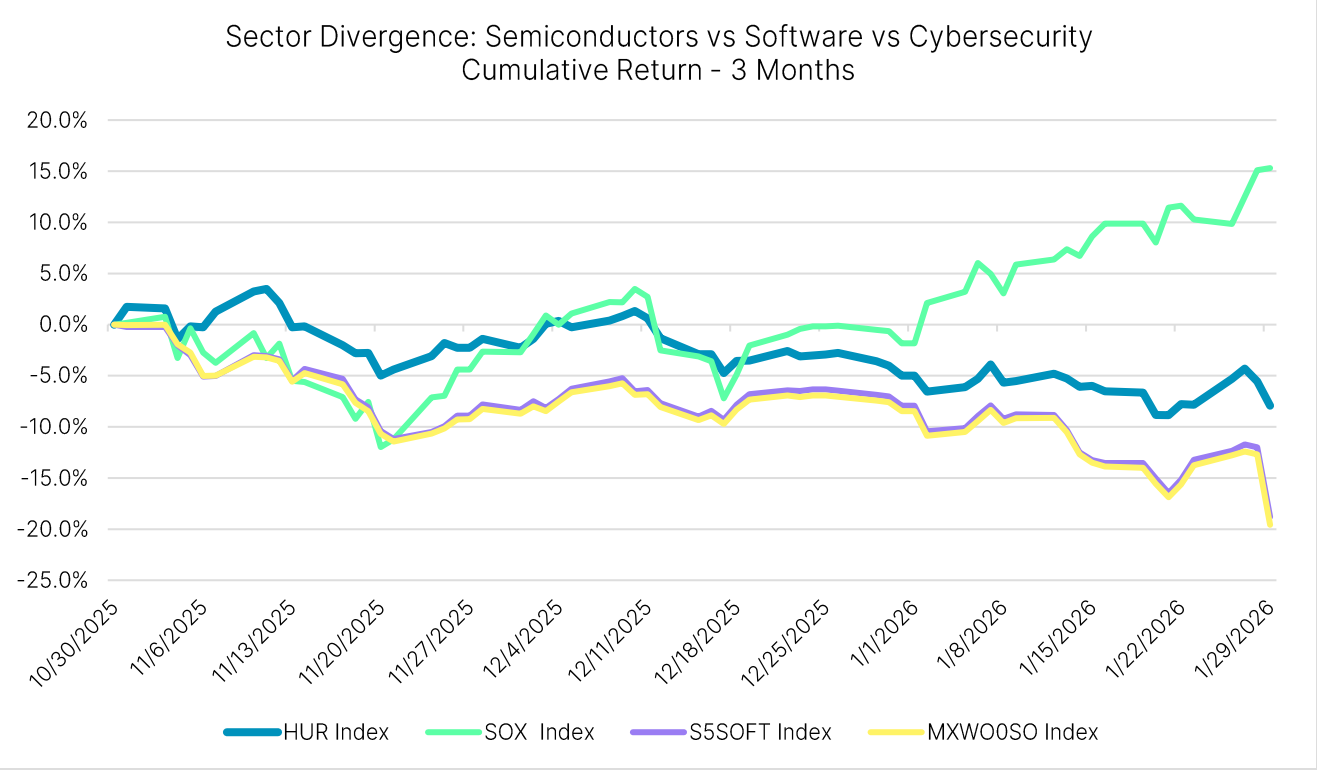
Technology Hardware & Equipment added a further -0.3% (6.9% average weight). By contrast, Telecommunications Equipment provided the only notable offset, contributing +0.2% at a 7.2% average weight, being the sole meaningful positive performer in the index. The only other contributor was the index's small exposure to Industrial Support Services, which added a modest +0.02%.

Software & Computer Services: structural headwinds amid long-term strengths

While AI is reshaping traditional Software & SaaS economics, cybersecurity is benefiting from a different set of structural dynamics. Security spend is supported by rising threat intensity, regulatory pressure, and the security implications of cloud and AI adoption. At the same time, many organisations are using renewal events as inflection points to reassess architectures, rationalise tool sprawl, and consolidate vendors.

These dynamics provide tangible support for cyber providers at a time when broader SaaS models face greater pricing and margin uncertainty from AI-driven change, enabling security vendors to compete for share as customers refresh platforms and modernise their security stacks.

As highlighted by Dylan Patel, the founder and chief analyst of SemiAnalysis[1], the traditional software model - long defined by recurring revenue, high switching costs, minimal COGS, and gross margins often exceeding 80% - is undergoing a structural shift. AI fundamentally alters this equation: inference-driven workloads raise the Cost of Goods Sold (COGS), hyperscalers gain cost advantages through vertically integrated stacks, and customer acquisition remains expensive even as pricing power diminishes. At the same time, AI lowers the cost of building software, enabling enterprises to insource workflows that previously justified SaaS spend. This pressure is evident in the erosion of the classic 80-90% gross-margin SaaS model, challenged by AI-native tools like ChatGPT and Claude, open-source LLMs that accelerate commoditisation, and the rise of internal low-code, no-code, and AI-assisted development capabilities.



Source: Bloomberg, Nasdaq. Data as of January 30, 2026

Performance trends reinforce this narrative. Based on return-index data sourced from Nasdaq and Bloomberg for the period 30 October 2025 to 30 January 2026, the HUR Index broadly tracked the S&P 500 Software Index (S5SOFT) and the MSCI World Software Index (MXWO0SO). Over this period, cybersecurity (HUR) continued to outperform these software benchmarks. In contrast, semiconductor performance diverged meaningfully: the PHLX Semiconductor Sector™ Index (SOX™) reflected widening

[1] An independent research firm widely followed across the semiconductor, AI hardware, and cloud infrastructure ecosystem. https://www.youtube.com/watch?v=kAIVualeQjM

dispersion within the semiconductor space, driven by select names benefiting from accelerating AI demand, while software companies continued to face structural headwinds.

While AI may gradually reshape certain software categories, its impact will vary widely across subsectors. Cybersecurity has shown relative resilience, given the accelerating pace of threats and the structural complexity of defending modern digital environments.

Deloitte's Cyber Threat Trends 2025 report notes that attack vectors are accelerating in sophistication, powered by new attacker motivations, AI-enabled tools, and a rapidly shifting ransomware ecosystem, making it difficult for new disruptors to replicate or replace established security vendors.[2]

According to Gartner, security software is currently the fastest-growing segment in the information security market, fueled primarily by organizations' continued migration from on-premises infrastructure to cloud environments. This shift introduces new vulnerabilities and operational complexities, making cloud security an urgent priority for businesses.[3]

Market research indicates that AI is also directly expanding cybersecurity demand: as threat actors weaponise AI to increase speed and sophistication, defensive software must evolve just as rapidly. This raises the minimum capability threshold any vendor must meet, reinforcing high barriers to entry and reducing the likelihood of rapid disruption compared with the broader software universe.

Darktrace's State of AI Cybersecurity Report 2025 highlights that most CIOs express limited confidence in non-AI-based cybersecurity solutions, doubting their ability to effectively detect or block increasingly sophisticated AI-powered threats.[4]

Finally, the World Economic Forum's Global Cybersecurity Outlook 2025 underscores a persistent global shortage of cybersecurity talent, which continues to widen capability gaps across organisations.[5] This structural skills deficit might further strengthen demand for automation-led, AI-driven security solutions as enterprises rely on software to compensate for constrained internal expertise.

Taken together, these factors indicate that cybersecurity software remains structurally resilient relative to other software categories, with AI reinforcing the sector's strategic importance and long-term demand profile.

[2] https://www.deloitte.com/us/en/services/consulting/articles/cybersecurity-trends-report.html
[3] https://www.gartner.com/en/newsroom/press-releases/2025-07-29-gartner-forecasts-worldwide-end-user-spending-on-information-security-to-total-213-billion-us-dollars-in-2025
[4] https://cdn.prod.website-files.com/626ff19cdd07d1258d49238d/67c5b7b24b8f30bb4878f9f5_Darktrace%20State%20of%20AI%20Cybersecurity%202025.pdf
[5] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Disclaimer: