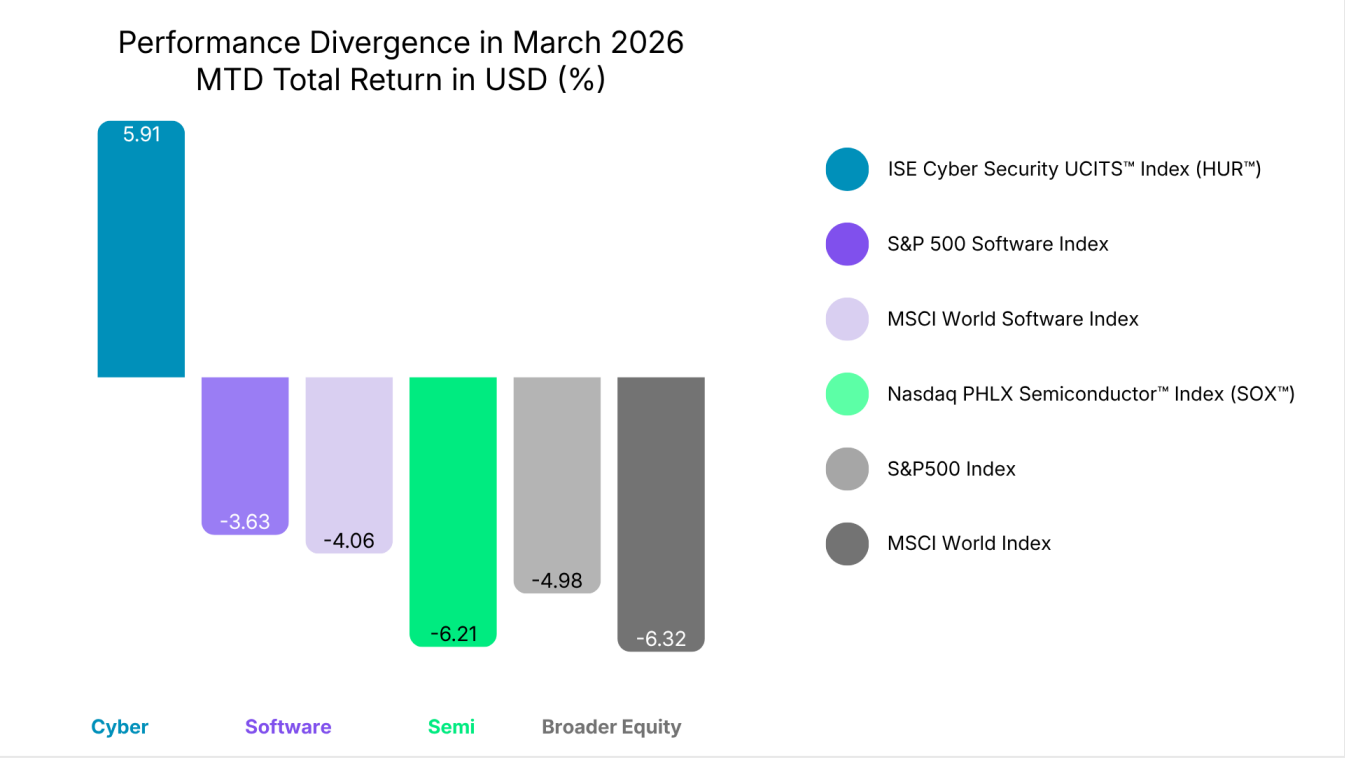
Geopolitical Tensions Drive Renewed Focus on Cybersecurity

March 2026 – Monthly Cybersecurity Update

Ilaria Sangalli, Head of Index Insights, EMEA

In March, amid elevated geopolitical tensions in the Middle East, cybersecurity equities outperformed broader equity markets, despite a generally weaker environment for technology stocks. The ISE Cyber Security UCITS™ Index (HUR™) gained 5.91%, compared with declines of 4.98% for the S&P 500 (SPX) and 6.32% for the MSCI World Index (MXWO). This performance coincided with increased investors' focus on cyber resilience, even as the broader software sector remained under pressure over the period.



Source: Bloomberg. Data as of March 31, 2026

The divergence highlights a shift in investor behavior. After January and February, when broader skepticism toward software weighed on the cybersecurity sector, March marked a clearer differentiation. Investors increasingly separated cyber-defense from broader software exposure, treating cybersecurity as a distinct, mission-critical segment within the technology universe amid rising geopolitical uncertainty.

Rising Geopolitical Risk Reinforces Cybersecurity's Strategic Importance

Market performance has moved in parallel with warnings from cybersecurity experts that geopolitical tensions may translate into elevated levels of cyber disruption. Threat-intelligence analysis from Palo Alto Networks' Unit 42 indicates increased activity from Iran-affiliated groups operating outside the country. At the same time, near-term threat activity from nation-state actors operating within Iran appears constrained by the country's limited internet connectivity. As a result, activity is expected to concentrate on low- to medium-complexity attacks, such as distributed denial-of-service incidents and data-leak campaigns.[1]

Bloomberg reported that cybersecurity researchers at Sophos warned that government entities, critical infrastructure, financial services, and defense-adjacent commercial organizations face the highest risk of elevated threats in the coming days and weeks. The article also quoted Cynthia Kaiser of Halcyon[2] (a former FBI cyber official), who noted that Iran-affiliated groups have historically retaliated against perceived political slights through tactics such as disrupting financial services websites, data-destructive incidents, and website defacements.[3,4]

From a market perspective, heightened geopolitical risk has increased investor focus on cybersecurity, supporting stronger relative performance and reinforcing the sector's strategic importance as digital resilience remains a priority for both organizations and governments. This focus aligns with the World Economic Forum's Global Cybersecurity Outlook 2026, which shows that 64% of organizations already factor geopolitically motivated cyberattacks into their risk frameworks, while 91% of large organizations (with over 100,000 employees) have adjusted cybersecurity strategies in response to geopolitical volatility.[5]

Iran-Linked Cyber Activity Escalates: From Warnings to Confirmed Disruption

Since mid-March, news reports have begun identifying a possibly significant data-destructive cyberattack originating in, or tied to Iran, against U.S. medical technology company, Stryker. Public reporting described a significant disruption to the company's internal Microsoft environment, with operations temporarily affected across multiple geographies. Notably, the incident was widely described as destructive rather than financially motivated, distinguishing it from traditional ransomware activity. Subsequent analysis by cybersecurity researchers, along with U.S. government assessments, attributed the attack to Iran-aligned threat actors.[6]

In March 2026, the U.S. Department of Justice announced the seizure of four internet domains used by Iran's Ministry of Intelligence and Security (MOIS) to conduct cyber-enabled psychological operations. These campaigns leveraged hacking and online platforms not only to compromise systems, but also to intimidate targets, spread fear, and influence behavior. According to U.S. authorities, the seized sites were used to publicly claim responsibility for cyberattacks, leak stolen personal data, issue explicit threats, and incite violence.[7]

[1] https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[2] An anti-ransomware solutions provider
[3] https://news.bloomberglaw.com/privacy-and-data-security/iran-war-puts-companies-infrastructure-on-cyber-threat-alert
[4] Web defacement is a cyberattack in which attackers take control of a website and replace its content with unauthorized messages or imagery, typically to make a political or symbolic statement.
[5] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf
[6] https://www.nbcnews.com/world/iran/iran-appears-conducted-significant-cyberattack-us-company-first-war-st-rcna263084
[7] https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations

In Europe, Poland is investigating whether Iran may be behind a foiled cyberattack on the National Centre for Nuclear Research, a key nuclear research facility in the country.[8]

Augur Security reported that within 24 hours of the February 28, 2026 U.S.-Israel strikes, an "Electronic Operations Room" was established to centrally coordinate more than 60 Iran-linked hacktivist groups. According to the report, intended targets included U.S. and Israeli government entities, financial institutions, critical infrastructure, and Gulf states perceived to be facilitating U.S. or Israeli action.[9]

In a period of elevated geopolitical tension, this makes cyber hygiene more critical than ever. As reported by SecurityWeek, according to Shaun Williams, a former FBI and CIA officer and now a senior director at cybersecurity firm SentinelOne, organizations that have failed to keep pace with baseline cybersecurity practices may face severe disruption.[10]

A Deep Dive into the ISE Cyber Security UCITS Index

Performance

The ISE Cyber Security UCITS™ Index gained 5.91% over the month, supported by strong performance in early March as heightened geopolitical and cyber risk sustained investor focus on cybersecurity exposures.

As the month progressed, performance became increasingly driven by a small group of leaders. Fastly, Cloudflare and Ziff Davis were the primary contributors, together accounting for 5.73% of total index return.

Overall performance reflected selective participation rather than broad-based gains. 11 of the 28 constituents delivered positive total returns, generating a combined +8.49% contribution to index performance. This highlights the strength of a core group of names that captured the majority of upside during the month.

At the same time, contributions from weaker performers remained measured. The remaining constituents recorded negative returns, with a combined impact of -2.58%, while the three largest detractors (Gen Digital, Check Point and BlackBerry) together reduced index performance by a modest -1.18%.

Q4 2025 Earnings

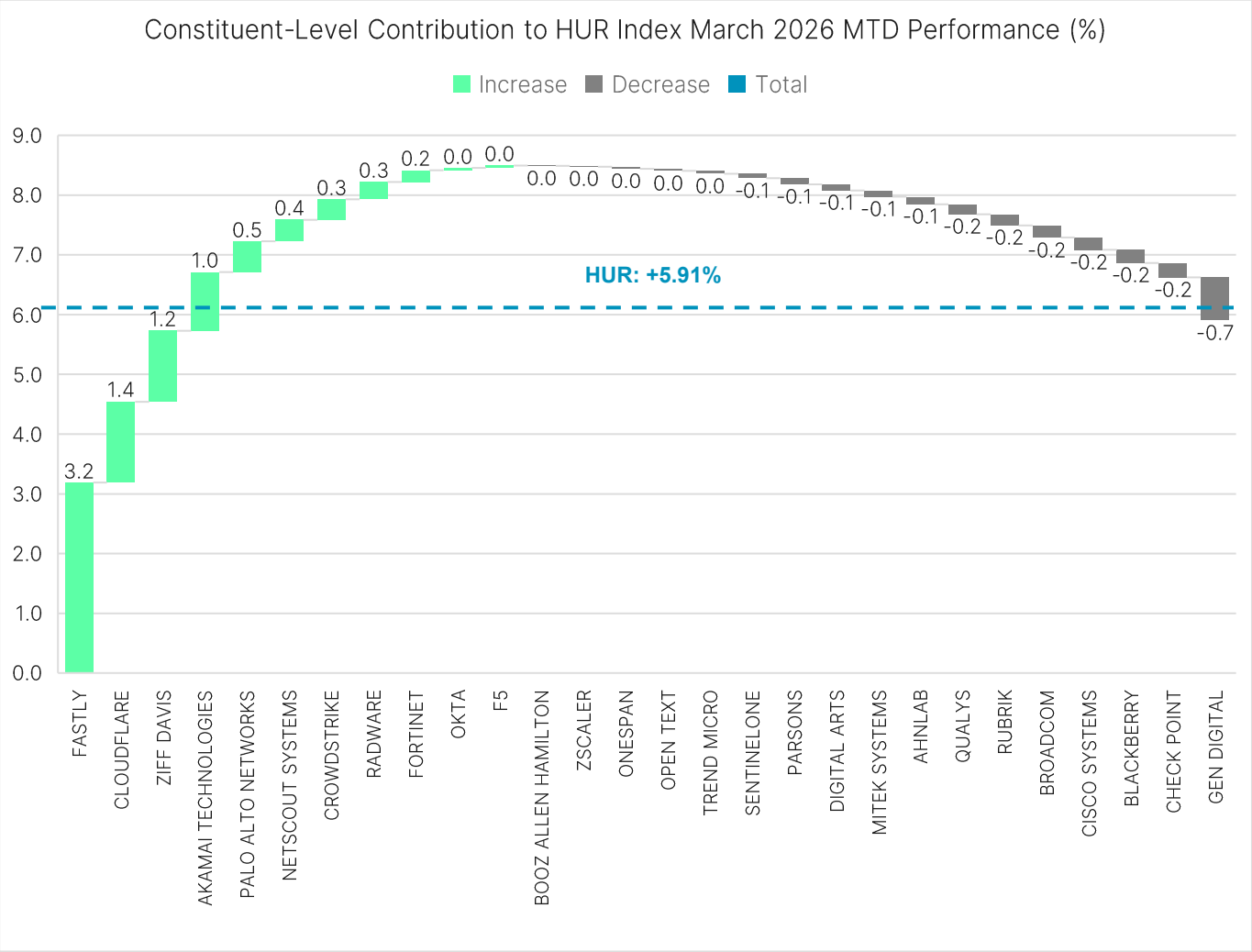
Earnings season has been broadly positive for companies within the ISE Cyber Security UCITS™ Index, with five additional companies reporting during March. As of March 31, 26 out of 27 companies, representing 95.6% of total index weight, had reported Q4 2025 results.[11]

Among reporting companies, 20 firms (81.5% by weight) exceeded revenue expectations, while 6 firms (13.4% by weight) reported revenue misses. Revenue estimates were unavailable for one company (0.7% by weight).

Bottom-line results were equally supportive. 23 firms (90.4% by weight) reported EPS beats, compared with 2 firms (3.6% by weight) reporting misses, while two companies (1.6% by weight) lacked EPS estimates. 20 firms, representing 81.5% of index weight, exceeded expectations on both revenue and earnings.

[8] https://www.politico.eu/article/poland-investigates-iran-links-as-hackers-target-nuclear-facility/
[9] https://www.securityweek.com/iran-readied-cyberattack-capabilities-for-response-prior-to-epic-fury/
[10] https://www.securityweek.com/iran-linked-hackers-take-aim-at-us-and-other-targets-raising-risk-of-cyberattacks-during-war/
[11] Blackberry is expected to report Q42025 on April 9, 2026

On an aggregate basis, Q4 revenues increased 15.3% YoY, rising from $47.3bn to $52.2bn, while net income grew 27.0% YoY, from $10.0bn to $12.7bn, underscoring continued demand for cybersecurity solutions.



Source: Bloomberg. Data as of March 31, 2026