From Software Sell-Off to Cyber Rebound Amid Rising Geopolitical Risk

March 2026

Ilaria Sangalli, Head of Index Insights, EMEA

After a broad software sell-off in January and February that weighed on cybersecurity stocks, the sector rebounded in early March. Over the first nine days of March 2026, cybersecurity equities outperformed broader equity indices amid a recovery in investor sentiment.

This rebound has coincided with the sharp escalation of geopolitical tensions in the Middle East following the initial February 28 U.S.-Israel strikes on Iran, alongside renewed warnings from governments and leading cybersecurity firms about a heightened cyber-risk environment.

Geopolitical Tensions Raise the Risk of Spillover Cyber Activity

In a formal alert published on March 2, 2026, the UK's National Cyber Security Centre (NCSC) stated that while there was "no significant change in the direct cyber threat to the UK," there is "almost certainly a heightened risk of indirect cyber threat" for organizations with operations, assets, or supply chains in the Middle East. The agency emphasized that Iranian state and Iran-linked cyber actors retain the capability to conduct cyber activity and warned that fast-moving geopolitical conditions could rapidly alter the threat landscape.[1]

Similarly, CNBC reported that the U.S. Department of Homeland Security is working with federal intelligence and law enforcement partners to "closely monitor and thwart" potential threats, in the context of elevated Iran-linked cyber risk.[2]

Private-sector threat intelligence echoed these concerns. Zscaler's ThreatLabz reported on March 6 that threat actors are rapidly exploiting the volatile environment through opportunistic cybercrime, including the registration of more than 8,000 new domains using keywords associated with the Middle East conflict. While many remain inactive, they are assessed as potential infrastructure for future malicious campaigns. The report details multiple conflict-themed malware and phishing operations, including sites impersonating government or payment services to steal credentials and personal data. Zscaler emphasizes that these campaigns are financially motivated rather than ideological or state-directed, underscoring how quickly conflict narratives are weaponized for cybercrime.[3]

[1] https://www.ncsc.gov.uk/news/ncsc-advises-uk-organisations-take-action-following-conflict-in-middle-east
[2] https://www.cnbc.com/2026/03/03/iran-cisa-cybersecurity-war-threat.html
[3] https://www.zscaler.com/blogs/security-research/middle-east-conflict-fuels-opportunistic-cyber-attacks

Cisco's threat intelligence research organization Talos reported that it had not observed "significant" cyber impacts to date but noted early activity such as defacements and small-scale DDoS, and urged customers to reinforce basic hygiene including Multi-Factor Authentication (MFA), monitoring, and supply-chain awareness.[4]

Palo Alto Networks' Unit 42 similarly observed increased DDoS and hack-and-leak activity tied to Iran-aligned hacktivist groups. The firm noted that, given Iran's constrained internet connectivity, near-term activity is likely to remain low- to mid-level in sophistication, focused on disruption and signaling rather than advanced espionage.[5]

Cybersecurity Stocks Outperform as Geopolitical Tensions Drive a Risk-Off Rotation

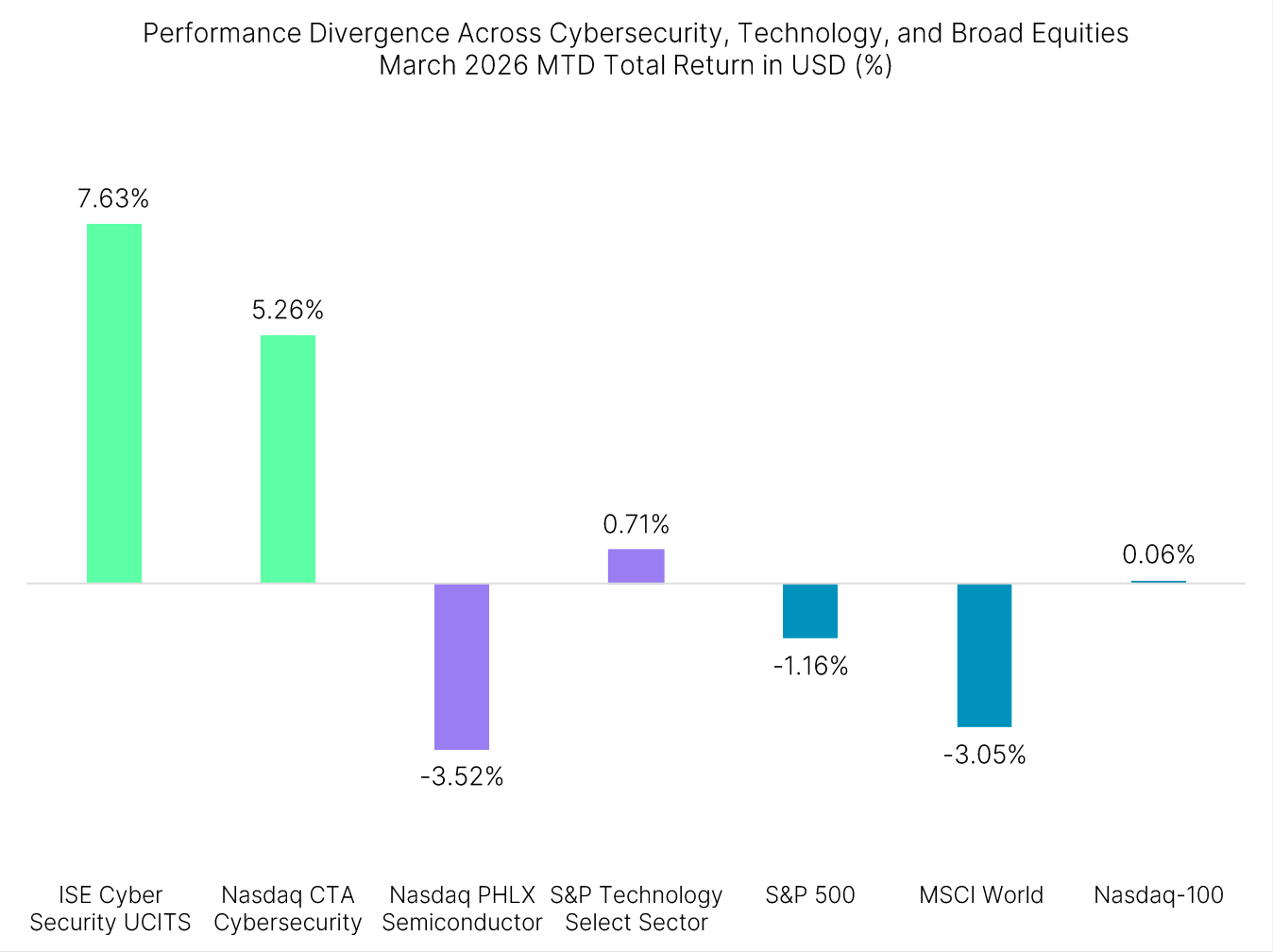
Against a backdrop of heightened cyber risk tied to rising geopolitical tensions, investors have rotated back into cybersecurity equities. In early March, the sector outperformed broader equity markets and other major tech segments, reflecting renewed interest in defense-oriented software and infrastructure amid growing concerns around digital resilience.

From February 27 to March 9, 2026, the Nasdaq CTA Cybersecurity™ Index (NQCYBR™) and the ISE Cyber Security UCITS™ Index (HUR™) gained 5.26% and 7.63%, respectively.

By contrast, performance across the rest of the technology sector was far more uneven. Semiconductor stocks declined, with the Nasdaq PHLX Semiconductor™ Index (SOX™) down 3.52%, compared with a modest gain in the S&P Technology Select Sector Index (+0.71%).

Broader equity indices remained under pressure over the same period, with the S&P 500 (SPX) declining 1.16% and MSCI World Index (MXWO) falling by 3.05%, while Nasdaq-100® (NDX®) was flat (0.06%).[6]

[4] https://blog.talosintelligence.com/talos-developing-situation-in-the-middle-east/
[5] https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[6] Source: Bloomberg. Total Return in USD. Performance from February 27 to March 9, 2026

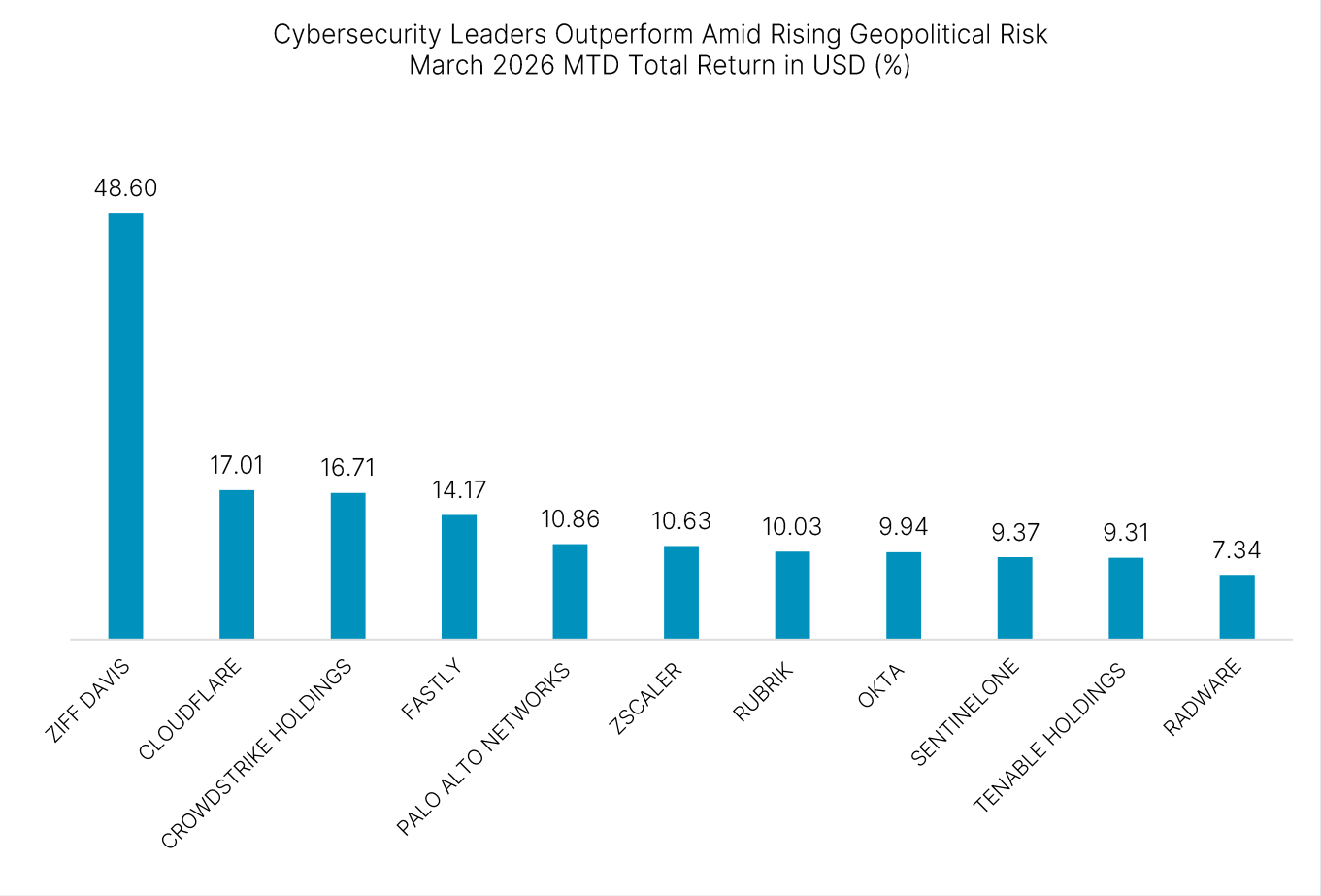


Source: Bloomberg. Data from February 27 to March 9, 2026

With the notable exception of Ziff Davis, whose outsized gains were driven by company-specific developments[7], cybersecurity stocks posted broadly positive gains ranging from high single digits to the mid-teens over the period.

Ziff Davis recorded total returns of 48.60%, followed by Cloudflare, CrowdStrike and Fastly, which rose 17.01%, 16.71% and 14.17%, respectively. More established security vendors such as Palo Alto Networks, Zscaler, Rubrik, and Okta posted solid high-single-digit to low-double-digit returns, broadly in the 9%-14% range.

[7] Ziff Davis disclosed that it had reached a definitive agreement to sell its Connectivity division to Accenture for $1.2 billion in cash on March 3, 2026, a move the company described as "transformative" and aimed at unlocking shareholder value. The announcement immediately triggered a sharp re-pricing of the stock. https://investor.ziffdavis.com/news/news-details/2026/Ziff-Davis-Announces-Definitive-Agreement-to-Sell-Connectivity-Division-to-Accenture/default.aspx



Source: Bloomberg. Data from February 27 to March 9, 2026

Overall, the early March rebound in cybersecurity equities underscores how quickly investor attention has refocused on digital defense as geopolitical risks escalate in a highly dynamic, still-evolving situation. Just in the past few days, news reports have begun identifying a possibly significant cyberattack originating in, or tied to Iran, against a large U.S. company, Stryker[8]. Even as observed activity remains largely opportunistic and limited in sophistication, the consistent cadence of government alerts and threat-intelligence updates has reinforced concerns around cyber resilience. Taken together, these dynamics continue to underscore the strategic importance of cybersecurity as a core layer of digital infrastructure in an increasingly complex risk environment.

The First Trust Nasdaq Cybersecurity UCITS ETF (CIBR) tracks NQCYBR. The L&G Cyber Security UCITS ETF (USPY) tracks HUR.

[8] https://www.nbcnews.com/world/iran/iran-appears-conducted-significant-cyberattack-us-company-first-war-st-rcna263084

Disclaimer: