ARTICLE BY AYESHA SHETTY

Why Cybersecurity

INDUSTRY / TECHNOLOGY | JUNE 8, 2026

Read Online

Cybersecurity has become one of the defining infrastructure layers of the digital economy. As businesses, governments, and financial systems become more connected, the scale of cyber risk has expanded alongside them creating sustained demand for technologies designed to secure data, networks, cloud environments, and digital operations.

That demand is being reinforced by several structural forces simultaneously: rising cybercrime costs, stricter regulatory standards, accelerating cloud adoption, and the growing use of artificial intelligence in both cyberattacks and cyber defence.

For investors, this has positioned cybersecurity as a sector closely tied to some of the most significant long-term trends shaping enterprise technology and digital infrastructure.

In our view, the Themes Cybersecurity ETF (SPAM) is designed to provide exposure to this landscape by tracking the Solactive Cybersecurity Index (SOCYBERN), which identifies 35 large-cap companies operating in digital security software.

By seeking exposure to companies across areas such as cloud security, identity protection, threat detection, and AI-enabled cybersecurity infrastructure, SPAM may allow investors to participate in the sector's evolving dynamics.

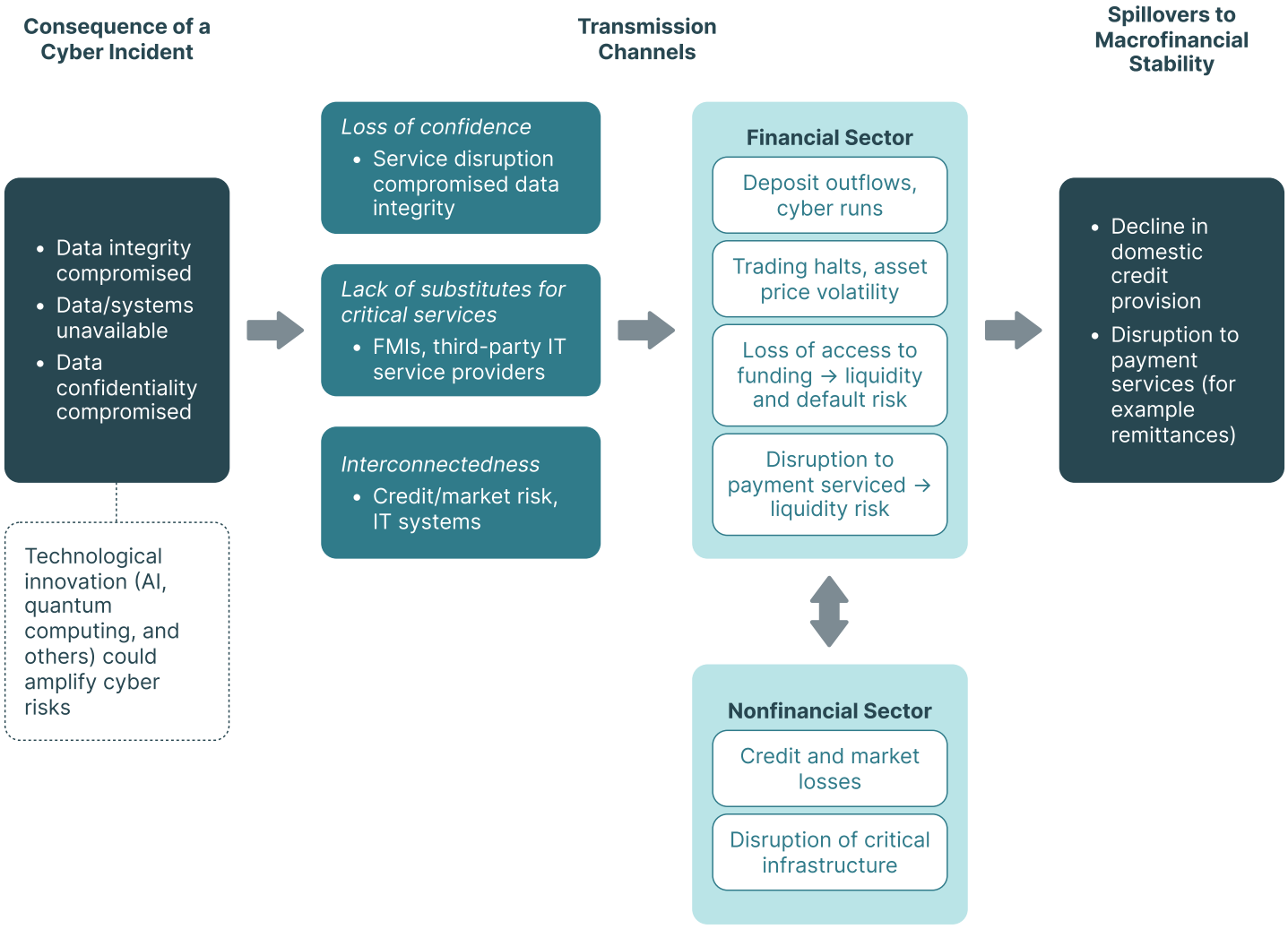
Key Takeaways

- Cybersecurity demand is increasingly being driven by structural factors including rising cybercrime costs, regulatory mandates, cloud adoption, and AI-enabled threat complexity rather than discretionary enterprise spending cycles.
- Artificial intelligence is simultaneously increasing cyber risk and strengthening defensive capabilities, reshaping competitive dynamics, capital allocation, and enterprise security priorities across the industry.

#1 The Cost of Cybercrime Is Now Systemic

The financial damage inflicted by cybercrime has reached a scale that makes it a systemic economic risk, not merely an operational inconvenience.

The IMF's Global Financial Stability Report 2024 has described the rising probability of severe cyber incidents as an acute threat to macrofinancial stability. Since 2020, the aggregated reported direct losses from cyber incidents have amounted to almost US$ 28 billion (in real terms), with billions of records stolen or compromised and nearly one-fifth of all reported incidents directly affecting financial firms.[1]



Source: IMF's Global Financial Stability Report, as of April 2024

In 2025, the FBI's Internet Crime Complaint Center (IC3) surpassed one million complaints for the first time in its 25-year history, receiving 1,008,597 reports of suspected internet crime with total losses of US$ 20.87 billion, a 26% increase from 2024.

Phishing and spoofing remained the top crime type by complaint volume, while investment fraud dominated by financial loss, with cryptocurrency-related investment scams alone accounting for US$7.2 billion of those losses. AI-enabled crimes generated over US$893 million in losses across more than 22,000 complaints, with investment scams the largest AI-linked category at US$632 million.[2]

At the organizational level, the global average cost of a data breach stood at US$ 4.44 million in 2025 based on a survey of 600 organizations across 17 industries and 16 countries.[3] Approximately 86% of breached organizations reported operational disruption, and 45% stated they would raise the price of goods or services to offset breach costs.[3]

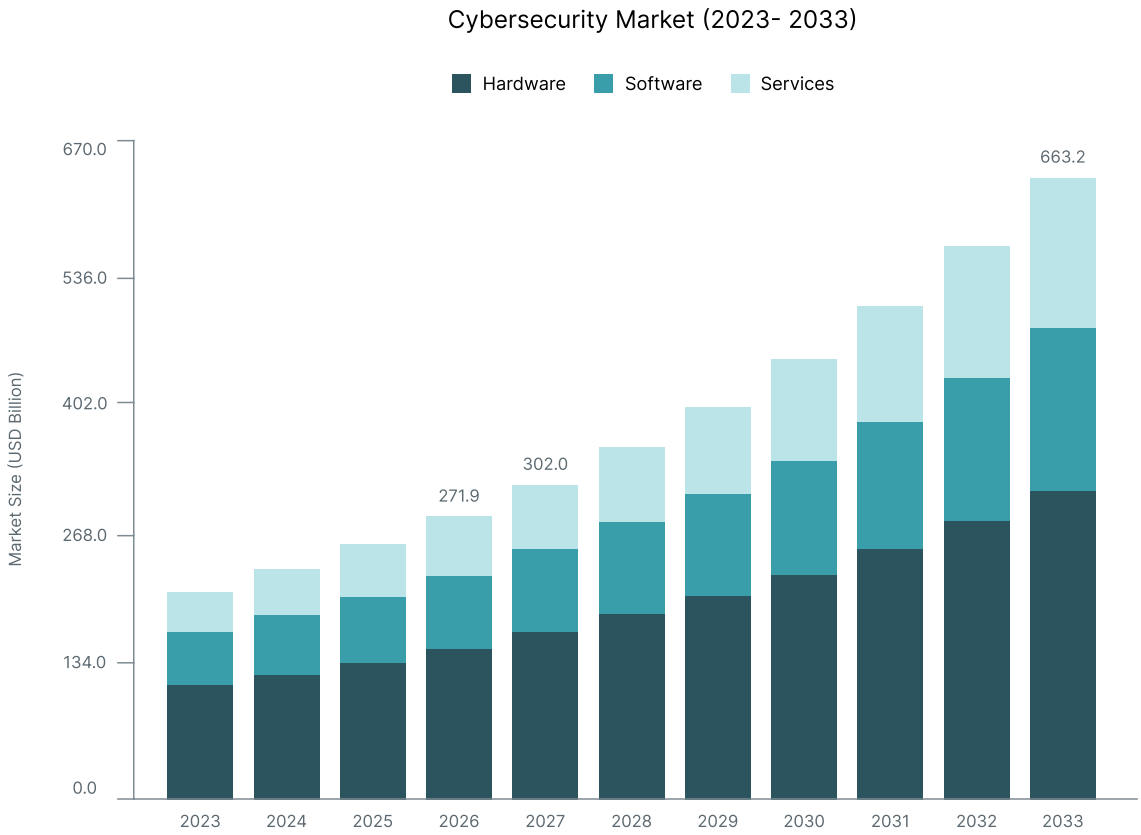
The consequences are not evenly distributed. Healthcare remained the costliest industry for breaches for the twelfth consecutive year, with average breach costs of US$ 7.42 million.[3]

The United States diverged sharply from the global trend: US breach costs surged 9% to a record US$ 10.22 million per incident, the highest figure ever recorded for any country in the study, driven by steeper regulatory penalties and rising detection and escalation costs.[3]

These figures establish a clear economic logic: when the cost of a single breach can exceed US$ 10 million, security investment becomes not a discretionary budget item but an economic necessity.

#2 A Market Expanding at Scale

The scale of the threat environment is being matched by the scale of the market. The global cybersecurity market was valued at US$ 271.9 billion in 2025 and is projected to reach US$ 302 billion in 2026 growing to US$ 663.2 billion by 2033 at a compound annual growth rate of 11.9%.[4]



Source: Grand View Research, as of 2026

This is expected to be on the back of rapid adoption of zero-trust architectures, AI/ML-powered threat detection, and extended detection and response (XDR) solutions, as organizations aim to proactively detect, prevent, and respond to increasingly complex cyberattacks.

Vendors are differentiating through features such as behavioral analytics, automated incident response, cloud-native security orchestration, and compliance management.

The spending base is broadening both geographically and structurally. North America accounted for the largest market share at 37.9% in 2025, driven by early adoption of zero-trust architectures, AI-powered threat detection, and identity and access management platforms.[4]

Asia Pacific is the fastest-growing region, as digitization accelerates across BFSI, healthcare, IT and telecommunications, and government sectors.[4]

Cloud-based deployments now represent 67.7% of the global cybersecurity market, reflecting the migration of enterprise workloads to hybrid and multi-cloud environments that introduce new categories of risk requiring dedicated security tooling.[4]

Among end-use segments, healthcare is forecast to register the fastest growth over the coming years, driven by the digitization of patient records, telehealth services, and connected medical devices, each expanding the attack surface that organizations must defend.[4]

#3 AI Is Reshaping Both the Threat and the Defense

Artificial intelligence has become central to the evolution of cybersecurity, functioning simultaneously as both a threat amplifier and a defensive capability. This dual role is accelerating investment across the sector and reshaping how enterprises approach digital security.

On the threat side, generative AI has fundamentally weakened the traditional assumptions underpinning security awareness. Phishing emails, impersonation attempts, and social engineering attacks were once often identifiable through poor grammar, unusual phrasing, or inconsistencies in identity. AI-generated content and deepfakes have significantly narrowed those signals, enabling attackers to produce highly convincing communications at scale.[5]

This shift is already influencing enterprise risk priorities. Some 66% of organizations expect AI to have a major impact on cybersecurity, yet only 37% currently have processes in place to assess the security of AI tools before deployment.[6]

Nearly half of global organizations now identify the malicious use of generative AI as their leading cybersecurity concern.[6] At the same time, attackers are increasingly deploying AI agents autonomously within attack chains - scanning for vulnerabilities, crafting tailored lures, and executing intrusions at machine speed and scale.[7]

On the defence side, AI and automation delivered measurable financial impact in 2025: organizations using these tools extensively contained breaches 80 days faster and incurred US$1.9 million less per breach, averaging US$ 3.62 million versus US$ 5.52 million for those without, a 34% cost reduction. [3]

#4 Capital Is Concentrating: M&A Activity Signals Sector Conviction

One of the most direct indicators of a maturing investment theme is the behaviour of sophisticated capital and by that measure, the cybersecurity sector is attracting sustained institutional and strategic attention at an accelerating pace.

Goldman Sachs Research observes that cybersecurity companies have honed a distinctive agility over time using M&A to continuously fill capability gaps and adapt to disruptive technologies demonstrating what durable competitive moats look like in a sector where existential threats have been a constant.[8]

The sector has attracted sustained strategic and financial buyer interest even as broader M&A activity has remained uneven, with large platform companies making transformative acquisitions to strengthen competitive position.[8]

This consolidation dynamic is visible in deal flow. In Q3 2025, Cybersecurity M&A volume rose 13% year-over-year, with 111 transactions recorded versus 98 in Q3 2024, and that momentum carried into Q4 as

improving financing conditions narrowed the bid-ask spread and pushed buyers toward larger, AI-ready assets.[9]

Strategic acquirers rather than financial sponsors drove the majority of this activity, accounting for approximately 60% of deal volume and nearly 80% of aggregate deal value, reflecting the platform-consolidation imperative that now defines the sector.[9]

The quarter's defining transaction, Google's US$ 32 billion acquisition of Wiz validated agentless cloud-native application protection platforms at hyperscale and set a valuation benchmark that reverberated across the sector. Veeam's US$ 1.725 billion acquisition of Securiti AI and Dataminr's US$ 290 million acquisition of ThreatConnect further illustrated that strategics are prepared to pay meaningful premiums.[9]

In early 2026, OpenAI acquired Promptfoo, signalling that the largest AI companies now view cybersecurity as a core rather than adjacent capability.[10]

For investors, this combination of structurally elevated threat levels and institutional capital drawn to the sector's durable growth profile represents a solid opportunity in the technology landscape.

#5 Regulation Is Creating a Structural Spending Floor

For investors, one of the most compelling characteristics of a sector is demand that cannot be deferred. Cybersecurity is increasingly in that category not because organizations choose to prioritize it, but because regulation is making investment mandatory.

Across major economies, governments have moved decisively to establish minimum cybersecurity standards, creating layers of non-discretionary demand that are structurally independent of macro cycles or IT budget pressures.

In the European Union, the NIS2 Directive, which broadens mandatory cybersecurity obligations across critical sectors including energy, healthcare, transport, banking, and digital infrastructure, has been in national force since October 2024, with full compliance required by October 2026.[11]

The Digital Operational Resilience Act (DORA), which mandates ICT risk management, resilience testing, and incident reporting across all EU financial entities including banks, insurers, investment firms, and fintechs, has been fully applicable since January 2025.[12]

The Cyber Resilience Act, covering manufacturers of digital products, adds further obligations from 2027.[13]

In the United States, SEC cybersecurity disclosure rules require public companies to report material incidents within four business days and to disclose their cybersecurity risk management frameworks annually.[14]

Gartner identifies increasing regulatory pressure as one of the three primary structural drivers of sustained cybersecurity spending growth alongside rising threats and AI proliferation.[7]

The financial consequences of non-compliance reinforce the spending imperative. NIS2 authorizes penalties of up to €10 million or 2% of global annual turnover for essential entities.15 DORA carries fines of up to 2% of total annual worldwide turnover for the most serious violations, with periodic penalty payments to compel compliance.[16]

For organizations operating across multiple jurisdictions, the compliance surface is expanding continuously: each new framework creates fresh demand for governance, risk management, identity, incident response, and audit tooling.

The investment significance is direct. Unlike enterprise software that competes for discretionary budget, cybersecurity in regulated industries now carries a legal floor. Providers serving financial services, healthcare, critical infrastructure, and government face customers whose minimum security investment is effectively set by statute.

How to Play It

The Themes Cybersecurity ETF (SPAM) seeks to track the Solactive Cybersecurity Index (SOCYBERN), which identifies the largest 35 companies by market capitalization in digital security software.

SPAM seeks to provide investment results that correspond generally to the price and yield performance, before fees and expenses, of the SOCYBERN Index.

Fund Facts

Expense Ratio	Strategy	Index	Holdings
0.35%	Passive	Solactive Cyber Security Index	36

Holdings subject to change.

Conclusion

The structural case for cybersecurity as an investment theme rests on a characteristic that is rare in enterprise technology: demand that is not meaningfully exposed to discretionary spending cycles. It does not pause in a downturn, compress in a rising rate environment, or reverse with a shift in technology preference.

For investors evaluating thematic allocations, this distinction matters. Cybersecurity demand is anchored in the threat environment, in compliance obligations that are binding rather than advisory, and in the irreversible expansion of the digital infrastructure that organizations must protect.

At the same time, the sector continues to evolve rapidly. Artificial intelligence is changing both the nature of cyber threats and the tools designed to defend against them. Regulatory frameworks are expanding across jurisdictions, while consolidation activity reflects an industry still defining its long-term competitive structure. The result is a market shaped not by a single catalyst, but by multiple structural forces operating simultaneously.

How investors interpret that combination of risk, regulation, technological change, and long-duration demand will ultimately determine the role cybersecurity occupies within broader portfolio strategy.

For more information about the fund, including fees/expenses, holdings, standardized performance, risks and more, please visit https://themesetfs.com/etfs/spam

Footnotes:

[1]IMF, Global Financial Stability Report, April 2024, as of April 2024

[2]FBI Internet Crime Complaint Center, 2025 Internet Crime Report, as of April 2026

[3]IBM, Cost of a Data Breach Report 2025: The AI Oversight Gap, as of 2025

[4]Grand View Research, Cybersecurity Market Size, Share & Trends Analysis Report, 2026–2033, as of 2026

[5]World Economic Forum, Cybersecurity Awareness: AI Threats and Cybercrime in 2025, as of September 30, 2025

[6]World Economic Forum, Global Cybersecurity Outlook 2025, as of January 2025

[7]Gartner, Top Cybersecurity Trends for 2026, as of February 5, 2026

[8]Goldman Sachs Research, Cybersecurity Firms Show Software Industry How to Navigate AI, as of April 23, 2026

[9]Windsor Drake, Cybersecurity Valuation Report: Q4 2025

[10]Open AI, OpenAI to acquire Promptfoo, as of March 9, 2026

[11]European Commission, NIS2 Directive: Securing Network and Information Systems, last updated January 20, 2026

[12]European Commission, Cyber Resilience Act, last updated December 3, 2025

[13]IBM, What Is the Digital Operational Resilience Act (DORA)?

[14]U.S. Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Final Rule, Release No. 33-11216), effective September 5, 2023

[15]NIS2 Directive, NIS2 Fines

[16]DORA Regulation EU, DORA Penalties and Fines 2026, as of November 20, 2025

Disclosure

ALPS Distributors, Inc. (1290 Broadway, Suite 1000, Denver, Colorado 80203) is the distributor for the Themes ETFs Trust.

An investor should carefully consider a Fund's investment objective, risks, charges, and expenses before investing. A Fund's prospectus and summary prospectus contain this and other information about Themes ETFs. To obtain a Fund's prospectus and summary prospectus call 886-584-3637 or visit themesetfs.com. A Fund's prospectus and summary prospectus should be read carefully before investing.

Investing involves risk, including the possible loss of principal. Cybersecurity Companies are subject to risks associated with additional regulatory oversight with regard to privacy/cybersecurity concerns. Declining or fluctuating subscription renewal rates for products/services or the loss or impairment of intellectual property rights could adversely affect profits. The investable universe of companies in which SPAM may invest may be limited. The Fund invests in securities of companies engaged in Information Technology, which can be affected by rapid product obsolescence and intense industry competition. International investments may involve risk of capital loss from unfavorable fluctuation in currency values, from differences in generally accepted accounting principles or from social, economic or political instability in other nations. SPAM is non-diversified.

Shares of ETFs are bought and sold at market price (not NAV) and are not individually redeemed from the Fund. Brokerage commissions will reduce returns. The market price returns are based on the official closing price of an ETF share or, if the official closing price isn't available, the midpoint between the national best bid and national best offer ("NBBO") as of the time the ETF calculates current NAV per share, and do not represent the returns you would receive if you traded shares at other times. NAVs are calculated using prices as of 4:00 PM Eastern Time. Indices are unmanaged and do not include the effect of fees, expenses, or sales charges. One cannot invest directly in an index.

Themes Management Company LLC serves as an adviser to the Themes ETFs Trust. The funds are distributed by ALPS Distributors, Inc (1290 Broadway, Suite 1000, Denver, Colorado 80203). ALPS is not affiliated with any mentioned entity. Client brokerage services not offered by ALPS. Please see third part site for more information about any mentioned services. Solactive, STOXX and BITA have been licensed by Solactive AG, ISS STOXX, and BITA Gmbh, respectively, for use by Themes Management Company LLC. Themes ETFs are not sponsored, endorsed, issued, sold, or promoted by these entities, nor do these entities make any representations regarding the advisability of investing in the Themes ETFs. Neither ALPS Distributors, Inc, Themes Management Company LLC nor Themes ETFs are affiliated with these entities.