Author:

Ryan O. Issakainen, CFA
Senior Vice President
ETF Strategist
First Trust Advisors L.P.

Co-authors:

Andrew Hull, CFA
Vice President
ETF Strategist
First Trust Advisors L.P.

Roberto Fatta
Associate ETF Strategist
First Trust Advisors L.P.

Will Demand for Cybersecurity Be Strengthened or Disintermediated by AI?

The rapid emergence of powerful artificial intelligence (AI) coding agents in the first quarter of 2026 sent shockwaves through the software industry. Investors suddenly found themselves confronting two pressing questions: if AI coding tools enable companies to cost-effectively build and maintain their own internal software, will they begin abandoning Software-as-a-Service (SaaS) subscriptions? And if AI dramatically boosts employee productivity, will organizations need fewer software licenses, ultimately compressing recurring revenue streams?

In our view, these questions are valid. But when it comes to cybersecurity, the implications are far less straightforward—and potentially more constructive—than they appear at first blush. In fact, we believe several key dynamics unleashed by AI are more likely to bolster demand for cybersecurity solutions than disintermediate the industry. Below, we explore these dynamics and assess their implications for the First Trust Nasdaq Cybersecurity ETF (CIBR).

The Rise of Vibe Coding May Increase Demand For Cybersecurity

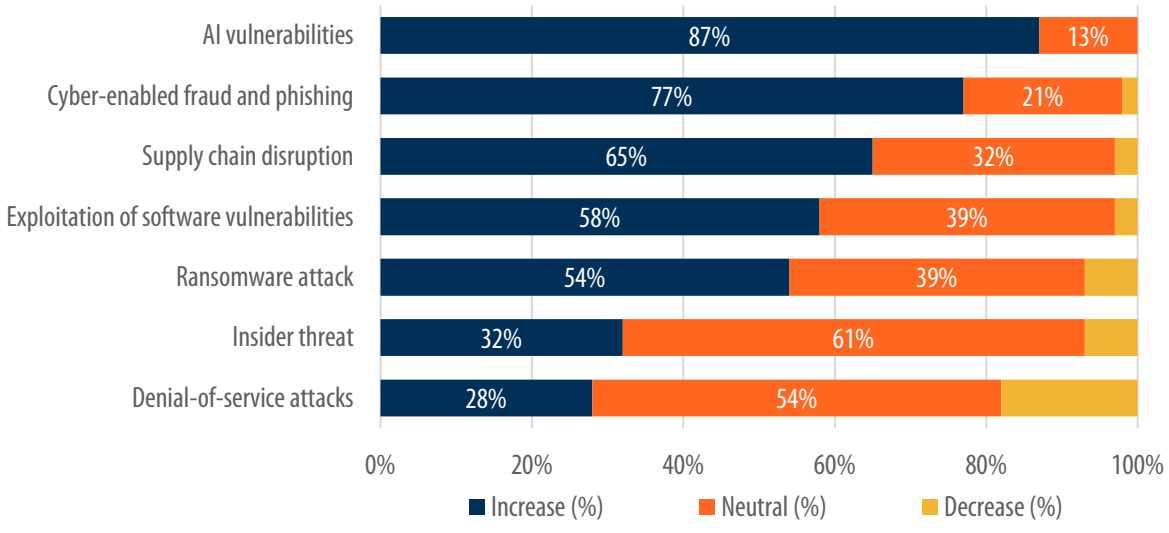
The term "vibe coding" recently entered the mainstream, referring to the practice of using AI tools to create new software applications via natural-language prompts with little or no traditional computer programming skills. Tools like Anthropic's Claude Code, OpenAI's Codex, and other emerging agentic platforms enable non-technical users to quickly generate working software solutions. This capability has understandably alarmed many software investors. If enterprises can cost-effectively build and maintain customized internal tools, why continue paying for SaaS subscriptions? For many software companies, we also see this as a legitimate concern.

However, for the cybersecurity industry, vibe coding could prove to be a powerful tailwind rather than a headwind, in our view. By emphasizing speed and functionality, vibe coded software may work quite well, but contain serious vulnerabilities. According to Veracode's 2025 GenAI Code Security Report, 45% of AI-generated code samples failed security tests and introduced OWASP Top 10 security vulnerabilities into the code.[1] Another study that tested applications built on leading vibe coding platforms found several critical vulnerabilities, including authentication bypass, broken access control, and exposed personal data, even when the platforms' own scanners reported the applications as clean.[2]

In our view, the proliferation of vibe coded applications may meaningfully expand the attack surface that enterprises must defend. Every new vibe coded application built without a formal security review creates a potential entry point for hackers. Hence, we think the rise of vibe coding may accelerate rather than diminish cybersecurity demand, as organizations need stronger application security testing (AST), runtime protection, and continuous monitoring to manage this risk.

Chart 1: Cyber Threats Are Perceived To Be Increasing

"In the past year, do you think the following cyber risks have increased, decreased or stayed the same?"



Source: World Economic Forum, "Global Cybersecurity Outlook 2026" January 2026. The World Economic Forum received responses from 873 survey participants including C-suite executives, academics, civil society and public-sector cybersecurity leaders from 99 countries.

[1]Veracode, July 2025. The OWASP Top 10 is a standard awareness document for developers and web application security representing a broad consensus about the most critical security risks to web applications.

[2]Bright Security, "Vibe Coding Security Analysis," November 2025.

Competitive Moats for Cybersecurity

As investors consider the disruptive potential of AI among software providers, some have questioned whether the cybersecurity industry enjoys greater insulation. The February 2026 launch of Anthropic's Claude Code Security—a tool designed to scan software code for vulnerabilities and recommend patches—triggered a sharp selloff in several cybersecurity stocks. Investors worried that advanced AI could eventually compete directly with established cybersecurity solutions, particularly in code-level vulnerability detection.

However, while many have acknowledged that this tool represents a meaningful advance in automated code analysis, it addresses only a narrow slice of the broader cybersecurity market. Claude Code Security does not monitor live networks or endpoints, protect organizational data and systems in real time, defend against active cyberattacks, or serve as a comprehensive operations platform.

In our view, the cybersecurity industry has several competitive moats that suggest AI is more likely to augment rather than replace established cybersecurity companies.

- *High reliability requirements:* Organizations have near-zero tolerance for cybersecurity failures, and the cost of even rare mistakes can be catastrophic. Unlike traditional deterministic software, which produces consistent outputs from the same inputs, modern AI systems are inherently probabilistic. They infer responses based on patterns in training data, and even high-quality models can generate variable or incorrect results from identical prompts. A 99.999% success rate may suffice in many domains, but in cybersecurity, that 0.001% failure rate could enable a breach with outsized financial, operational, and reputational damage.
- *Proprietary data:* Leading cybersecurity companies have vast proprietary datasets on security events, which have been collected from years of defending real-world environments. In our opinion, the compounding of this data creates formidable data moats that generic AI models cannot easily replicate.
- *Network effects:* Network effects further amplify this edge, as data from customers around the world can be used to improve detection models in real time. For example, CrowdStrike's Threat Graph processes trillions of security events daily across its global customer base, continuously refining detection models, based on actual attack patterns observed in the wild.[3]
- *Regulatory entrenchment:* Cybersecurity platforms function as systems of record for enterprise risk. They generate immutable audit trails, compliance documentation, and incident histories that regulators and auditors routinely demand. Strict regulatory requirements, such as HIPAA in the US or the General Data Protection Regulation (GDPR) in the EU, create powerful incentives for sustained investment in proven solutions. Migrating away from incumbent cybersecurity platforms is rarely a simple technical exercise and can expose organizations to significant fines for noncompliance and lengthy re-certification timeframes.

Will AI Disrupt Seat-Based Software Licenses?

Another major concern that has emerged for software investors is that AI-driven productivity gains could lead employers to reduce headcounts, thereby reducing demand for seat-based software licenses. If fewer employees need access to these tools, the argument goes, recurring revenue from per-user pricing models could come under pressure, particularly in categories such as CRM, collaboration platforms, and other headcount-linked SaaS applications.

While we view this as a valid risk for certain segments of the software industry, we believe the dynamics look markedly different for cybersecurity. Unlike many enterprise applications, cybersecurity spending does not primarily scale with the number of employees at an organization, but rather with the size and complexity of the digital attack surface being defended. For many organizations, that surface now includes an expanding number of endpoints, cloud workloads, containers, data repositories, APIs, and interconnected networks. Even in a scenario of modest workforce reductions, the volume of assets requiring protection continues to grow.

The rise of agentic AI further amplifies this divergence. As organizations increase their use of autonomous AI agents, or digital "workers" that can act and make decisions independently, the number of entities needing security oversight grows rapidly. These agents introduce new identities, behavioral patterns, API interactions, and potential vectors for compromise.

Do Historically Cheap Relative Valuations Represent an Opportunity?

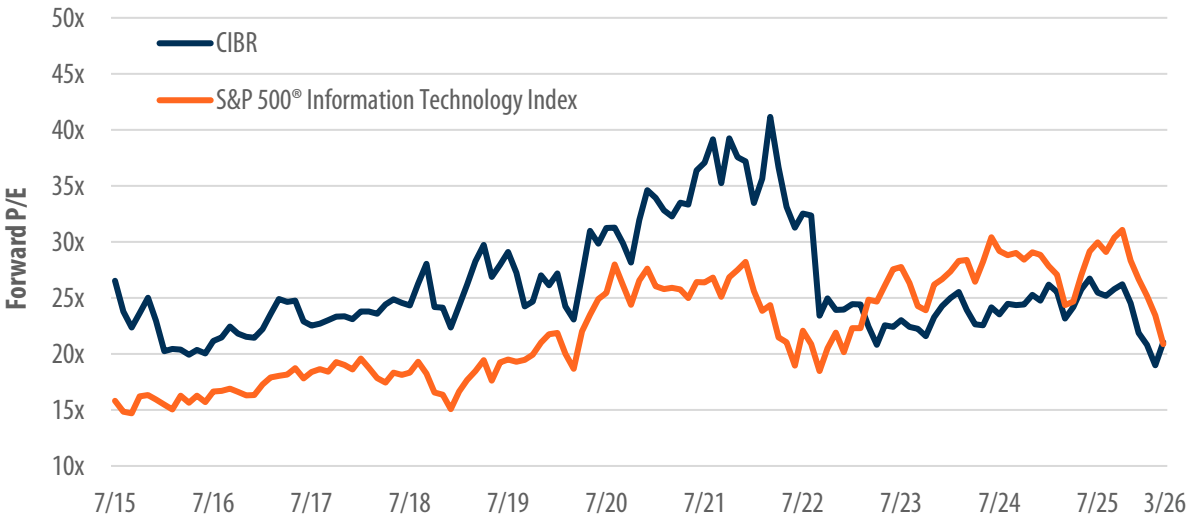
The First Trust Nasdaq Cybersecurity ETF (CIBR) includes companies primarily involved in the building, implementation, and management of security protocols applied to private and public networks, computers, and mobile devices in order to provide protection of the integrity of data and network operations.

As AI disintermediation fears led to a selloff in software stocks in recent months, CIBR meaningfully outperformed. During the first quarter, the S&P 500® Software Industry Index declined by 23.7%, while CIBR fell by 12.1%.

(continued on next page)

[3]Crowdstrike.

Chart 2: CIBR vs S&P 500® Information Technology Index Forward P/E



Sources: Bloomberg and FactSet, based on monthly data from 31/7/2015-31/3/2026. **Forward Price-to-Earnings (P/E)** is the price of a stock divided by the forecasted earnings per share of the company over the next 12 months. There is no assurance past trends will continue or forecasts will be achieved.

Despite a modest rebound in cybersecurity stocks more recently, we view today's valuations as attractive. CIBR currently trades at a 12-month forward P/E ratio of 21.1x, a slight premium to the S&P 500® Information Technology Index, and one of the lowest forward multiples in years. Since inception, CIBR has traded at an average premium of 21% to the S&P 500® Information Technology Index, compared to a premium of only 1% today.

More volatility may emerge in the months ahead, but as the dust settles, we believe cybersecurity firms may be less susceptible to AI disruption. If we're correct, CIBR may benefit from a rare setup in which long-term demand is strengthened by the very forces that threaten its peers, creating intriguing entry points as valuations are dragged down by association with a broader software correction.

CIBR Performance Summary (%) as of 31/3/2026

Fund Performance*	3 Month	1 Year	5 Year	10 Year	Since Fund Inception
Net Asset Value (NAV)	-12.10	0.01	8.97	14.50	11.85
Market Price	-12.02	0.12	8.95	14.52	11.86
Index Performance**					
Nasdaq CTA Cybersecurity™ Index	-12.13	0.31	9.59	15.24	12.59
S&P Composite 1500® Information Technology Index	-8.61	29.68	17.81	22.48	21.51
S&P 500® Index	-4.33	17.80	12.06	14.16	13.26

Performance data quoted represents past performance. Past performance is not a guarantee of future results and current performance may be higher or lower than performance quoted. Investment returns and principal value will fluctuate and shares when sold or redeemed, may be worth more or less than their original cost. You can obtain performance information which is current through the most recent month-end by visiting www.ftportfolios.jp.

Fund Inception: 6/7/2015. Total Expense Ratio: 0.58%. The Investment Advisor has implemented fee breakpoints, which reduce the fund's investment management fee at certain assets levels. Please see the fund's Statement of Additional Information for full details.

*__NAV__ returns are based on the fund's net asset value which represents the fund's net assets (assets less liabilities) divided by the fund's outstanding shares. **Market Price** returns are determined by using the midpoint of the national best bid offer price ("NBBO") as of the time that the fund's NAV is calculated. Returns are average annualized total returns, except those for periods of less than one year, which are cumulative.

**Performance information for each listed index is for illustrative purposes only and does not represent actual fund performance. Indexes do not charge management fees or brokerage expenses, and no such fees or expenses were deducted from the performance shown. Indexes are unmanaged and an investor cannot invest directly in an index.

You should consider the fund's investment objectives, risks, and charges and expenses carefully before investing. Contact First Trust Japan at www.ftportfolios.jp to obtain a prospectus which contains this and other information about the fund. The prospectus should be read carefully before investing.

Risk Considerations

You could lose money by investing in a fund. An investment in a fund is not a deposit of a bank and is not insured or guaranteed. There can be no assurance that a fund's objective(s) will be achieved. Investors buying or selling shares on the secondary market may incur customary brokerage commissions. Please refer to each fund's prospectus and Statement of Additional Information for additional details on a fund's risks. The order of the below risk factors does not indicate the significance of any particular risk factor.

Unlike mutual funds, shares of the fund may only be redeemed directly from a fund by authorized participants in very large creation/redemption units. If a fund's authorized participants are unable to proceed with creation/redemption orders and no other authorized participant is able to step forward to create or redeem, fund shares may trade at a premium or discount to a fund's net asset value and possibly face delisting and the bid/ask spread may widen.

Changes in currency exchange rates and the relative value of non-US currencies may affect the value of a fund's investments and the value of a fund's shares.

Current market conditions risk is the risk that a particular investment, or shares of the fund in general, may fall in value due to current market conditions. For example, changes in governmental fiscal and regulatory policies, disruptions to banking and real estate markets, actual and threatened international armed conflicts and hostilities, and public health crises, among other significant events, could have a material impact on the value of the fund's investments.

A fund is susceptible to operational risks through breaches in cyber security. Such events could cause a fund to incur regulatory penalties, reputational damage, additional compliance costs associated with corrective measures and/or financial loss.

Information technology companies and cyber security companies are generally subject to the risks of rapidly changing technologies, short product life cycles, fierce competition, aggressive pricing and reduced profit margins, loss of patent, copyright and trademark protections, cyclical market patterns, evolving industry standards and frequent new product introductions. Cyber security companies may also be smaller and less experienced companies, with limited product lines, markets, qualified personnel or financial resources.

Depositary receipts may be less liquid than the underlying shares in their primary trading market and distributions may be subject to a fee. Holders may have limited voting rights, and investment restrictions in certain countries may adversely impact their value.

Equity securities may decline significantly in price over short or extended periods of time, and such declines may occur in the equity market as a whole, or they may occur in only a particular country, company, industry or sector of the market.

An index fund will be concentrated in an industry or a group of industries to the extent that the index is so concentrated. A fund with significant exposure to a single asset class, or the securities of issuers within the same country, state, region, industry, or sector may have its value more affected by an adverse economic, business or political development than a broadly diversified fund.

A fund may be a constituent of one or more indices or models which could greatly affect a fund's trading activity, size and volatility.

There is no assurance that the index provider or its agents will compile or maintain the index accurately. Losses or costs associated with any index provider errors generally will be borne by a fund and its shareholders.

Information technology companies are subject to certain risks, including rapidly changing technologies, short product life cycles, fierce competition, aggressive pricing and reduced profit margins, loss of patent, copyright and trademark protections, cyclical market patterns, evolving industry standards and regulation and frequent new product introductions.

A fund that holds securities that traded on non-U.S. exchanges that are closed when the fund's primary exchange is open, will likely experience deviations between the current price of a security and the last quoted foreign price from the closed foreign market. This can result in wider premiums or discounts to a fund's net asset value. Additionally, investors may be unable to trade fund shares on days when events in foreign markets could materially affect a fund's value.

Large capitalization companies may grow at a slower rate than the overall market.

Certain fund investments may be subject to restrictions on resale, trade over-the-counter or in limited volume, or lack an active trading market. Illiquid securities may trade at a discount and may be subject to wide fluctuations in market value.

Market risk is the risk that a particular security, or shares of a fund in general may fall in value. Securities are subject to market fluctuations caused by such factors as general economic conditions, political events, regulatory or market developments, changes in interest rates and perceived trends in securities prices. Shares of a fund could decline in value or underperform other investments as a result. In addition, local, regional or global events such as war, acts of terrorism, spread of infectious disease or other public health issues, recessions, natural disasters or other events could have significant negative impact on a fund.

A fund faces numerous market trading risks, including the potential lack of an active market for fund shares due to a limited number of market makers. Decisions by market makers or authorized participants to reduce their role or step away in times of market stress could inhibit the effectiveness of the arbitrage process in maintaining the relationship between the underlying values of a fund's portfolio securities and a fund's market price.

An index fund's return may not match the return of the index for a number of reasons including operating expenses, costs of buying and selling securities to reflect changes in the index, and the fact that a fund's portfolio holdings may not exactly replicate the index.

A fund classified as "non-diversified" may invest a relatively high percentage of its assets in a limited number of issuers. As a result, a fund may be more susceptible to a single adverse economic or regulatory occurrence affecting one or more of these issuers, experience increased volatility and be highly concentrated in certain issuers.

Securities of non-U.S. issuers are subject to additional risks, including currency fluctuations, political risks, withholding, lack of liquidity, lack of adequate financial information, and exchange control restrictions impacting non-U.S. issuers.

A fund and a fund's advisor may seek to reduce various operational risks through controls and procedures, but it is not possible to completely protect against such risks. The fund also relies on third parties for a range of services, including custody, and any delay or failure related to those services may affect the fund's ability to meet its objective.

A fund that invests in securities included in or representative of an index will hold those securities regardless of investment merit and the fund generally will not take defensive positions in declining markets.

High portfolio turnover may result in higher levels of transaction costs and may generate greater tax liabilities for shareholders.

The market price of a fund's shares will generally fluctuate in accordance with changes in the fund's net asset value ("NAV") as well as the relative supply of and demand for shares on the exchange, and a fund's investment advisor cannot predict whether shares will trade below, at or above their NAV.

Securities of small- and mid-capitalization companies may experience greater price volatility and be less liquid than larger, more established companies.

Trading on an exchange may be halted due to market conditions or other reasons. There can be no assurance that a fund's requirements to maintain the exchange listing will continue to be met or be unchanged.

A fund may hold securities or other assets that may be valued on the basis of factors other than market quotations. This may occur because the asset or security does not trade on a centralized exchange, or in times of market turmoil or reduced liquidity. Portfolio holdings that are valued using techniques other than market quotations, including "fair valued" assets or securities, may be subject to greater fluctuation in their valuations from one day to the next than if market quotations were used. There is no assurance that a fund could sell or close out a portfolio position for the value established for it at any time.

First Trust Advisors L.P. is the adviser to the fund. First Trust Advisors L.P. is an affiliate of First Trust Portfolios L.P., the fund's distributor. First Trust Japan is the fund's sub-distributor.

The information presented is not intended to constitute an investment recommendation for, or advice to, any specific person. Nor does the document implicitly or explicitly recommend or suggest an investment strategy, reach conclusions in relation to an investment strategy for the reader or provide an opinion as to the present or future value or price of any fund. First Trust has no knowledge of and has not been provided any information regarding any investor. Financial professionals must determine whether particular investments are appropriate for their clients.

Nasdaq® and Nasdaq CTA Cybersecurity™ Index ("NQCYBRT™") are registered trademarks and service marks of Nasdaq, Inc. (together with its affiliates hereinafter referred to as the "Corporations") and are licensed for use by First Trust. The Fund has not been passed on by the Corporations as to its legality or suitability. The Fund is not issued, endorsed, sold or promoted by the Corporations. THE CORPORATIONS MAKE NO WARRANTIES AND BEAR NO LIABILITY WITH RESPECT TO THE FUND.

Definitions

S&P 500® Index is an unmanaged index of 500 companies used to measure large-cap U.S. stock market performance.

S&P 500® Information Technology Index is an unmanaged index which includes the stocks in the information technology sector of the S&P 500® Index.

S&P Composite 1500® Information Technology Index is a capitalization-weighted index of companies classified by GICS as information technology within the S&P Composite 1500® Index.

S&P 500® Software Industry Index includes companies in the S&P 500® Index classified in the Global Industry Classification Standard® (GICS) Level 3 Software industry.