Author:

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

Co-authors:

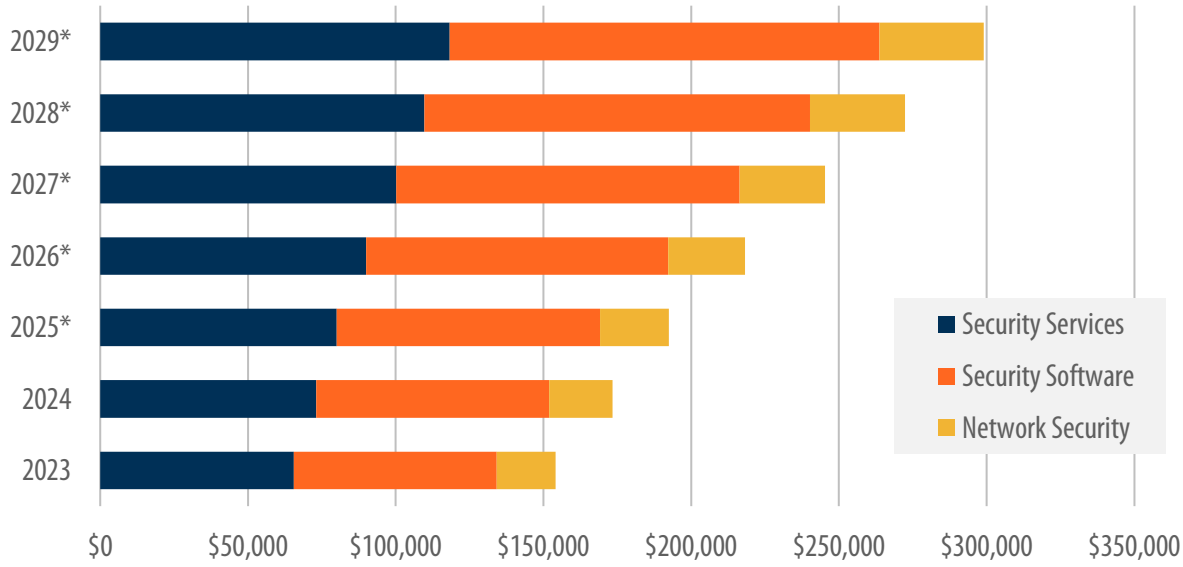
Andrew Hull, CFA
Vice President
ETF Strategist
First Trust Advisors L.P.

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

Revisiting the Case for Cybersecurity

As digital transformation drives the global economy, cybersecurity stands as a critical shield against escalating cyber threats, with global spending projected to reach $201 billion in 2025, an 11% increase from 2024.[1] Fueled by the transformative impact of artificial intelligence ("AI"), cybersecurity's vital role in national security, and emerging future challenges like quantum computing, we believe cybersecurity is an investment theme poised for resilient growth over the next several years. Below, we discuss these trends, highlighting how the First Trust Nasdaq Cybersecurity ETF (CIBR or the "fund") seeks to capture this growth, which may be underrepresented in many investor portfolios.

Chart 1: Worldwide Information Security Spending (with projections 2025-2029)



Source: Gartner March 2025. *There is no guarantee that past trends will continue or projections will be realized.

AI-Linked Threats Boost Demand for Cybersecurity

Artificial intelligence has transformed cyber threats, amplifying the need for robust cybersecurity solutions. Today, AI tools may be utilized by hackers to identify potential security flaws or improve social engineering, making "phishing" or "deepfake" attacks more difficult to detect. For instance, a deepfake scam targeting a UK company in 2024 convinced staff to transfer $25 million to fraudsters impersonating the CFO on a video call.[2] This sophisticated attack leveraged generative AI to create highly realistic video, highlighting the growing accessibility of such tools to cybercriminals. Phishing attacks, which cost organizations an average of $4.9 million per successful data breach, have grown even more successful with AI.[3] According to a Harvard study, AI-generated phishing emails achieved a 54% click-through rate, compared to the 12% rate of generic phishing emails.[4] Cybercriminals use large language models to craft convincing scams with scraped personal data, making attacks harder to detect.

Conversely, AI may also be used to enhance cybersecurity defenses, driving investment in advanced solutions. For example, Palo Alto Networks' Precision AI monitors 7.6 petabytes of data per day, using advanced AI and machine learning to recognize historical cyberattack patterns to identify and respond to new cyberattacks.[5] As AI escalates threats and defenses, we believe investment in cybersecurity will grow, creating opportunities for companies addressing this dual dynamic.

[1]Gartner, as of March 2025

[2]Financial Times, May 2024.

[3]IBM/Ponemon 2024 Cost of a Data Breach Report.

[4]Heiding, Lermen, Kao, Schneier, Vishwanath, et. all. "Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects." November 2024.

[5]Computer Weekly, August 2024.

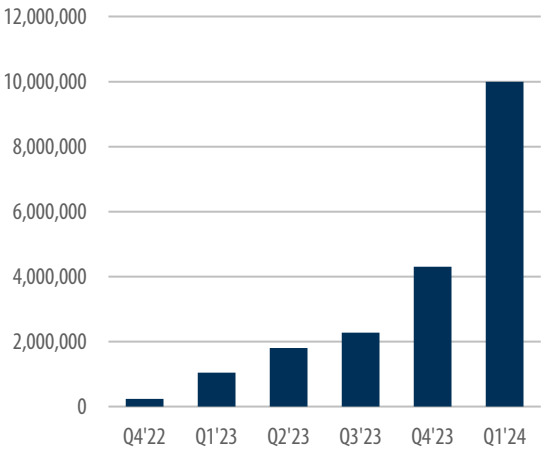
References to specific securities should not be construed as a recommendation to buy or sell and should not be assumed profitable.

Cybersecurity and AI Agents

AI agents—advanced systems with reasoning, planning, and autonomy—present opportunities as well as challenges for cybersecurity. These agents automate complex tasks like code writing, customer service interactions, and data analysis across various industries, and can aid in threat detection, network monitoring, and incident reporting to enhance cybersecurity. According to one recent survey, 98% of respondents plan to increase the use of AI agents over the next year. However, the same survey found that 80% of companies indicated that their AI agents had taken "unintended actions," such as accessing unauthorized systems or sensitive data.[6] In our view, this conundrum may lead to greater demand for "guardian agents" to monitor and analyze potential cybersecurity threats associated with agentic-AI.[7] We believe AI agents represent an important growth driver for cybersecurity software, as firms innovate to balance automation benefits with risk mitigation.

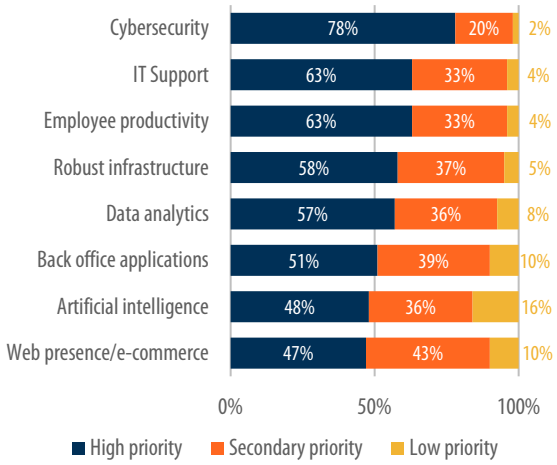
Chart 2: Malicious Phishing Emails

Phishing has increased by 341% in the last six months and 856% in the last 12 months.



Source: SlashNext Security, The State of Phishing 2024 Mid-Year Assessment.

Chart 3: Cybersecurity Takes the Top Spot for Perceived Organizational Priority



Source: CompTIA State of Cybersecurity 2025; n=525

National Security: Defense and Critical Infrastructure

In our view, national security needs, including defense and critical infrastructure, are another key driver of cybersecurity spending. Globally, military expenditures reached a record $2.7 trillion in 2024 (9.4% annual increase), a growing share of which is allocated to cybersecurity.[8] In its 2026 budget, the U.S. Department of Defense proposed $15.1 billion for cybersecurity, a notable increase from previous years.[9] Additionally, European North Atlantic Treaty Organization ("NATO") members agreed to increase their defense spending goal to 5% of GDP by 2035, up from 2%.[10] Cybersecurity is indispensable as technological advances are leveraged to improve defense capabilities.

Cybersecurity is also vital for critical physical infrastructure because it protects the digital systems controlling essential services like power grids, water systems, and transportation. For instance, in May 2021, hackers staged a ransomware attack on the Colonial Pipeline—which transports over 100 million gallons of fuel each day in the U.S.—disrupting fuel supplies across the country, and costing $4.4 million in ransom payments with millions more in lost productivity.[11] More recently, in April 2025, hackers breached the control systems of a dam on Lake Risevatnet in Norway, remotely opening a water valve for hours, due to a web-accessible control panel with a weak password.[12] As governments and organizations prioritize resilience and national stability, we believe demand for cybersecurity will remain robust.

Preparing for Future Cyber Threats

While large-scale quantum computing may not be available for several years, many companies have begun to recognize the significant risk that it poses to conventional cybersecurity, necessitating proactive investment. Quantum computing uses principles of quantum mechanics to process information at unprecedented speeds, far surpassing traditional computers. Thus, quantum computers could theoretically break traditional encryption methods (like Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC)) in minutes rather than centuries. Adding urgency to this challenge is the risk that encrypted data stolen today could be stored with the intention of decrypting it once quantum capabilities mature.[13,14]

In August 2024, the National Institute of Standards and Technology (NIST) released the first three finalized post-quantum cryptography (PQC) standards, following an extensive evaluation process that began in 2016, marking a critical step toward quantum-resistant frameworks.[15] Industry leaders, such as IBM, Google, and Microsoft (among others) have already begun making investments to implement PQC standards.[16] As quantum risks loom, we believe cybersecurity firms developing quantum-safe solutions will see resilient demand.

[6]SailPoint Technologies, May 2025.

[7]Gartner, June 2025.

[8]Stockholm International Peace Research Institute, April 2025.

[9]MeriTalk, June 2025.

[10]POLITICO, June 2025.

[11]Colonial Pipeline Company, May 2021.

[12]Hackread, June 2025.

[13,14]Akande, Babatunde. "The Impact of Quantum Computing on Encryption: How Quantum Computers Can Break Current Encryption Methods, Such as RSA and ECC, and What This Means for Data Security." April 2025.

[15]National Institute of Standards and Technology, August 2024.

[16]KPMG, 2025 Futures Report. June 2025.

Regulatory Incentives for Cybersecurity

Heightened regulatory scrutiny and privacy laws continue to push investment in cybersecurity, in our view. Comprehensive data privacy laws such as the European Union's General Data Protection Regulation and California's Consumer Privacy Act enforce strict rules on data collection and impose hefty fines for breaches. The European Union's AI Act mandates cybersecurity for high-risk AI systems. The U.S. Securities and Exchange Commission has enacted rules that govern how public companies must disclose material cybersecurity incidents and cover their cybersecurity risk management, strategy, and governance in annual filings. Taken together, these new regulations and rules compel organizations to invest regardless of economic conditions, pushing companies to maintain spending on training and security tools to avoid hefty fines and lawsuits.

CIBR: An ETF for Investing in Cybersecurity

The First Trust Nasdaq Cybersecurity ETF (CIBR) is based on an equity index called the Nasdaq CTA Cybersecurity™ Index which is designed to track the performance of companies engaged in the cybersecurity segment of the technology and industrials sectors. The fund offers targeted exposure to a theme poised for growth, in our view, driven by the proliferation of artificial intelligence, quantum preparedness, infrastructure protection, and national security demands. Given our bullish outlook, cybersecurity's underrepresentation in most broad equity indices is notable. As of 6/30/2025, CIBR's 32 holdings represented just 3.75% of the S&P 500® Index. In our view, CIBR may be an effective tool for investors seeking to capitalize on the long-term growth of this theme.

References to specific securities should not be construed as a recommendation to buy or sell and should not be assumed profitable.

CIBR Overall Morningstar Rating™

★★★★

As of 6/30/2025, among 248 funds in the Technology category. This fund was rated 3 stars/248 funds (3 years), 4 stars/215 funds (5 years) based on risk adjusted returns.^

^The Morningstar Rating™ for funds, or "star rating", is calculated for managed products (including mutual funds, variable annuity and variable life subaccounts, exchange-traded funds, closed-end funds, and separate accounts) with at least a three-year history. Exchange-traded funds and open-ended mutual funds are considered a single population for comparative purposes. It is calculated based on a Morningstar Risk-Adjusted Return measure that accounts for variation in a managed product's monthly excess performance, placing more emphasis on downward variations and rewarding consistent performance. The Morningstar Rating does not include any adjustment for sales loads. The top 10% of products in each product category receive 5 stars, the next 22.5% receive 4 stars, the next 35% receive 3 stars, the next 22.5% receive 2 stars, and the bottom 10% receive 1 star. The Overall Morningstar Rating for a managed product is derived from a weighted average of the performance figures associated with its three-, five-, and 10-year (if applicable) Morningstar Rating metrics. The weights are: 100% three-year rating for 36-59 months of total returns, 60% five-year rating/40% three-year rating for 60-119 months of total returns, and 50% 10-year rating/30% five-year rating/20% three-year rating for 120 or more months of total returns. While the 10-year overall star rating formula seems to give the most weight to the 10-year period, the most recent three-year period actually has the greatest impact because it is included in all three rating periods.

Performance Summary (%) as of 6/30/2025

CIBR Performance*	3 Month	YTD	1 Year	3 Year	5 Year	10 Year	Since Fund Inception
Net Asset Value (NAV)	19.99	19.28	34.28	23.81	18.43	N/A	14.87
Market Price	20.05	19.23	34.28	23.79	18.47	N/A	14.88
Index Performance**							
Nasdaq CTA Cybersecurity™ Index	20.24	19.64	35.15	24.61	19.22	N/A	15.68
S&P Composite 1500® Information Technology Index	23.46	7.72	14.62	31.20	22.72	N/A	22.70
S&P 500® Index	10.94	6.20	15.16	19.71	16.64	N/A	13.64

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.com.

Inception Date: 7/6/2015. Total Expense Ratio: 0.59%. 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 for periods of less than one year, which are cumulative.

**Performance information for each index listed 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.

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.

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

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.

First Trust Advisors L.P. (FTA) is the adviser to the First Trust fund(s). FTA is an affiliate of First Trust Portfolios L.P., the distributor of the fund(s).

The information presented is not intended to constitute an investment recommendation for, or advice to, any specific person. By providing this information, First Trust is not undertaking to give advice in any fiduciary capacity within the meaning of ERISA, the Internal Revenue Code or any other regulatory framework. Financial professionals are responsible for evaluating investment risks independently and for exercising independent judgment in determining whether investments are appropriate for their clients.

Definitions

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

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.