When AI Risk Becomes Everyone's Risk

Published November 18, 2026

Christopher Gannatti, CFA
Global Head of Research

Key Takeaways

- AI agents create new vulnerabilities as companies give them access to systems and data, increasing the need for access controls and recovery capabilities.
- Cybersecurity fund definitions matter: some include broader technology businesses, while others emphasize specialized security companies and revenue growth.
- The WisdomTree Cybersecurity Fund (WCBR) combines cybersecurity focus and revenue growth criteria, with AI Security among its index's development themes.

The Question Has Changed

For the first few years of the generative AI boom, the dominant question was what the technology could do. Increasingly, the question is what could go wrong. Companies that spent last year experimenting with chatbots are now giving software "agents" (AI programs that take actions, such as moving data or approving a request, rather than only answering questions) real access to real systems. Every one of those models, data pipelines and agents is one more place an attacker could try to get in. Security professionals call the full set of those places the attack surface, and AI is enlarging it at the same moment it is handing attackers better tools.

The annual breach study from IBM and the Ponemon Institute, a research firm, covers 602 organizations that suffered a data breach between March 2025 and February 2026.

- About one in four of the organizations hit by a malicious attack said the attack was AI-driven, a 56% increase over the prior year.
- Those breaches also cost more: $6.04 million on average, against $5.03 million for malicious breaches that did not involve AI, a gap of about $1 million.

Statistics like this turn an abstract worry into a number a budget committee can use. Two cautions apply. The sample is organizations that were already breached, so it tells us what AI-driven attacks cost when they succeed, not how common they are across the economy. And IBM itself sells security services.1

The same study points to organizations' own use of AI as a weak spot.

- Security incidents involving "shadow AI," meaning employees using AI tools their employer has not approved, rose to 43%, up from 20% a year earlier.

- Among organizations that suffered an AI-related breach, 92% lacked proper AI access controls, which are the rules about which people and programs can reach a model and the data behind it.
- Across organizations generally, only 40% reported using such controls on AI models and data.

It would appear that companies are adopting AI faster than they are governing it, and that gap is the commercial opening for security vendors.1

Anthropic, in a September 2026 threat report, covered misuse it detected and disrupted between December 2025 and August 2026. It describes multi-agent systems, in which a lead AI agent splits reconnaissance, break-in and data-theft work among subordinate agents, running for hours or days with little human involvement. The report adds two cautions of its own.

- Humans still made the most consequential decisions.
- Automation changed the scale and cost of attacks more than their severity.

One case is especially relevant to this discussion.

An actor compromised an AI vendor's testing environment to obtain production access keys, then ran a campaign against about 30 AI companies in roughly four days. AI companies are themselves targets. Because Anthropic is a frontier AI lab, the report reflects what it can see on its own platform, which is informative but not the whole threat landscape.2

Two Funds, Two Definitions

The First Trust Nasdaq Cybersecurity ETF (CIBR) is the largest, by assets under management, incumbent player among cybersecurity-focused exchange-traded funds in the U.S.3 The WisdomTree Cybersecurity Fund (WCBR) is more the competitive upstart. What we find of particular interest is the difference in definition, basically asking "what is cybersecurity in 2026?" because it determines how each fund responds as new themes, like AI security, reshape the industry.

CIBR tracks the Nasdaq CTA Cybersecurity Index, which sorts companies into two buckets.

- "Core" firms sell cybersecurity itself, in areas such as application security, identity and access management or network security.
- "Complementary" firms touch cybersecurity as part of a broader business, such as diversified technology providers, consultants and managed service providers.

The index ranks eligible companies by "notional thematic revenue," which is the index provider's estimate of the share of a company's revenue that is cybersecurity multiplied by the company's total revenue. It then weights by modified free-float market capitalization (the market value of shares available to the public, adjusted by index rules), with the five largest Core names capped at 8% each.

Key point: Multiplying a revenue share by total revenue means a small cyber slice of a giant business can outrank a smaller company that does nothing but security.

The construction rewards scale and aims at total thematic exposure, wherever it resides.4

WCBR takes a narrower view. It tracks the WisdomTree Team8 Cybersecurity Index, built with the regular consultation of Team8, a venture group specializing in cyber, data, AI and fintech. Companies are then scored on two axes.

- A Focus Score reflects how many of Team8's eight cyber development themes a company has high exposure to, among them Security of Things, Data Security, Resilience & Recovery and AI Security.
- A Growth Score is based on trailing three-year revenue growth, expressed as a compound annual growth rate (the steady yearly pace that would produce the same total growth), where 20% or more earns the top "Growing Fast" tier.

Companies must show both focus and growth to be included, and the strongest combination, broad focus with fast growth, receives a larger weight.

This Is Where AI Security Becomes More Than a Talking Point

Team8 named AI Security as one of its themes, the idea that AI systems create new vulnerabilities across data pipelines, training environments and inference (the stage where a trained model is actually answering requests), and that a new class of security vendor is emerging to govern and protect them. A methodology that rewards focus on that theme, together with fast revenue growth, is by design more likely to tilt toward newer, specialized companies building for that future than toward mega-cap technology companies for which cybersecurity is a mature, slower-growing division.

Inside CIBR: Scale, Wherever It Sits

*In this section, the percentages in parentheses are CIBR's weights as of November 13, 2026.*5

CIBR holds 46 companies. Its five largest positions, all publicly traded, are CrowdStrike (8.3%), whose software protects individual computers and servers; Broadcom (7.9%), a chip and infrastructure software maker; Cisco (7.3%), a networking equipment maker; Palo Alto Networks (7.1%), a firewall and security platform company; and Fortinet (6.3%), which also builds firewalls and security hardware and software. Together they make up 36.8% of the fund. The second and third positions deserve attention. Neither Broadcom nor Cisco is a cybersecurity-native business, and together they hold 15.2%, more than twice the weight of Palo Alto Networks.

Further down sits a wider ring of diversified companies: Accenture (2.8%), a global consulting and technology services firm; IBM (2.2%); Microsoft (2.2%); and Alphabet (1.8%), plus government technology contractors such as Leidos (2.0%) and Booz Allen Hamilton (1.6%). Adding Broadcom, Cisco, Accenture, IBM, Microsoft and Alphabet gives 24.2%, so roughly a quarter of the fund is in six companies where security is one business line among many.

What does that mean for the AI-risk story? CIBR is built to capture security revenue wherever it lands, which gives broad exposure to security spending and also sizable exposure to companies whose fortunes depend on much else, including the AI infrastructure build-out that investors are now scrutinizing more

closely. Broadcom and Cisco, for instance, both supply networking technology that AI data centers run on. That is neither good nor bad in itself. It is the consequence of defining the theme by where the revenue sits, and whether it is a feature or a drawback depends on what an investor wants the exposure to do.

Inside WCBR: Focus, with a Growth Screen

*In this section, the percentages in parentheses are WCBR's weights.*6

WCBR holds 25 companies, and its largest position is Zscaler (6.4%), a publicly traded provider of cloud security that checks every connection between users and applications rather than trusting anything simply because it sits inside a company network, an approach known as zero trust. Next come SentinelOne (6.1%), an endpoint security company built around automated, AI-driven detection; CrowdStrike (5.9%); Netskope (5.8%), which secures access to cloud applications and the web; Tenable (5.2%), whose software finds and ranks weaknesses in a company's systems; Rubrik (5.0%), a data backup and recovery company; Trend Micro (5.0%), a Tokyo-listed security software maker; and SailPoint (4.8%), which manages who has access to what inside an organization. The smallest position is AhnLab (0.8%), a South Korean security software company.

Two of those names show why the AI-risk frame matters for this portfolio. SailPoint sits in identity, and the IBM study's recommendation is that AI agents operate under dynamic, identity-based access controls, an approach that treats each agent as something that needs its own permissions. Rubrik sits in recovery, which fits the Resilience & Recovery theme and the practical reality that some attacks will succeed. These are our readings of how the companies fit the storyline rather than company claims. The weights are also fairly even. The top five positions total 29.3% of the fund, and even the established scale leaders Palo Alto Networks (3.9%) and Fortinet (3.3%) are held at modest weights. WCBR is narrow in what it counts as cybersecurity, but it is not top-heavy in how it weights it. The trade-off is that smaller, faster-growing companies can carry narrower product lines and larger swings in their share prices.

Conclusion: Did the Difference in Strategy Translate to a Difference in Performance?

It is true that no single strategy, at least that we have found, outperforms in all markets at all times. It's one thing to have an idea that seems to make sense, but it is quite another to see that idea deliver in a real performance outcome. Additionally, we have seen October 2026 and roughly the first half of November 2026 getting quite volatile for technology stocks. Against all of that, it is critical to look at how WCBR is doing versus CIBR, particularly during this year, shown in Figure 1a, where AI has been a nearly daily focus for equity investors. In Figure 1b, we also provide a look at the longer-term standardized performance picture as of September 30, 2026 for fuller context.

Figure 1a: Cumulative Returns for Year-to-Date 2026



Figure 1b: Standardized Performance

Fund Name	Fund Ticker Symbol	Fund Inception Date	Fund Expense Ratio	Fund SEC 30-Day Yield	Year-to-Date	1-Year	3-Year	5-Year	10-Year	Since Fund Inception
WisdomTree Cybersecurity Fund (NAV)	WCBR	1/28/2021	0.45%	-0.35%	63.96%	45.57%	30.77%	12.27%	N/A	11.97%
WisdomTree Cybersecurity Fund (MP)	WCBR	1/28/2021	0.45%	-0.35%	64.33%	45.84%	30.80%	12.28%	N/A	12.00%
First Trust Nasdaq Cybersecurity ETF (NAV)	CIBR	7/6/2015	0.58%	0.05%	34.58%	26.85%	28.80%	14.97%	17.66%	16.33%
First Trust Nasdaq Cybersecurity ETF (MP)	CIBR	7/6/2015	0.58%	0.05%	34.72%	26.99%	28.87%	15.05%	17.65%	16.35%

Sources: Morningstar, FactSet and WisdomTree, with data from the PATH Fund Comparison Tool, accessed November 14, 2026, but showing returns for the period ended November 13, 2026 for Figure 1a and September 30, 2026 for Figure 1b. NAV denotes total return performance at net asset value. MP denotes market price performance. **Past performance is not indicative of future results. Investment return and principal value of an investment will fluctuate so that an investor's shares, when redeemed, may be worth more or less than their original cost. Current performance may be lower or higher than the performance data quoted. For the most recent month-end and standardized performance, click the relevant ticker: WCBR, CIBR.**

Within Figure 1a, it is clear that, even amid the October/November 2026 drawdown, WCBR has held up against CIBR, after starting the year more in lockstep. It'll be important for us to monitor whether this continues. In the spirit of the fuller context, Figure 1b shows WCBR ahead Year-to-Date, 1-Year and 3-Year, but CIBR is ahead on the 5-Year horizon. The funds have different inception dates, so that period is not relevant for comparison here.

For those thinking about a necessary area of technology focus amid everything happening with AI, cybersecurity and WCBR could be worth a deeper look.

Figure 2: Additional Information

Fundamentals	WisdomTree Cybersecurity Fund (WCBR)	First Trust Nasdaq Cybersecurity ETF (CIBR)
Objective	The WisdomTree Cybersecurity Fund seeks to track the price and yield performance, before fees and expenses, of the WisdomTree Team8 Cybersecurity Index.	The First Trust Nasdaq Cybersecurity ETF seeks investment results that correspond generally to the price and yield (before the Fund's fees and expenses) of an equity index called the Nasdaq CTA Cybersecurity™ Index.
SEC 30-Day Yield	-0.35%	0.05%
Total Expense Ratio	0.45%	0.58%
Total Assets Under Management (millions)	$218.84	$16,545.85

Sources: WisdomTree, First Trust, respective fund pages, with assets under management shown as of November 13, 2026. **Subject to change.**

1 Source: IBM & Ponemon Institute. (2026). *Cost of a data breach report 2026: The AI tipping point*. IBM.

2 Source: Anthropic. (2026, September). *Detecting and countering misuse of AI: September 2026*.

3 As of November 13, 2026, CIBR had roughly $16.5 billion in assets under management, per the CIBR fund webpage on the First Trust website. **Subject to change.**

4 Source: Nasdaq, Inc. (2026). *Nasdaq CTA Cybersecurity Index (NQCYBR) index methodology* [Version effective March 23, 2026].

5 Source: CIBR fund page. **Holdings subject to change.**

6 Source: WCBR fund page, with data on holdings as of November 13, 2026. **Holdings subject to change.**

Important Risks Related to this Article

All funds are managed differently and do not react the same to economic or market events. The investment objectives, strategies, policies or restrictions of other funds may differ and more information can be found in their respective prospectuses. Therefore, we generally do not believe it is possible to make direct fund-to-fund comparisons in an effort to highlight the benefits of a fund versus another similarly managed fund.

WCBR: There are risks associated with investing, including possible loss of principal. The Fund invests in cybersecurity companies, which generate a meaningful part of their revenue from security protocols that prevent intrusion and attacks to systems, networks, applications, computers and mobile devices. Cybersecurity companies are particularly vulnerable to rapid changes in technology, rapid obsolescence of products and services, the loss of patent, copyright and trademark protections, government regulation and competition, both domestically and internationally. Cybersecurity company stocks, especially those which are internet related, have experienced extreme price and volume fluctuations in the past that have often been unrelated to their operating performance. These companies may also be smaller and less experienced companies, with limited product or service lines, markets or financial resources and fewer experienced management or marketing personnel. The Fund invests in the securities included in, or representative of, its Index regardless of their investment merit and the Fund does not attempt to outperform its Index. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.

To view CIBR's risk disclosures, click here.