Cybercriminals Are Winning—Cybersecurity Must Strike Back Now

Published March 13, 2025

Christopher Gannatti, CFA
Global Head of Research

Mobeen Tahir
Director, Research

Key Takeaways

- As cybercriminals leverage AI and sophisticated tactics to breach defenses faster than ever, sometimes in just 51 seconds, cybersecurity must evolve rapidly to stay ahead.
- The rising cost of data breaches, now averaging nearly $5 million in 2024, underscores the financial and reputational risks businesses face, making proactive cybersecurity investments essential.
- The WisdomTree Cybersecurity Fund (WCBR) offers investors exposure to high-growth cybersecurity companies tackling the latest threats, from AI-driven attacks to geopolitical cyber risks.

My colleague, Mobeen Tahir, recently created a website, but soon after launching it, he noticed it wasn't appearing in Google searches. While researching how to fix this, he received an email with step-by-step instructions on what to do. Nothing about it seemed suspicious, not even the sender's address. But when Mobeen used AI to verify its authenticity, the AI flagged it as suspicious.

I was recently talking to my wife about another attempt—a series of text messages I had received seeking to create urgency around a hypothetical unpaid highway toll bill; mind you, from an "iCloud" email address. One day, there was a request to settle a bill, and the next day, there was a statement that law enforcement would be knocking on my door. I can respect psychology. It is difficult to remember the exact experience of driving on the highway minute by minute, and then you see the ramping up of urgency with an offer to solve the problem by just clicking on a "helpful" link.

A few years ago, phishing emails had obvious red flags—poor grammar, strange formatting or sketchy links. Today, with AI-powered tools at their disposal, cybercriminals are far more sophisticated. And if they're getting smarter, cybersecurity must become smarter still.

A Smart Way to Capture a Fast-Growing Theme

The WisdomTree Cybersecurity Fund (WCBR), which is designed to track the total return performance, before fees and expenses, of the WisdomTree Team8 Cybersecurity Index, identifies eight key areas of focus.

1. Cloud Security
2. Security of Things
3. Perimeterless World
4. Data Privacy & Security
5. Resilience & Recovery
6. Shift-Left
7. AI & Smarter Security
8. Layer 8, the Human Factor

The critical point is that each of these cybersecurity themes can be applied to the specific cybersecurity solutions that companies are building and providing to customers. They place the focus not on what was helpful in protecting against past attacks but rather upon what could be helpful in getting ready for the future.

WCBR is a portfolio of pure-play cybersecurity businesses, with a focus on companies that are growing their revenues quickly and span multiple cybersecurity themes. For investors seeking smart exposure to this vital theme, WCBR can help add growth potential to their portfolio.

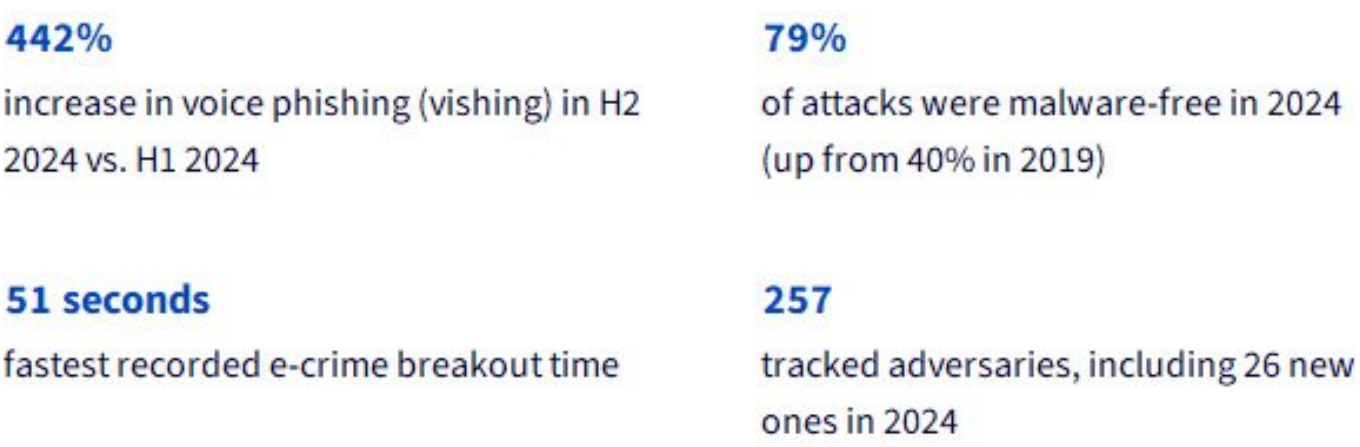
The Unbearable Cost of a Data Breach

In 2024, the average cost of a data breach soared to nearly $5 million.1 And that's just the average, meaning many breaches resulted in far greater losses. While this number has been rising for years, 2024 saw a sharp uptick, underscoring how the widespread adoption of advanced AI tools is making cybercriminals smarter and attacks more costly than ever.

"Attack speeds could increase up to 100x as threat actors leverage generative AI." – Palo Alto Networks

In many cases, the true cost of a data breach goes beyond dollars and cents; it's immeasurable. What happens when customer trust in a business's security is shattered? The reputational damage could be irreversible. What if a hospital is hacked and a life is lost? The stakes couldn't be higher. That's why cybersecurity isn't just a priority; it's a necessity. And the world is finally waking up to that reality.

Cybercriminals Are Becoming Smarter



Source: CrowdStrike 2025 Global Threat Report, 3/25.

When cybercriminals compromise a target, their intention is to infiltrate the organization via a weak link and move deeper into the network. E-crime breakout time refers to how quickly they escalate control, spreading from the initial breach to critical systems, stealing data, disabling security or deploying ransomware. Some attackers achieve this in under an hour, making rapid detection and response crucial. In 2024, the fastest recorded time attackers were able to do this in was 51 seconds.2

Attackers aren't always relying on emails; the nuisance calls we receive can often be quite nefarious. Vishing (voice phishing) attacks involve cybercriminals using phone calls to impersonate trusted entities, such as banks, government agencies or service providers, to trick victims into revealing sensitive information or transferring money. These scams have surged dramatically, with a 442% increase in voice phishing (vishing) in H2 2024 versus H1 2024,3 highlighting how criminals are exploiting human trust over the phone to bypass traditional cybersecurity defenses.

A few weeks ago, Mobeen saw a post on LinkedIn of a man surrounded by police officers. The man was telling the story of how he physically hacked into an organization, walking through security checkpoints, accessing restricted areas and pushing his luck until he finally got caught. But this wasn't a real attack, it was a penetration test—a controlled security exercise designed to identify vulnerabilities before actual criminals exploit them. Organizations conduct these tests because hackers are employing increasingly sophisticated social engineering techniques, manipulating people rather than systems, to bypass security and gain access. The threat is growing, with 79% of attacks in 2024 being malware-free, up from 40% in 2019,4 proving that cybercriminals don't always need malware when they can simply trick humans into opening the door.

High-Profile Attacks Underscore Geopolitical Risks

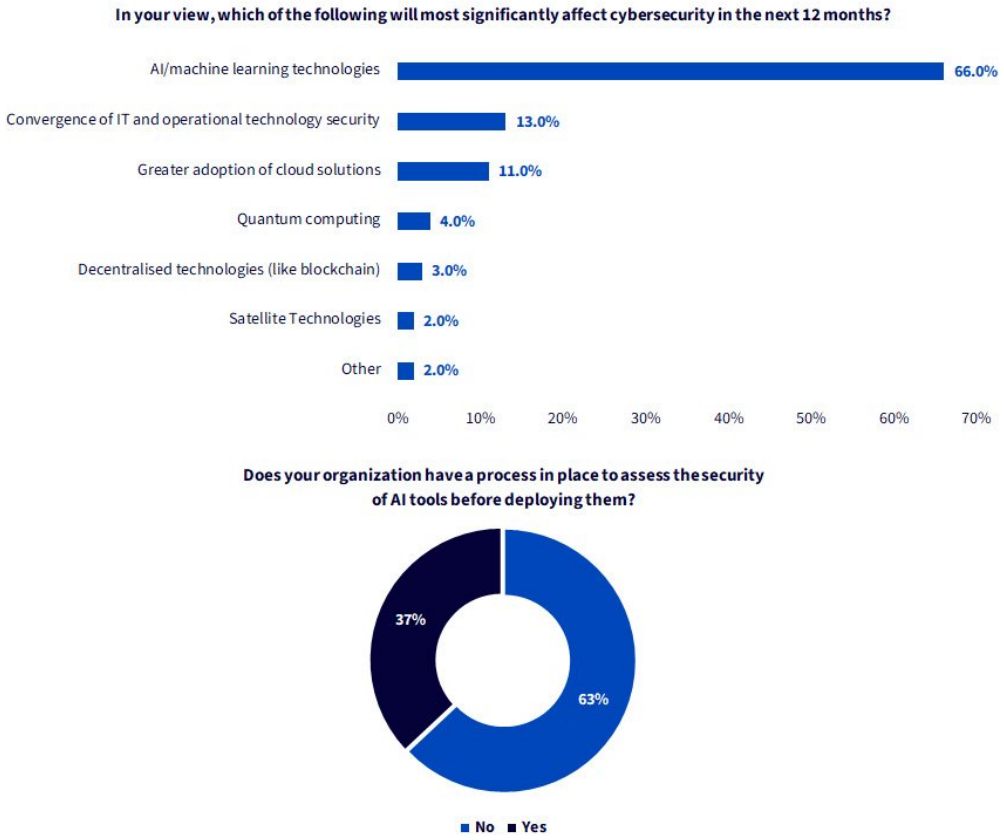
At the outset of 2024, concerns about cyber risks in the election year were widespread. While many countries navigated the electoral cycle without major known cyber incidents, Romania's December presidential election was notably annulled due to allegations of Russian interference. Far-right candidate

Calin Georgescu's unexpected lead in the first round prompted investigations that revealed a coordinated online campaign and cyberattacks supporting his candidacy, leading the courts to void the election.

In the same month, the U.S. Treasury Department reported a significant cybersecurity breach attributed to Chinese state-sponsored hackers. The attackers exploited a third-party software provider to access Treasury workstations and unclassified documents. The breach involved the theft of a security key, allowing remote access to the department's systems. Although China's foreign ministry denied these allegations, the incident underscores the growing intersection of geopolitical and cybersecurity risks.

Executives Are Concerned about Risks from AI

A recent World Economic Forum survey5 of executives revealed that 66% believe AI and machine learning will have the biggest impact on cybersecurity in the next 12 months. Yet, 63% admitted their organizations lack processes to assess the security of AI tools before deploying them, highlighting a critical gap between innovation and risk management.



Source: World Economic Forum, Global Cybersecurity Report 2025.

Cybersecurity Must Stay One Step Ahead

Cybersecurity must constantly innovate, leveraging cutting-edge technology to stay one step ahead of evolving threats. This relentless race between defenders and attackers is what makes cybersecurity such an exciting and dynamic field. Recent headlines around quantum computing suggest that the age of

quantum might be closer than we once thought, a future where a quantum computer could shatter even the most sophisticated encryption effortlessly. This would redefine cybersecurity as we know it. Whether it's quantum computing, AI or blockchain, every breakthrough introduces new vulnerabilities, and safeguarding them must be a proactive pursuit, not a reactive one. Because if we wait until the attack happens, it might already be too late.

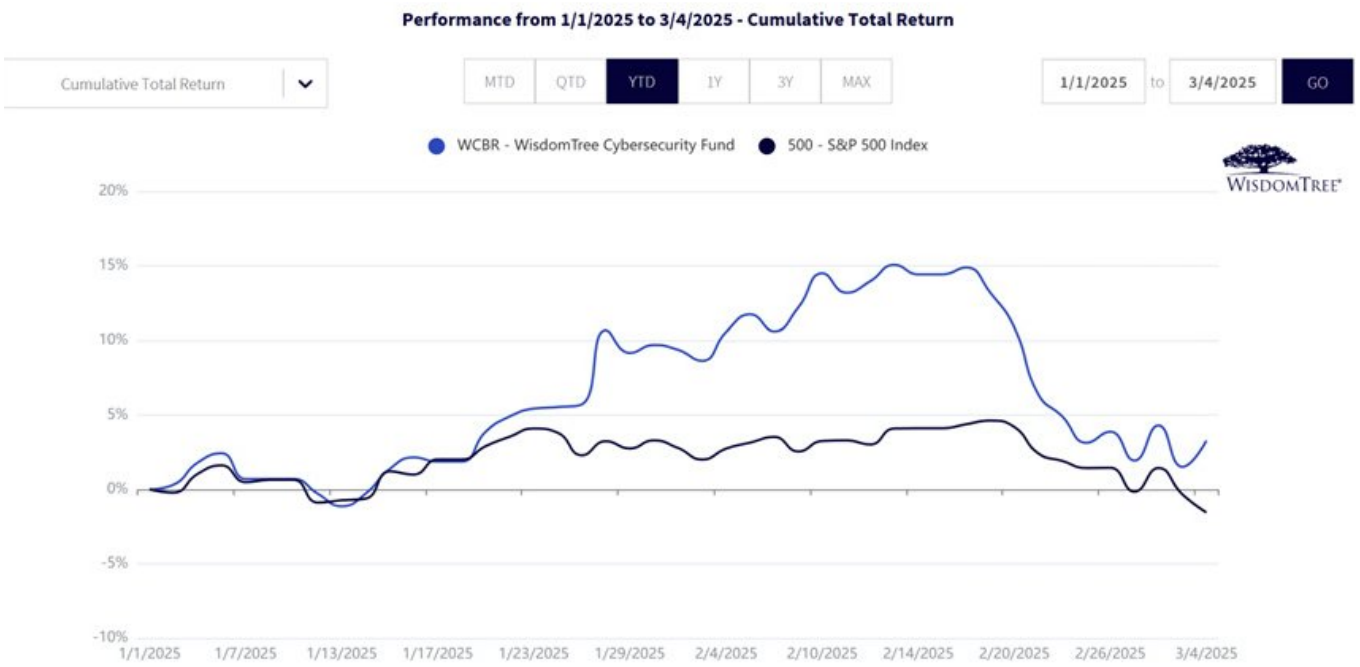
It's interesting to see how these concepts have been translating into returns, since many of us would imagine the need for cybersecurity is only progressing in an upward manner, but the returns of the companies themselves can be far more volatile.

Standardized Returns

Fund/Index Name	Fund Ticker Symbol	Fund Inception Date	Fund Expense Ratio	1-Year	3-Year	5-Year	10-Year	Since Fund Inception
WisdomTree Cybersecurity Fund (NAV)	WCBR	1/28/21	0.45%	11.82%	2.83%	N/A	N/A	4.27%
WisdomTree Cybersecurity Fund (MP)	WCBR	1/28/21	0.45%	11.62%	2.76%	N/A	N/A	4.23%
S&P 500 Index				25.02%	8.94%	14.53%	13.10%	N/A

As we started 2025, WCBR enjoyed a strong rally from late January 2025, around the time of the so-called "DeepSeek" moment, to about the third week of February 2025. From there, volatility has increased. We'd note that the specific focus on cybersecurity companies providing solutions, per Team8, with the potential to protect against the future of cybersecurity attacks, has not translated to a lower-volatility investment strategy. In our opinion, cybersecurity is a constant battleground that will continue to play out over years, and the companies within WCBR represent software-oriented solutions to help users deal with these threats.

Performance



1 IBM, 2025.

2 Source: CrowdStrike 2025 Global Threat Report, 3/25.

3 Source: CrowdStrike 2025 Global Threat Report, 3/25.

4 Source: CrowdStrike 2025 Global Threat Report, 3/25.

5 Source: World Economic Forum, Global Cybersecurity Report 2025.

Important Risks Related to this Article

You cannot invest directly in an index.

There are risks associated with investing, including the 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 that 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 or take defensive positions in declining markets. The composition of the Index is heavily dependent on quantitative and qualitative information and data from one or more third parties, and the Index may not perform as intended. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.