Cybercriminals are winning—cybersecurity must strike back now

Published 31 March 2025

Mobeen Tahir
Director, Research

Key Takeaways

- Cybercriminals are using AI and social engineering to launch more sophisticated attacks.
- Rapid detection is critical—some breaches escalate in under a minute.
- High-profile cyber-attacks are exposing geopolitical risks, from election interference to government breaches.

I recently created a website, but soon after launching it, I noticed it wasn't appearing in Google searches. While researching how to fix this, I 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 I used artificial intelligence (AI) to verify its authenticity, it was flagged as suspicious.

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.

The unbearable cost of a data breach

In 2024, the average cost of a data breach soared to nearly $5 million1. 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' 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

increase in voice phishing (vishing) in H2 2024 vs H1 2024

of attacks were malware-free in 2024 (up from 40% in 2019)

51 seconds

Fastest recorded e-crime breakout time

tracked adversaries including 26 new ones in 2024

Source: CrowdStrike 2025 Global Threat Report, March 2025.

When cybercriminals compromise a target, their intention is to infiltrate the organisation 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 was 51 seconds2.

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 vishing in H2 2024 vs H1 20243, highlighting how criminals are exploiting human trust over the phone to bypass traditional cybersecurity defences.

A few weeks ago, I saw a post on LinkedIn of a man surrounded by police officers. He was telling the story of how he physically hacked into an organisation, 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. Organisations 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 20194, 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 revealing a coordinated online campaign and cyberattacks supporting his candidacy, leading the courts to void the election.

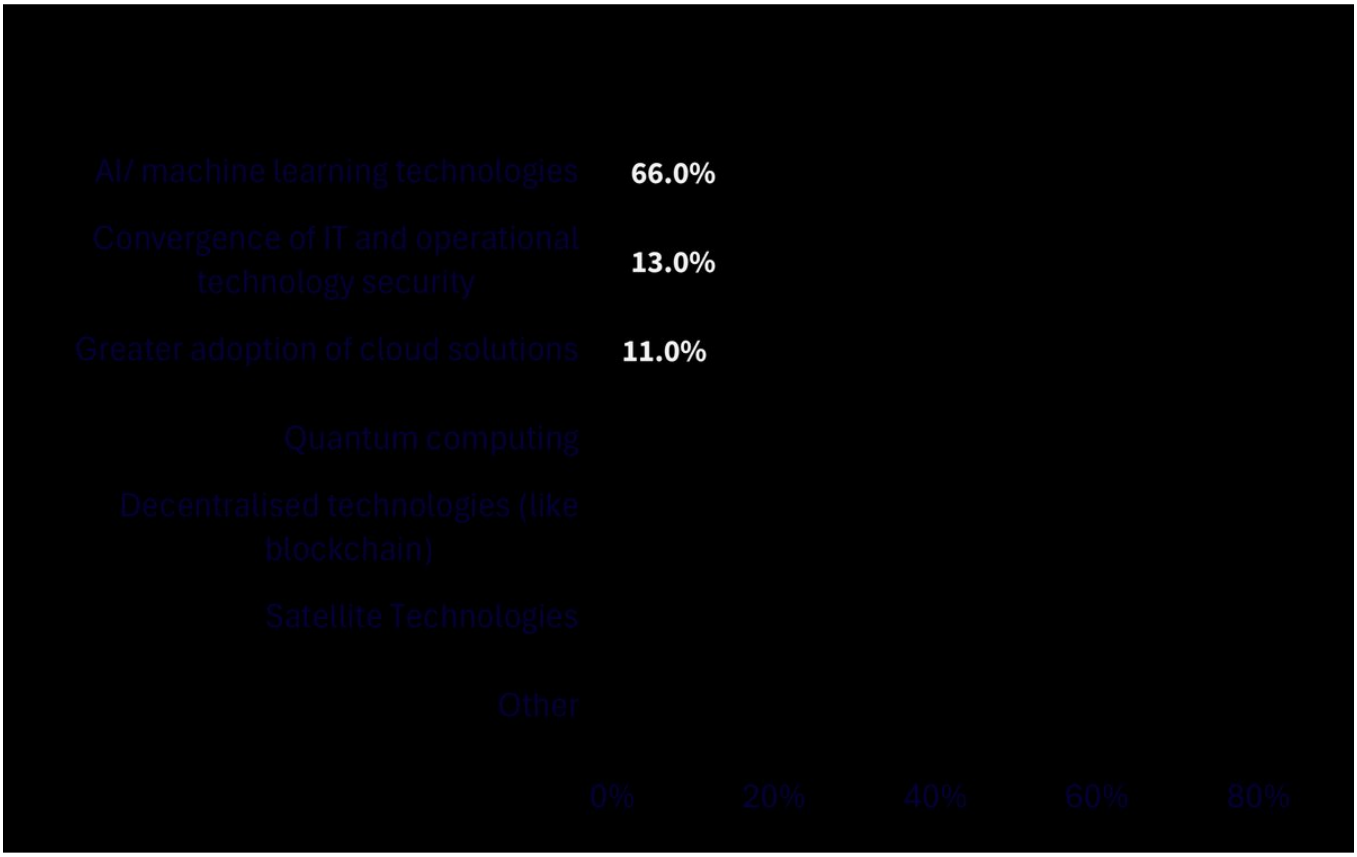
In the same month, the US Treasury Department reported a significant cybersecurity breach attributed to Chinese state-sponsored hackers. The attackers exploited a third-party software provider to access

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

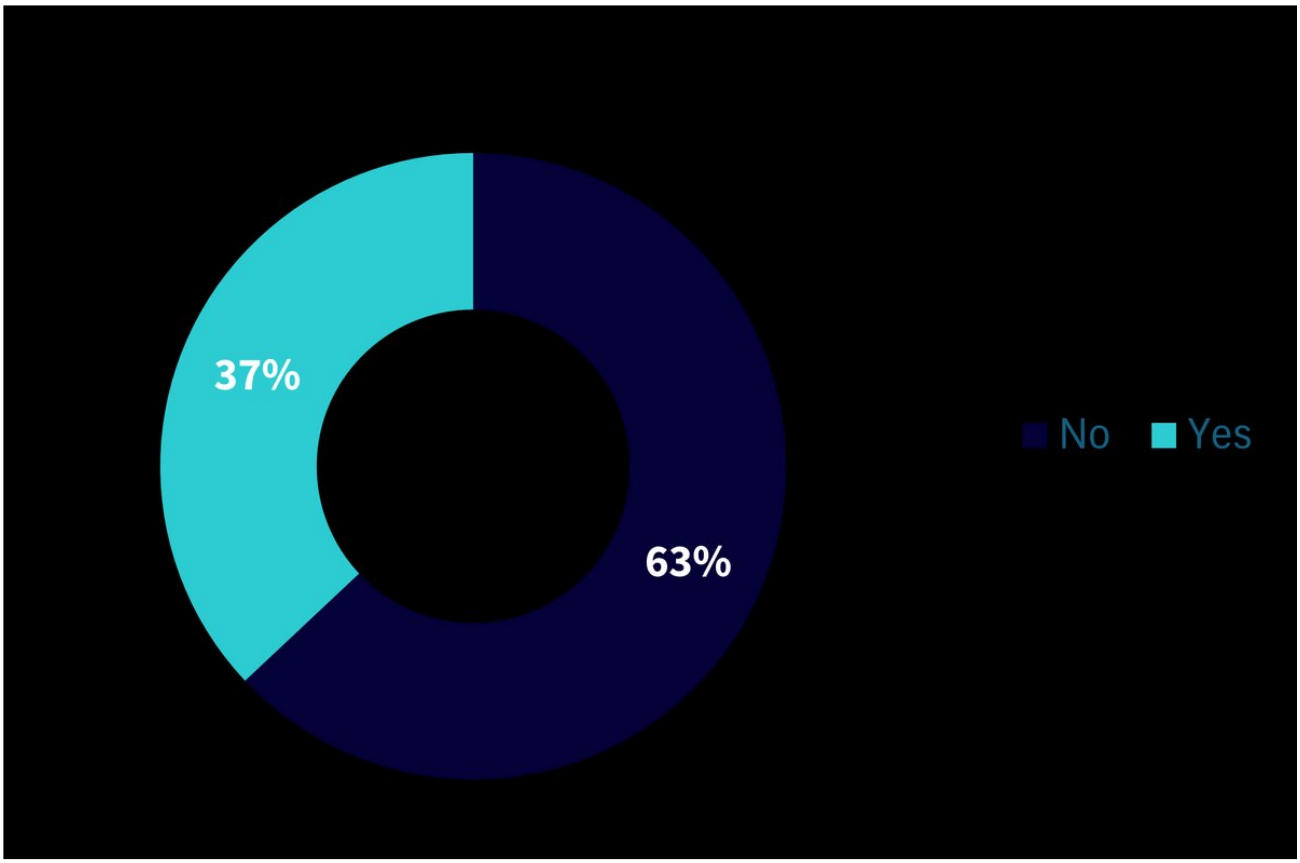
A recent World Economic Forum survey5 of executives revealed that 66% believe AI and machine learning will have the biggest impact on cybersecurity in the next 12 months. Yet, 63% admitted their organisations lack processes to assess the security of AI tools before deploying them—highlighting a critical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

Figure 1: In your view, which of the following will most significantly affect cybersecurity in the next 12 months?



Source: World Economic Forum, Global Cybersecurity Report 2025.

Figure 2: Does your organisation have a process in place to assess the security of AI tools before deploying them?



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.

1 IBM, 2025.
2 Source: CrowdStrike 2025 Global Threat Report, March 2025.
3 Source: CrowdStrike 2025 Global Threat Report, March 2025.
4 Source: CrowdStrike 2025 Global Threat Report, March 2025.
5 Source: World Economic Forum, Global Cybersecurity Report 2025.

Important Risks Related to this Article

IMPORTANT INFORMATION

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

This marketing communication has been prepared for professional investors, but the WisdomTree products set out in this document may be available in some jurisdictions to any investors, subject to applicable laws and regulations. As the product may not be authorised or its oering may be restricted in your jurisdiction, it is the responsibility of every person or entity to satisfy themselves as to the full observance of the laws and regulations of the relevant jurisdiction. Prior to any application investors are advised to take all necessary legal, regulatory, tax and investment advice on the suitability and consequences of an investment in the products. Past performance is not a reliable indicator of future performance. Any historical performance included in this document may be based on back testing. Back testing is the process of evaluating an investment strategy by applying it to historical data to simulate what the performance of such strategy would have been. Back tested performance is purely hypothetical and is provided in this document solely for informational purposes. Back tested data does not represent actual performance and should not be interpreted as an indication of actual or future performance. The value of any investment may be aected by exchange rate movements. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice. These products may not be available in your market or suitable for you. The content of this document does not constitute investment advice nor an oer for sale nor a solicitation of an oer to buy any product or make any investment.

An investment in exchange-traded products ("ETPs") is dependent on the performance of the underlying index, less costs, but it is not expected to match that performance precisely. ETPs involve numerous risks including among others, general market risks relating to the relevant underlying index, credit risks on the provider of index swaps utilised in the ETP, exchange rate risks, interest rate risks, inflationary risks, liquidity risks and legal and regulatory risks.

The information contained in this document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public oering of shares in the United States or any province or territory thereof, where none of the issuers or their products are authorised or registered for distribution and where no prospectus of any of the issuers has been filed with any securities commission or regulatory authority. No document or information in this document should be taken, transmitted or

distributed (directly or indirectly) into the United States. None of the issuers, nor any securities issued by them, have been or will be registered under the United States Securities Act of 1933 or the Investment Company Act of 1940 or qualified under any applicable state securities statutes.

This document may contain independent market commentary prepared by WisdomTree based on publicly available information. Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Any third party data providers used to source the information in this document make no warranties or representation of any kind relating to such data. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any ailiate, nor any of their respective oicers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.

This document may contain forward looking statements including statements regarding our belief or current expectations with regards to the performance of certain assets classes and/or sectors. Forward looking statements are subject to certain risks, uncertainties and assumptions. There can be no assurance that such statements will be accurate and actual results could dier materially from those anticipated in such statements. WisdomTree strongly recommends that you do not place undue reliance on these forward-looking statements.

WisdomTree Issuer ICAV

The products discussed in this document are issued by WisdomTree Issuer ICAV (“WT Issuer”). WT Issuer is an umbrella investment company with variable capital having segregated liability between its funds organised under the laws of Ireland as an Irish Collective Asset-management Vehicle and authorised by the Central Bank of Ireland (“CBI”). WT Issuer is organised as an Undertaking for Collective Investment in Transferable Securities (“UCITS”) under the laws of Ireland and shall issue a separate class of shares ("Shares”) representing each fund.

The Fund is described in a Key Information Document (KID) or Key Investor Information Document (KIID) for UK investors, and the prospectus of WT Issuer (“WT Prospectus”). A copy of the WT Prospectus and the KID / KIID is available, for EEA/UK only, in English at www.wisdomtree.eu. Where required under national rules, the KID will also be available in the local language of the relevant EEA Member State. Investors should read the WT Prospectus before investing and should refer to the section of the WT Prospectus entitled »Risk Factors¼ for further details of risks associated with an investment in the Shares.

The summary of investor rights associated with an investment in the fund is available in English on WisdomTree Europe¼s website. WisdomTree Management Limited may decide to terminate the arrangements made for the marketing of its collective investment undertakings. In such circumstances, shareholders in the aected EEA Member State will be notified of this decision and will be provided with the opportunity to redeem their shareholding in the fund free of any charges or deductions for at least 30 working days from the date of such notification.

Notice to Investors in Switzerland – Qualified Investors

This document constitutes an advertisement of the financial product(s) mentioned herein.

The prospectus and the key investor information documents (KIID) are available from WisdomTree¼s website: https://www.wisdomtree.eu/en-ch/resource-library/prospectus-and-regulatory-reports

Some of the sub-funds referred to in this document may not have been registered with the Swiss Financial Market Supervisory Authority ("FINMA"). In Switzerland, such sub-funds that have not been registered with FINMA shall be distributed exclusively to qualified investors, as defined in the Swiss Federal Act on Collective Investment Schemes or its implementing ordinance (each, as amended from time to time). The representative and paying agent of the sub-funds in Switzerland is Société Générale Paris, Zurich Branch, Talacker 50, PO Box 5070, 8021 Zurich, Switzerland. The prospectus, the key investor information documents (KIID), the articles of association and the annual and semi-annual reports of the sub-funds are available free of charge from the representative and paying agent. As regards distribution in Switzerland, the place of jurisdiction and performance is at the registered seat of the representative and paying agent.

For Investors in France:

The information in this document is intended exclusively for professional investors (as defined under the MiFID) investing for their own account and this material may not in any way be distributed to the public. The distribution of the Prospectus and the oering, sale and delivery of Shares in other jurisdictions may be restricted by law. WT Issuer is a UCITS governed by Irish legislation, and approved by the Financial Regulatory as UCITS compliant with European regulations although may not have to comply with the same rules as those applicable to a similar product approved in France. The Fund has been registered for marketing in France by the Financial Markets Authority (Autorité des Marchés Financiers) and may be distributed to investors in France. Copies of all documents (i.e. the Prospectus, the Key Investor Information Document, any supplements or addenda thereto, the latest annual reports and the memorandum of incorporation and articles of association) are available in France, free of charge at the French centralizing agent, Societe Generale at 29, Boulevard Haussmann, 75009, Paris, France. Any subscription for Shares of the Fund will be made on the basis of the terms of the prospectus and any supplements or addenda thereto.

For Investors in Malta: This document does not constitute or form part of any oer or invitation to the public to subscribe for or purchase shares in the Fund and shall not be construed as such and no person other than the person to whom this document has been addressed or delivered shall be eligible to subscribe for or purchase shares in the Fund. Shares in the

Fund will not in any event be marketed to the public in Malta without the prior authorisation of the Maltese Financial Services Authority.

For Investors in Monaco: This communication is only intended for duly registered banks and/or licensed portfolio management companies in Monaco. This communication must not be sent to the public in Monaco.