Authored by:
Tejas Dessai

Date: April 26, 2024
Topic: Thematic, Disruptive Technology

GLOBAL X ETFs INSIGHTS

Cybersecurity Faces Transformation from Generative AI

Cybersecurity is a compelling theme in 2024 for multiple reasons. First, an evolving attack landscape requires corporations to keep their guard up and security spending elevated. Second is the growing relevance of generative AI, which is a double-edged sword. Generative AI enables malicious actors to discover vulnerabilities and improve attack methods, but it also enables security teams to build better defences, detect threats, and manage operations more efficiently. The cybersecurity industry appears to be on the verge of yet another transformation amid AI's proliferation, and it is expected to create numerous opportunities for share wins, including through consolidation. For investors seeking exposure to AI outside of the obvious beneficiaries, cybersecurity may have appeal.

Key Takeaways

- High-profile cyberattacks continue to cripple organisations despite growing cybersecurity investments. The emergence of generative AI presents new threats.
- Generative AI also helps cyber professionals build effective defences. Major cybersecurity vendors are rapidly developing AI-powered tools to augment human analysts, automate security operations, and detect anomalies.
- Despite economic headwinds, global cybersecurity spending is projected to grow over 14% in 2024 to $215 billion, driven by growing attacks and the urgency to strengthen defences against AI-enabled threats.[1]

Generative AI Complicates an Already Complex Cyber Attack Landscape

Even the most technologically sophisticated organisations aren't immune to cyberattacks. In 2023, Microsoft was hit with a nation-state sponsored attack, perpetuated by Russian hacking organisation Midnight Blizzard that wanted to use information harvested from corporate email systems to breach Microsoft's source code repositories and internal systems.[2] Johnson Controls, a leading electrical equipment supplier, received a $51 million ransomware demand from the Dark Angels after they claimed access to the company's private drives with over 27 terabytes of data.[3] At MGM Resorts, hackers stole personal data of over 10 million customers.[4]

Government assets are also a growing target. China-based hackers managed to get access to email accounts of employees of nearly two dozen organisations starting in May 2023, including the U.S. State and Commerce Departments. The breach was not discovered for three months.[5]

By 2025, cyberattacks are expected to cause $10.5 trillion worth of annual damage to enterprises and governments, a nearly 300% increase since 2015.[6] Annual global cybersecurity spending of $225 billion is insufficient to defend against these attacks and keep up with what will be dynamic changes in the technology landscape.[7]

One such change is the growing prominence of sophisticated generative AI models, which are particularly consequential to phishing and social engineering-based attacks. Large language models can take in information, whether real-time news and updates or personally identifiable information, and generate malicious links, emails, and spurious websites that appear increasingly realistic. As nearly 88% of all security breaches happen because of human error, generative AI can help hackers exploit human vulnerabilities to

access broader systems.[8] In 2022, cloud security leader Zscaler reported a 47% surge in phishing attacks enabled by AI.[9]

Moreover, unlike human hackers, AI agents are available 24x7, and they can be designed to monitor digital assets such as websites, tools, and systems for vulnerabilities. Due to their high uptime, AI agents that can attack and overwhelm websites is also a growing threat.[10] Another threat is the rising unmonitored access to online digital assistants, which could result in corporate employees sharing private information. Many large corporations have restricted access to these models until guardrails are in place.[11]

AI Could Also Help Fortify Cybersecurity

Primarily, AI can help with anomaly detection by scanning mundane enterprise traffic for deviations from the norm and surface those patterns quickly to human decision makers. These tools could be particularly effective for technologically less sophisticated businesses and businesses with small teams. AI can also help summarise cybersecurity alerts, breaches, and log data in simple language so engineers can get up to speed on IT issues. With understaffing in cyber jobs high, these simple systems can significantly boost productivity. Organisations can also use AI to perform penetration testing and craft scenarios that attempt to breach enterprise systems to determine weaknesses in networks.

The industry is responding swiftly to this dynamic AI-induced demand. In 2023, CrowdStrike, the leader in end-point security, launched Charlotte AI, which is designed to act as a low-level security analyst that can perform mundane operations.[12] The system features a tight feedback loop that includes insights from human operators, intrusion detectors, and incident response teams. The system is also designed to improve the intelligence that CrowdStrike tracks across more than 200 adversaries, learning their increasingly sophisticated tactics and breach techniques.

Similarly, Check Point launched a generative AI support and automation assistant called Infinity AI Copilot that automates operations, potentially being a solution for the global shortage of cybersecurity professionals.[13] Identity management services provider Okta launched a series of AI-specific tools to help with workforce and customer identity.[14] Palo Alto Networks, Zscaler, Fortinet, and nearly all other major cybersecurity vendors have plans to launch similar products.[15]

Large cloud vendors are also looking to expand their market share in cybersecurity by using AI. Available in April 2024, Microsoft Security for CoPilot will allow security and IT professionals to ask questions, assess threats, write code, and help with security and defence operations.[16] The model powering Security for CoPilot has been improved on over 78 trillion security signals that Microsoft processes each day.[17] The platform is expected to make experienced security professionals 22% faster and nearly 7% more accurate across analysis. Ninety-seven percent of security professionals who have used the platform cited interest in using it again.[18]

Last year, Google integrated generative AI across its threat intelligence and cybersecurity operations platform. Google will combine its Mandiant cyber intelligence offerings and its Chronicle security operations platform with its Vertex AI infrastructure solutions to create an AI system called Sec-PaLM, which will form the core of its AI-based security offerings.[19] Core to this system is software from Mandiant, which Google acquired in 2022.

AI Could Benefit Security Spending

Cybersecurity spending was forecasted to grow 10.6% in 2022 and 14.2% in 2023, despite the broader IT industry entering a slowdown.[20] This resilience signals the urgency and commitment to continue to build comprehensive defences, particularly with new threats likely to emerge with AI's proliferation. According to Global X forecast, annual security spending could top $450 billion by 2030.[21] Spending on artificial intelligence solutions for cybersecurity is expected to grow to $61 billion by 2028.[22]

Software-based spending seems to show unique resilience, given the predictable nature of the recurring revenue models that are common in cybersecurity. The industry is also migrating towards a consumption-based pricing model, which favours unit economics significantly.[23] Areas such as identity security, application security, penetration testing, end point security, zero-trust solutions, are expected to show tremendous momentum.

Also, it is believed that industrywide M&A (mergers and acquisitions) is poised for a comeback this year and likely to remain a trend, as large players continue to favour buying solutions from diversified vendors in an increasingly fragmented market.[24] Already in 2024, Zscaler acquired Avalor and CrowdStrike has announced it will acquire Flow Security, both of which were deals targeted at adding AI-first solutions in their portfolios.[25,26]

Conclusion: AI Could Be Fuel for Cybersecurity's Continued Growth

Generative AI poses new cybersecurity threats, but it's also helping companies create dynamic solutions that can thwart attacks. Major cybersecurity vendors are rapidly developing AI-powered tools to augment human analysts and automate security operations, and cloud providers are integrating generative AI into their cybersecurity stack. Despite economic headwinds, cybersecurity spending is projected to grow robustly, and industry consolidation is expected to continue as companies seek AI capabilities to enhance their product portfolios. These growth-oriented moves signal that there's an urgency to cybersecurity growth that investors may want to consider.

Footnotes

1. Gartner. (2023. September 28). Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024
2. Microsoft Security. (2024, March 08). Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard.
3. MSSPAlert. (2024, January 08). Top 10 Cyberattacks of 2023.
4. Ibid.
5. Ibid.
6. McKinsey. (2023, April 3). What is cybersecurity?
7. Gartner. (2023. September 28). Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.
8. CISOMAG. (2020, September 12). “Psychology of Human Error” Could Help Businesses Prevent Security Breaches.
9. Okta Blog. (2023, September 15). What the GenAI paradigm shift means for Identity.
10. New Scientist. (2024, February 24). GPT-4 developer tool can hack websites without human help.
11. CBS News. (2023, February 23). JPMorgan Chase bars employees from using ChatGPT.
12. CrowdStrike Blog. (2023, May 30). Introducing Charlotte AI, CrowdStrike’s Generative AI Security Analyst: Ushering in the Future of AI-Powered Cybersecurity.
13. Check Point Press Releases. (2024, Jan 30). Check Point Software Unveils Infinity AI Copilot: Transforming Cyber security with Intelligent GenAI Automation and Support.
14. Okta Blog. (2023, September 15). What the GenAI paradigm shift means for Identity.
15. Cybersecurity Dive. (2023, May 31). Palo Alto Networks teases plans for generative AI across security services.
16. Microsoft. (2024, March 13). Microsoft Copilot for Security is generally available on April 1, 2024, with new capabilities.
17. Ibid.
18. Ibid.
19. Google Cloud. (2023, August 29). New AI capabilities that can help address your security challenges.
20. Gartner. (2023. September 28). Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.
21. Global X Estimates with data derived from Gartner 2023, Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.
22. Markets and Markets. (2024, January 11). Artificial Intelligence in Cybersecurity.
23. Business Reporter (2024, August). Why usage-based models are the future of cyber-security.
24. CSO Online. (2024, April 12, Top Cybersecurity M&A deals for 2024.
25. Zscaler Blog. (2024, March 14). Zscaler acquires Avalor to unleash the power of enterprise security data with Avalor’s Data Fabric for Security™ to bring real-time AI-driven security insights and threat prevention.
26. CrowdStrike. (2024, March 5). CrowdStrike to Acquire Flow Security to Expand Its Cloud Security Leadership with Data Security Posture Management (DSPM).

The Global X UCITS ETFs are regulated by the Central Bank of Ireland.

This is a marketing communication.

Please refer to the relevant prospectus, supplement, and the Key Information Document ("KID") of the relevant UCITS ETFs before making any final investment decisions.

Investors should also refer to the section entitled "Risk Factors" in the relevant prospectus of the UCITS ETFs in advance of any investment decision for information on the risks associated with an investment in the UCITS ETFs, and for details on portfolio transparency. The relevant prospectus and KID for the UCITS ETFs are available in English at www.globalxetfs.eu/funds.

Investment in the UCITS ETFs concern the purchase of shares in the UCITS ETFs and not in a given underlying asset such as a building or shares of a company, as these are only the underlying assets that may be owned by the UCITS ETFs.

A UCITS ETF's shares purchased on the secondary market cannot usually be sold directly back to a UCITS ETF. Investors must buy and sell shares on a secondary market with the assistance of an intermediary (e.g. a stockbroker) and may incur fees for doing so. In addition, investors may pay more than the current net asset value when buying shares and may receive less than the current net asset value when selling them. Changes in exchange rates may have an adverse effect on the value price or income of the UCITS ETF.

Past performance of a UCITS ETF does not predict future returns. Future performance is subject to taxation which depends on the personal situation of each investor, and which may change in the future. Neither past experience nor the current situation are necessarily accurate guides to the future growth in value or rate of return of a UCITS ETF.

Investment may be subject to sudden and large falls in value, and, if it is the case, the investor could lose the total value of the initial investment. Income may fluctuate in accordance with market conditions and taxation arrangements. The difference at any one time between the sale and repurchase price of a share in the UCITS ETF means that the investment should be viewed as medium term to long term.

Any investment in a UCITS ETF may lead to a financial loss. The value of an investment can reduce as well as increase and, therefore, the return on the investment will be variable.

Global X ETFs ICAV is an open-ended Irish collective asset management vehicle issuing under the terms of its prospectus and relevant supplements as approved by the Central Bank of Ireland and is the issuer of certain of the ETFs where stated.

Global X ETFs ICAV II is an open-ended Irish collective asset management vehicle issuing under the terms of its prospectus and relevant supplements as approved by the Central Bank of Ireland and is the issuer of certain of the ETFs where stated.

Communications issued in the European Union relating to Global X UCITS ETFs are issued by Global X Management Company (Europe) Limited ("GXM Europe") acting in its capacity as management company of Global X ETFs ICAV. GXM Europe is authorised and regulated by the Central Bank of Ireland. GXM Europe is registered in Ireland with registration number 711633.

Communications issued in the United Kingdom and Switzerland relating to Global X UCITS ETFs are issued by Global X Management Company (UK) Limited ("GXM UK"), which is authorised and regulated by the Financial Conduct Authority. The registered office of GXM UK is 77 Coleman Street, London, EC2R 5BJ, UK. Information about GXM UK can be found on the Financial Services Register (register number 965081).

Information for Investors in Switzerland

This is an advertising document. The state of the origin of the fund is Ireland. In Switzerland, the representative is 1741 Fund Solutions AG, Burggraben 16, CH-9000 St.Gallen. The paying agent is Tellco Bank AG, Bahnhofstrasse 4, 6430 Schwyz.

The prospectus, the key information documents or the key investor information documents, the articles of association as well as the annual and semi-annual reports may be obtained free of charge from the representative.

Past performance is no indication of current or future performance. The performance data do not take account of the commissions and costs incurred on the issue and redemption of units.