

Cybersecurity should remain a top focus in 2023

Published 6 December 2022

Christopher Gannatti, CFA

Global Head of Research

As we move through the fourth quarter of 2022, it makes sense to start looking ahead at potential opportunities within the thematic equity space. 2022 has been a difficult year in terms of share price performance for many of these strategies but, if one can focus beyond the tough period of returns, there are various demand catalysts that remain on the horizon.

In our opinion, some of the best demand catalysts are becoming visible within cybersecurity.

WisdomTree's Thematic Universe analysis for the first 3 quarters of 2022

Even if we step back and think that the difficulties of the macro environment for growth investments for the first nine months of 2022 are well known, we can still track where investors were focused within a broad range of more than 40 distinct themes. Seeing the Top 5 and Bottom 5 themes in terms of flows can be quite telling¹:

Top 5 themes amongst European investors in ETFs by flows: first 9-months of 2022

- Sustainable Energy Production: \$1,525 million
- Equality & Diversity: \$883 million
- Cybersecurity: \$761 million
- Agriculture: \$682 million
- Semiconductors: \$277 million

Bottom 5 themes amongst European investors in ETFs by flows: first 9-months of 2022

- Robotics & Automation: -\$244 million
- Platforms: -\$162 million
- Digital Health: -\$156 million
- Sustainable Resource Management: -\$149 million
- Aging Population: -\$135 million

So, as we turn our focus back to the topic of cybersecurity, we can at least note that even in the face of very difficult share price performance, cybersecurity has been amongst the top inflow-gathering topics within WisdomTree's Thematic Universe of more than 40 distinct themes.

Attacks & incidents have not let up

In 2021, the Colonial Pipeline ransomware attack had a big impact on the eastern United States. However, hospitals have been another significant target over the course of the pandemic period. CommonSpirit Health, a hospital operator, disclosed an attack during October 2022.

The Federal Bureau of Investigation (FBI) tends to respond to many cyber attacks. Their Internet Crime Complaint Centre indicated it received a record 847,376 complaints during 2021, and the estimated potential losses could be in excess of \$6.9 billion³.

Chief Information Security Officers (CIOs) say they will increase their spending

Gartner, a consulting firm, publishes significant surveys on information technology topics over the course of a given year. In mid-October 2022, they released some conclusions from a survey of 2,200 respondents—their annual CIO survey. 66% of these respondents said they planned to increase their investment in cybersecurity⁴.

In fact, increasing investment in cybersecurity beat the topic of increasing investment in 'business intelligence and analytics', where 55% of the respondents said they would be increasing their investments⁵.

Gartner estimates that the total market size for information security and risk-management spending will be more than \$188 billion in 2023, which would represent a greater than 11% increase relative to the current year⁶.

How much of the budget goes to cyber?

This is a difficult question to answer, and it's always best if you can hear it directly from CIOs such that you see how they are addressing the challenges they face. The CIO of Kellogg Co., a packaged food manufacturer, indicated that safety and security represent about 15% of the total corporate information and technology spend⁷.

15% of the IT spend is probably at the higher end of the spectrum of large companies, but it very much depends on the industry under discussion. Financial services companies tend to make big investments in cybersecurity, whereas we would wish that utilities and essential infrastructure companies would spend more on cybersecurity.

There is a labour shortage in cybersecurity

It has been reported that the cybersecurity talent gap has grown by 26.2% in the past year, and that there could be around 3.4 million unfilled jobs worldwide. The regional breakdown indicates a particular shortage in the Asia Pacific region, with each region short by⁸:

- North America: 436,080

- Latin America: 515,879
- Europe, Middle East and Africa: 317,050
- Asia Pacific: 2,163,468

Companies are looking at all available options to fill in these roles. Some are investing in programs where more junior employees are trained into certain necessary skills. Other solutions could involve the better utilisation of software, machine learning and artificial intelligence. There is no singular 'quick fix', but cybersecurity is a notable growth area in employment that could persist throughout the 2020's.

Consolidation is a major trend amongst cybersecurity companies

As we have been studying the activities of cybersecurity companies, we have noticed customers wanting to maintain fewer individual tools across their cybersecurity stack. While every company could be unique, there are reports that the general Chief Information Security Officer (CISO) could be dealing with something like 70 different cybersecurity tools⁹.

There is a desire for the top tier solutions within the different technical domains (like end point protection, cloud security, email security to name a few) but there is also a risk associated with getting a large number of tools to work seamlessly together.

For the first nine months of 2022, we have seen about \$111.5 billion in merger and acquisition activity within the cybersecurity space. This compares to \$80.9 billion for the full year of 2021, indicating an acceleration. The 2022 figure has 203 individual deals behind it, whereas the 2021 figure had 293 individual deals behind it¹⁰.

Anyone watching the cybersecurity space has seen the activity of Thoma Bravo and Vista Equity Partners during 2022. Thoma Bravo has either announced or closed on ForgeRock (\$2.3 billion), Ping Identity Holding Corp. (\$2.8 billion) and SailPoint (\$6.9 billion) during 2022. The large cloud computing companies also tend to have cash on hand and could also do deals¹¹:

- Google Cloud's purchase of Mandiant at roughly \$5.4 billion was widely reported
- Microsoft, more quietly, acquired threat intelligence firm Miburo and cybersecurity company RiskIQ Inc.

The continually expanding attack surface means that the demand for cybersecurity innovation should remain insatiable, but whether customers get this from the individual providers, broader cybersecurity platforms that private equity player may be assembling, or seamlessly through their cloud computing relationships, remains to be seen.

Conclusion: an interesting theme for the next chapter of the macroeconomic cycle

The current chapter of the macroeconomic cycle, where many of the world's major central banks are focused on inflation and raising policy rates significantly at nearly every meeting, makes it difficult for cybersecurity company share prices to rise on a sustained basis. Many of the companies that we believe

are the most exciting are newer and growing quite quickly, but they may not yet be at a stage with robust positive earnings.

Growth companies focused on scaling their operations and focused more on reinvesting rather than drawing positive net income have not been favored in a high inflation, rising interest rate environment. However, we remind investors that the US Federal Reserve will not raise policy rates by 75 basis points forever, meeting by meeting, and that inflation will ultimately ease as it has in past cycles. When this time comes, we believe the lower valuations of many software-focused cybersecurity companies, relative to 2021 levels, combined with the view that cybersecurity is an essential business imperative, could be well-positioned. While we never know exactly what companies or services will do the best, it is fairly certain that attacks, hacks and risks will be important to guard against for the foreseeable future.

1 Sources: WisdomTree, Morningstar, Bloomberg. All data is as of 30 September 2022 based on WisdomTree's internal classification of thematic funds. As of 30 September 2022, this tracked 42 distinct themes.

2 Source: Rosenbush, Steven. "Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate." Wall Street Journal. 17 October 2022.

3 Source: Rosenbush, 17 October 2022.

4 Source: Rosenbush, 17 October 2022.

5 Source: Rosenbush, 17 October 2022.

6 Source: Rosenbush, 17 October 2022.

7 Source: Rosenbush, 17 October 2022.

8 Source: "(ISC)2 Cybersecurity Workforce Study." 2022. <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>

9 Source: Rundle, James. "Cyber M&A Expected to Remain Robust Into 2023." Wall Street Journal. 19 October 2022.

10 Source: Rundle, 19 October 2022.

11 Source: Rundle, 19 October 2022.

Related blogs

+ [In a bleak market for growth stocks, cybersecurity could be a future bright spot](#)

Related products

+ [WisdomTree Cybersecurity UCITS ETF - USD Acc \(WCBR/CYSE\)](#)

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.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

The application of regulations and tax laws can often lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.