

Cybersecurity Should Remain a Top Focus in 2023

Published October 31, 2022

Christopher Gannatti, CFA

Global Head of Research

As we move through the fourth quarter of 2022, it makes sense to start looking forward across the thematic equity space. The year has been a difficult one thus far 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 Three Quarters of 2022

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

Top 5 Themes among U.S. Investors in ETFs by Flows: First 9 Months of 2022

- Semiconductors: \$1,660 million
- China tech: \$1,526 million
- Cybersecurity: \$842 million
- Natural resources: \$752 million
- Agriculture: \$694 million

Bottom 5 Themes among U.S. Investors in ETFs by Flows: First 9 Months of 2022

- Cloud computing: -\$850 million
- Rise of the middle class: -\$809 million
- Next generation computing: -\$601 million
- Platforms: -\$569 million
- Sustainable energy production: -\$465 million

So, as we turn our focus back to the topic of cybersecurity, we note that even in the face of very difficult share price performance, cybersecurity has been among the top inflow-gathering topics of WisdomTree's thematic universe. We also point out that many of the newest cybersecurity companies have a Software-as-a-Service (SaaS) business model and take advantage of cloud computing infrastructure to deliver their services.

Cybersecurity was the third-largest asset gathering theme for the first nine months of 2022, while cloud computing was the WORST, in terms of having the most outflows, for that same period. It tells us that specific types of SaaS have been preferred to the broader cloud computing concept that looks at many distinct types of solutions, with cybersecurity one among many.

Attacks and Incidents Have Not Let Up

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

The Federal Bureau of Investigation (FBI) responds to many cybersecurity 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 billion.³

Chief Information Security Officers (CIOs) Say They Will Increase Spending

Gartner, a consulting firm, publishes significant surveys on information technology topics. In mid-October 2022, they released some conclusions from a survey of 2,200 respondents—their annual CIO survey. *Of these respondents, 66% said they planned to increase their investment in cybersecurity.*⁴

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 investments.⁵

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 year.⁶

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 so 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 total corporate information and technology spend.⁷

Kellogg's 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 wish that utilities and essential infrastructure companies would spend more.

There Is a Labor 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 by:

- North America: 436,080
- Latin American: 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 that train more junior employees in certain necessary skills. Other solutions could involve the better utilization of software, machine learning and artificial intelligence. There is no single 'quick fix,' but cybersecurity is a notable growth area in employment that could persist in the 2020s.

Consolidation Is a Major Trend Among Cybersecurity Companies

As we have been studying the activities of cybersecurity companies, we have noticed a pull on the customer side toward being able to maintain fewer individual tools across a 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 tools.⁹

There is a desire for the top tier solutions within the different technical domains—things 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 2021, indicating an acceleration. The 2022 figure has 203 individual deals behind it, whereas the 2021 figure involved 293 individual deals.¹⁰

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 deal¹¹:

- 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. It remains to be seen whether customers get this from the individual providers, broader cybersecurity platforms that private equity players may be assembling or seamlessly through their cloud computing relationships.

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 reinvesting rather than drawing positive net income have not been favored in high inflation, rising interest rate environments. However, we remind investors that the U.S. 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 best, it is fairly certain that it will be important to guard against attacks and hacks and risks for the foreseeable future.

The [WisdomTree Cybersecurity Fund \(WCBR\)](#) could be interesting to look at for those looking to gain exposure to the thesis of these essential types of solutions.

Christopher Gannatti is an employee of WisdomTree UK Limited, a European subsidiary of WisdomTree Asset Management Inc.'s parent company, WisdomTree Investments, Inc.

As of October 31, 2022, WCBR held 2.88% and 0% in ForgeRock and Microsoft, respectively. Google and Mandiant are subsidiaries of Alphabet. As of October 31, 2022, WCBR held 0% in Alphabet. Miboro and Risk IQ are subsidiaries of Microsoft. As of October 31, 2022, WCBR held 0% in Microsoft. Click [here](#) for a full list of Fund holdings.

1 Sources: WisdomTree, Morningstar, Bloomberg. All data as of 9/30/22, based on WisdomTree's internal classification of thematic funds. As of 9/30/22, this tracked 42 distinct themes.

2 Source: Steven Rosenbush, "Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate," *Wall Street Journal*, 10/17/22.

3 Source: Rosenbush, 10/17/22.

4 Source: Rosenbush, 10/17/22.

5 Source: Rosenbush, 10/17/22.

6 Source: Rosenbush, 10/17/22.

7 Source: Rosenbush, 10/17/22.

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

[search/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx](#)

9 Source: James Rundle, "Cyber M&A Expected to Remain Robust into 2023," *Wall Street Journal*, 10/19/22.

10 Source: Rundle, 10/19/22.

11 Source: Rundle, 10/19/22.

Important Risks Related to this Article

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 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 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.