In a Bleak Market for Growth Stocks, Cybersecurity Could Be a Future Bright Spot

Published October 10, 2022

Christopher Gannatti, CFA
Global Head of Research

Members from our WisdomTree team recently completed a roadshow across Milan, Geneva, Madrid, London and Paris, talking to investors about cybersecurity. WisdomTree features a broad range of thematic investment strategies, and there is often a partnership between a subject-matter expert and WisdomTree behind the specific topics. In this case, we had the opportunity to travel with Team8, the firm that provides data to properly classify the cybersecurity offerings of the underlying companies.

Attacks Continued as We Traveled

While we were on the trip, a breach of some of Uber's systems was widely publicized. While certainly not the only breach occurring globally during this period, the method was notable in that it repeatedly hit an employee with a two-factor authorization request until they accepted1. It goes to remind us all of an important truth in cybersecurity—usually, the simplest path into a system is through a person, especially if you can frazzle or frustrate the person.

Since we returned, there's been another notable article about what we'd consider a critical topic:

Brands Review Data Privacy Policies After $1.2 Million Sephora Settlement2

We were traveling in Europe, where every single investor was widely aware of the General Data Protection Regulation (GDPR). Many in the U.S. might think that the U.S. doesn't have any such laws, but the California Consumer Privacy Act was passed in 2018 and came into effect in 2020. On January 1, 2023, the California Privacy Rights Act, which expands and amends the prior law, could have many companies in for a rude awakening.

More than 100 public and private companies received letters from California Attorney General Rob Bonta as part of the sweep of large retailers that led to the Sephora settlement, and many more letters have gone out more recently.

Data protection is one of our critical cyber themes, and it's notable to see anything that widens the circle beyond GDPR in Europe.

Separate the Macro from the Megatrend

Many of the more innovative cybersecurity companies operate using the Software-as-a-Service (SaaS) business model that has been popularized in the cloud computing space. The key attribute of businesses operating this way lies in how the customers subscribe to a particular service for a period of time.

Successful SaaS businesses will tend to have “sticky” products, meaning that customers will subscribe and then not quickly turn around and cancel the subscription.

If we consider that the average retention for a particular product is 5–7 years, a SaaS business can do a few different things. One thing often discussed—having a net retention ratio above 100%. This means that customers are not only continuing the service—they are spending more on the service or possibly adding on different services from the company’s offering. Another thing often discussed regards the cost of customer acquisition. We tend to hear that “growth” is “all that matters.” Now, if it costs roughly one year of customer revenue to acquire a customer and the average tenure is 5–7 years, then it may make sense to spend that money on increasing growth. If the business is working, one can always turn down that spending in the future—hopefully with more customers—and have a more profitable business.

Our bottom-line view is that we have to remember that even if today’s narrative is all about profitability over growth, in the SaaS space, growth is still important. If one can look at the specifics of these underlying businesses, it is clear that there is a lot of underlying strength that could be stuck behind a current fog of being presently unprofitable.

Are Companies Going to Keep Spending?

It was relatively easy to convince the people with whom we spoke that everyone, be it companies or individuals, needs a cyber strategy.

A statistic widely discussed in the information technology and chief information security officer (CISO) space is that around 7%–10% of IT spending should be dedicated to cybersecurity3. This tells us simply that if we believe overall IT spending will grow over a given period, then cybersecurity spending should also increase in a similar fashion.

However, another angle on this discussion regards how different types of IT spending can toggle up and down at different times. From the evidence that we can see, it is clear that the threat environment as it relates to cybersecurity is quite high. CISOs at some of the largest companies in the world are aware of this and are responding accordingly. The thought is first and foremost on defense and protection and spending what is needed to take care of these needs. It is, therefore, the case, in an environment where we are watching, for example, the Russia/Ukraine crisis unfold, that cybersecurity budgets could increase more than general IT spending.

The Themes That Are the Future of Cybersecurity

WisdomTree focuses on seven key themes in cybersecurity that are believed to represent the most critical zones of focus for the future. It’s important to think not about what worked in cybersecurity in the past but rather to consider what will work in the future. These themes are:

1. Cloud Security
2. Smarter Security
3. Resilience and Recovery

4. Security of Things
5. Perimeterless World
6. Data Security
7. Shift-Left

One of the most fun parts of any cybersecurity discussion is looking at these themes and seeing how they touch the world in which we live. For instance, “Shift-Left” may sound like we forgot some words. However, it is a software development term, meaning that you think of security earlier in the software development process. This may be one way to mitigate the risk of unsecured code going out that could lead to “supply chain hacks,” like what we saw with Solar Winds a few years ago. These hacks are pernicious because the attacker gains access to a piece of software used by many customers.

Another aspect of the themes is that each might have its own specific timeline to it. Cloud security is continuing to grow fast, and it continues to be very necessary, but at a certain future point, everyone may have already “moved to the cloud.” Once everyone is in the cloud and properly configured, it may be the case that it’s time to focus elsewhere. Data security, on the only hand, could only be beginning if different countries outside of Europe start passing stronger data protection laws with real teeth to them. Frequently, it’s the potential for liability that drives changes in behavior.

Conclusion: Don’t Let Short-Term Performance Point You Away from Cybersecurity

2022 has been a difficult year for the performance of many Software-as-a-Service stocks, and those within cybersecurity have been no exception. In our opinion, the decreased valuations that we see now compared to one year ago could be a more interesting point of entry for anyone with a longer-term thesis on this important theme. If people are interested in a specific strategy that incorporates a focus on the specific themes mentioned in this piece, the WisdomTree Cybersecurity Fund (WCBR) could be worth a further look.

1 Source: Davey Winder, “Uber Hack Update: Was Sensitive User Data Stolen & Did 2FA Open Door To Hacker?,” Forbes, 9/18/22.
2 Source: Patrick Coffee, “Brands Review Data Privacy Policies After $1.2 Million Sephora Settlement,” Wall Street Journal, 9/27/22.
3 Source: Bob Violino, “How much should you spend on security?,” CSO, 8/20/19.

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

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.