IN A BLEAK MARKET FOR GROWTH STOCKS, CYBERSECURITY COULD BE A FUTURE BRIGHT SPOT

Christopher Gannatti – Global Head of Research, WisdomTree.
24 Oct 2022

We 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, for each theme, there is often a partnership between a subject-matter expert and WisdomTree. 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 travelled

While we were on the trip, a breach of some of Uber's systems was widely publicised. The method was particularly notable in that it repeatedly hit an employee with a two-factor authorisation request until they accepted[1]. 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 them.

Since then, there has been another noteworthy article: Brands Review Data Privacy Policies After $1.2 Million Sephora Settlement[2].

We were travelling in Europe, where every single investor was widely aware of the General Data Protection Regulation (GDPR). Many in the US might think that the US doesn't have any such laws, but the California Consumer Privacy Act was passed in 2018 and came into effect in 2020. On 1 January 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 since.

Data protection is one of our critical cyber themes, and it's significant 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 popularised 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 is having a net retention ratio above 100%. This means that customers are not only continuing the service, but 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 regularly hear that 'growth is all that matters'. Now, if it costs roughly 1-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, 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 that is widely discussed amongst the Information Technology and Chief Information Security Officer space is that around 7-10% of IT-spending should be dedicated to cybersecurity[3]. This tells us that, if we believe overall IT-spending will grow over a given period, then the cybersecurity spending should also increase in 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, the 'threat environment', as relates to cybersecurity, is quite high. CISOs at some of the largest companies in the world are aware of this, and they are responding accordingly. The thought is first and foremost on defense and protection and spending what is needed to take care of these areas. It is therefore the case that, in an environment where we are watching, for example, the Russia/Ukraine crisis unfold, 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 of 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 to 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 unsecure code going out that could lead to 'supply chain hacks', as 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, we may find that everyone has already 'moved to the cloud'. Once everyone is in the cloud and properly configured, it could be time to focus elsewhere. Data security, on the only hand, might only be beginning if different countries outside of Europe start passing stronger data protection laws. Frequently, it's the potential for liability that drives changes in behaviour.

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 relative to one year ago could be a more interesting point of entry for anyone with a longer-term thesis on this important theme.

Sources

[1] Source: Winder, Davey. "Uber Hack Update: Was Sensitive User Data Stolen & Did 2FA Open Door To Hacker?" Forbes. 18 September 2022.

[2] Source: Coffee, Patrick. "Brands Review Data Privacy Policies After $1.2 Million Sephora Settlement." Wall Street Journal. 27 September 2022.

[3] Source: Violino, Bob. "How much should you spend on security?" CSO. 20 August 2019.

Related blogs

+ Central bank policy has catalysed a valuation opportunity in the software space
+ Why has the Ukraine war put a spotlight on cybersecurity and the energy transition?

Related products

+ WisdomTree Cybersecurity UCITS ETF – USD Acc (WCBR/CYSE)

View the online version of this article here.

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.