Cybersecurity has never been this important…but 2022 returns may be challenged

Published 19 January 2022

Christopher Gannatti, CFA
Global Head of Research

As we begin 2022, the initial case has been clear: cutting edge tech companies that have exhibited strong revenue growth but that might have low or even negative net income have been challenged. Many cybersecurity companies that are focused on the future—things like cloud security rather than on premise security, for instance—have been no exception.

However, many of us would also recall that 2021 was a year of some major hacks, like the Colonial Pipeline, and it would be difficult to imagine any business today of any size with zero spending on or investment in cybersecurity.

There are few megatrends like cybersecurity in this sense: with artificial intelligence (AI), for example, there may be many reasons to use it or many benefits to be derived, but it's still a choice. Not doing anything in cybersecurity really isn't a choice anymore, so it's more a question of the specific services to use and specific companies to work with.

Massive Growth Potential

It is estimated that in 2020, spending on cloud computing, specifically infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) was $106.4 billion, expected to grow to $217.7 billion by 20231.

Now, cloud workloads need to be protected—but how much spending is estimated on the cybersecurity element? In 2020, it was roughly $1.2 billion, and in 2023, it is estimated to be $2.0 billion. That means that in 2023, it's possible that spending on cloud security will be less than 1% of spending on cloud services2.

It is estimated that 'security spend' should be closer to a figure between 5 and 10% of a given information technology budget. This means it would be more reasonable to see a figure of $12.4 billion of spending on cloud security in 2023, which would be a magnitude of growth of about 10x relative to the aforementioned estimate for the 2020 spending3. There is no guarantee that spending would ever reach this level, but the concept that firms need to take the topic more seriously is clearly being discussed.

What's More Expensive—Dealing with a Cybersecurity Issue or Spending on Preventative Efforts?

This is one of the critical questions in cybersecurity, because if it is less expensive to just deal with issues after they occur, there would be no market for preventative measures. Towards the end of December 2021, we saw one example of a company needing to settle a particular case4:

- A hacker stole the personal data of more than 100 million people in 2019 from Capital One and its cloud services provider, Amazon Web Services, in 2019.
- Capital One agreed, in 2021, to pay $190 million to settle a class action lawsuit filed by these customers.
- In 2020, Capital One agreed to pay $80 million to settle regulators' claims that it lacked proper cybersecurity procedures as it began to use cloud storage technology.

The settlements make the headlines, but think of the costs of time, the costs of legal fees, the turnover in certain employees that may happen…while it may never be possible to have 100% protection from all hackers, the case is clear for a focus on preventative measures.

Governments are Taking Action

The government angle on cybersecurity seems to have, at least presently, two major avenues in:

1. **Data protection:** Citizens have become much more aware of their data being used and stored in different ways they may not realise and governments want to take action to 'protect' people's personal data when and where possible.
2. **Infrastructure protection:** The Colonial pipeline, which led to many difficulties for consumers to get gasoline in May 2021 up and down the eastern seaboard of the US

In July 2021, the US Senate confirmed Chris Inglis as the first national cyber director. In May 2021, President Biden issued an executive order that dramatically shifted the general regulatory stance, which had formerly been much more voluntary and hands-off5.

Conclusion: The Demand for Cybersecurity Solutions should be Relatively Constant

We must remember that certain trends are already in place that may not be very sensitive to changes in interest rate policy. One is a shift from 'on-premise' hardware to cloud computing, where many companies can realise efficiencies and cost benefits. These shifts require different, updated security packages, and they are expected to continue through 2022. The key risk, as we see it, is that many cloud-focused cybersecurity companies delivered unbelievable share price returns in recent years and these firms may see their valuations adjust as interest rates rise—even if their revenue growth continues. Thinking beyond simply the returns of 2022 could be important when thinking about the cybersecurity megatrend.

1 Source: Crowdstrike Corporate Overview, December 2021 version, using International Data Corporation Estimates.

2 Source: Crowdstrike, December 2021.

3 Source: Crowdstrike, December 2021.

4 Source for Bullets: Nguyen, Lananh. "Capital One Settles a Class-Action Lawsuit for $190 Million in a 2019 Hacking." The New York Times. 23 December 2021.

5 Source: Rundle, James. “Companies Face Stricter Cyber Rules in 2022.” Wall Street Journal. 3 January 2022.

Related blogs

+ Cybersecurity is Hot—but did it ever cool off?

+ Cybersecurity is national security

+ If you use a Computer, You’ve Gotta think about Ransomware…

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 oer for sale nor a solicitation of an oer 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 aer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can oen lead to a number of dierent 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 aer 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 oering 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 ailiate, nor any of their respective oicers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.