A Rational Perspective on Global Cybersecurity

Published June 7, 2021

Jeremy Schwartz, CFA
Global Chief Investment Officer

On a recent Behind the Markets podcast, I spoke with an expert panel on cybersecurity that gave listeners a rational perspective on the recent cyberattacks gaining significant global publicity. The panel included:

- Bob Blakley, Operating Partner at Team8
- Brian Dunphy, Vice President of Product Management at Claroty
- David Yates, Chief Information Officer at WisdomTree

Our podcasts usually have an organizing principle or catalyst. In this case, it was the Colonial Pipeline ransomware attack. We wanted listeners to have a better understanding of what occurred and whether companies can mitigate their risk of these types of events. However, another attack occurred last week on the exact date of the recording—the group responsible for the SolarWinds hack in early 2020 struck again.

The SolarWinds attack was particularly notable because the attackers were able to latch onto an access mechanism, in this case the widely spread SolarWinds software, that users would trust without question. The latest effort used emails from the USAID domain to gain the trust of users so that they would be more likely to click on malicious links.

Bob noted that once these groups find an avenue of attack that infiltrates the target's security systems, they will likely continue to try that tactic.

Our discussion went into detail about what the panelists knew of the Colonial Pipeline ransomware attack. It was emphasized that the company contacted law enforcement very quickly, as well as Mandiant, an expert in cybersecurity and ransomware. These attacks require immediate involvement of experts and law enforcement when they occur.

Colonial was also very focused on mitigating the spread of the attack. Frequently, attackers focus on gaining access to a system through IT services and structures. Even if they manage to infiltrate, it is not guaranteed that they will also have access to all the target company's industrial control systems. In the past, these systems were not even connected. But with modernization, they are becoming more connected, which helps with efficiency and usability. This might pose security challenges.

Criminal enterprises are doing their homework to figure out where they should apply their ransomware tactics. DarkSide is the group publicized as being behind the Colonial Pipeline event, but in fact, DarkSide provides a sort of a 'malware platform.' Customers, in this case, criminal enterprises, use the malware for

their specific purposes after doing their research on possible victims. They want to structure the attack in a way that maximizes the chance of receiving a payment, and they want to ensure that the entity being attacked has the resources to pay.

The rise of cryptocurrency raised an interesting line of thinking—does its mere existence encourage these types of attacks? When bitcoin was starting out, it was thought that transactions using bitcoin were anonymous. The more precise way to frame this, given that the bitcoin blockchain is publicly viewable, is that bitcoin transactions are difficult to track quickly, but that they most certainly should not be viewed as completely anonymous. Other cryptocurrencies may provide better anonymity than bitcoin.

At WisdomTree, we are always focusing on how investors—if they believe in a theme—might structure a thesis that could align with a given topic or megatrend. The panel considered that if investors are seeking companies providing solutions that could help with ransomware attacks, themes they might focus on could include ‘resilience and recovery,’ ‘smarter security’ or ‘the Internet of Things.’ WisdomTree has worked with Team8 on publicizing these themes in prior blog posts.

This was a fantastic and very timely discussion on a big topic. Please listen below.

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.