Authored by:

Jon Maier

Date: 4/22/2022
Topic: Conversational Alpha

Conversational Alpha: Cybersecurity from Nice to Have to an Essential Technology

In today's digital world, data is gold, and more malicious actors are trying to get their hands on the prize. Just recently, two heavyweight technology companies provided customer data to hackers disguised as law enforcement officials proving that their cyber defenses are not as robust as they should be.[1] This raised concerns, which were exacerbated by the cyberwarfare component of Putin's attack on Ukraine, putting nerves on edge as individuals, companies, and governments consider who may be lurking within their networks. In response, the Biden administration warned companies of potentially higher levels of cybercrime related to Western-imposed sanctions and tense geopolitical relationships.[2] In this environment, no one can escape cyber attacks, but they can work to prevent them. As a result, we expect cybersecurity spending to continue to increase and cybersecurity companies to attract investor interest due to their recurring revenue model. In our view, these factors, along with the Cybersecurity theme's ability to help manage geopolitical risk in a portfolio make this exposure essential.

Key Takeaways

- We expect public and private action plans that assist in preventing cybercrime to increase in scope and result in greater sustained spending on cybersecurity. A leading research company predicts global cybersecurity spending to exceed $1.75 trillion, cumulatively, between 2021 and 2025.[3]
- The Biden Administration has increased their message of urgency to U.S. businesses regarding the need to protect against cyber-attacks which have impacts on governments, government contractors, and private businesses alike. The downstream implication is likely more spending on cybersecurity.
- Exposure to the Cybersecurity theme brings the defensiveness of consistent recurring revenue and the growth potential associated with public and private sector responses to increasingly sophisticated cybercriminal behavior.

The SolarWinds Hack Was a Call to Action

The Solar Winds hack discovered in December 2020 was a pivotal moment for cybersecurity. This hack is believed to be the work of the Russian Foreign Intelligence Service. For background, about 100 companies and a dozen government agencies were compromised, including the U.S. Treasury, Justice, and Energy departments, as well as the Pentagon.[4] The attack was a wake-up call on how invasive and widespread the implications can be, especially when attackers compromise highly-utilized software. The Biden administration understands the need to modernize cybersecurity defenses and update security requirements for organizations that contract with the US Government.[5] In light of Russian aggression into Ukraine, the Biden Administration increased their message of urgency to U.S. businesses regarding the need to protect against cyber-attacks. The downstream implications will likely be more spending on cybersecurity.

And Then There Was War and More Spending on Cybersecurity

Recent cybersecurity threats targeting Ukrainian banks and government departments bring the Cybersecurity theme to the frontlines of war. To help defend Ukraine from cyberattacks, the European Union provided a cyber rapid-response team comprised of experts from Lithuania, Croatia, Poland, Estonia, Romania, and the Netherlands. The private sector is lending a helpful hand as well. Just before Putin's invasion, Microsoft's Threat Intelligence Center identified unusual activity aimed at Ukraine's government departments and financial institutions and quickly became involved in disclosing it.[6] Alphabet has also been key in preventing cyber-attacks in Ukraine.[7]

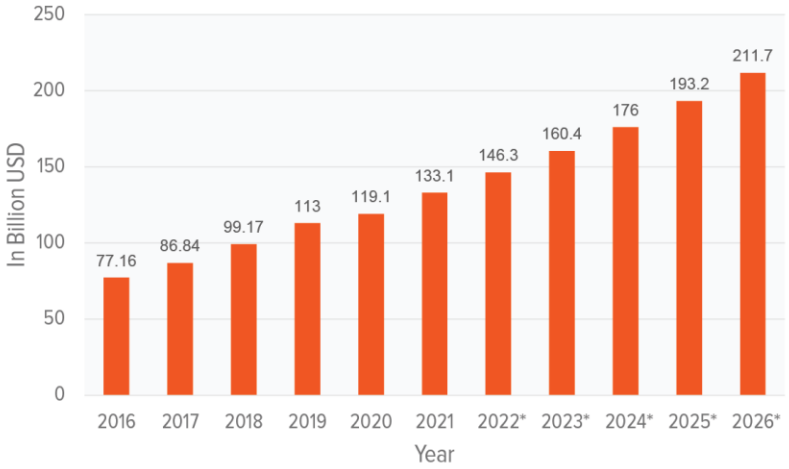
These responses resemble the public and private action plans started by the Biden Administration to secure the electricity, pipeline, and water sectors in the United States, and to use governmental authority to mandate new cybersecurity and network defense measures.[8] The administration's goal of modernizing cyber defenses also includes continued cooperation with numerous international allies and partners to thwart ransomware strikes and publicly attribute cybercriminal activity.[9]

The close coordination of the Technology sector with Ukraine's government, the EU, and the North Atlantic Treaty Organization (NATO) is unprecedented in its scope and pace. The response speaks to the advancement of cyber technology and the critical role it plays in the global economy. We expect efforts like these to continue and likely increase spending on cybersecurity, as cybercrime is a persistent risk.

Cybersecurity Could Be a High Growth Opportunity

The war in Ukraine and the geopolitical machinations associated draw further attention to the importance of strong cyber defense. Executive orders and the White House's new cybersecurity strategy will likely increase adoption, particularly when there are plans for government oversight and rules mandating minimum standards.[10] We believe that shifting cybersecurity from a voluntary investment into a regulated investment necessary to do business is likely to increase rapid adoption in the U.S., Europe, and elsewhere.[11] Absolute protection of data is aspirational given the direct trade-off between data security and accessibility, but cybersecurity spending, which will likely continue to grow can mitigate risks, and this theme should be considered for a broader portfolio.

GLOBAL CYBERSECURITY REVENUE
Source: Statista data as of March 2022



Year	Growth Rate
2017	12.55%
2018	14.20%
2019	13.95%
2020	5.40%
2021	11.75%
2022*	9.92%
2023*	9.64%
2024*	9.73%
2025*	9.77%
2026*	9.58%

*Predicted data
Note: Data shown does not yet reflect market impacts of Russia-Ukraine war.

A Cybersecurity ETF May Add Resiliency to a Portfolio

Cybersecurity technologies work to proactively shield against possible attacks while mitigating and repairing the damage from incidents that already occurred. Increased occurrence and severity of cyberattacks demonstrates the permanent need for cybersecurity spending. For cybersecurity companies, this increasingly critical need creates a business model that generates robust recurring revenue. As a result, by investing at the broader level of this theme, investors can diversify their exposure across companies because the factors spurring adoption are unlikely to wane anytime soon.

It is always difficult to pick the winner in any sector or theme. While detailed information is required to effectively pick an individual company that could beat the market, investing in a theme could lead investors

towards an ETF, where one can diversify their risk. Since cybersecurity stocks can move up on price performance following the announcement of large-scale hacks, or down if an application developer falls victim to a large breach, an ETF could be a good, diversified solution.

Footnotes:

[1] White House FACT SHEET: Act Now to Protect Against Potential Cyberattacks, 3/21/2022
[2] White House FACT SHEET: Act Now to Protect Against Potential Cyberattacks, 3/21/2022
[3] Cybersecurity Ventures, Global Cybersecurity Spending to Exceed $1.75 Trillion From 2021-2025, 9/10/2021
[4] NPR, A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, 4/16/21
[5] NPR, A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, 4/16/21
[6] Cybersecurity & Infrastructure Security Agency, Destructive Malware Targeting Organizations in Ukraine, 3/1/2022
[7] Chamber Business News, As threats grow, experts assess government and private sector preparation for cyberattacks, March 24, 2022
[8] NYT, As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War, 2/28/2022
[9] CSIS, A Shared Responsibility: Public-Private Cooperation for Cybersecurity, 3/22/2022
[10] MIT Technology Review, Inside the plan to fix America's never-ending cybersecurity failures, 18 March 2022
[11] Reuters, EU proposes cybersecurity rules for EU bodies amid cybersecurity worries, 22 March 2022