Cybersecurity is More Essential Than Ever

Ryan O. Issakainen, CFA | Senior Vice President | ETF Strategist

Thesis: The COVID-19 crisis has shed new light on our understanding of "essential" products and services. As thousands of people have begun to work remotely for the first time, the importance of a well-functioning and secure internet ecosystem has been viscerally reinforced. In the near-term, we expect spending on cybersecurity to remain resilient as working remotely has become the lifeblood of many companies. Longer-term, we believe the critical importance of cybersecurity will spur continued investment by companies and government agencies seeking to avoid potential disruptions in the future.

The critical importance of cybersecurity has been reinforced over the past few weeks, as an increasing share of the workforce has been made to work remotely in response to the COVID-19 crisis. As we imagine events that could cause our predicament to quickly go from bad to worse, cyberthreats are high on the list. While many areas of the economy have ground to a halt, our ability to communicate and conduct business online has been an important positive factor that shouldn't be overlooked.

Unfortunately, cybercriminals recognize the potential vulnerability of online systems when organizations are under stress, and view these as opportunities. For example, the World Health Organization (WHO), the US Centers for Disease Control and Prevention (CDC), and the US Department of Health and Human Services (HHS) have all been targeted by hackers in recent weeks as they focused on responding to the COVID-19 crisis.[1,2,3] A report issued on March 25, 2020 from FireEye Inc. claimed that the company had detected a spike in hacking activity beginning on January 20th, which represented "one of the broadest campaigns by a Chinese cyber espionage actor we have observed in recent years."[4]

Employees that don't normally work remotely may be especially vulnerable, so many companies are taking necessary precautions. Cisco Systems reported a tenfold increase in requests for cybersecurity support from companies with remote workforces over the past few weeks.[5]

Last month in our ETF Newsletter, *Inside First Trust ETFs*, we laid out a longer-term case for the cybersecurity theme. We suggested that the global economy's increasing dependence on the internet, the growing threat from cybercriminals, and the heightened global regulatory environment regarding data privacy may lead to robust increases in cybersecurity spending in the years ahead. We also suggested that cybersecurity spending could be less susceptible to cyclical slowdowns than other technology spending. While we did not envision the current state of affairs, we believe incentives remain strong for cybersecurity spending to be resilient in this environment. Moreover, as the global economy emerges from the COVID-19 crisis, we believe cybersecurity will be viewed by companies, government agencies, and individuals as more essential than ever.

[1]Source: Bloomberg. "*Hackers Posing as CDC, WHO Using Coronavirus in Phishing Attacks*"
[2]Source: Bloomberg. "*Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak*"
[3]Source: *Reuters*. "*Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike*"
[4]Source: *Reuters*. "*U.S. cybersecurity experts see recent spike in Chinese digital espionage*"
[5]Source: *Reuters*. "*Mass move to work from home in coronavirus crisis creates opening for hackers: cyber experts*"