The Cyber threat is real, and Cybersecurity is investible.

written by Dean Bristow | October 28, 2021

Back in May of this year the world was reminded of how much of a threat cyberattacks or hacking play in our daily lives. You often hear stories about an individual or a company that suffers a ransomware attack and has to cough up gift cards or cryptocurrency as payment, or, perhaps, your personal information was stolen from someone's database putting you at risk of identity theft and other types of fraud, all of which are bad. However, the Colonial Pipeline hack had much greater ramifications on a large swath of the U.S. This time it wasn't the loss of information or merely the cost of the ransom (which wasn't particularly outrageous at approximately $4.4 million worth of bitcoin at the time) that was the worrying part, but the fact that a critical piece of U.S. infrastructure was basically brought to its knees by a foreign interest.

The Colonial Pipeline carries gasoline, diesel and jet fuel from Texas to as far away as New York. About 45% of all fuel consumed on the East Coast arrives via the pipeline system and life got pretty crazy, pretty quickly for over 25% of Americans. Things got so bad that President Joe Biden declared a state of emergency on May 9 followed by Georgia Governor Brian Kemp the following day. American Airlines changed flight schedules temporarily due to fuel shortages at the main airport in Charlotte, NC, while fuel shortages began to occur at gas stations amid panic buying in Alabama, Florida, Georgia, North Carolina, and South Carolina. Granted this wasn't life threatening for the most part given that the outage was relatively short lived, it, the outage, nevertheless shone a giant spotlight on the importance of cybersecurity, especially

in light of what other critical infrastructures could be hacked or incapacitated.

Without digressing into whether this was ultimately state sponsored activity, or simply for profit, as the alleged hackers claimed, it exposed a weakness that is rife within both the private and the public sectors. It even exposed a threat to your personal safety and wellbeing when you think about whether the system or utility that provides your household with heat in the winter or AC in the heat of summer were to become incapacitated. I'm sure we've all seen, or at least heard of, videos of an autonomous car that gets hacked and you lose control of the gas or brake pedal. Technology has become ingrained in our day-to-day lives, likely even more so than you realize, and I'm pretty sure we're only going to get more dependent on it in the future.

Now that I've done my best to scare the pants off everyone, what is the investment thesis here? I hope it's pretty obvious that cybersecurity is where this is headed. Despite the fact that many publicly traded cybersecurity stocks have seen pretty impressive returns over the last 12 months, I firmly believe we are still in the early innings of this trade. There are still hundreds, if not thousands, of connected entities around the world that don't have adequate protection from the threats of those with malicious intents. Granted many likely believe they are fine with what they have. In fact, I'm sure Colonial Pipeline thought they were covered. But as more and more events like this happen around the world and companies, governments and everyone else in between realizes there is value to protecting their systems, you know the revenue generation capacity of those who are good at providing cybersecurity will continue to grow.

Unfortunately, I don't know the best way to invest in this sector. As a big Formula 1 fan, I thought if the Ferrari team was willing to entrust all their data with Kaspersky then that

would be good enough for me, but Kaspersky isn't currently publicly traded. So I went back to the drawing board. The largest cybersecurity ETF based on assets under management is the First Trust NASDAQ Cybersecurity ETF (NASDAQ: CIBR), which is up 55% over the last year. The fund is described as focusing on cybersecurity companies, as so classified by the Consumer Technology Association, which means CIBR holdings are primarily software and networking companies. Top holdings include Accenture (NYSE: ACN) and Cisco Systems (NASDAQ: CSCO), which aren't exactly pure play cybersecurity equities but its other holdings include Okta (NASDAQ: OKTA), Cloudflare (NYSE: NET), and Zscaler (NASDAQ: ZS). The second largest ETF, the ETFMG Prime Cyber Security ETF (NYSE ARCA: HACK), splits the industry into 2 segments: (1), developers of cybersecurity hardware or software, and (2), providers of cybersecurity services. Here you find many of the same names in HACK as in the top 10 holdings of CIBR including Tenable Holdings (NASDAQ: TENB) and Splunk (NASDAQ: SPLK).

But if you want more of a pure play on this sector, I like either the Global X Cybersecurity ETF (NASDAQ: BUG) or iShare Cybersecurity and Tech ETF (NYSE ARCA: IHAK), both of which select holdings based on revenue, which must be at least 50% generated from cybersecurity activities. If you want to go one step further and invest in an individual equity then a look at the top holdings of these two ETFs, cross referenced with the two big ones mentioned above allows you to cull the list to Palo Alto Networks (NYSE: PANW) and CrowdStrike Holdings (NASDAQ: CRWD), which are top 10 holdings in all four of these ETFs. Its not only that all of these ETFs hold the above two mentioned equities, and likely many more. I simply focused on the funds' biggest holdings, which often drive the majority of an ETF's returns. Regardless, make sure you protect your data as best you can, because today there is always someone out to get it, which

is also why everyone should be able to profit from owning at least some of these ETFs or some of the most popular of their holdings.