Long-Term Outlook for Cybersecurity Remains Compelling

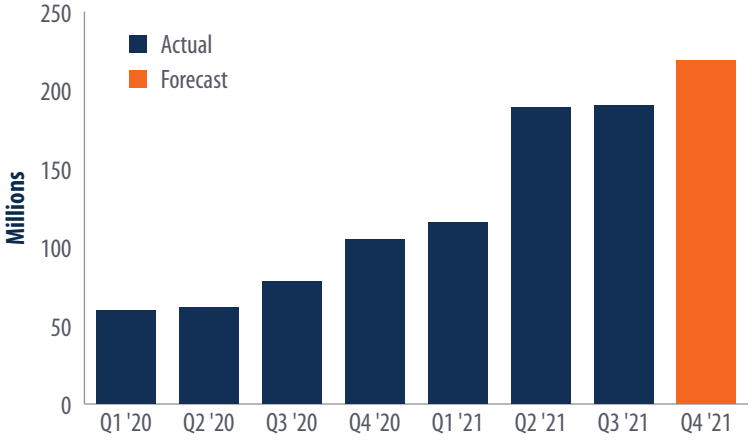
Ryan O. Issakainen, CFA | Senior Vice President | ETF Strategist **Andrew Hull** | Vice President | ETF Strategist

Cybercrime has been one of the most prominent storylines throughout 2021, with several highly publicized cyberattacks. These were not limited to high-tech industries. They included targets such as a critical oil pipeline in the southeastern U.S., a meatpacking plant in Minnesota, a chain of grocery stores in the U.K., gas stations in Iran, and many others. As the world becomes more digital, and many hackers face few deterrents to stepping up their efforts, we believe cybercrime is poised for robust growth in the years ahead. Consequently, while cybersecurity stocks faced bouts of volatility in 2021, we believe this theme is also well positioned for long-term secular growth, as companies, individuals, and government agencies seek to boost their defenses against such threats.

Cybercrime Risks Remain Elevated

Ransomware attacks, in which hackers use software to lock down servers and networks until a ransom is paid, have been prolific in 2021. Through the third quarter of this year, researchers from SonicWall identified 495.1 million global ransomware attacks, a 148% increase compared to last year[1]. The windfall hackers have received from such attacks helps to explain this rise. According to the Treasury Department, ransomware victims paid a record $590 million to cybercriminals during the first six months of 2021[2]. Unfortunately, these lucrative payouts provide strong incentives for hackers—many of whom operate from antagonistic foreign jurisdictions—to conduct future attacks.

Quarterly Global Ransomware Attacks



Source: SonicWall.

A Digital World Needs Robust Cybersecurity

As the global economy continues to reopen from restrictions related to the COVID-19 pandemic, many digital connectivity trends, such as e-commerce, remote work, and distance learning are proving more durable than expected. According to Gallup, 67% of U.S. employees in white collar jobs were still working remotely in some capacity in September[3]. Many colleges and schools continued to offer remote or hybrid instruction in the fall of 2021. Online transactions also continued to grow, as e-commerce sales in Q3 2021 were 42% higher than Q4 2019, the last quarter that was unaffected by the pandemic[4]. In our view, the ongoing popularity of these trends will likely be accompanied by a heightened demand for cybersecurity solutions. But digital connectivity—supported by cloud computing, 5G mobile networks, the internet-of-things, and many other technological advances—continues to grow more pervasive in nearly all industries. As the world grows more digitally connected, the need to provide comprehensive cybersecurity solutions should extend far beyond the pandemic, in our opinion.

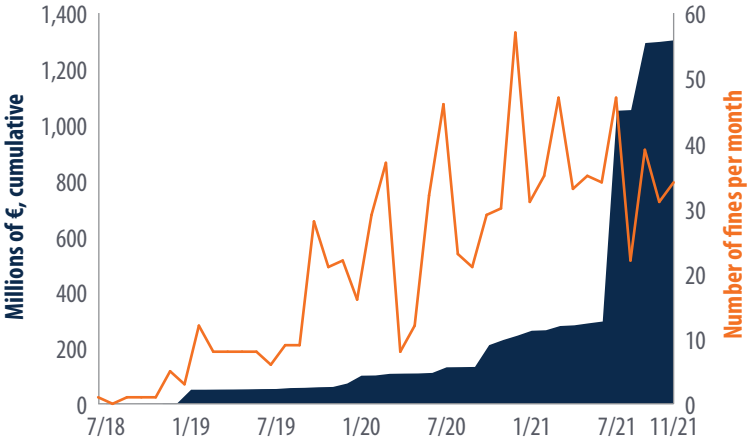
Public Spending on Cybersecurity Poised to Grow

After numerous high-profile hacks, cybersecurity and data privacy remain a priority for government officials around the world. In the U.S., the proposed federal budget for fiscal year 2022 includes $10.4 billion in new cybersecurity spending by the Department of Defense[5], and an additional $9.8 billion in funding to secure Federal civilian networks[6]. The Infrastructure Investment and Jobs Act, signed into law in November 2021, allocates nearly $2 billion in additional cybersecurity and related spending, including $1 billion earmarked for state and local governments[7]. Elsewhere, the U.K.'s new National Cyber Strategy, launched in December, includes £2.6 billion to strengthen the country's cyber ecosystem and resilience to cyberattacks[8]. Leaders in the EU also recently adopted a new plan with €269 million in new funding to build up cybersecurity equipment, tools, and infrastructure[9].

Regulatory Pressure to Require Robust Cybersecurity

Governments around the world have also stepped up regulatory pressure on companies' adherence to cybersecurity standards. For example, failure to comply with the General Data Protection Regulation (GDPR), a sweeping data privacy law that went into effect in Europe in 2018, has led to several significant enforcement actions, such as a €746 million fine imposed on Amazon in July 2021[10] and a €225 million fine imposed on WhatsApp in September 2021[11]. Such fines are also becoming more frequent. Through the first eleven months of 2021, there were 37% more GDPR fines issued than during the same period in 2020, according to Enforcement Tracker. While some fines have been appealed and may be reduced in the months ahead, regulatory pressure provides another strong incentive for companies around the world to guard against cyberattacks.

GDPR Fines



Source: Enforcement Tracker. As of 11/30/21.

[1] SonicWall, *SonicWall: 'The Year of Ransomware' Continues with Unprecedented Late-Summer Surge*, 10/28/21.

[2] U.S. Treasury Financial Crimes Enforcement Network, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021*.

[3] Gallup, *Remote Work Persisting and Trending Permanent*, 10/13/21.

[4] Federal Reserve Bank of St. Louis, *E-Commerce Retail Sales*, 11/18/21.

[5] U.S. Department of Defense, *Defense Budget Overview: Fiscal Year 2022 Budget Request*, May 2021.

[6] The White House, *Budget of the U.S. Government: Fiscal Year 2022*.

[7] CyberScoop, *Biden signs infrastructure bill that provides nearly $2 billion for cybersecurity*, 11/15/21.

[8] IT Pro, *UK unveils £2.6 billion National Cyber Strategy*, 12/15/21.

[9] European Commission, *Commission to invest nearly €2 billion from the Digital Europe Programme to advance on the digital transition*, 11/10/21.

[10] Bloomberg, *Amazon Gets Record $888 Million EU Fine Over Data Violations*, 7/30/21.

[11] BBC, *WhatsApp issued second-largest GDPR fine of €225m*, 9/2/21.

Long-Term Outlook for Cybersecurity Remains Compelling

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

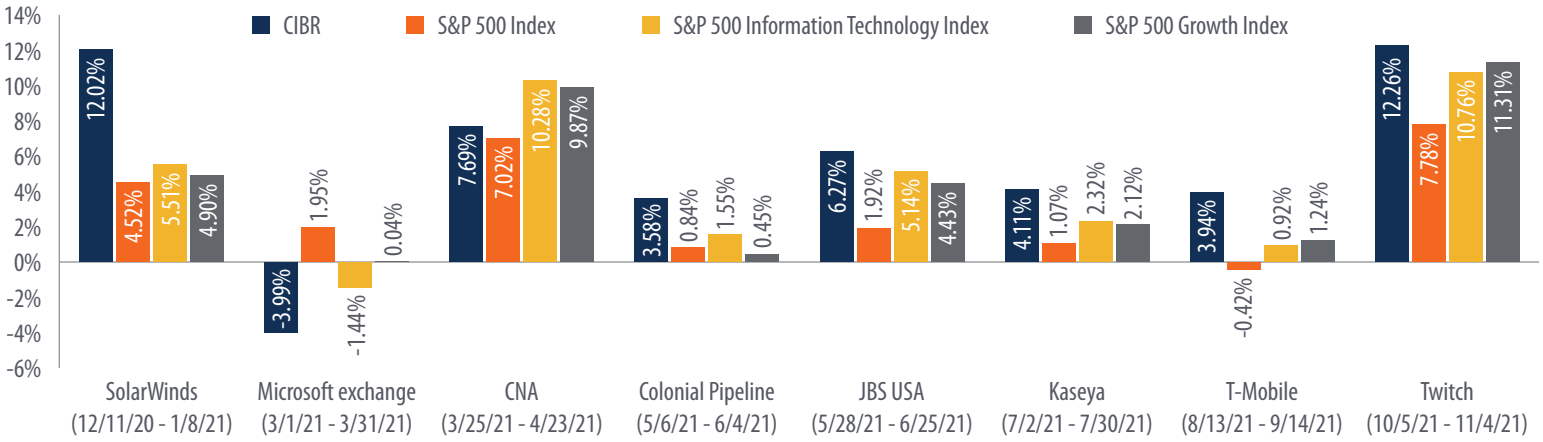
Cybersecurity Failures as a Potential Catalyst for CIBR Returns

The First Trust Nasdaq Cybersecurity ETF (CIBR) has often generated relatively strong performance following the announcement of high-profile cybersecurity breaches. While such failures may initially be viewed in a negative light, we believe positive performance for cybersecurity stocks in the days that follow may be related to a recognition that such public failures may induce more spending on cybersecurity. The chart below shows several examples from the past 12 months, including the SolarWinds hack announced last December, the Colonial Pipeline and JBS USA attacks announced in May, and the Kaseya attack announced in July, among others. For the month following each of these announcements, CIBR mostly produced relatively strong returns compared to the S&P 500 Index, the S&P 500 Growth Index, and the S&P 500 Information Technology Index. While cyberattacks are an undesirable drag on the economy, they may be meaningful catalysts for cybersecurity stocks.

While many investors in cybersecurity have enjoyed solid returns over the last several years, we continue to have a positive long-term outlook for this theme. As the global economy becomes ever more digitally connected, hackers are motivated to increase the quantity and sophistication of their attacks, while potential targets are incentivized to spend whatever it takes to prevent them. Together, we believe this may be a potent recipe for robust earnings growth for cybersecurity stocks in the years ahead.

CIBR vs. Index Returns

1 Month Total Returns After Notable Hacks Announced



Source: Bloomberg. Notable hacks are based on the number of search results after the hack as well as Google Trends data.

Performance Summary (%) as of 12/31/21	1 Year	5 Year	Since Fund Inception
CIBR Performance*			
Net Asset Value (NAV)	19.61	22.71	16.89
Market Price	19.49	22.62	16.89
Index Performance**			
Nasdaq CTA Cybersecurity Index™	20.40	23.56	17.73
S&P Composite 1500 Information Technology Index	33.76	31.35	26.79
S&P 500 Index	28.71	18.47	15.93

Performance data quoted represents past performance. Past performance is not a guarantee of future results and current performance may be higher or lower than performance quoted. Investment returns and principal value will fluctuate and shares when sold or redeemed, may be worth more or less than their original cost. You can obtain performance information which is current through the most recent month-end by visiting www.ftportfolios.com.

Inception date 7/6/2015. Expense Ratio: 0.60%.

*__NAV__ returns are based on the fund's net asset value which represents the fund's net assets (assets less liabilities) divided by the fund's outstanding shares. **Market Price** returns are determined by using the midpoint of the national best bid offer price ("NBBO") as of the time that the fund's NAV is calculated. Returns are average annualized total returns.

__Performance information for the Nasdaq CTA Cybersecurity Index™ is for illustrative purposes only and does not represent actual fund performance.__ Indexes do not charge management fees or brokerage expenses, and no such fees or expenses were deducted from the performance shown. Indexes are unmanaged and an investor cannot invest directly in an index. The **S&P Composite 1500 Information Technology Index is a capitalization weighted index of companies classified by GICS as information technology within the S&P Composite 1500 Index. The **S&P 500 Index** is an unmanaged index of 500 stocks used to measure large-cap U.S. stock market performance.

Long-Term Outlook for Cybersecurity Remains Compelling

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

You should consider a fund's investment objectives, risks, and charges and expenses carefully before investing. Contact First Trust Portfolios L.P. at 1-800-621-1675 or visit www.ftportfolios.com to obtain a prospectus or summary prospectus which contains this and other information about a fund. The prospectus or summary prospectus should be read carefully before investing.

Risk Considerations

A fund's return may not match the return of its underlying index. A fund invests in securities included in the index regardless of investment merit and the securities held by a fund will generally not be bought or sold in response to market fluctuations.

Investors buying or selling fund shares on the secondary market may incur customary brokerage commissions. Market prices may differ to some degree from the net asset value of the shares. Investors who sell fund shares may receive less than the share's net asset value. Shares may be sold throughout the day on the exchange through any brokerage account. However, unlike mutual funds, shares may only be redeemed directly from a fund by authorized participants in very large creation/redemption units. If a fund's authorized participants are unable to proceed with creation/redemption orders and no other authorized participant is able to step forward to create or redeem, fund shares may trade at a discount to a fund's net asset value and possibly face delisting.

A fund's shares will change in value, and you could lose money by investing in a fund. One of the principal risks of investing in a fund is market risk. Market risk is the risk that a particular stock owned by a fund, fund shares or stocks in general may fall in value. There can be no assurance that a fund's investment objective will be achieved. The outbreak of the respiratory disease designated as COVID-19 in December 2019 has caused significant volatility and declines in global financial markets, which have caused losses for investors. While the development of vaccines has slowed the spread of the virus and allowed for the resumption of "reasonably" normal business activity in the United States, many countries continue to impose lockdown measures in an attempt to slow the spread. Additionally, there is no guarantee that vaccines will be effective against emerging variants of the disease.

Changes in currency exchange rates and the relative value of non-U.S. currencies may affect the value of a fund's investments and the value of a fund's shares.

Information technology companies and cybersecurity companies are generally subject to the risks of rapidly changing technologies, short product life cycles, fierce competition, aggressive pricing and reduced profit margins, loss of patent, copyright and trademark protections, cyclical market patterns, evolving industry standards and frequent new product introductions. Cybersecurity companies may also be smaller and less experienced companies, with limited product lines, markets, qualified personnel or financial resources.

As the use of Internet technology has become more prevalent in the course of business, funds have become more susceptible to potential operational risks through breaches in cyber security.

Depositary receipts may be less liquid than the underlying shares in their primary trading market.

A fund may be a constituent of one or more indices which could greatly affect a fund's trading activity, size and volatility.

There is no assurance that the index provider or its agents will compile or maintain the index accurately.

A fund classified as "non-diversified" may invest a relatively high percentage of its assets in a limited number of issuers. As a result, a fund may be more susceptible to a single adverse economic or regulatory occurrence affecting one or more of these issuers, experience increased volatility and be highly concentrated in certain issuers.

Securities of non-U.S. issuers are subject to additional risks, including currency fluctuations, political risks, withholding, the lack of adequate financial information, and exchange control restrictions impacting non-U.S. issuers.

A fund and a fund's advisor may seek to reduce various operational risks through controls and procedures, but it is not possible to completely protect against such risks.

High portfolio turnover may result in higher levels of transaction costs and may generate greater tax liabilities for shareholders.

A fund with significant exposure to a single asset class, country, region, industry, or sector may be more affected by an adverse economic or political development than a broadly diversified fund.

Securities of small- and mid-capitalization companies may experience greater price volatility and be less liquid than larger, more established companies.

Trading on the exchange may be halted due to market conditions or other reasons. There can be no assurance that the requirements to maintain the listing of a fund on the exchange will continue to be met or be unchanged.

First Trust Advisors L.P. is the adviser to the fund. First Trust Advisors L.P. is an affiliate of First Trust Portfolios L.P., the fund's distributor.

The information presented is not intended to constitute an investment recommendation for, or advice to, any specific person. By providing this information, First Trust is not undertaking to give advice in any fiduciary capacity within the meaning of ERISA, the Internal Revenue Code or any other regulatory framework. Financial professionals are responsible for evaluating investment risks independently and for exercising independent judgment in determining whether investments are appropriate for their clients.

Not FDIC Insured | Not Bank Guaranteed | May Lose Value