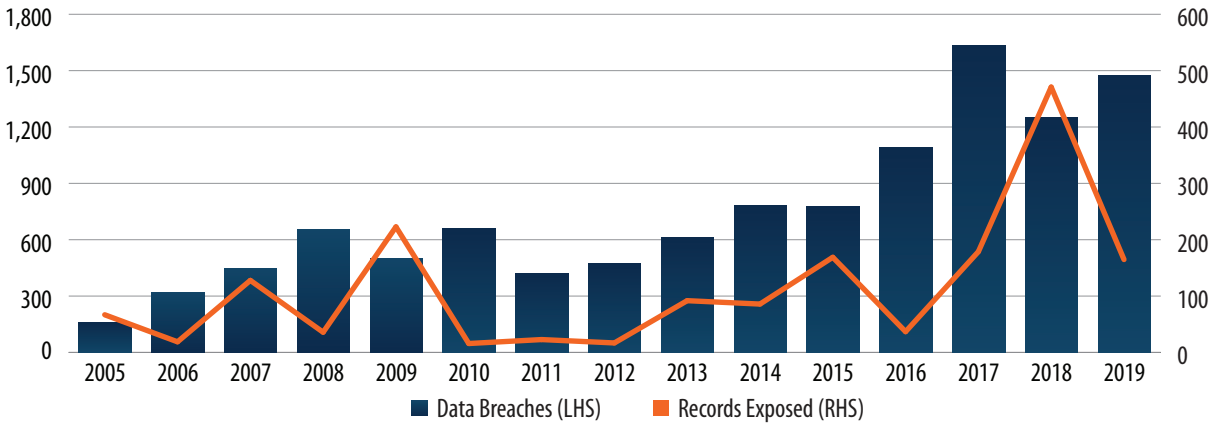
Cybersecurity Comes to the Forefront in 2020

Author:

Ryan O. Issakainen, CFA
Senior Vice President
Exchange Traded Fund Strategist
First Trust Advisors L.P.

Cybersecurity has been garnering more attention of late, as escalating geopolitical tensions have renewed concerns about cyberattacks from foreign nation-states. Yet the threat of cyberattacks is nothing new, and many organizations have made significant investments in cybersecurity in recent years. According to Gartner, cybersecurity spending stood at an estimated $124 billion in 2019.[1] Regardless of how geopolitical events unfold, we expect several important catalysts to remain drivers of growth for the cybersecurity industry throughout 2020 and beyond.

Chart 1: US Data Breaches and Records Exposed (2005 - 2019)



Source: Identity Theft Resource Center, CyberScout and Statista.

The Cybercrime Threat

Data on cybercrime indicates that organizations are facing an unprecedented level of cyberattacks. Last year, there were nearly 1,500 publicly reported data breaches and 165 million records exposed in the US alone.[2] The cost of cybercrime is likely growing as well. Cybersecurity Ventures estimates that cybercrime damages—including damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm—will cost up to $6 trillion annually by 2021, up from $3 trillion annually in 2015.[3]

Hackers also appear to be targeting the business sector more frequently, where a successful hack can result in access to potentially thousands of sensitive records. Through the first nine months of 2019, the business sector accounted for 66% of all reported breaches.[4] Faced with these dynamic and increasingly sophisticated threats, organizations today require robust and up-to-date cybersecurity.

Global connectivity trends are likely to entice hackers to continue looking for ways to exploit weaknesses in cybersecurity defenses going forward. The "Internet of Things," or ecosystem of devices connected to the internet, is expected to grow 21% in 2020,[5] and the number of people using the internet could grow to 6 billion worldwide by 2022.[6] While we believe such technological advancements are positive for living standards and future innovation, more internet users, connected devices, and data stored in the cloud also provides almost limitless opportunities for hackers seeking ways to gain unauthorized access to sensitive information.

Changing Regulatory Environment

In response to several high-profile data breaches, governments and regulators around the world are implementing new laws concerning data privacy and cybersecurity. One of the most important and far-reaching is the European Union's General Data Protection Regulation, or GDPR, which unified privacy laws across EU countries and applies to any company that collects the personal data of EU citizens. Among other provisions, GDPR gives citizens more rights over how and when companies use their personal information, and adds strict timelines for reporting data breaches to regulators. In order to maintain GDPR compliance, organizations around the world are committing immense manpower,[7] and spending billions of dollars.[8]

The EU isn't alone in enacting new data privacy regulations. Countries such as Brazil, Japan, and Thailand have also passed similar laws in recent years.[9] Thirty-one US states enacted cybersecurity-related legislation in 2019, typified by the California Consumer Privacy Act, or CCPA, which went into effect January 1, 2020. While no federal legislation like GDPR has yet been enacted in the US, six separate cybersecurity bills were passed by either the US House or Senate last year,[10] and support appears to be growing for comprehensive federal legislation.[11]

First Trust

Past performance is not a guarantee of future results and there is no assurance that the events or improvements mentioned herein will continue.

Throughout 2019, regulators handed down huge fines and penalties for noncompliance with these new regulations. In July 2019, European regulators fined British Airways £183.4 million and Marriott Hotels £99.2 million for noncompliance with GDPR.[12] In the US, the Federal Trade Commission fined both Equifax ($575 million) and Facebook ($5 billion) after large data breaches.[13] In our opinion, these onerous penalties provide significant incentives for organizations to remain compliant with new data privacy regulations.

Increasing Cybersecurity Spending

Faced with the threat of cyberattacks and stringent new data privacy laws, organizations around the world have little choice but to increase their cybersecurity defenses, in our opinion. Estimates are that worldwide cybersecurity spending will more than double from 2019 levels by 2024, rising to over $300 billion.[14] Moreover, given the growing sophistication and persistence of cybercriminals, we expect cybersecurity spending to be less susceptible to cyclical slowdowns than other forms of technology spending.

Investing in Cybersecurity

The First Trust Nasdaq Cybersecurity ETF (CIBR) tracks an index of companies that may benefit from these trends. The underlying index methodology includes companies classified by the Consumer Technology Association (CTA) as cybersecurity companies. These firms are involved in aiding organizations build, implement, and manage their security protocols. As of 12/31/2019, the portfolio included 42 companies from the information technology and industrial sectors, weighted by liquidity. CIBR's underlying index methodology also incorporates three robust liquidity screens to ensure larger allocations to the fund do not unnecessarily impact the price of the underlying securities.

Importantly, ETF investors don't have much unintentional exposure to the cybersecurity theme, as CIBR holdings made up just 1.7% of the S&P Total Market Index, as of 12/31/19. As the global economy grows more digitally interconnected, we believe the potential growth of the cybersecurity industry provides an intriguing opportunity for those seeking alpha.

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.

ETF Characteristics

The fund lists and principally trades its shares on The Nasdaq Stock Market LLC.

The fund's return may not match the return of the Nasdaq CTA Cybersecurity Index℠. Securities held by the 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 the fund by authorized participants, in very large creation/redemption units. If the 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 the fund's net asset value and possibly face delisting.

Risk Considerations

The fund's shares will change in value, and you could lose money by investing in the fund. One of the principal risks of investing in the fund is market risk. Market risk is the risk that a particular stock owned by the fund, fund shares or stocks in general may fall in value. There can be no assurance that the fund's investment objective will be achieved.

The fund may invest in small capitalization and mid capitalization companies. Such companies may experience greater price volatility than larger, more established companies.

An investment in a fund containing securities of non-U.S. issuers is 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. These risks may be heightened for securities of companies located in, or with significant operations in, emerging market countries. The fund may invest in depositary receipts which may be less liquid than the underlying shares in their primary trading market.

The fund may hold investments that are denominated in non-U.S. currencies, or in securities that provide exposure to such currencies, currency exchange rates or interest rates denominated in such currencies. Changes in currency exchange rates and the relative value of non-U.S. currencies will affect the value of the fund's investment and the value of fund 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.

The fund is classified as "non-diversified" and may invest a relatively high percentage of its assets in a limited number of issuers. As a result, the 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.

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 advisors are responsible for evaluating investment risks independently and for exercising independent judgment in determining whether investments are appropriate for their clients.

[1]Source: Gartner, Inc. *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*.
[2]Source: Identity Theft Resource Center. *2019 End-of-Year Data Breach Report.*
[3]Source: Cybersecurity Ventures. *Cybersecurity Ventures Official Annual Cybercrime Report*.
[4]Source: Risk Based Security, Inc. *Data Breach QuickView Report 2019 Q3 Trends*.
[5]Source: Gartner, Inc. *Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020*.
[6]Source: Cybersecurity Ventures. *Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion*.
[7]Source: Microsoft. *Microsoft's commitment to GDPR, privacy and putting customers in control of their own data*.
[8]Source: International Association of Privacy Professionals. *Global 500 companies to spend $7.8B on GDPR compliance*.
[9]Source: comforte. *6 Countries with GDPR-like Data Privacy Laws*.
[10]Source: NCSL. *Cybersecurity Legislation 2019*.
[11]Source: United States Government Accountability Office. *Internet Privacy.*
[12]Source: Information Commissioner's Office (ICO).
[13]Source: Federal Trade Commission (FTC).
[14]Source: Global Market Insights. *Global Cyber Security Market Size worth $300bn by 2024.*

This material is not intended to be relied upon as investment advice or recommendations.

Not FDIC Insured • Not Bank Guaranteed • May Lose Value