WELLS FARGO
Investment Institute

FIRST ANALYSIS
Institute Alert

News or events that may affect your investments

March 24, 2022

Douglas Beath
Global Investment Strategist
Wells Fargo Investment Institute

Tom Christopher
Equity Sector Analyst
Global Securities Research
Wells Fargo Advisors

Chris Haverland, CFA
Global Equity Strategist

Dorian Jamison
Senior Municipal Analyst
Global Securities Research
Wells Fargo Advisors

Ken Johnson, CFA
Investment Strategy Analyst
Wells Fargo Investment Institute

Justin Lenarcic
Senior Wealth Investment Solutions Analyst
Wells Fargo Investment Institute

Jim Sweetman
Head of Global Alternative Investments
Wells Fargo Investment Institute

Heightened cyberthreat may drive new corporate spending

Key takeaways

- Global Investment Strategy (GIS) sees a rising trend in information system hacking and other forms of cyberattacks.
- Cybersecurity spending is likely to broaden to industries that have not spent heavily on cybersecurity in the past.

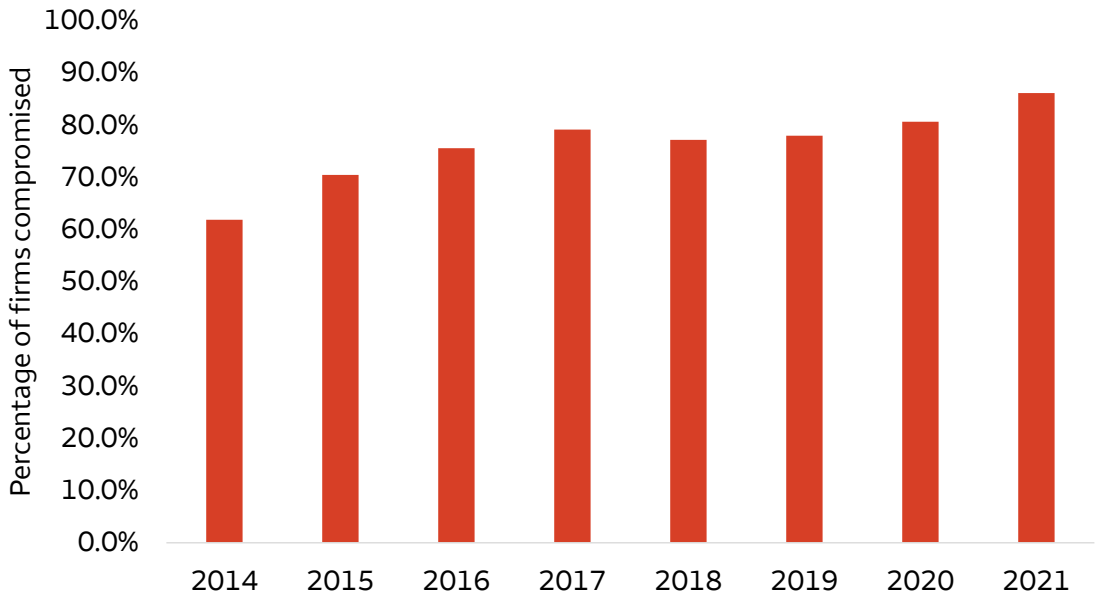
What it may mean for investors

- GIS preference for U.S. Large Cap over Small Cap companies and for the Information Technology sector aligns with an increase in cybersecurity spending across the U.S. Many cybersecurity firms are well positioned in our view, to benefit from our expectations for rising demand created by the elevated threat of cyberattacks. Finally, highly rated municipal bonds of critical-service infrastructure systems appear more resilient than smaller regional systems.

"I am convinced that there are only two types of companies: those that have been hacked, and those that will be." – Robert Mueller, former FBI Director, in a March 2012 speech

Just before the Russian invasion, Ukraine reported a cyberattack that took down four of its government websites. These events underscore a trend toward a rise in hacking and other forms of cyberattacks (see Chart 1). The trend has raised the profile of cyberattacks as an economic risk and as a potential investment opportunity. Cybersecurity protects systems, networks, and programs from myriad digital attacks that attempt to access, change, or destroy information; extort money from users; or interrupt normal business processes.

Chart 1. Percentage of organizations compromised by at least one successful cyberattack



Source: CyberEdge 2021 Cyberthreat Defense Report and Wells Fargo Investment Institute.

To meet this challenge, the cybersecurity industry has adapted and may grow its global market size to reach $345.4 billion by 2026.[1] Worldwide spending on information security and related services is expected to reach $150 billion this year, up 12% from a year ago, according to the research company Gartner. We believe that understanding the core cybersecurity threats that companies face, as well as the industries and sectors at the center of the ongoing battle, should be an important consideration for investors.

There are four main types of cybersecurity threats:

1. *Phishing* is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. This is the most common type of cyber-attack.

2. *Ransomware* is a type of malicious software designed to extort money by blocking access to files or the computer system until the ransom is paid.

3. *Malware* is a type of software designed to gain unauthorized access or to cause damage to a computer.

4. *Social engineering* is a tactic used to trick a system owner into revealing sensitive information. The hoax can solicit a payment or gain access to a user's confidential data.

Additionally, cyberattacks generally fall under three main categories:

1. *eCrime*, is a financially motivated criminal intrusion activity.

2. *Targeted state-sponsored intrusion* includes cyberespionage, state-nexus destruction attacks, and generating currency to support a regime.

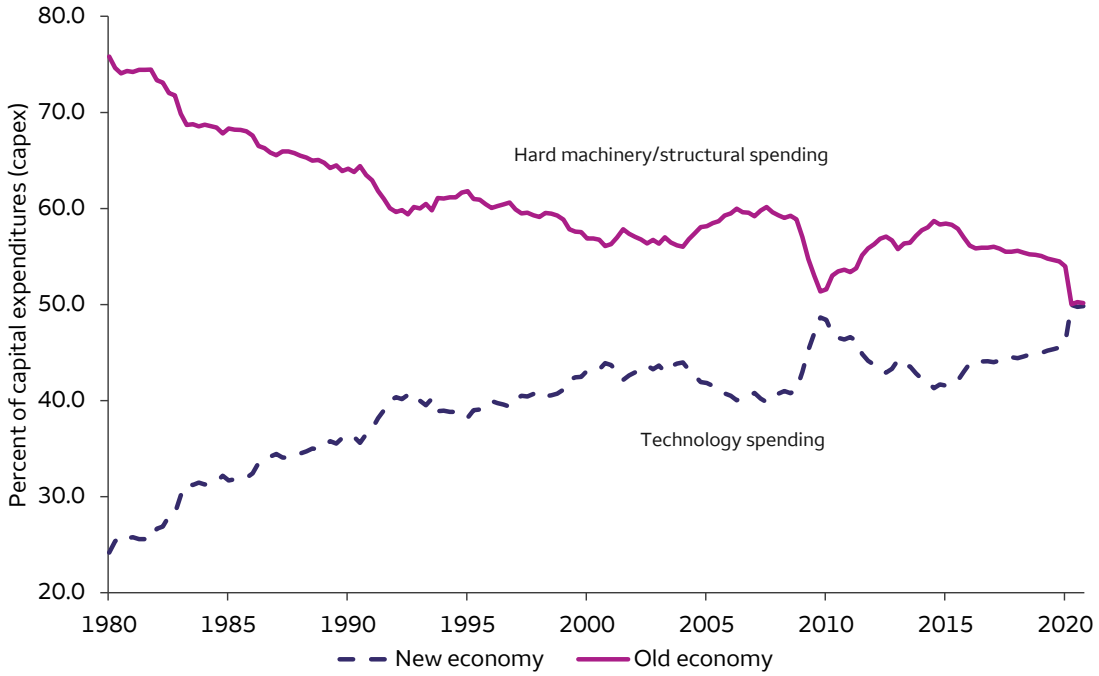
3. *Hacktivist intrusion* is undertaken to gain momentum, visibility, or publicity for a cause or ideology.

1. Statista. "The History of cybersecurity," Cyber Magazine, October 2021.

Addressing the cybersecurity challenge: Analysis from Global Investment Strategy (GIS)

Information Technology (IT) security spending has grown sharply. In the U.S., the percentage of capital spending on technology surpassed traditional hard machinery and structural capital spending for the first time in 2020 (Chart 2). While larger companies are vulnerable to cyberattacks, many have ramped up spending on cybersecurity and should have better resources to handle an attack. Smaller companies have been cyberattack targets more frequently and have fewer resources to spend when it comes to strengthening information technology security and dealing with the potential fallout from an attack.

Chart 2. Technology spending continues to grow



Source: Bureau of Economic Analysis – U.S. Department of Commerce and Wells Fargo Investment Institute. Data as of June 30, 2020. Technology spending = sum of software, information processing equipment, and research & development spending divided by total non-residential capex. Hard machinery/structural spending = sum of transportation equipment, industrial equipment, and structures divided by total non-residential capital expenditures.

Investment implications at the asset-class and sector level: Some of our current tactical (6- to 18-month) preferences align with the patterns in risk and spending. In particular, we favor U.S. Large Cap over Small Cap companies, which GIS believes aligns with the comparatively greater exposure of smaller companies to cyberattacks. Moreover, we believe that the IT sector is a clear beneficiary of increased cybersecurity spending. As security threats grow, companies are likely to allocate a larger portion of their capital spending budgets to fortifying IT infrastructure. We see this as a key growth area in the IT sector and maintain our favorable tactical guidance.

Fighting the good fight: Equity analysis from Global Securities Research (GSR)

Some of the most targeted industries for cyberattacks include financial services, technology/telecom, education, health care, government agencies, and energy, primarily a result of the sensitive information they possess and their control of and access to critical infrastructure. Consequently, these industries have historically been at the top of the list for annual cybersecurity spending. GSR suspects that recent alerts from multiple U.S. agencies (FBI, National Security Agency, Cybersecurity and Infrastructure Security Agency) have led to increased demand for cyberdefense products and solutions, including multi-factor authentication (technology requiring multiple pieces of evidence before granting access), zero-trust principles (a strict identity verification architecture within a network),

and endpoint protection and monitoring. (technology that secures end-user devices, such as laptops and smartphones)[2] GSR believes demand is also likely broadening out to industries that historically have not invested large amounts of capital into defending their environment, including manufacturing, utilities, transportation, and construction.

Often overlooked is operational technology, which connects, monitors, and secures industrial assets and equipment. Operational technology integrates hardware and software with network connections to control essential processes. These systems increasingly connect to an enterprise's IT infrastructure, and this rising integration between IT and operational technology systems means that any disruption could snowball and affect multiple industries. For example, the primary target in the Colonial Pipeline ransomware cyberattack in 2021 was the billing infrastructure, not the actual pumping systems. The attackers targeted the electrical equipment that manages and monitors the flow of product moving through the pipeline. However, the breach forced the pipeline to be shut-down out of concern that additional points along the pipeline would be vulnerable.

Investment implications at the sub-industry level: GSR believes the initial reaction to the war in Ukraine likely will lift the cybersecurity industry as a whole. Many cybersecurity firms are well-positioned, in our view, to benefit from expectations for rising demand created by the elevated threat of cyberattacks. Although an increase of cyberthreats is likely to lift all ships, we believe the cybersecurity firms most likely to benefit are those with a focus on enhanced monitoring capabilities, advanced threat intelligence, incident response, and security-breach remediation solutions to protect mission-critical points along the infrastructure.

Protecting our infrastructure: Municipal analysis from Global Securities Research (GSR)

Even before the war in Ukraine, the threat of cyberattacks to critical U.S. infrastructure was on the rise, and as a result, municipal bond issuers in the infrastructure sector will likely have to invest in better protections. As a recent example, in January, the Port of Los Angeles launched the Cyber Resilience Center to protect both port administration systems and the shipping companies that operate there. The development of the center came after cyberattacks in 2017 and 2018 struck some of the largest shipping companies. In October 2021, Moody's Investors Service affirmed the Aa2 rating of the Port of Los Angeles with a stable outlook based on the port's significant competitive advantages, which includes excellent physical infrastructure.

According to the Cybersecurity and Infrastructure Security Agency (CISA), more than 90% of the volume of overseas trade enters or leaves the U.S. by ship. In order to operate efficiently, maritime facilities use IT and operational technology systems for various functions, including communication, equipment operation, cargo tracking, and business operations. Compromise of these systems could lead to disruptions of port operations and related supply chains, resulting in financial losses. Previous cyberattacks have resulted in facilities being partially or completely offline, resulting in significant business losses.

Other critical infrastructure systems also have been targeted in recent years. Amid the coronavirus pandemic, cyberattacks struck 560 healthcare facilities in 2020, including Universal Health Services, which operates about 400 hospitals nationwide.. In April and June 2021, the New York Metropolitan Transportation Authority (MTA), the nation's largest transit system, experienced ransomware attacks. CISA issued recommendations for fixes and patches, which the MTA implemented using its 24-hour protocol, limiting the impact to three of its 18 different systems. According to the MTA, there was no evidence of compromise to its operational systems or employee or customer information.

In recent years, rating agencies have begun to view cybersecurity matters as a key governance matter, which is a factor in their credit analysis. Given the current focus on cybersecurity, we believe state and local government issuers will face additional demands to harden their defenses against potential cyberattacks. Some of the initial

2. CISA is the U.S. Cybersecurity and Infrastructure Security Agency.

funding for cybersecurity improvements may come from the $1.2 trillion Infrastructure Investment and Jobs Act which includes: $110 billion in new spending for roads and bridges,; $73 billion for electric grid upgrades; $66 billion for rail and Amtrak; $65 billion for broadband expansion; $55 billion for clean drinking water; $39 billion for public transit; $25 billion for airport; and $17 billion for ports.

Investment implications at the municipal bond level: In general, while not completely immune, highly rated municipal bonds of infrastructure systems that provide a critical service and possess monopolistic control over large service areas should continue to be more resilient against cybersecurity threats compared to smaller regional systems. Specific subsectors such as airports, seaports, and toll roads are also better positioned to receive attention and (most importantly) cybersecurity funding, due to their economic and commercial importance.

Large international gateway airports and ports with diverse cargo and business lines have already had to address the growing threat of cyberattacks in recent years. As of March 22, 2022, The S&P Municipal Bond Infrastructure Index has returned -3.6% over the last twelve months, slightly underperforming the S&P Municipal Bond Index, which has returned -2.3%. However, credit spreads remain wide compared to pre-pandemic levels, which suggests the municipal infrastructure sector still has room to outperform.

Risks Considerations

Each asset class has its own risk and return characteristics. The level of risk associated with a particular investment or asset class generally correlates with the level of return the investment or asset class might achieve. **Stock markets**, especially foreign markets, are volatile. Stock values may fluctuate in response to general economic and market conditions, the prospects of individual companies, and industry sectors. **Foreign investing** has additional risks including those associated with currency fluctuation, political and economic instability, and different accounting standards. These risks are heightened in emerging markets. **Small- and mid-cap stocks** are generally more volatile, subject to greater risks and are less liquid than large company stocks. **Bonds** are subject to market, interest rate, price, credit/default, liquidity, inflation and other risks. Prices tend to be inversely affected by changes in interest rates. **High yield (junk) bonds** have lower credit ratings and are subject to greater risk of default and greater principal risk. **Municipal bonds** offer interest payments exempt from federal taxes, and potentially state and local income taxes. Municipal bonds are subject to credit risk and potentially the Alternative Minimum Tax (AMT). Quality varies widely depending on the specific issuer. Municipal securities are also subject to legislative and regulatory risk which is the risk that a change in the tax code could affect the value of taxable or tax-exempt interest income.

Sector investing can be more volatile than investments that are broadly diversified over numerous sectors of the economy and will increase a portfolio's vulnerability to any single economic, political, or regulatory development affecting the sector. This can result in greater price volatility. Risks associated with the Real estate investments have special risks, including possible illiquidity of the underlying properties, credit risk, interest rate fluctuations, and the impact of varied economic conditions. Risks associated with the **Technology** sector include increased competition from domestic and international companies, unexpected changes in demand, regulatory actions, technical problems with key products, and the departure of key members of management. Technology and Internet-related stocks smaller, less-seasoned companies, tend to be more volatile than the overall market.

Definitions

An index is unmanaged and not available for direct investment.

S&P Municipal Bond Index is a broad, market value-weighted index that seeks to measure the performance of the U.S. municipal bond market. All bonds in the index are exempt from U.S. federal income taxes or subject to the alternative minimum tax. The state level municipal bond indices consist of bonds that have been issued by municipalities or municipal authorities within the 50 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands.

S&P Municipal Bond Infrastructure Index consists of bonds in the S&P Municipal Bond Index that are related to infrastructure.

Moody's uses a lettering system consisting of upper and lower case, as well as numeric modifiers. 'Aaa' and 'Aa' (high credit quality) and 'A' and 'Baa' (medium credit quality) are considered investment grade. Credit ratings for bonds below these designations ('Ba', 'B', 'Caa', etc.) are considered low credit quality, and are commonly referred to as "junk bonds". The modifier 1 indicates that the obligation ranks in the higher end of its generic rating category; the modifier 2 indicates a mid-range ranking; and the modifier 3 indicates a ranking in the lower end of that generic rating category.

General Disclosures

Global Investment Strategy (GIS) is a division of Wells Fargo Investment Institute, Inc. (WFII). WFII is a registered investment adviser and wholly owned subsidiary of Wells Fargo Bank, N.A., a bank affiliate of Wells Fargo & Company.

The information in this report was prepared by Global Investment Strategy. Opinions represent GIS' opinion as of the date of this report and are for general information purposes only and are not intended to predict or guarantee the future performance of any individual security, market sector or the markets generally. GIS does not undertake to advise you of any change in its opinions or the information contained in this report. Wells Fargo & Company affiliates may issue reports or have opinions that are inconsistent with, and reach different conclusions from, this report.

The information contained herein constitutes general information and is not directed to, designed for, or individually tailored to, any particular investor or potential investor. This report is not intended to be a client-specific suitability or best interest analysis or recommendation, an offer to participate in any investment, or a recommendation to buy, hold or sell securities. Do not use this report as the sole basis for investment decisions. Do not select an asset class or investment product based on performance alone. Consider all relevant information, including your existing portfolio, investment objectives, risk tolerance, liquidity needs and investment time horizon. The material contained herein has been prepared from sources and data we believe to be reliable but we make no guarantee to its accuracy or completeness.

Wells Fargo Advisors is registered with the U.S. Securities and Exchange Commission and the Financial Industry Regulatory Authority, but is not licensed or registered with any financial services regulatory authority outside of the U.S. Non-U.S. residents who maintain U.S.-based financial services account(s) with Wells Fargo Advisors may not be afforded certain protections conferred by legislation and regulations in their country of residence in respect of any investments, investment transactions or communications made with Wells Fargo Advisors.

Wells Fargo Advisors is a trade name used by Wells Fargo Clearing Services, LLC and Wells Fargo Advisors Financial Network, LLC, Members SIPC, separate registered broker-dealers and non-bank affiliates of Wells Fargo & Company. CAR 0322-03730