Cybersecurity: A Growing Risk

Russia's invasion of Ukraine has raised the threat of Russian cyberattacks on businesses, and underscores the critical importance of cybersecurity to all industries.

David Bridges
Senior Geopolitical Advisor

Priyanka Singh
ESG Analyst

Anna White
ESG Analyst

KEY TAKEAWAYS

- For many years, cybersecurity attacks have posed a serious threat to private industry from a growing a roster of state actors, sub-state actors, and criminal enterprises, including Russia; not only from data breaches but damaging strikes on physical, virtual, and cloud-based systems and applications.
- Economic sanctions and other aggressive moves against Russia to force an end to its warfare in Ukraine have escalated concerns about retaliatory Russian cyberattacks on governments, central banks, and businesses.
- Such attacks could target financial services in particular, but also harm water and food supplies, manufacturing chains, communication networks, transportation, and industrial production.
- The renewed cyberthreat from Russia increases the importance for companies to be vigilant in their cyber defenses and cyber resiliency.
- At Fidelity, we believe cybersecurity is material to all industries and sectors, and is a key component of the firm's proprietary sustainability research and environmental, social, and governance (ESG) ratings.

Introduction

Long before Russia's invasion of Ukraine, cybersecurity attacks have posed a serious threat to private industry from a growing roster of state actors, sub-state actors, and criminal enterprises, including Russia. Cyberattacks encompass not only data breaches but damaging strikes on physical, virtual, and cloud-based systems and applications. Now, the severe economic sanctions against Russia to force an end to its warfare in Ukraine have escalated concerns about retaliatory Russian cyberattacks on governments, central banks, and businesses. Such attacks could target the financial services industry but also could harm water and food supplies, manufacturing chains, communication networks, transportation, and industrial production.

Fidelity INVESTMENTS

At Fidelity, we believe cybersecurity is a fundamental consideration and material to all industries and sectors, and is a key component of the firm's proprietary sustainability research and environmental, social, and governance (ESG) ratings. In this article, we explore the geopolitics of cybersecurity, the latest on the potential threat from Russia, and how cybersecurity breaches can damage corporate fundamentals across all industries.

The geopolitics of cybersecurity

Cyberspace has emerged as the newest domain of international competition and conflict, that realm where countries strive to secure for themselves advantage over adversaries then bend it to fulfillment of national objectives. And since mathematical and coding ability is spread pretty much evenly across the world, all it takes to emerge as a major cyber state actor is access to the internet, modest funding, some operational direction, and a dedicated cadre of coders and hackers. Today, the roster of the world's major state cyber actors includes the United States, the U.K., China, and Russia, as well as potentially surprising players such as Iran, North Korea, Pakistan, Romania, Ukraine, and Belarus.

Criminal groups and sub-state actors such as Lebanon's Hizballah or international drug cartels have also been drawn to cyberspace. This is the reality of a world where international codes of conduct are undefined, rules of conduct have yet to be stipulated, and the barriers to entry and competition are very low. The failure particularly of industrialized democracies to throw up meaningful barriers has only accelerated this development as both criminal and sub-state actors have moved adroitly to capitalize on an absence of internationally accepted laws, agreements or protocols governing cyberspace to pursue their interests and objectives.

One of the most worrying developments has been the blurring of lines that separate state-actor cyber operations and those of criminal groups. The number of incidents where state actors have provided targeting information to criminal cyber groups, facilitated their access to targets of interest, and shared in the illicit financial gains has increased sharply. The enduring difficulty in establishing responsibility and attribution for cyberattacks is only encouraging this phenomenon. In one recent case, Russia denied any involvement with the cyberattack on a U.S. oil pipeline by a Russia-linked cybercrime group known as DarkSide. The attack shut down the pipeline, led to severe gas shortages along the Eastern Seaboard, and disrupted fuel supplies after the hackers stole a single password. The company paid the hackers a $4.4 million ransom, in a case that underscored the considerable vulnerability of U.S. businesses, transportation networks, and industries.

Russia, backed into a corner

Russia over the years has built formidable offensive cyber capabilities, embedded in the security services of the Russian Federation as well as in criminal hacking groups. We have seen repeated examples of significant overlap between these two groups, with both sides dividing the profits of the attacks. The breadth of Russia's capabilities, and the totality of the offensive strikes they have made, suggest that the criminal hackers are taking direction from the government.

Now, Russia's invasion of Ukraine and its continual onslaught of attacks by land, sea, and air has triggered harsh economic sanctions that have pushed the country into a corner. Russia, once a promising emerging growth market, has in a matter of weeks become an international pariah with its economy essentially shut down, its currency devalued and near worthless. Its banks have been frozen out of the global SWIFT payments system,[1] while companies worldwide are boycotting Russian goods and services. Airline manufacturers have suspended the leases on Russia's mostly leased fleet of aircraft, which could risk their seizure, while a growing list of Fortune 500 countries are suspending in-country operations. Faced with draconian punishment in the billions of dollars, Russia is unlikely to take such severe actions and economic damage without striking back—in a potentially significant response.

One key target of Russia's has been financial services, but fortunately the sector has invested more significantly than many other segments of the economy. However, even though financial services may be better resourced, they must recognize they are up against highly sophisticated Russian hackers who can draw on all of their state/criminal capabilities to capitalize on weaknesses. For years, Russia has been mapping U.S. public/private cyber infrastructure, part of which may entail "sleeper software" with the ability to fire up upon direction. In addition, Russian hackers are eyeing U.S. satellites that enable GPS tracking. Efforts to damage or disrupt U.S. GPS capabilities could have a significant effect on planes, trucks, and shipping traffic worldwide; it could hurt not only transportation but manufacturing and commodity production.

Weak cybersecurity can hurt fundamentals

It's difficult to conceive of a cyberattack that does not cause significant damage. Proper corporate vigilance is key to cyber safety, and it is not simply a question of allocating cash to the problem. Companies should take a thoughtful and systematic approach to preventing cyberattack, across its infrastructure and the people who use it. Such measures must include investment in technology, but also deployment and management of that technology. Companies should also take care to ensure good "cyber hygiene" to ensure their infrastructure is protected and that their employees and customers are educated and aware of the threats. The human element is often one of the most common points of failure for cyberattacks. Insider access to data from contractors, subcontractors, or disgruntled employees can cause serious damage.

Even a breach that may seem minor, such as the theft of inadvertently exposed, non-personal consumer data in the cloud, could lead to negative headlines and reputational risk. A single ransomware attack is enough to bring manufacturing plants to a halt, negatively impacting sales and disrupting the broader supply chain. For example, one multinational tech company was hit with a malware attack that resulted in leaked content, and therefore lost revenue, as well as embarrassing executive emails.

Hackers who target intellectual property can also damage a company's competitive advantage. In one recent case, the U.S. Justice Department indicted China sub-state hackers for trying to steal intellectual property related to the COVID vaccine.[2] The indictments followed another claim by the U.S. and its allies that Russian hackers were trying to steal information on vaccine development.[3] In another recent case, hackers from North Korea accessed confidential data and unreleased movies from a U.S. film studio. The hackers later issued a warning about possible movie theater terror attacks, all of which impacted revenue.

Ironically, some of the most devastating attacks on companies are those providing IT support. In one breach, an IT performance monitoring network was hit by malicious code. The hacker was able to inject the phony code into the "build" portion of the company's software supply chain, and it was pushed out to several thousand customers in an update. The company's perceived lack of transparency following the event slowed revenue growth and damaged customer retention and expansion.

Cybersecurity is also relevant to capital allocation: Mergers and acquisitions can translate into security risk because as companies are acquired they can be prone to introducing vulnerabilities to their networks. For example, in one case a hotel company that had acquired another hotel company was subject to a hack of its reservation system, exposing information in its global guest database spanning credit card and passport information, resulting in stocks losses and litigation.

Why cybersecurity is material to all industries

At Fidelity, we view cybersecurity as a material consideration across its proprietary environmental, social, and governance (ESG) research and ratings. For example, within the "E," cyberthreats are relevant to drinking water and wastewater systems that are infrastructure-intensive; in the "S," lax supply-chain management can hurt data security; and in the "G," cyberattacks can disrupt business operations, hurt share prices, and threaten management. We have found that cybersecurity is impacting every industry in part due to accelerated trends in digitization and use of the cloud.

The migration to the cloud—new risks

The cloud migration push and hybrid operating environment introduces a new level of cybersecurity risk. The availability of public cloud infrastructure and SaaS services are allowing businesses to free themselves from IT "toil" (upgrades/patching/staffing) and focus more on their business operations. But enterprises still have some responsibilities in the cloud; securely configuring their storage services so they are not readable on the internet, protecting their passwords that allow administrative access, backing up data, purging old data, etc. The cloud is a great equalizer and enabler for businesses large and small, but you still need the software/cloud engineering talent to properly configure and run your business on these platforms. There remains a talent shortage worldwide. This has caused the managed IT service sector to mushroom to help companies in their digital transformation and get to the "other side" where they are running operations in cloud services, with security built in.

Viewed by industry, the financial sector has invested heavily in cybersecurity and has the resources to hire and train staff and run their own security operations.

Within manufacturing-intensive industries and energy industries, managements must ensure their process control systems and supply chains maintain proper cyber hygiene to avoid crippling disruptions, as seen by the attack on the oil pipeline described above.

Utilities and energy companies have traditionally emphasized physical security of their assets over cybersecurity, but we expect the trend to shift for a number of reasons. First, critical infrastructure has increasingly been a target for cyber and ransomware attacks. Second, the increased connection of smart devices, coupled with legacy infrastructure that was not built to be connected to the internet, elevates potential vulnerabilities. Third, the Biden administration and Department of Energy recently issued a "100 Day Plan for Cybersecurity" for the electric power sector to identify and deploy new technology to identify and prevent such attacks.[4]

Next steps for cybersecurity

We have seen some positive signals recently that may indicate a greater focus on cybersecurity. For example, Microsoft recently identified malware in Ukraine that was targeting government ministries and financial institutions.[5] Microsoft was able to disable the malware, which it named FoxBlade, before it caused any damage. In addition, the U.S. Securities and Exchange Commission recently announced a proposed rule that publicly traded companies would be required to disclose data breaches and other significant cybersecurity incidents within four days.[6]

In general, recent moves by the Biden administration to improve public/private sector cybersecurity, while a step in the right direction, may not be enough to significantly diminish the pace of cyberattacks. The core element of the administration's strategy—improving the security of federal government IT systems, placing renewed emphasis on cyber as a central feature of national security, and calling for closer public-private sector cooperation in improving critical infrastructure security—are aimed at sparking a wildly overdue national dialogue but will have limited near- or medium-term practical effects. Poor security practices, weak vigilance, outdated software, vulnerable supply chains, a global abundance of networks that presume all users are trusted users, and low probability of significant reprisals continue to make cyberattacks for a wide array of motivations—from advancing national strategic interests to making money fast—too attractive to pass up. The core problem is that governments operate about 10% of networks globally, while the private sector operates 90%. The private sector must step up and improve its cyber game.

Endnotes:

1. Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a global banking system used for electronic payments. **2.** NPR, July 21, 2020. "DOJ Charges 2 Suspected Chinese Hackers Who Allegedly Targeted COVID-19 Research." https://www.npr.org/2020/07/21/893832580/doj-charges-2-suspected-chinese-hackers-who-allegedly-targeted-covid-19-research **3.** NPR, July 16, 2020. "U.S. Says Russian Hackers Are Trying to Steal Coronavirus Vaccine Research." https://www.npr.org/sections/coronavirus-live-updates/2020/07/16/891834251/u-s-says-russian-hackers-are-trying-to-steal-covid-19-vaccine-research **4.** Department of Energy, "Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats," April 20, 2021. https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0 **5.** CNBC, Feb. 28, 2022. "Microsoft Said It Informed the Ukrainian Government of Cyberattacks." https://www.cnbc.com/2022/02/28/microsoft-says-it-informed-the-ukrainian-government-about-cyberattacks.html **6.** *Wall Street Journal*, March 9, 2022. "SEC Proposes Requiring Firms to Report Cyber Attacks within Four Days." https://www.wsj.com/articles/sec-considers-rule-requiring-firms-to-report-cyber-attacks-within-four-days-11646838001

Authors

David Bridges

Senior Geopolitical Advisor

David Bridges is a senior geopolitical advisor at Fidelity Investments. In this role, Mr. Bridges provides expert geopolitical assessment to Fidelity investors and institutional clients. Prior to joining Fidelity, Mr. Bridges served a 25-year career in the Central Intelligence Agency's (CIA) Clandestine Service. At the time of his retirement in 2011, he was a member of the Senior Intelligence Service, the elite leadership team that guides CIA activities across the globe. Mr. Bridges held a number of critical positions, to include executive direction of all CIA activity in Russia, the former Soviet Union, central and eastern Europe, and the Balkans, operational command of all CIA offensive and defensive counterintelligence operations worldwide, and several assignments as chief of station.

Priyanka Singh

ESG Analyst

Priyanka Singh is an Environmental, Social, and Governance (ESG) analyst in the Equity Division at Fidelity Investments. In this this role, Ms. Singh is responsible for leading efforts to build out ESG capabilities within Fidelity's Equity and Fixed Income divisions. Additionally, she works closely with equity and fixed income portfolio managers and analysts to integrate ESG investment strategies and research signals into Fidelity's investment process.

Anna White

ESG Analyst

Anna White is an Environmental, Social, and Governance (ESG) analyst in the Equity Division at Fidelity Investments. In this this role, Ms. White is a generalist ESG analyst covering many sectors and is responsible for leading efforts to build out ESG capabilities within Fidelity's Equity and Fixed Income divisions. Additionally, she works closely with equity and fixed income portfolio managers and analysts to integrate ESG investment strategies and research signals into Fidelity's investment process.

Fidelity Thought Leadership Vice President Martine Costello Duffy provided editorial direction for this article.

1019776.1.0 1.9905326.100