The Hack Effect:

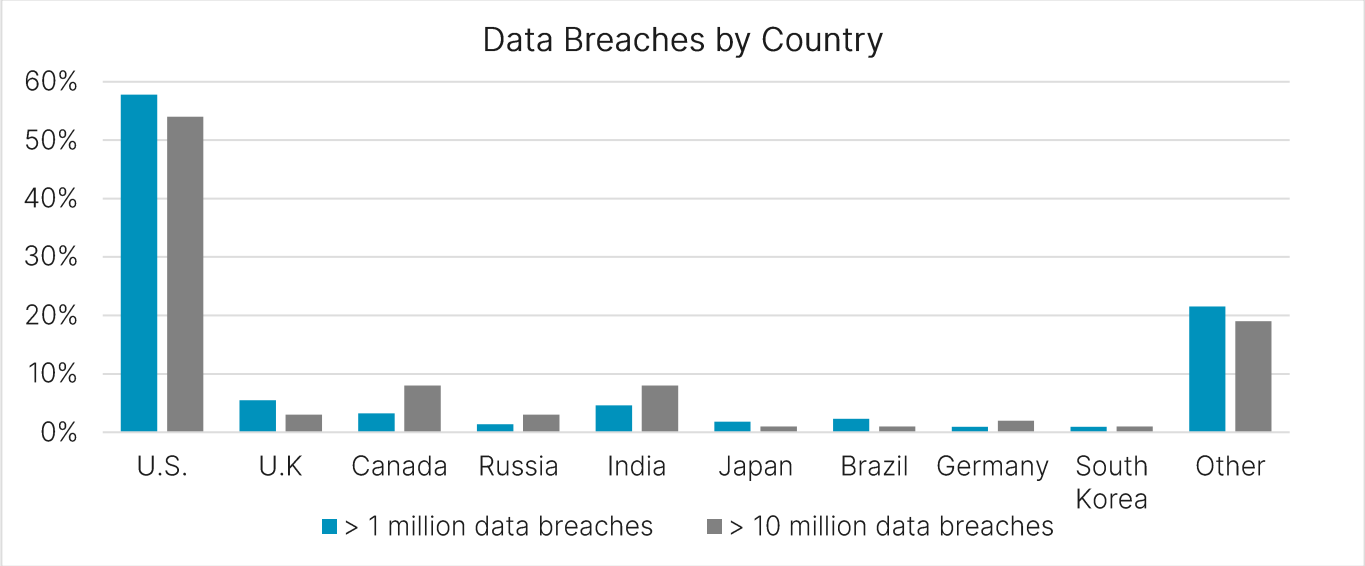
The Effect of Data Breaches on the Nasdaq CTA Cybersecurity Index™

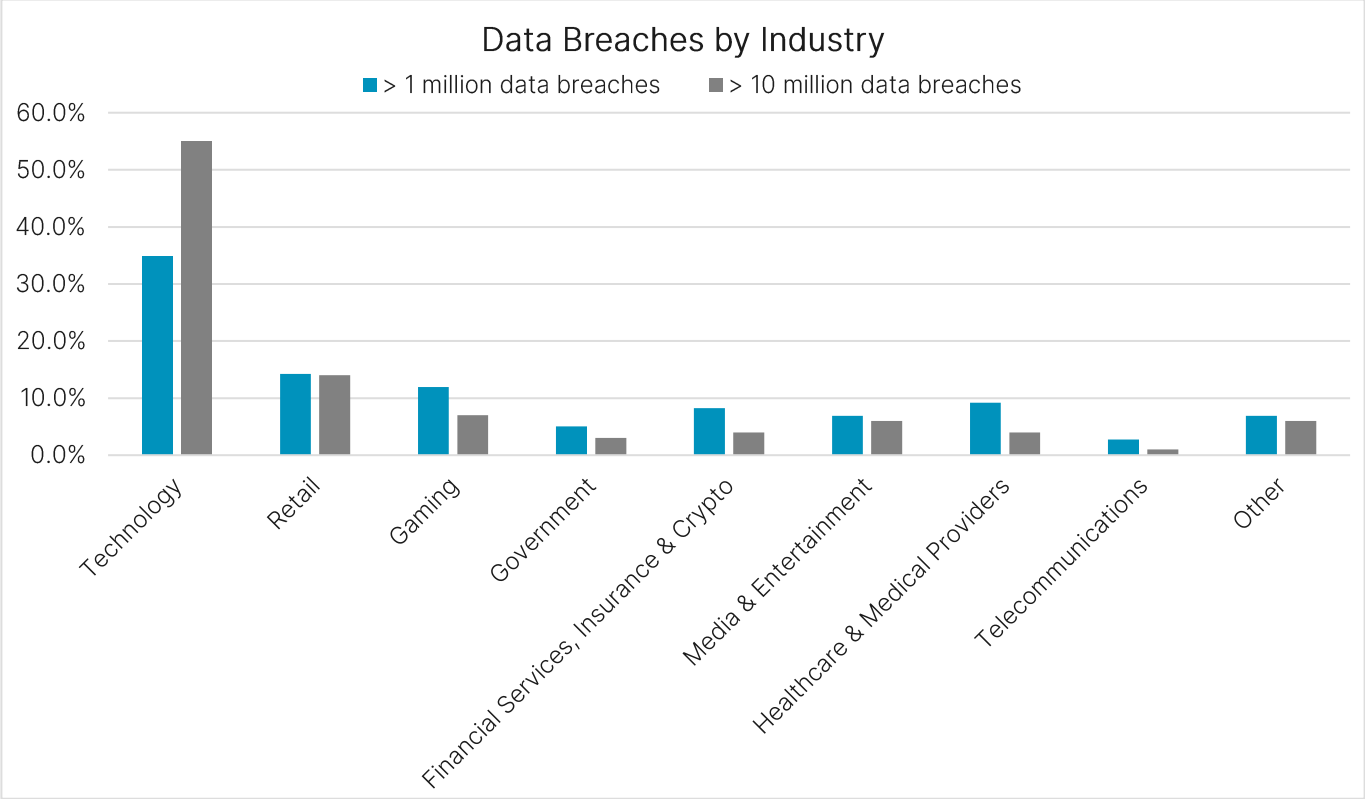
Cyberattacks pose major threats to business continuity and performance with far-reaching effects such as lowered consumer trust. With threats becoming more sophisticated, businesses are shoring up their efforts to mitigate cyber-risks. According to Bloomberg[1] and other news sources[2] that have recorded breaches, there have been 318 data breaches worldwide reported since April 2014, with at least 1 million data records exposed. Of those 318 data breaches, there were 100 instances where over 10 million records were breached. On average, this translates to a hack approximately every 29 days where at least 10 million records were breached. With a major attack every month, cyberattacks have become ubiquitous and a major threat for businesses. Given the increased focus towards digitization across industries, there is expected to be an increase in vulnerabilities across the technology stack. The recurrent nature of cyberattacks has put cybersecurity front and center of challenges faced by CEOs with Satya Nadella of Microsoft characterizing it as the central challenge of the digital age. Further, according to a Gartner survey of over 2,000 Chief Information Officers, security remains the top spending priority in 2022[3]. Even if we consider the risks of a recession, cybersecurity spend is least likely to be cut given the defensive nature of the business, according to a survey done by AlphaWise, Morgan Stanley Research[4].

From an investment perspective, we analyze whether cyberattacks have had a material impact on share prices of cybersecurity companies. The following analysis indicates that breaches have served as a catalyst for the performance of the index. The Nasdaq CTA Cybersecurity Index (NQCYBR™), which is designed to track public companies involved in providing cybersecurity technology and services, has shown material outperformance following major data breaches. Investors may benefit from owning the product tied to NQCYBR, the First Trust Nasdaq Cybersecurity ETF™ (CIBR™), as cybersecurity attacks continue to pose significant challenges to business continuity and performance.

The chart below provides additional details around the 218 data incidents with between 1 million and 10 million records breached, and the 100 incidents with more than 10 million records breached over the last 8 years. As with our findings last time, the Technology sector has emerged as the industry most vulnerable to cyberattacks with a 55% share of the largest breaches (over 10 million records) and 35% of all breaches analyzed. Other sectors that have also been vulnerable to cyberattacks include Gaming, Retail, Government, Financial Services, Media & Entertainment, Healthcare & Medical Providers, and Telecommunications, suggesting that cyberattacks now affect nearly all major industries that power the economy. From a geographic perspective, more than half of the incidents occurred in the U.S. with 58% of data breaches with over 1 million records affected, and 54% of data breaches with over 10 million records affected. Other countries that have recorded a significant number of breaches include the U.K, Canada, Russia, India, Japan, Brazil and South Korea. Companies around the world are likely to invest more in solutions to mitigate risk to business performance as there are significant pain points to be addressed.

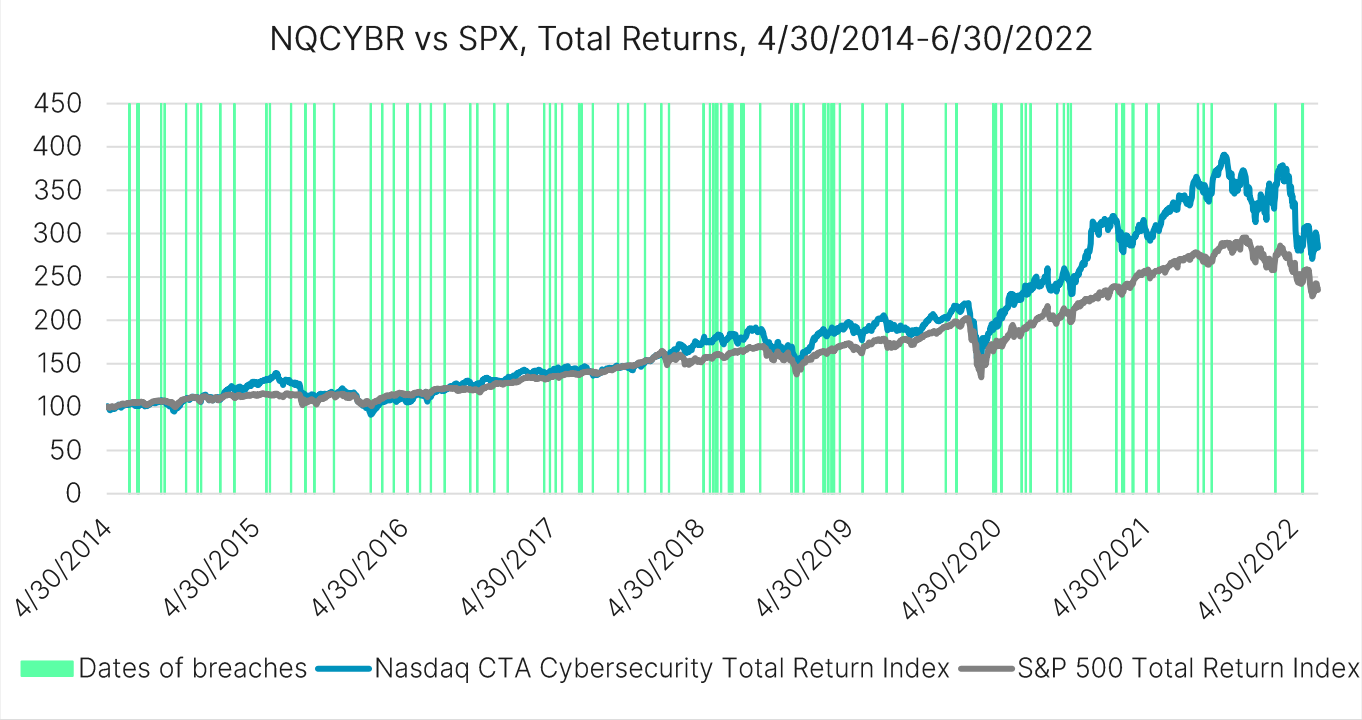
1 https://www.bloomberg.com/graphics/corporate-hacks-cyber-attacks/
2 https://www.crn.com/news/security/the-10-biggest-data-breaches-of-2022-so-far-; https://haveibeenpwned.com/
3 https://www.gartner.com/en/newsroom/press-releases/2021-10-18-gartner-survey-of-over-2000-cios-reveals-the-need-for-enterprises-to-embrace-business-composability-in-2022
4 https://www.techrepublic.com/article/recession-cios-cut-increase-spending/



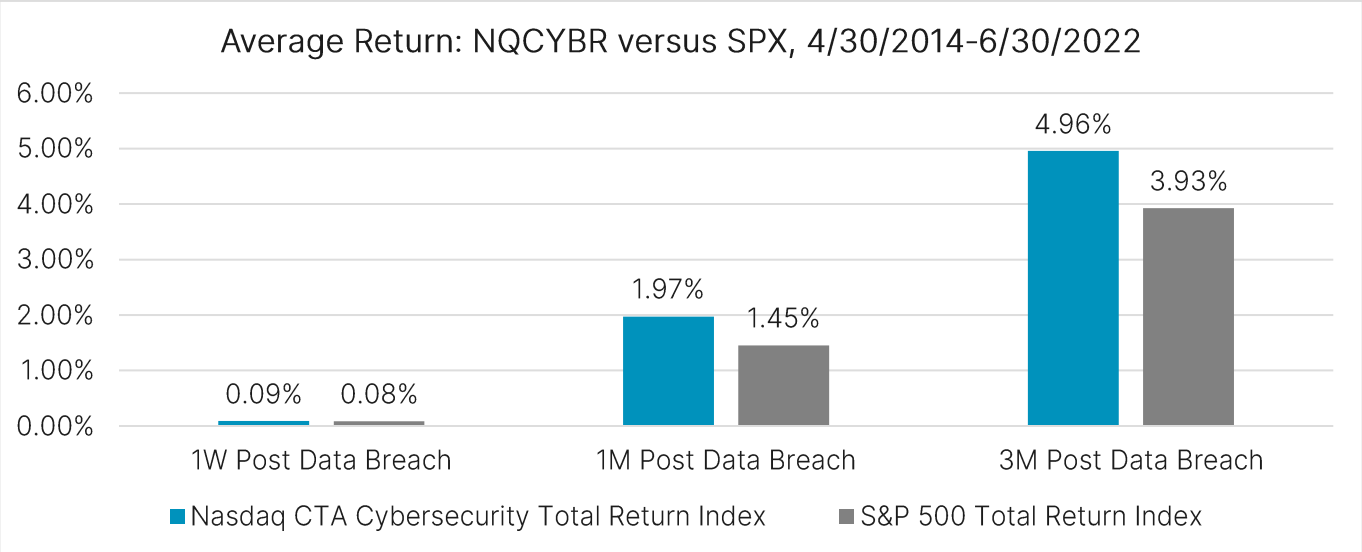


In the chart below, we have compared the performance of NQCYBR with the S&P 500 over an approximately 8-year time period, with data breaches overlaid. The NQCYBR Index has outperformed the S&P 500 by about 49 percentage points cumulatively over the period, from April 30, 2014 through June 30, 2022. The breaches overlaid below illustrate the recurrent nature of the cyberattacks as well as the intensity. The largest cyberattack recorded in the time period was that of Yahoo! in late 2014, with 500 million user records exposed containing sensitive information such as names, email addresses, birth dates, passwords and other vital information. It is highly unlikely that cybersecurity risks arising from threat actors who perpetuate cybersecurity risks or human error will ever be fully eliminated. Given the likelihood of continued threats on the horizon, there is expected to be

strong demand for cybersecurity services and products. Breaches will likely continue to be a long-term tailwind for growth.



Cyber attacks have had a material impact on the performance of the NQCYBR Index as illustrated below. We have analyzed the performance of the NQCYBR Index versus the S&P 500 following a major data breach over three time periods: 1 week post data breach, 1 month post data breach and 3 months post data breach. As seen below, NQCYBR has on average outperformed SPX across all three time horizons. The outperformance varies depending upon the time period under review. The NQCYBR Index has outperformed the S&P 500 by 1 basis point 1 week after data breach, 52 basis points 1 month after data breach and 103 basis points 3 months after data breach, on an average basis. This illustrates that the uptick in outperformance of cybersecurity companies vs. the broader market compounds over time with the accumulation of multiple major breaches in succession.



Cyberattacks continue to be a significant risk faced by people, businesses and governments alike. Post-pandemic, several corporates shifted to the hybrid working model which resulted in an increase in endpoint devices and network access. IT systems were at an increased risk for cyberattacks. To add fuel to the fire, the continued tensions between Russia and Ukraine have increased the risk of cyberattacks in the U.S. Cybercrimes are costly and heavily impact the bottom line. Keeping this in mind, governments are introducing legislation to protect end-users, and other efforts are being made to shore up cybersecurity. For example, the Biden administration most recently allocated more than $10 billion in cyber-security funds in their $1.9 trillion COVID-19 stimulus recovery proposal[5]. In May 2021, President Biden issued an executive order to strengthen the security of the government's technology[6]. On July 28th2021, the President issued a National Security Memorandum[7] which outlined cybersecurity goals for owners and operators of critical infrastructure across the electric sector, and on August 25th 2021, Biden met with private sector leaders in the technology industry to encourage them to invest heavily in cybersecurity efforts[8].

With a more robust regulatory framework in place, there is expected to be steady growth in the cybersecurity space with technically sound offerings to address critical vulnerabilities. As demonstrated earlier, the NQCYBR Index has outperformed the S&P 500 following major data breaches, which indicates that cyberattacks have served as a tailwind for growth. Investors looking to gain exposure to this powerful trend will benefit from considering the First Trust Nasdaq Cybersecurity ETF (CIBR) which tracks NQCYBR.

5 https://thehill.com/policy/cybersecurity/534323-biden-includes-over-10-billion-in-cyber-it-funds-as-part-of-covid-19/
6 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
7 https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/
8 https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/