

Cybersecurity:

Industry Report & Investment Case – NQCYBR

What is Cybersecurity and Why is it Important?

Cybersecurity focuses on protecting computers, networks, programs, and data from unauthorized and/or unintended access. Cybersecurity has become increasingly important recently as governments, corporations, and people collect, process, and store vast amounts of confidential information and transmit that data across networks. Data breaches have become almost commonplace in recent years. Over the last few years, high-profile cases of cyber hacks have increased the demand for sophisticated software and security products. Companies across the globe are growing more aware of the potential threat which is leading to a greater allocation of resources towards companies that help mitigate such risks.

The table below highlights the variety of ways in which industries were affected by different types of incidents. While certain industries experience cyberattacks from specific incidents (e.g., about 58% of incidents in 2020 in the Entertainment industry were because of Denial of Service)¹, this table shows that all industries are prone to cybercrime in numerous ways. As such, with the sophistication of cyberattacks, there has been an increased demand for cybersecurity services.

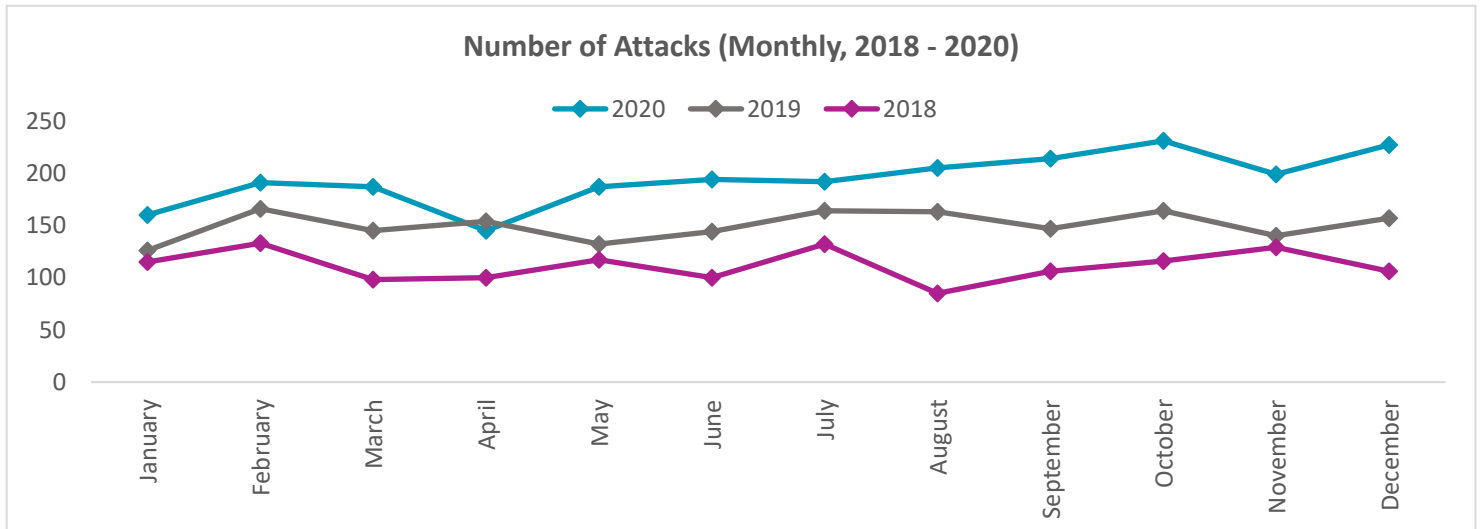
2020 Incidents by Industry	Basic Web Application Attacks	Denial of Service	Everything Else	Lost and Stolen Assets	Miscellaneous Errors	Privilege Misuse	Social Engineering	System Intrusion
Accommodation	1%	0%	0%	0%	0%	0%	1%	1%
Administrative	1%	3%	0%	0%	0%	0%	0%	1%
Construction	1%	0%	0%	0%	0%	0%	1%	1%
Education	5%	8%	0%	0%	8%	2%	8%	4%
Entertainment	3%	58%	0%	1%	3%	2%	1%	2%
Finance	15%	0%	5%	1%	21%	14%	8%	4%
Healthcare	12%	0%	1%	3%	16%	25%	5%	7%
Information	15%	20%	2%	1%	15%	6%	5%	7%
Manufacturing	7%	1%	0%	0%	5%	5%	4%	9%
Mining & Utilities	2%	0%	0%	0%	1%	0%	20%	2%
Other Services	4%	0%	0%	0%	1%	0%	5%	1%
Professional	12%	0%	68%	1%	9%	30%	10%	42%
Public Administration	13%	7%	15%	92%	16%	9%	28%	8%
Real Estate	1%	0%	0%	0%	1%	0%	1%	2%
Retail	4%	3%	9%	0%	2%	3%	3%	6%
Transportation	3%	0%	0%	0%	1%	3%	1%	5%

Source: <https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>

One way in which investors can get exposure to the cybersecurity industry is through the Nasdaq CTA Cybersecurity Index (NQCYBR). In order to adequately understand the reasons as to why cybersecurity is important from an investment perspective, it is first vital to understand the growth drivers for cybersecurity as well as the industry outlook. The following research will discuss the growth drivers and industry outlook for cybersecurity and then show the ways in which NQCYBR is poised to capture these positive trends in the cybersecurity industry.

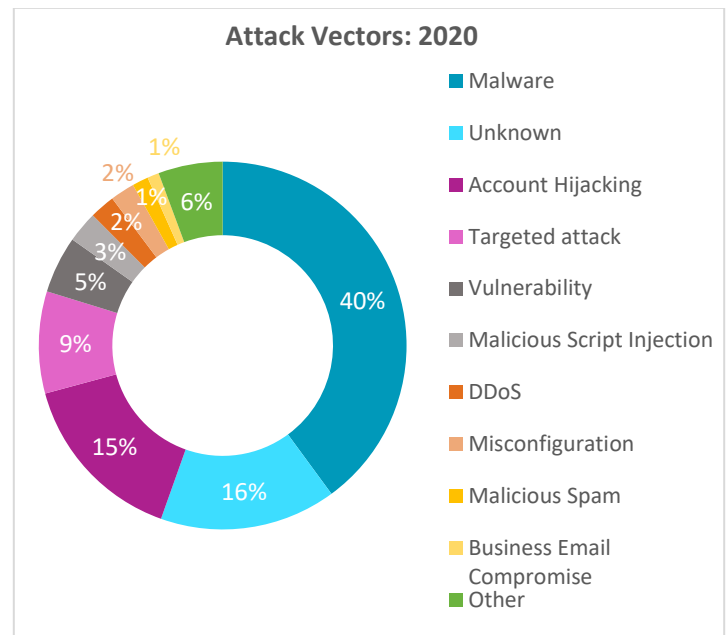
What is Driving the Growth in Cybersecurity?

The growth in cybersecurity is primarily driven by the measures needed to counteract the increasing number of cyber-attacks that people, businesses, and governments face daily. As the chart below shows, the total number of major attacks reported in the news globally was higher in almost every month of 2020 (except April), versus the same month in 2019 as well as 2018.² It's also important to note how the number of attacks has increased over consecutive years, particularly in 2020, as attacks started to trend higher following the early stages of the COVID-19 pandemic.



Source: <https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/>

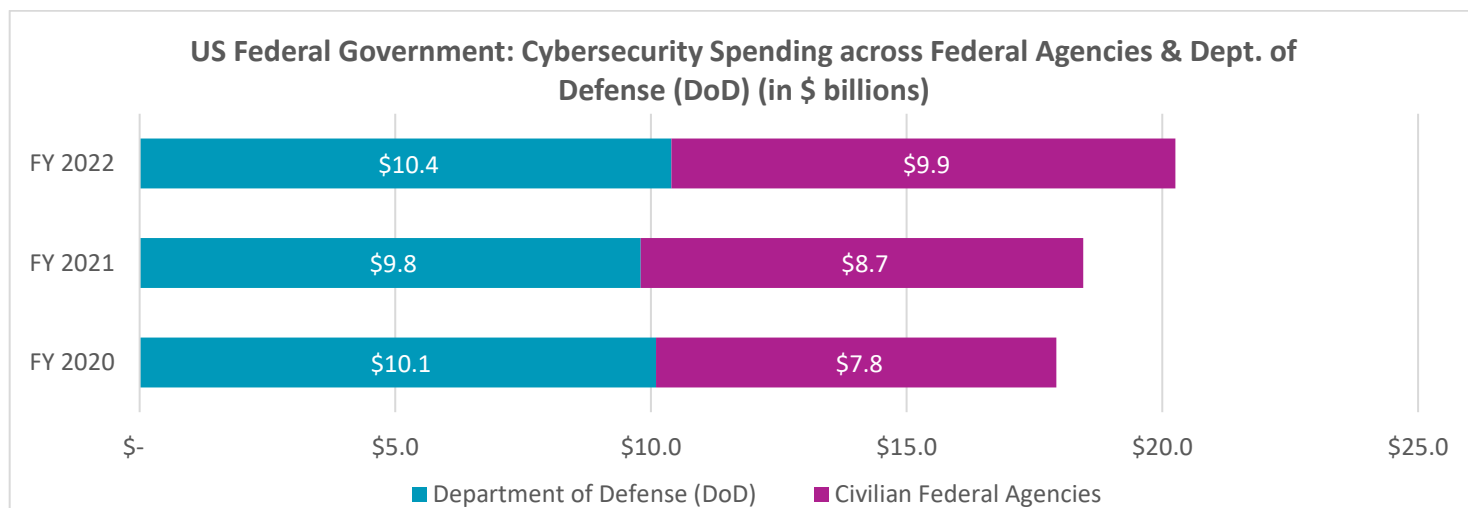
In addition, the two charts below break down the attacks to highlight toward whom the attacks were targeted as well as the ways in which the attacks occurred. The charts illustrate that multiple industries, governments, and individuals were the most affected by cyberattacks in 2020 and that most of those attacks were done via malware or account hijacking.³



Source: <https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/>

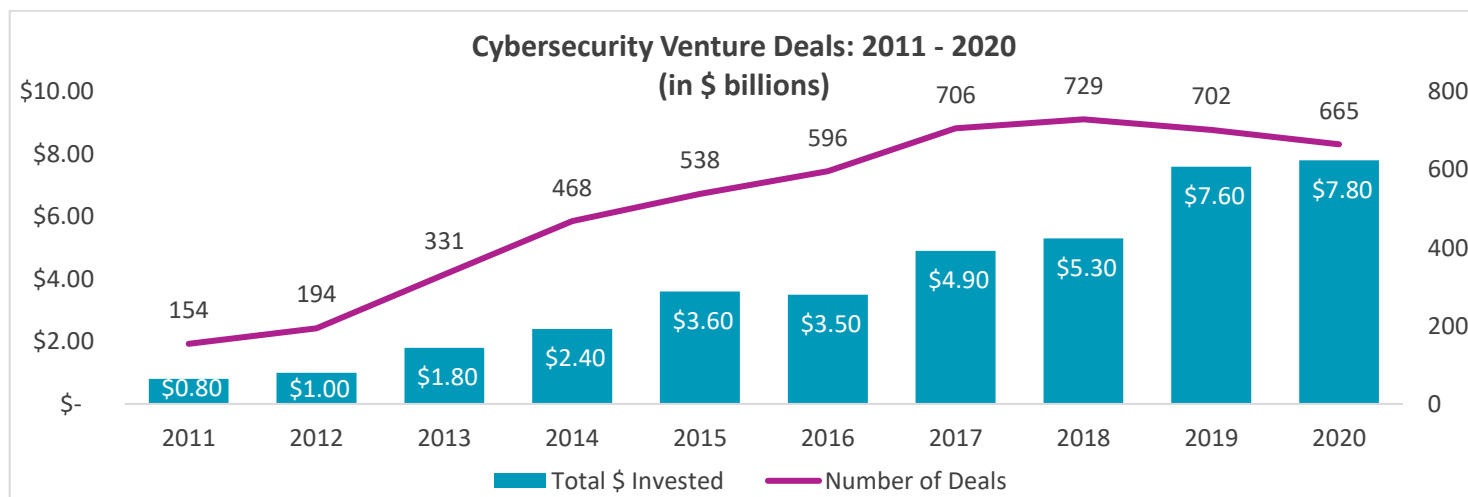
Source: <https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/>

With the increasing number of cyber-attacks, especially those targeting US businesses and critical infrastructure, the White House and US Congress have made cybersecurity an important national policy issue. In fact, President Biden issued the “Executive Order on Improving the Nation’s Cybersecurity” in May 2021, calling for a number of changes to how the nation responds to and defends against cyber-attacks, as well as proclaiming that “the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.”⁴ In addition to the executive order, the President and leaders of Congress have added a number of cybersecurity related provisions in the +\$1 trillion dollar Infrastructure bill. In addition, cybersecurity related spending continues to rise across the government’s federal agencies and military (Department of Defense (DoD)).



Source: US Government Publishing Office

Aside from the rising number of targeted attacks that is driving the growth in cybersecurity as well as the increase in cyber security spending, particularly in the US, the number of cybersecurity venture deals also highlights the dynamism in this space. The chart below shows that venture capital firms have invested almost \$39 billion into cybersecurity companies since 2011.⁵

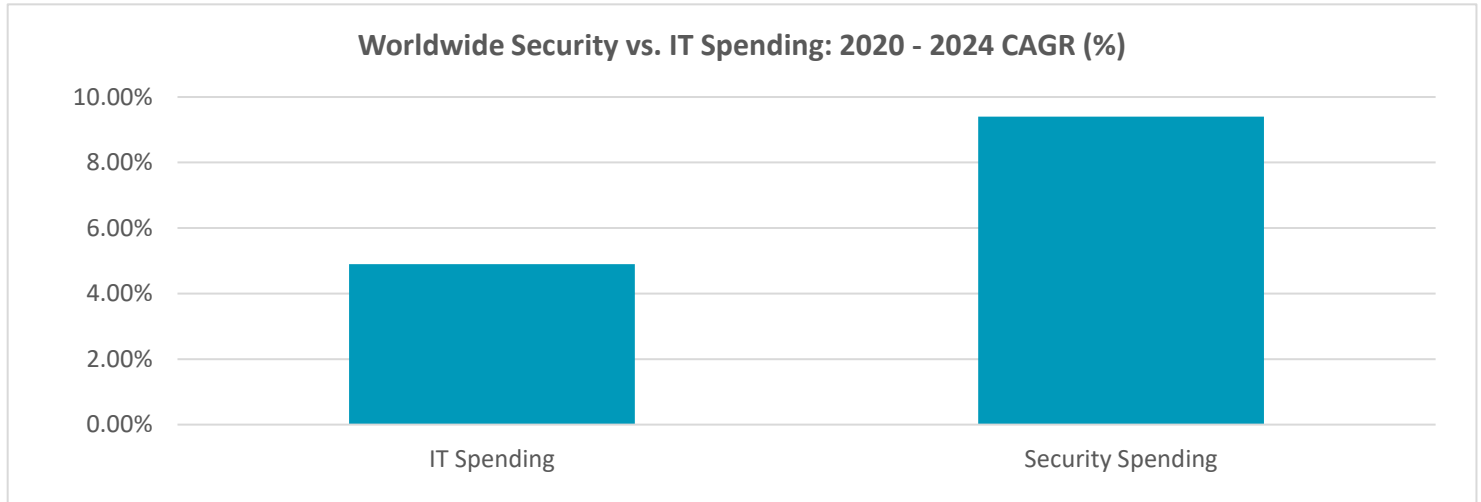


Source: <https://about.crunchbase.com/cybersecurity-research-report-2021/>

This explicitly demonstrates that the increasing number of targeted attacks and cybercrimes is driving the growth in cybersecurity and is continuing to augment the demand for these services, as venture capital firms have continued to pour money into this space. The above also shows that the growing raft of cybersecurity measures taken by governments, corporations, and other organizations bodes well for the cybersecurity industry from an investment perspective.

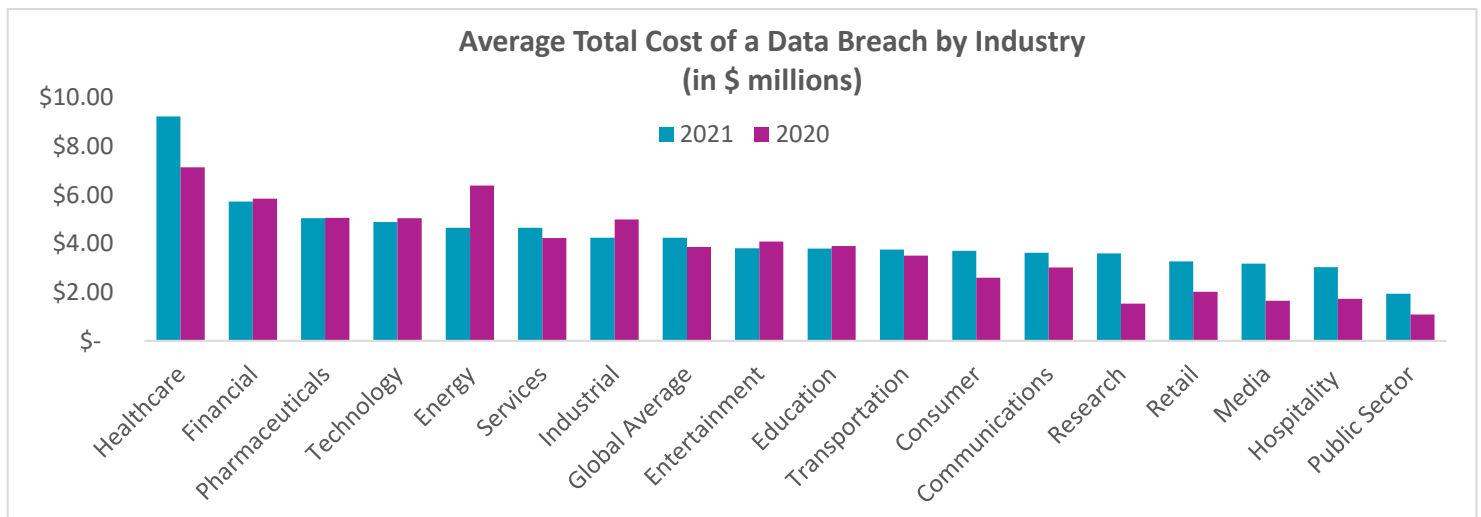
What is the Industry Outlook for Cybersecurity?

In addition to the rise of cyberattacks and cybersecurity spending driving the industry's growth, the overall outlook for cybersecurity from an investment perspective is also positive. According to analysis by Bloomberg Intelligence, cybersecurity spending could surpass \$200 billion by 2024. Based on IDC data and Bloomberg Intelligence analysis, cybersecurity spending is expected to outpace traditional IT spending through 2024, 9.4% versus 4.9%, respectively.



Source: Bloomberg Intelligence (Mandeep Singh - Senior Industry Analyst), August 25, 2021 & IDC

Recent research conducted by IBM in conjunction with Ponemon Institute found that the average total cost of a data breach is \$4.24 million in 2021, which is up from \$3.86 in 2020. In addition, as the chart below illustrates, the healthcare, financial, and pharmaceutical industries have the highest data breach cost per company among all industries.⁸ In a 2019 study by Accenture and Ponemon Institute, which looked at a variety of different cyber-attacks (not just data breaches), they found that average cost of cybercrime per organization was \$13 million.⁹ All of this is to say, the stakes are high.



Source: <https://www.ibm.com/security/data-breach>

This suggests that, as cyber-attacks occur and as costs continue to rise for corporations, cybersecurity spending for cybersecurity measures will continue to rise as well, thus positively impacting the cybersecurity industry.

Survey-based research from Deloitte (gathered from 500 C-suite leaders of major corporations with at least \$500 million in annual revenue) emphasized that most executives planned as many as six different initiatives within the enterprise identity security market, including migration to cloud security, access management, and multi-factor authentication. This illustrates the depth and breadth of security measures that are being undertaken in many organizations and further highlights the continued investment in cybersecurity initiatives.¹⁰

In most instances, corporations are hesitant to reveal breaches and cyberattacks that they've been exposed to, primarily for fear of reputational damage. As such, Cybersecurity Ventures is predicting slightly higher growth rates, at about 12-15% year-over-year through 2025, which is higher than the 8-10% being predicted by other industry analysts.¹¹ *As a result, the actual spending on cybersecurity may be far more than what's revealed publicly, as companies may be understating their cybersecurity budgets to protect their reputation.*

Overall, the above shows that the industry outlook for cybersecurity is very positive. Due to the increasing number of cyberattacks the expectations for cybersecurity spending going forward remain very high. Some of the key growth areas within cybersecurity, such as cloud-based security, will help sustain overall growth, even if other areas decelerate. The rising costs of cyber-attacks -- and corporations' willingness to invest time and money into various cybersecurity initiatives -- further justify the elevated growth expectations for the industry, as well as the likelihood of it remaining a profitable investment for the foreseeable future.

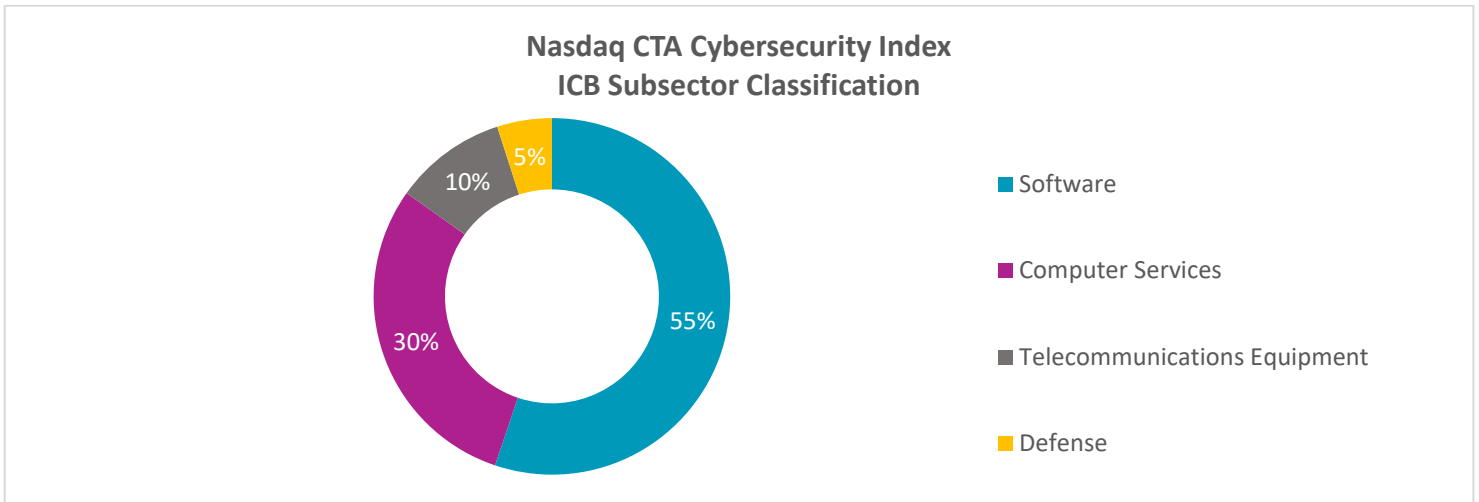
How to Invest in the Cybersecurity Theme?

As mentioned above, one way investors can gain access to the cybersecurity space is through the Nasdaq CTA Cybersecurity Index (NQCYBR).

The methodology for NQCYBR is as follows:

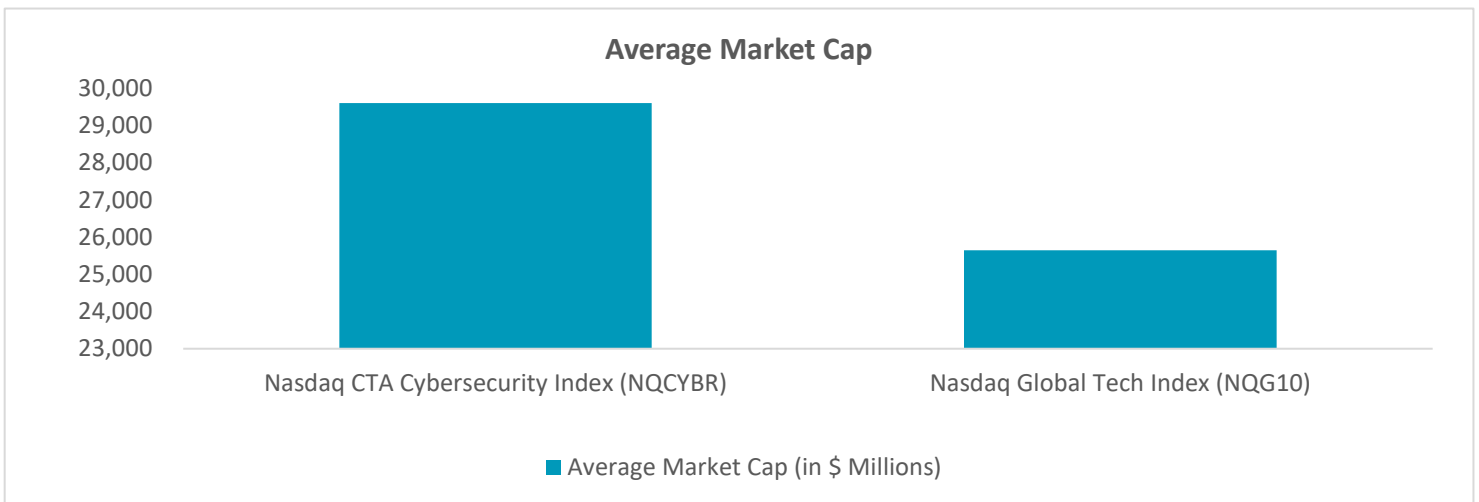
Nasdaq CTA Cybersecurity Index is poised to track companies that are engaged in the cybersecurity segment of the technology and industrial sectors. The Index includes companies, classified as a cybersecurity company by the Consumer Technology Association (CTA), primarily involved in the building, implementation and management of security protocols applied to private and public networks, computers and mobile devices in order to provide protection of the integrity of data and network operations. All index components must have a minimum market capitalization of \$250 million, three-month average daily dollar trading volume of \$1 million, and a minimum free float of 20%.¹¹

In looking at the Industry Classification Benchmark (ICB) sub-sector breakdown of NQCYBR, one can see the diversification across sub-sectors in this index. From the chart below, it is evident that the components in the Nasdaq CTA Cybersecurity Index are diversified across numerous sectors, including, but not limited to, Software, Computer Services, Telecommunications Equipment, Semiconductors, and Defense. This illustrates that investors are getting diversified exposure levels when they invest in the products tied to this index.

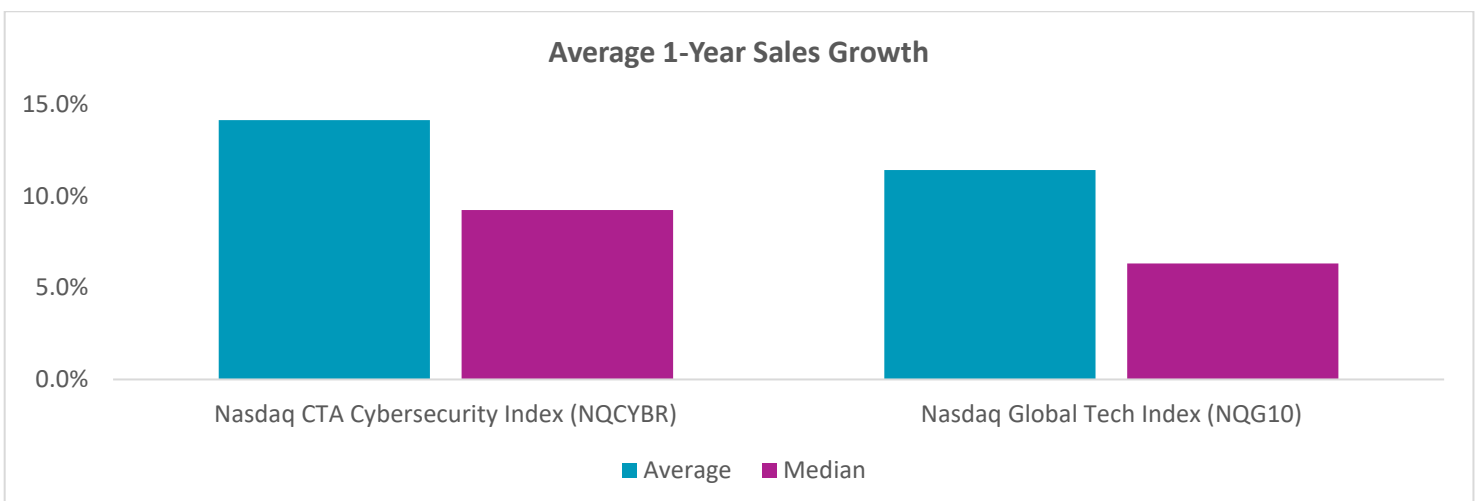


As of 8/31/2021

The components in this index are slightly larger, on average, than those in the Nasdaq Global Technology Index. In addition, as the subsequent chart shows, components in this index have comparable sales growth over the last year, on average, when compared to the Nasdaq Global Technology Index.¹² This is an indication that the components of the index are growing.

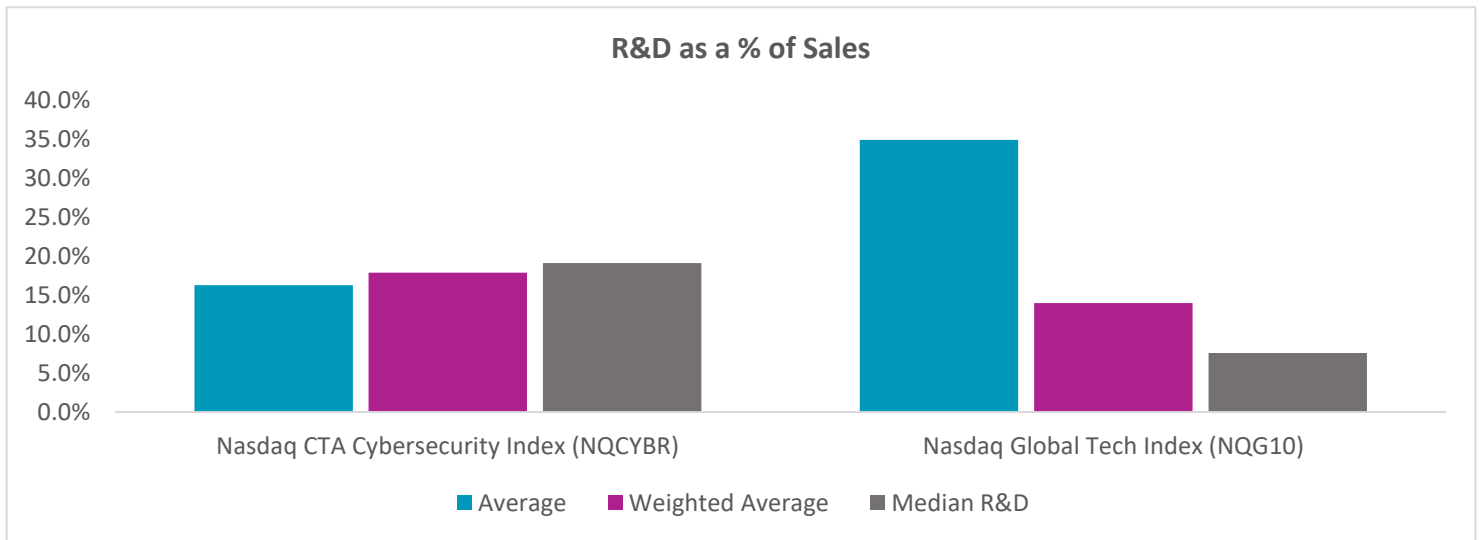


As of 8/31/2021



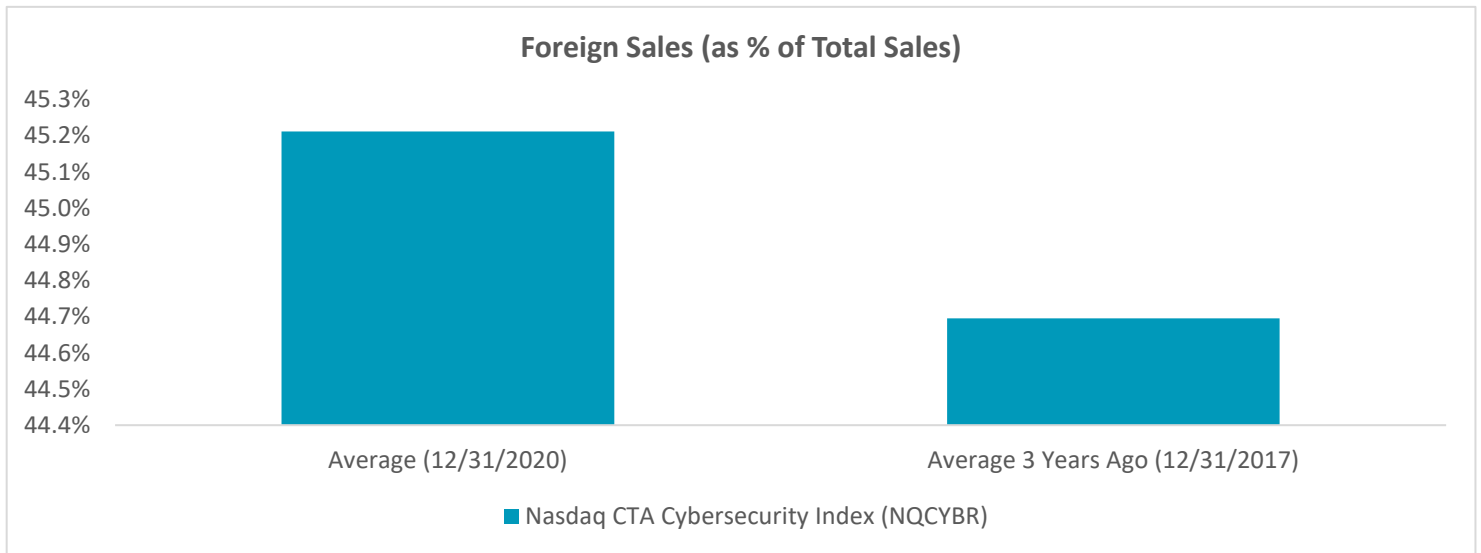
As of 12/31/2020

Since the components in this index are growing, it would be reassuring to know that they are adequately investing their earnings into research and development to remain competitive in the fast-evolving cybersecurity landscape. On a weighted average basis, companies in NQCYBR are investing more into R&D as those in the Nasdaq Global Technology Index – 18.00% versus 14%, respectively.



As of 12/31/2020

In addition, because cybercrimes affect people, governments, and organizations all over the world, the components in this index should strive to capture the demand for cybersecurity services globally. The proportion of sales derived internationally averages around 45.2% across all companies in this index currently, compared to 44.7% three years ago, which suggests that they are indeed taking advantage of the global nature of cybersecurity demand (note: “foreign sales” refers to revenue derived from countries outside of the company’s domicile).



As of 12/31/2020

Conclusion

In summary, the analysis covered herein illustrates that cybercrimes have increasingly affected multiple industries in numerous ways, thereby boosting corporate demand for cybersecurity services. The continued rise in targeted attacks is also driving growth in cybersecurity services from major governments, including the US, while venture capital firms are investing many times more into the space versus only a few years ago. In addition to the high projected growth rates by various industry research firms and analysts, cloud-based security services and increasing cybercrime costs are going to continue to underpin spending in this industry moving forward.

The Nasdaq CTA Cybersecurity Index offers investors technology-focused exposure to the cybersecurity industry. The index is comprised of components that have experienced strong sales growth and a high proportion of sales derived internationally, showing that they have adequately captured the demand for cybersecurity services thus far. More importantly, the components in this index continue to meaningfully invest into research and development, which will help drive their revenue growth as the cybersecurity industry continues to evolve.

Footnotes:

1. <https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>
2. <https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/>
3. https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf
4. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/><https://www.cbinsights.com/research/smart-money-vcs-early-stage-cybersecurity-startups-expert-intelligence/>
5. <https://about.crunchbase.com/cybersecurity-research-report-2021/>
6. <https://www.idc.com/getdoc.jsp?containerId=prUS46773220>
7. Bloomberg Intelligence (Mandeep Singh – Senior Analyst), December 26th, 2019 and IDC
8. <https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>
9. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50
10. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>
11. <http://cybersecurityventures.com/cybersecurity-market-report/>
12. Average “1 Year Sales Growth” excludes any extreme outliers.
13. https://indexes.nasdaqomx.com/docs/Methodology_NQCYBR.pdf
14. Data mentioned in the piece is from Nasdaq Index Research, Bloomberg, and/or FactSet, unless otherwise stated.

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. **ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.**

© 2021. Nasdaq, Inc. All Rights Reserved.