

# 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 45% of incidents in 2019 in the Accommodation industry were because of Point-of-Sale)<sup>1</sup>, 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.

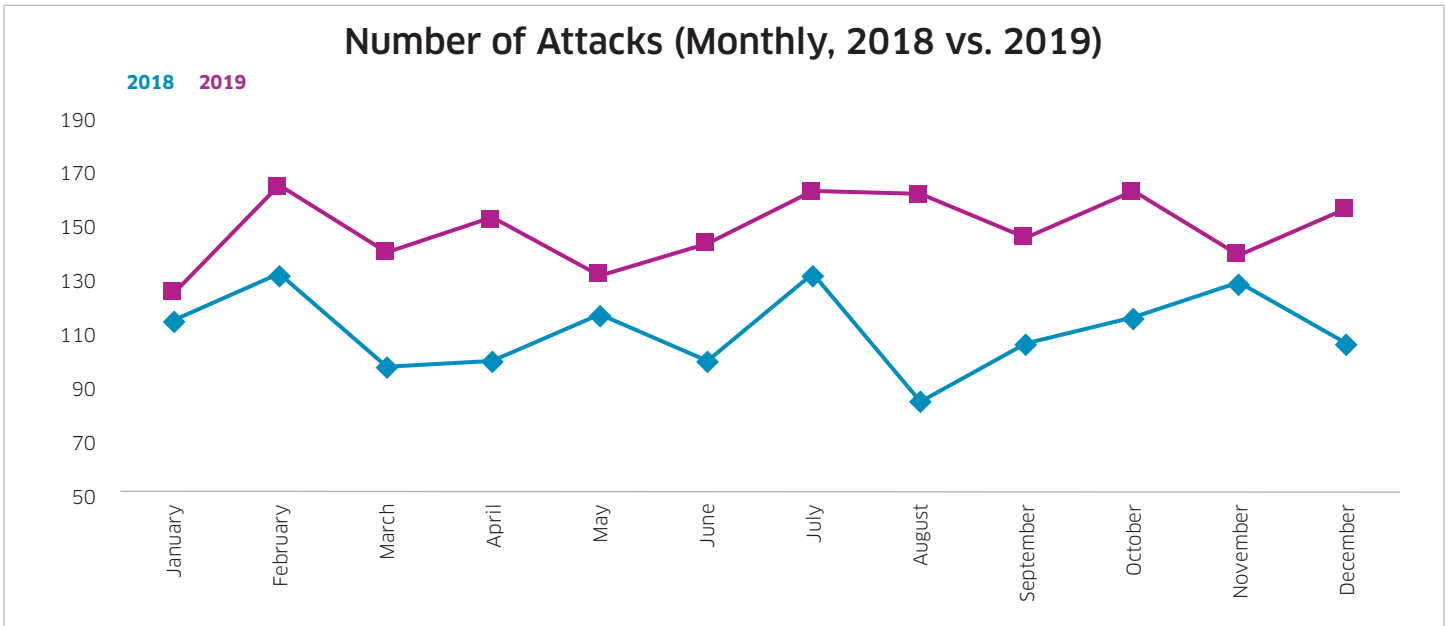
| 2019 INCIDENTS BY INDUSTRY | CRIME-WARE | WEB APPLI-CATIONS | PRIVILEGE MISUSE | EVERY-THING ELSE | DENIAL OF SERVICE | CYBER-ESPIONAGE | MISCEL-LANEOUS ERRORS | LOST AND STOLEN ASSETS | POINT OF SALE | PAYMENT CARD SKIMMERS |
|----------------------------|------------|-------------------|------------------|------------------|-------------------|-----------------|-----------------------|------------------------|---------------|-----------------------|
| Accommodation              | 19%        | 16%               | 1%               | 8%               | 0%                |                 | 6%                    | 4%                     | 45%           | 0%                    |
| Education                  | 8%         | 8%                | 5%               | 6%               | 59%               | 2%              | 10%                   | 2%                     | 0%            | 0%                    |
| Finance                    | 6%         | 8%                | 11%              | 3%               | 62%               | 3%              | 4%                    | 1%                     | 0%            | 2%                    |
| Healthcare                 | 16%        | 15%               | 23%              | 8%               | 1%                | 1%              | 22%                   | 13%                    | 0%            | 0%                    |
| Information                | 19%        | 7%                | 1%               | 2%               | 62%               | 2%              | 6%                    | 0%                     | 0%            | 0%                    |
| Manufacturing              | 16%        | 11%               | 10%              | 6%               | 46%               | 5%              | 4%                    | 1%                     | 0%            | 0%                    |
| Professional               | 9%         | 12%               | 2%               | 9%               | 61%               | 1%              | 4%                    | 2%                     | 0%            | 0%                    |
| Public                     | 20%        | 0%                | 56%              | 0%               | 4%                | 1%              | 6%                    | 12%                    | 0%            | 0%                    |
| Retail                     | 9%         | 39%               | 7%               | 6%               | 23%               | 1%              | 5%                    | 3%                     | 4%            | 4%                    |

Source: <https://enterprise.verizon.com/resources/reports/2019-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.

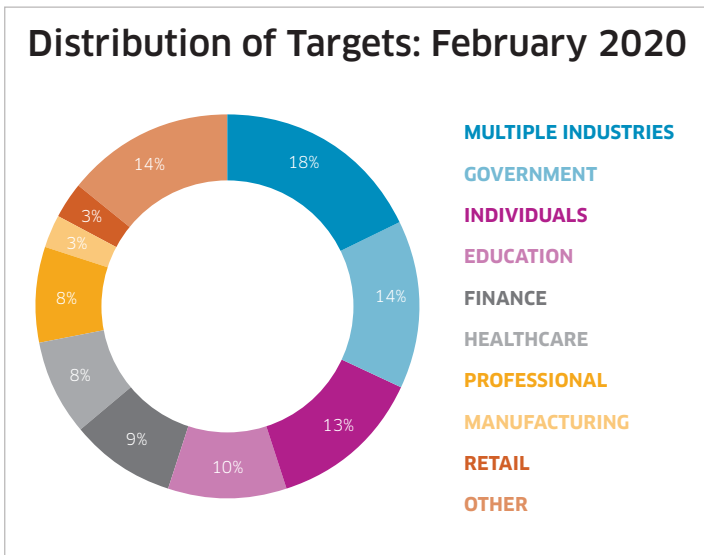
### What is Driving the Growth in Cybersecurity?

The growth in cybersecurity is primarily driven by the measures needed to counteract the increasing number of cybercrimes that people, businesses, and governments face on a daily basis. As the chart below shows, the total number of major attacks reported in the news globally was higher in every month of 2019 versus the same month in 2018<sup>2</sup>.

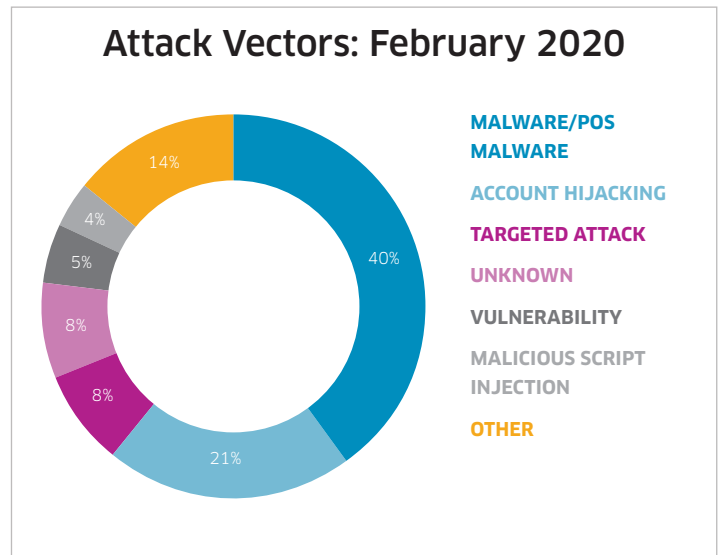


Source: <https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/>

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 February 2020 and that most of those attacks were done via malware or account hijacking<sup>3</sup>.



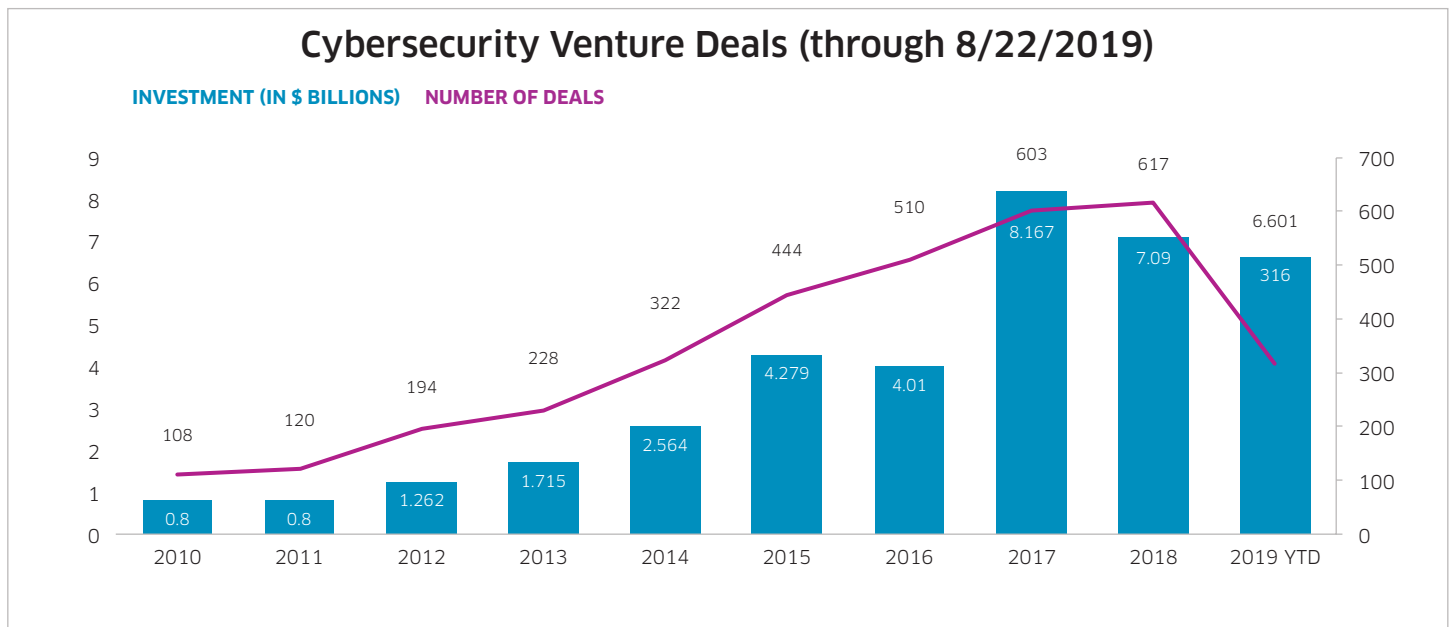
Source: <https://www.hackmageddon.com/2020/03/19/february-2020-cyber-attacks-statistics/>



Source: <https://www.hackmageddon.com/2020/03/19/february-2020-cyber-attacks-statistics/>

The impact of cyberattacks has grabbed the attention of the White House, as President Trump has deemed cybercrime one of the biggest issues facing national security. In addition, the President's 2020 Budget is proposing to allocate \$17.4 billion in spending to fund critical initiatives and research in the cybersecurity space, a 5% increase from the 2019 budget<sup>4</sup>.

Aside from the rising number of targeted attacks that is driving the growth in cybersecurity, the number of cybersecurity venture deals also highlights the dynamism in this space. The chart below shows that venture capital firms have invested more than \$37 billion into cybersecurity companies since 2010<sup>5</sup>.



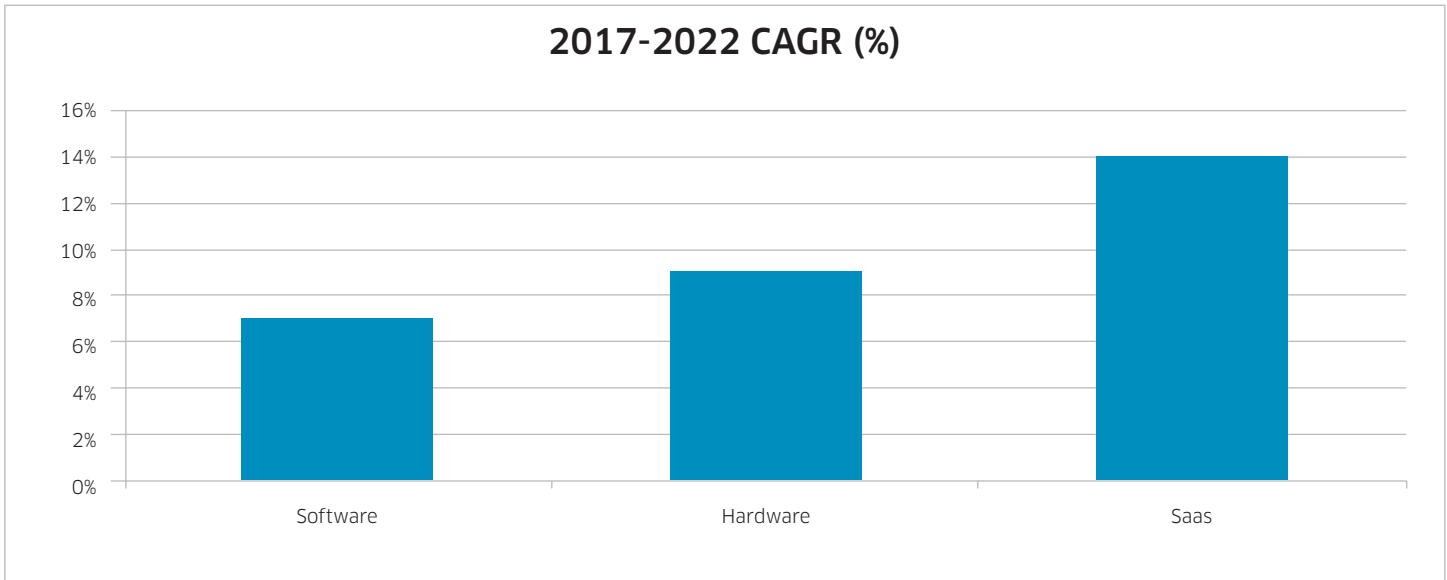
Source: <https://www.cbinsights.com/research/smart-money-vcs-early-stage-cybersecurity-startups-expert-intelligence/>

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?

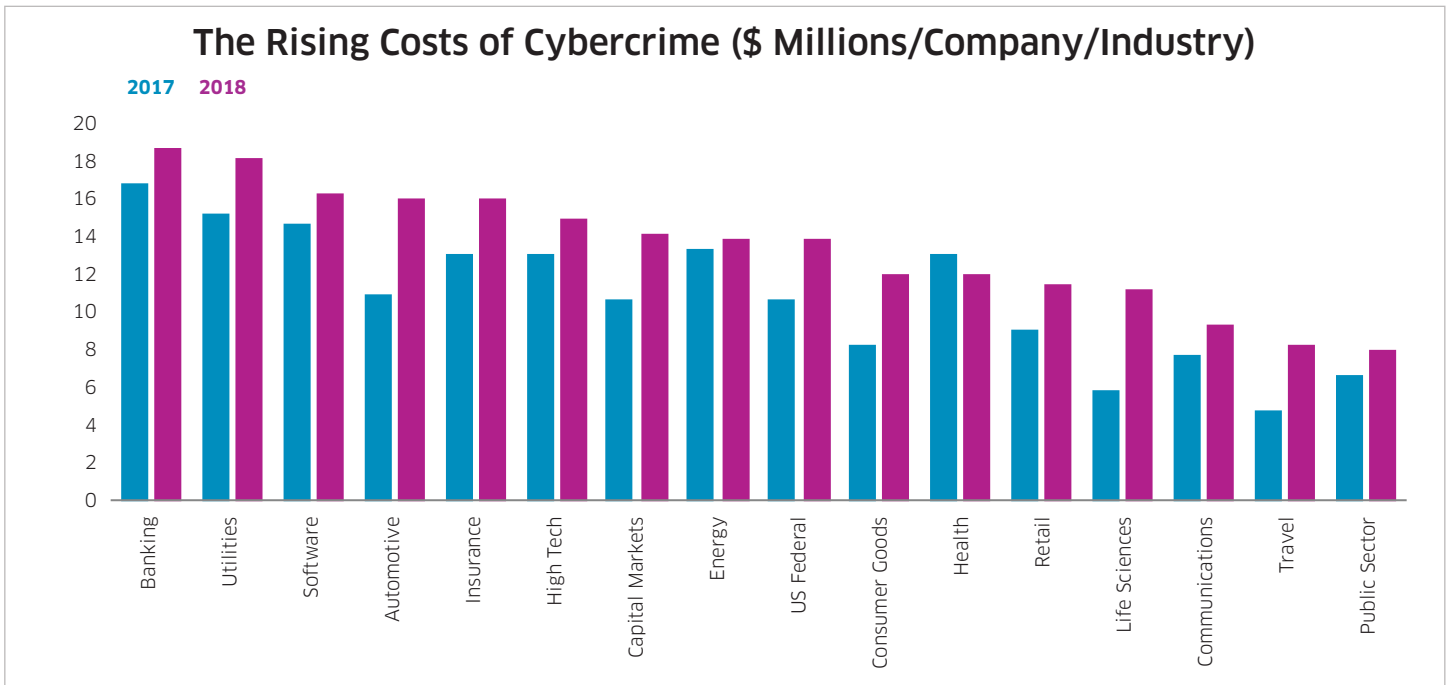
In addition to the increasing cyberattacks driving the industry's growth, the overall outlook for cybersecurity from an investment perspective is also positive.

A forecast from International Data Corporation (IDC) estimated that worldwide spending on security-related hardware, software, and services will reach more than \$151 billion in 2023 with a compound annual growth rate (CAGR) of 9.4% over the forecast period of 2019-2023<sup>6</sup>. According to Bloomberg and IDC, the largest area of growth within cybersecurity is likely to come from software-as-a-service (SaaS) companies<sup>7</sup>. The chart below forecasts that while traditional software and hardware are going to continue to grow and play an important role, network security will begin to meaningfully shift to the cloud, as most providers will keep boosting their cloud capabilities organically and via acquisitions<sup>7</sup>. As such, this reveals that cloud-based cyber security will continue to propel and expand the cybersecurity industry going forward.



Source: Bloomberg Intelligence (Mandeep Singh - Senior Analyst), December 26th, 2019 and IDC

Research conducted by Accenture suggests that cybercrime costs for organizations continue to rise as the average cost of cybercrime per organization was \$13 million in 2018, up from \$11.7 million in 2017 and a 72% increase in the last 5 years<sup>8</sup>. In addition, as the chart below illustrates, banking, utilities, and software industries have the highest cybercrime cost per company among all industries<sup>8</sup>.



Source: [https://www.accenture.com/\\_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)

This suggests that, as cybercrime costs continue to rise for corporations, so will overall spending for cybersecurity measures, 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<sup>9</sup>.

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 2021, which is higher than the 8-10% being predicted by other industry analysts<sup>10</sup>. *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 in order 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 cybercrime – 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.

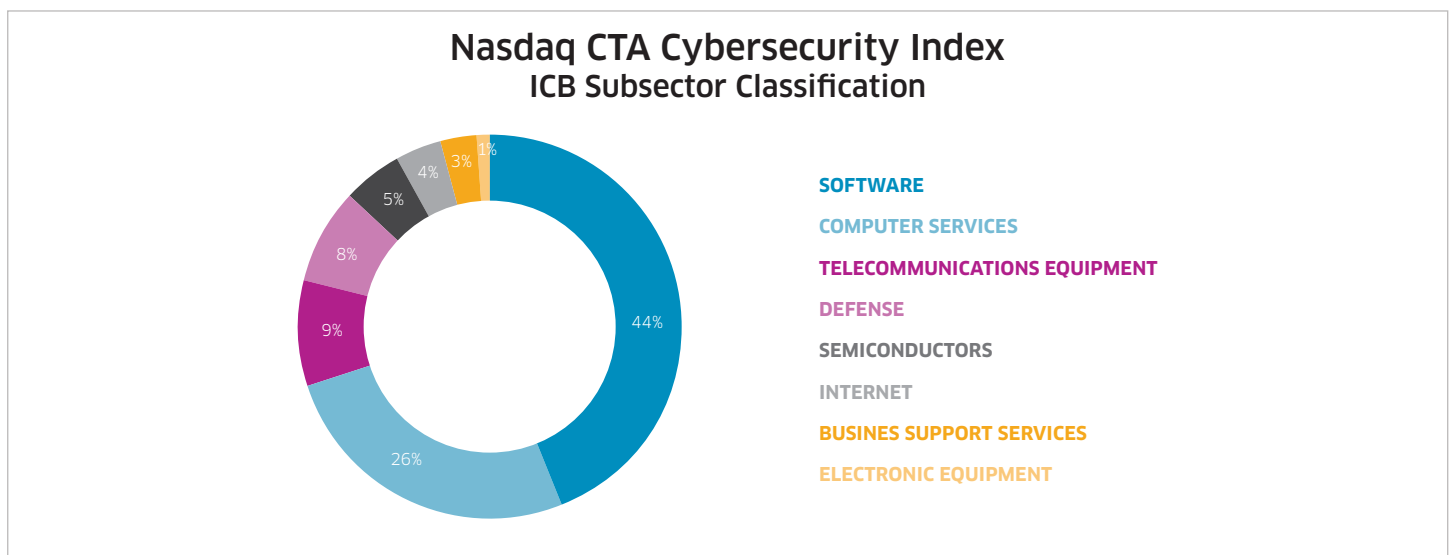
## How can People Invest in Cybersecurity?

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:

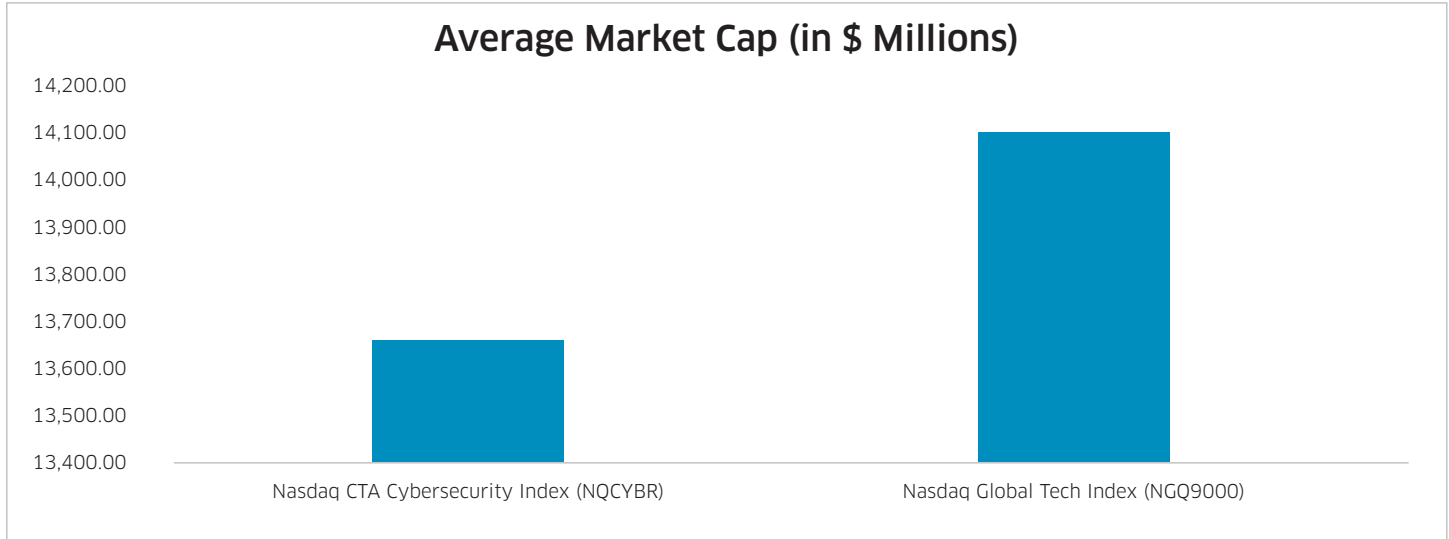
Nasdaq CTA Cybersecurity Index is poised to track companies that are engaged in the cybersecurity segment of the technology and industrial sectors. The Index includes companies, classified as a cybersecurity company by the Consumer Technology Association (CTA), primarily involved in the building, implementation 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%. <sup>11</sup>

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.

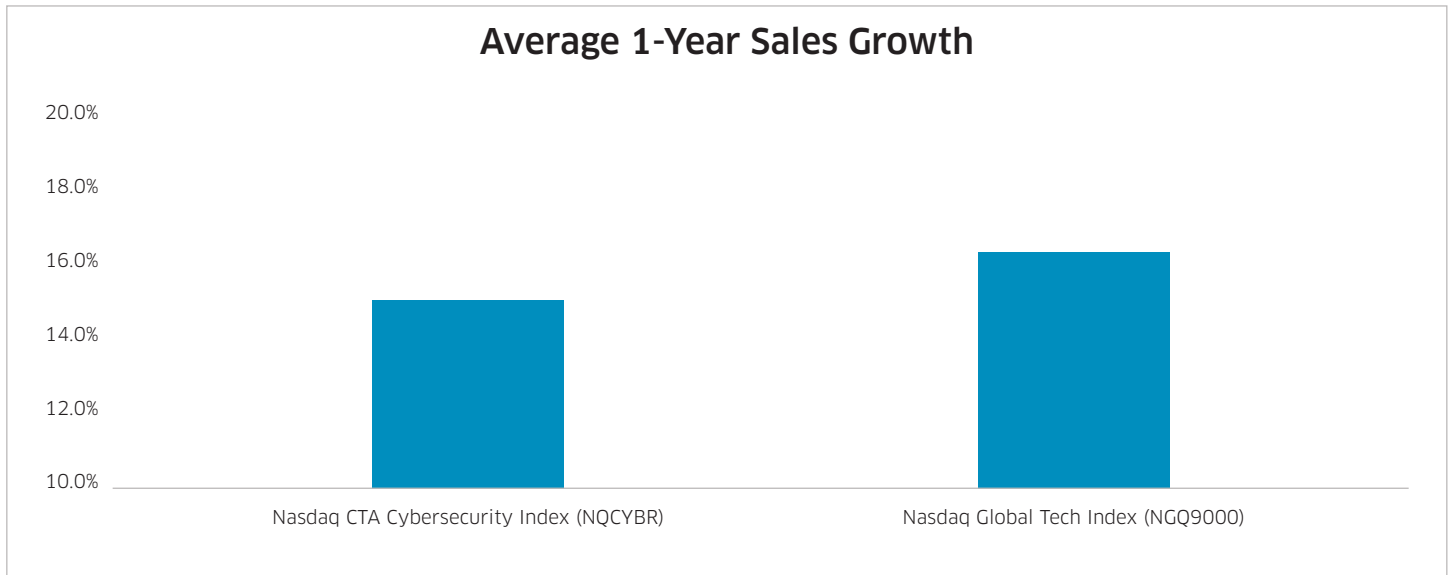


As of 3/31/2020

The components in this index are noticeably smaller, on average, than those in the Nasdaq Global Technology Index, which suggests that they may experience higher growth in the future. 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. This is an indication that that components of the index, which are smaller sized companies, are experiencing sales growth that is nearly in line with the benchmark.

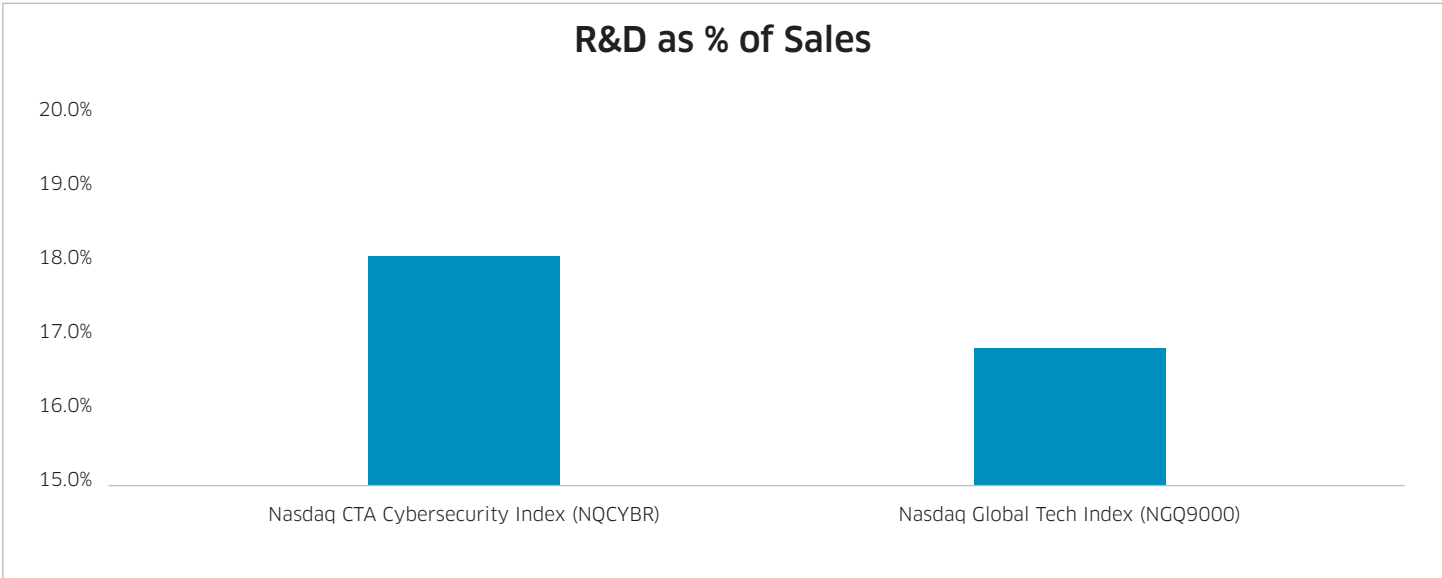


As of 3/31/2020



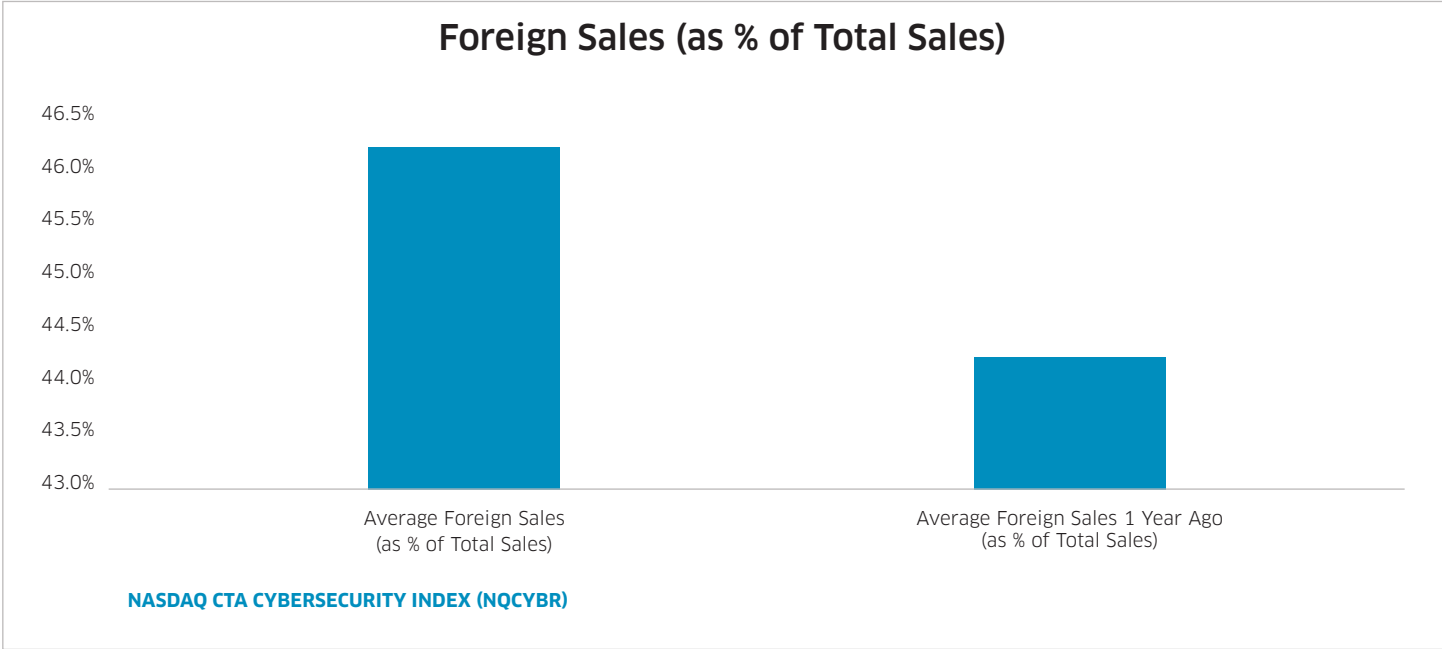
As of 3/31/2020

Since the components in this index are smaller and 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 average, companies in NQCYBR are investing more into R&D as those in the Nasdaq Global Technology Index - 18.00% versus 16.8%, respectively.



As of 3/31/2020

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 46.2% across all companies in this index currently, compared to 44.2% one year 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 3/31/2020

## 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/2019-data-breach-investigations-report.pdf>
2. <https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/>
3. <https://www.hackmageddon.com/2020/03/19/february-2020-cyber-attacks-statistics/>
4. [https://www.whitehouse.gov/wp-content/uploads/2019/03/ap\\_24\\_cyber\\_security-fy2020.pdf](https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf)
5. <https://www.cbinsights.com/research/smart-money-vcs-early-stage-cybersecurity-startups-expert-intelligence/>
6. <https://www.idc.com/getdoc.jsp?containerId=prUS45591619>
7. Bloomberg Intelligence (Mandeep Singh – Senior Analyst), December 26th, 2019 and IDC
8. [https://www.accenture.com/\\_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)
9. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>
10. <http://cybersecurityventures.com/cybersecurity-market-report/>
11. [https://indexes.nasdaqomx.com/docs/Methodology\\_NQCYBR.pdf](https://indexes.nasdaqomx.com/docs/Methodology_NQCYBR.pdf)
12. Data mentioned in the piece is from Nasdaq Index Research, Bloomberg, and/or FactSet, unless otherwise stated.

### Disclaimer

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.**

© 2020. Nasdaq, Inc. All Rights Reserved. 0893-Q20