Cybersecurity

Industry Report & Investment Case – NQCYBR

BY GAURAV PENDSE, PRODUCT DEVELOPMENT SPECIALIST, NASDAQ GLOBAL INFORMATION SERVICES

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 82% of incidents in 2017 in the Accommodation industry were because of Point-of-Sale)[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.

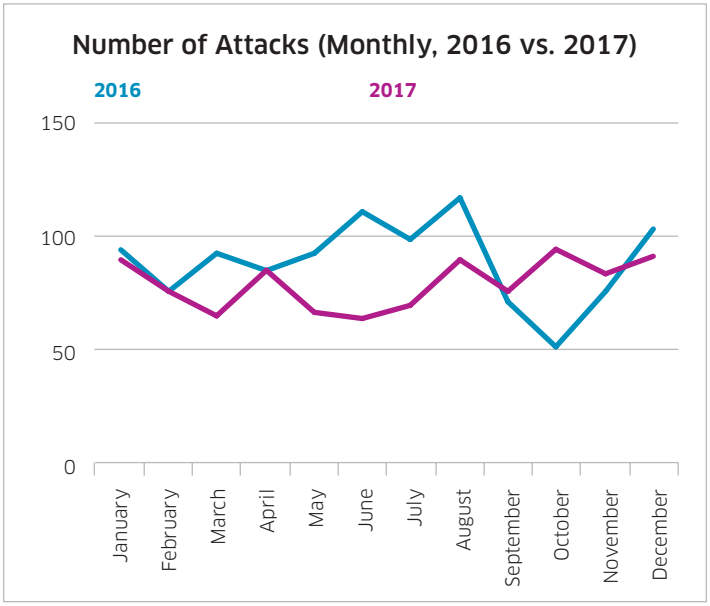
2017 INCIDENTS BY INDUSTRY	CRIME-WARE	CYBER-ES-PIONAGE	DENIAL OF SERVICE	EVERY-THING ELSE	STOLEN ASSETS	MISC. ER-RORS	CARD SKIMMERS	PRIVILEGE MISUSE	POINT OF SALE	WEB APPLICA-TIONS
Accommodation	5.65%	1.88%	0.27%	3.49%	1.08%	0.54%	1.61%	0.27%	82.26%	2.96%
Education	6.51%	2.40%	51.71%	16.44%	3.42%	5.48%	0.00%	4.11%	0.00%	9.93%
Financial	8.18%	3.51%	56.09%	9.85%	2.67%	3.67%	8.18%	1.50%	0.33%	6.01%
Healthcare	20.51%	18.38%	0.13%	8.39%	12.78%	24.10%	0.67%	3.20%	0.13%	11.72%
Information	1.87%	0.16%	19.06%	2.66%	0.10%	1.12%	0.00%	0.13%	0.07%	74.83%
Manufacturing	52.89%	4.10%	13.78%	7.26%	2.79%	0.56%	0.19%	15.27%	0.00%	3.17%
Professional	45.59%	5.15%	19.12%	7.54%	3.13%	5.51%	0.00%	7.54%	0.18%	6.25%
Public	26.27%	45.24%	3.08%	0.30%	16.36%	7.78%	0.00%	0.53%	0.00%	0.43%
Retail	8.20%	3.47%	26.81%	3.79%	2.21%	3.47%	25.55%	0.00%	3.47%	23.03%

Source: https://teiss.co.uk/wp-content/uploads/2018/04/FINAL-FINAL-C739-Verizon-DBIR_2018-Main_report-180404-24-optimised.pdf

Investors can get exposure to the cybersecurity industry in the US through the First Trust Nasdaq Cybersecurity ETF (Nasdaq: CIBR) and in Australia through the BetaShares Global Cybersecurity ETF (ASX: HACK) products. The underlying index for both of the ETFs is 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 the cybersecurity index above is poised to capture these positive trends in the cybersecurity industry.

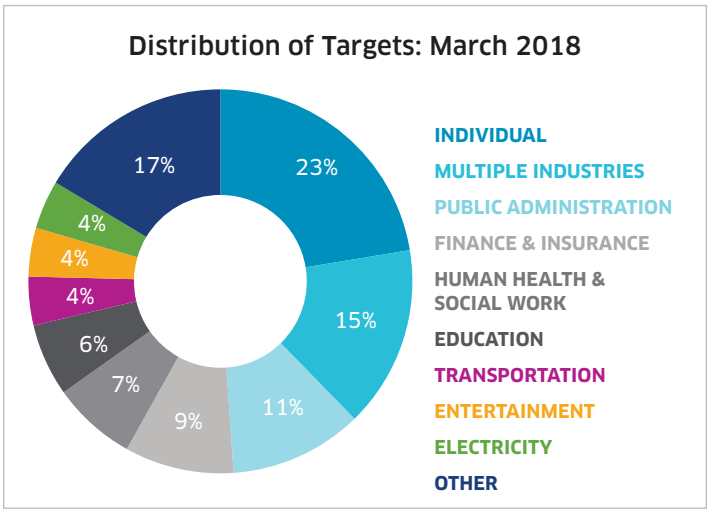
What is Driving the Growth in Cybersecurity?

The growth in cybersecurity is primarily driven by the necessary measures needed to counteract the increasing number of cybercrimes that people, businesses, and governments face on a daily basis. As the chart below shows, although the total number of major/publicized attacks worldwide that make it in the news decreased month-over-month for most of the months from 2016 to 2017, there are still sizeable and consistent number of major attacks on a monthly basis[2].

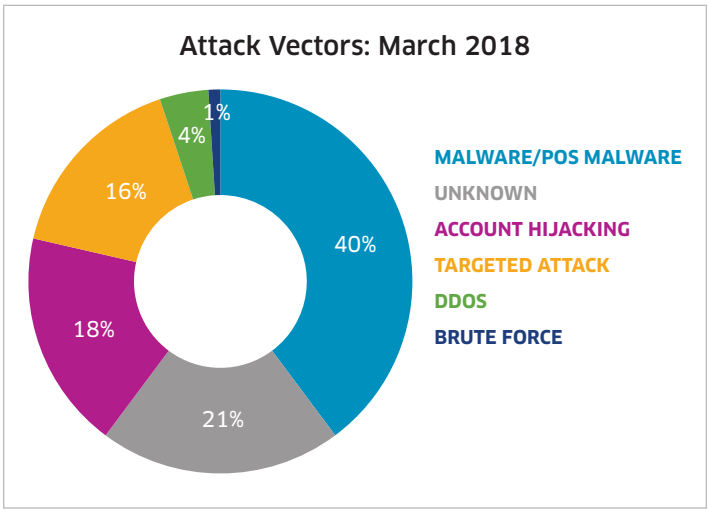


Source: https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/

In addition, the two charts below break down the attacks to highlight to whom the attacks are targeted towards as well as the way in which they were attacked. The charts illustrate that individuals, public administration, and finance are most targeted by cyberattacks, and malware and account hijacking were the most used modes of cyber attacks[3].



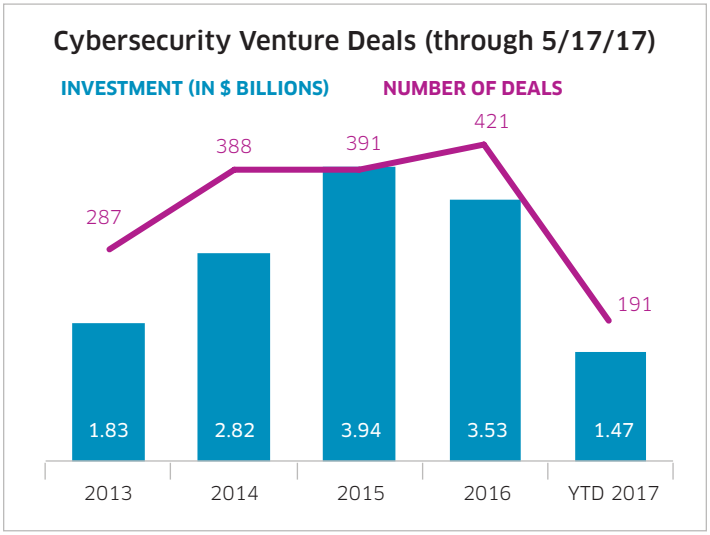
Source: https://www.hackmageddon.com/2018/04/19/march-2018-cyber-attacks-statistics/



Source: https://www.hackmageddon.com/2018/04/19/march-2018-cyber-attacks-statistics/

The impact of cyberattacks has grabbed the attention of the White House; President Trump has deemed cybercrime one of the biggest issues facing national security. In addition, the President's 2019 Budget is proposing to allocate $14.98 billion in spending to fund critical initiatives and research in the cybersecurity space, up from $14.4 billion in 2018 and $13.1 billion in 2017[4].

Aside from the growing number of targeted attacks that is driving the growth in cybersecurity, the number of cybersecurity venture deals also highlights the growth in this space. The chart below shows that venture capital firms have invested about $13.6 billion into cybersecurity companies since 2013[5].



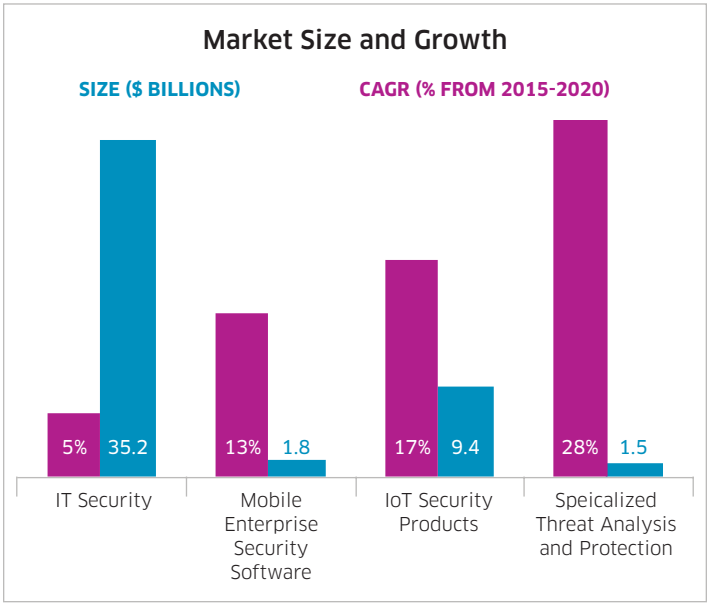
Source: https://www.cbinsights.com/research/cybersecurity-startup-deals-funding/

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 increasing cybersecurity measures taken by governments, organizations, and corporations bode well for the cybersecurity industry from an investment perspective.

What is the Industry Outlook for Cybersecurity?

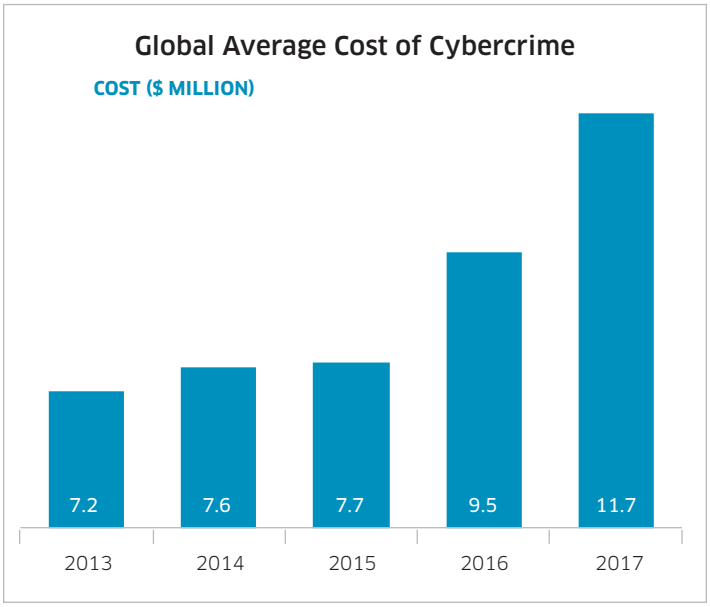
In addition to the increasing cyberattacks that is driving the growth in cybersecurity, the overall industry outlook for cybersecurity from an investment perspective is also positive.

A report from Business Insider Intelligence estimated that $655 billion will be spent on cybersecurity initiatives to protect PCs, mobile devices, and Internet of Things (IoT) devices by 2020, of which $386 billion will be spent on securing PCs, $172 billion on securing IoT devices, and $113 billion will be spent on securing mobile devices6. According to Bloomberg and IDC, the largest areas of growth within cybersecurity are mobile security, Internet of Things (IoT) security, and specialized threat analysis and protection[7]. The chart below reveals that while the three aforementioned growth areas are dwarfed by the overall IT Security market by size, their projected compound annual growth rates are expected to be significantly higher than that of the IT Security market. For instance, while the Specialized Threat Analysis and Protection segment is only about $1.5 billion in size (minuscule compared to the $35 billion IT Security segment), its projected compound annual growth rate is about 28%, much higher than the 5% projected growth rate for the IT Security segment[7]. This reveals that these three growth areas will continue to propel and expand the cybersecurity industry going forward.



Source: Bloomberg Intelligence (Anurag Rana – Senior Industry Analyst), Sept. 22nd, 2016 and IDC

Research conducted by Morgan Stanley suggests that the cybersecurity market could grow by more than four times the overall information technology spending by 2020[8]. In addition, research conducted by Accenture, as the chart below illustrates, shows that cybercrime costs for organizations continue to rise as the average cost of cybercrime per organization was up about 62.5% since 2013[9].



Source: http://www.morganstanley.com/ideas/cybersecurity-needs-new-paradigm

This suggests that, as cybercrime costs continue to rise for corporations, so will overall spending for cybersecurity measures, thus positively impacting the cybersecurity industry.

Other research from Morgan Stanley (survey from Chief Information Officers of major corporations) highlights that most of the executives surveyed planned to buy more than 15 different security technologies, showing the vast layers of security that are undertaken in many organizations and further highlighting the continued spending on cybersecurity services[8].

While on-premise cybersecurity solutions will continue to increase, cloud-based security, which represented roughly 12% of total spending on cybersecurity in 2015, is expected to grow to 20% of total spending on cybersecurity by 2019[8]. This will be, as mentioned above, in large part due to the proliferation of the Internet of Things, or connected devices such as household appliances, medical devices, cars, and more, which could all be vulnerable to cyberattacks. This expected growth in cloud-based security solutions for connected devices will continue to drive the overall growth for the cybersecurity industry.

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[10]. 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 reputations.

Overall, the above shows that the industry outlook for cybersecurity is very positive. Due to the increasing number of cyberattacks, as described in the previous section, the growth expectations for cybersecurity spending going forward are very high. Some of the key growth areas within cybersecurity, such as IoT security and cloud security, will help drive the growth of this industry. In addition, the rising costs of cybercrime and corporations' willingness to spend large amounts on cybersecurity is further justifying these growth expectations for the industry. As a result, continued growth and increased spending in this space strongly shows that the cybersecurity industry will be a profitable investment for the foreseeable future.

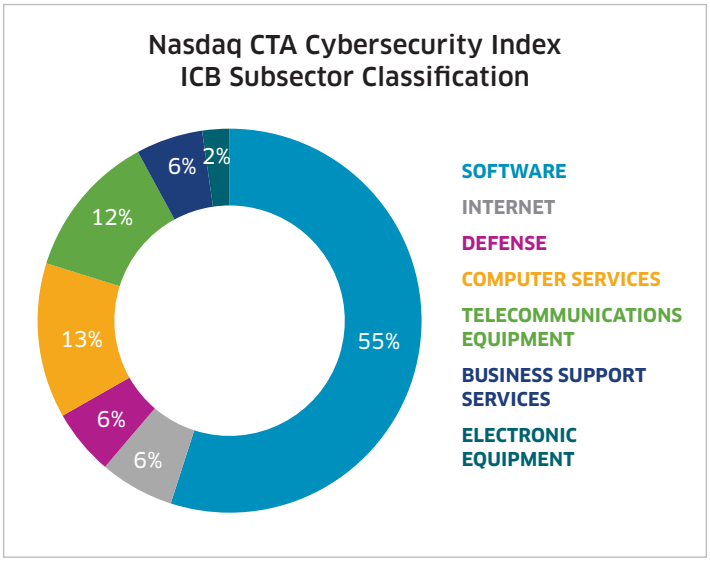
How can People Invest in Cybersecurity?

As mentioned above, investors can gain access to the cybersecurity space through the First Trust Nasdaq Cybersecurity ETF (Nasdaq: CIBR) and BetaShares Global Cybersecurity ETF (ASX: HACK) products; the underlying index for both of the ETFs is the Nasdaq CTA Cybersecurity Index (NQCYBR).

The methodology for NQCYBR is as follows:

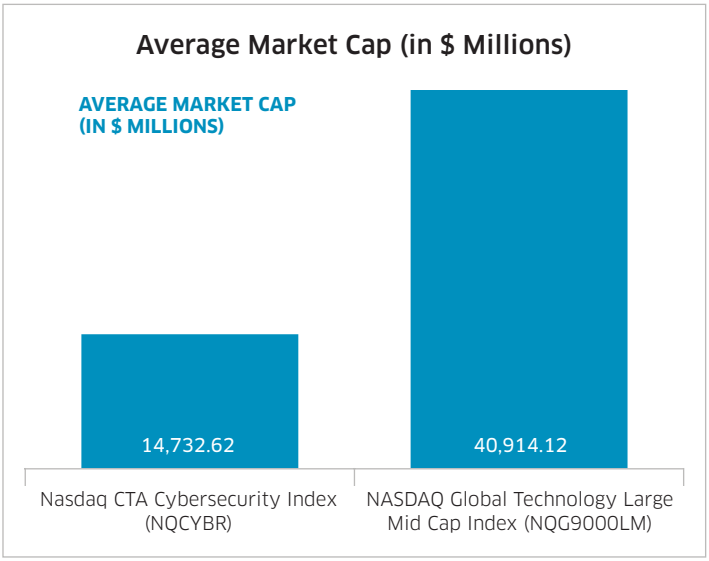
Nasdaq CTA Cybersecurity Index is poised to track companies that are engaged in the cybersecurity segment of the technology and industrial sectors. The Index includes companies, classified as a cybersecurity company by the Consumer Technology Association (CTA), primarily involved in the building, implementation 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, Electronic Equipment, Business Support Services, and Defense. This illustrates that investors are getting diversified exposure levels when they invest in the products tied to this index.

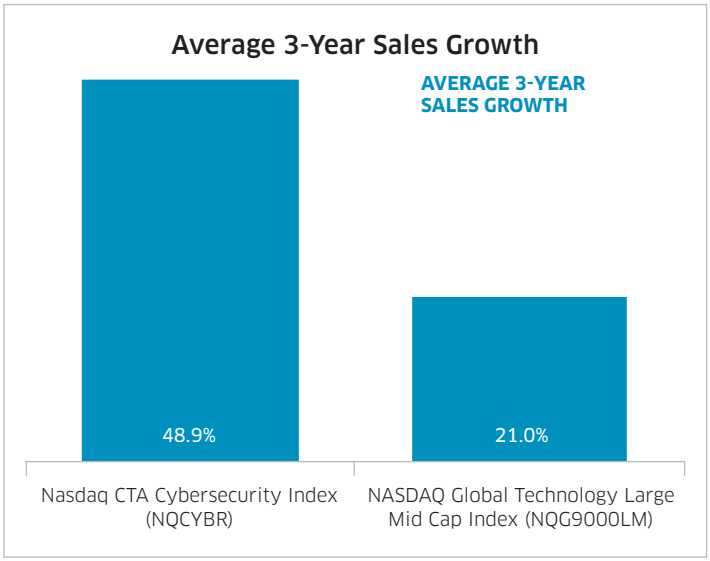


As of 5/31/2018

The components in this index are smaller, on average, than those in the NASDAQ Global Technology Large Mid Cap Index (NQG9000LM), which indicates that they are up-and-coming cybersecurity companies that may experience high growth in the future. In fact, as the chart below shows, components in this index have experienced higher sales growth over the last 3 years, on average, when compared to NQG9000LM.

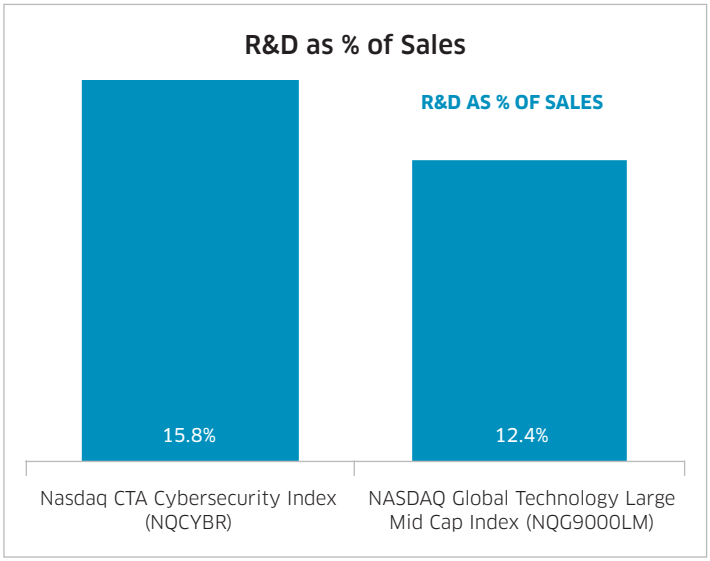


As of 5/31/2018



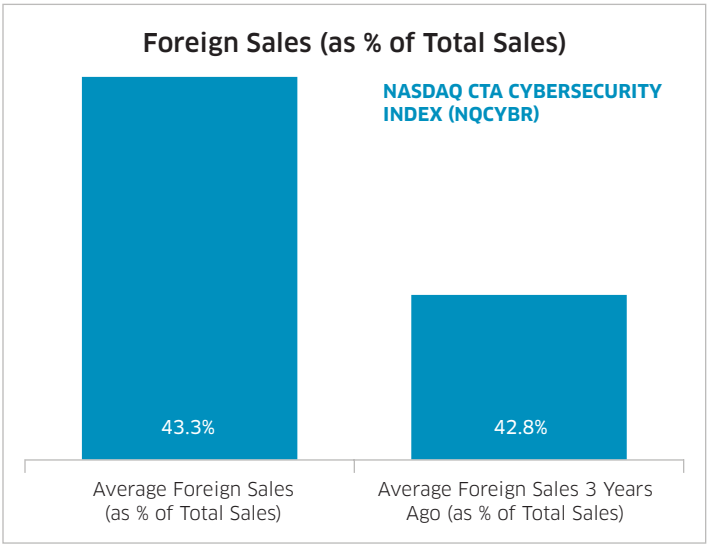
As of 5/31/2018

Since the components in this index are small and have experienced high sales growth, it is imperative to ensure that these companies are adequately investing their earnings into research and development to remain competitive in the fast-evolving cybersecurity landscape. This is, in fact, the case, as components in NQCYBR are, on average, investing more of their sales into R&D than those components in the NASDAQ Global Technology Large Mid Cap Index.



As of 5/31/2018

In addition, because cybercrimes affect people, governments, and organizations worldwide, it is vital that the components in this index capture the demand for cybersecurity services globally. In order to show that the revenue for the cybersecurity companies in NQCYBR is expanding globally, due to the demand for cybersecurity services internationally, one can look at the proportion of sales derived internationally of the companies in this index.



As of 5/31/2018

It is clear, then, from the chart above that the average foreign revenue of the components within this index is higher than it was five years ago, suggesting that the demand for cybersecurity has been continuing to expand globally and that these companies have taken advantage of that demand (note: foreign revenue is referring to revenue derived from countries in which the company is not domiciled in).

This analysis clearly shows that NQCYBR offers diversified exposure to investors looking to invest in cybersecurity. It also illustrates that, when compared to the broader NASDAQ Global Technology Large Mid Cap Index, the components in this index are relatively smaller but have experienced higher average sales growth thus far as well as spent a higher percentage of their revenue on research and development. In addition to this, the companies in NQCYBR have increased their proportion of sales internationally, on average. This shows that the components of the Nasdaq CTA Cybersecurity Index are up-and-coming companies poised to capture the strong projected growth in the cybersecurity industry.

Conclusion

In summary, the above analysis illustrates that cybercrimes have increasingly affected multiple industries in numerous ways, thereby boosting the demand for cybersecurity services. The continuingly increasing number of targeted attacks is driving the growth in cybersecurity services as major governments, such as the US government, and venture capital firms have continued to invest money into cybersecurity companies. In addition to the high projected growth rates by various industry research firms and analysts, IoT security, cloud security, and increasing cybercrime costs are going to continue to drive the spending in this industry moving forward. The Nasdaq CTA Cybersecurity Index offers investors a way to track diversified exposure to the cybersecurity industry. The index is composed of components that have experienced high sales growth and have increased their 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 are continuing to invest their revenue into research and development, which will help drive their revenue growth going forward, as the cybersecurity industry continues to evolve. In order to capture these positive trends for the cybersecurity industry, investors can invest in the products tied to the Nasdaq CTA Cybersecurity Index: First Trust Nasdaq Cybersecurity ETF (Nasdaq: CIBR) and BetaShares Global Cybersecurity ETF (ASX: HACK).

FOOTNOTES:

1. https://teiss.co.uk/wp-content/uploads/2018/04/FINAL-FINAL-C739-Verizon-DBIR_2018-Main_report-180404-24-optimised.pdf
2. https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/
3. https://www.hackmageddon.com/2018/04/19/march-2018-cyber-attacks-statistics/
4. https://fedtechmagazine.com/article/2018/02/cybersecurity-funding-would-jump-trumps-2019-budget
5. https://www.cbinsights.com/research/cybersecurity-startup-deals-funding/
6. http://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3
7. Bloomberg Intelligence (Anurag Rana – Senior Industry Analyst), Sept. 22nd, 2016 and IDC
8. http://www.morganstanley.com/ideas/cybersecurity-needs-new-paradigm
9. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
10. http://cybersecurityventures.com/cybersecurity-market-report/
11. 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.