Navigating the Dynamic Cyber Security World through the ISE Cyber Security UCITS Index (HUR)

Ben Jones, Product Development Specialist, Nasdaq

In 2015 Ginni Rometty, current executive chairman and former president and CEO of IBM, said, "cybercrime is the greatest threat to every company in the world."[1] The threat only continues to grow. In 2017, cyber theft was reported as the fastest growing crime in the US with cybercrime damages expecting to cost $6 trillion annually by 2021.[2] To combat the rise in cybercrime, the cyber security industry has grown and evolved over the past few years and is expected to grow as cybercrime remains a constant threat.

For instance, the cybersecurity market was valued at USD 161.07 billion in 2019, and it is expected to reach USD 363.05 billion by 2025.[3] Given these growth prospects, interest in the cyber security industry should continue to grow. In addition, the cyber security theme is diverse and constantly evolving, so in order to track it, any index must be robust enough to capture the nature of the theme as well as dynamic enough to evolve as cyber criminals and cyber security companies innovate alongside rapid technological and societal change. The ISE Cyber Security UCITS® Index (HUR) was one of the first cyber security benchmarks and has met the demand for tracking and measuring the cyber security market.

What sets HUR apart from its peers is the fact that it incorporates a unique cyber security classification framework, providing a way to track and measure the cyber security theme by identifying companies offering cyber security through infrastructure and services. Although the scope of the definition of cyber security can be quite broad and the fact that cyber security industry continues to change, HUR manages to capture the industry through its classification process of identifying cyber security infrastructure providers and service providers, setting it apart from other indexes seeking to track this space.

Dynamic Cyber Security World

For starters, businesses, organizations, and governments are constantly being bombarded with cybercrime and threats. To make matters worse, the global crisis sparked by the COVID-19 pandemic has led to an increase in cybercrime as well as hastened many businesses adoption of digital and cloud technologies, which has led to additional vulnerabilities. All of this is to stay that the cyber security industry and the world it protects is in a constant state of flux, meaning that a robust yet adaptable process for identifying and classifying cyber security companies is necessary for tracking and measuring this theme. Below is a quick list of recent cyber security anecdotes generated by the recent global crisis:

[1] https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/
[2] https://cybersecurityventures.com/annual-cybercrime-report-2020/
[3] https://www.mordorintelligence.com/industry-reports/cyber-security-market

- U.S. Threats - FBI's Internet Crime Complaint Center (IC3) received between 3,000-4,000 cybersecurity complaints daily – a rise from the normal average of 1,000.[4]
- U.K. Cyber Attacks - "February and March 2020, UK cyber attacks rose 37% month to month in the midst of the coronavirus crisis."[5]
- Financial Companies - Alert from Office of Compliance Inspections and Examinations (OCIE) observed an "apparent increase in sophistication of ransomware attacks on SEC registrants, which include broker-dealers, investment advisers, and investment companies."[6]
- The COVID-19 pandemic and the "global crisis is driving cloud adoption. 40% [of businesses] said COVID-19 is accelerating their move to the cloud.[7]" As a result, according to Gartner, "the coronavirus pandemic is driving short-term demand in areas such as cloud adoption, remote worker technologies and cost saving measures." [8]
- According to McKinsey & Co., the shift to working from home during the COVID-19 pandemic has "opened multiple vectors for cyberattacks," sparked a rise in "social engineer ploys," and has put more cyber threat pressure on public sector organizations.[9]

Another issue with properly tracking this theme is that there are so many different cyber threats and bad actors in the world, so it takes a number of different tools and companies to provide proper cyber security to defend against them. According to Norton LifeLock, a cyber-security company, "a cyberattack occurs when cybercriminals try to gain illegal access to electronic data stored on a computer or a network. The intent might be to inflict reputational damage or harm to a business or person, or theft of valuable data. Cyberattacks can target individuals, groups, organizations, or governments."[10]

More importantly, the cyber attackers can range from individuals to government-sponsored groups.[10] Because of the diverse nature of the cyber security problem, not only do traditional software and computer technology companies provide cyber security services, but there are also more traditional defense companies that have experience with providing defense services against government sponsors groups as well. Below is a list of different cyber threats and their descriptions from the Government Accountability Office (GAO).[11]

GAO Threat List:

- **Bot-network Operators** - Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
- **Criminal Groups** - Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
- **Foreign Intelligence Services** - Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of U.S. citizens across the country.

[4] https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
[5] https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/
[6] https://www.sec.gov/ocie/announcement/risk-alert-ransomware
[7] https://virtualizationreview.com/articles/2020/06/03/mariadb-survey.aspx
[8] https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem
[9] https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis)
[10] https://us.norton.com/internetsecurity-emerging-threats-cyberattacks-on-the-rise-what-to-do.html
[11] https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions

- **Hackers** - Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
- **Insiders** - The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
- **Phishers** - Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
- **Spammers** - Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
- **Spyware/Malware Authors** - Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
- **Terrorists** - Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken a target economy, and damage public morale and confidence.

(Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005). https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions)

Cyber security is a dynamic theme and sits at the cross-section of multiple industries, especially technology and industrials, as well as multiple sectors within technology, such as software and computer services. The diverse nature of this theme is a direct result of the diversity of challenges that businesses, governments, individuals, and organizations face, and the solutions that are available to address them. As well, some cyber security companies provide single or multiple solutions to the market, while other elements of cyber security are provided as offerings from diversified technology companies. Below is a list of various elements of cyber security sourced from the Digital Guardian.[12]

Digital Guardian's Elements of Cyber Security:

- **Network Security** - The process of protecting the network from unwanted users, attacks and intrusions.
- **Application Security** - Apps require constant updates and testing to ensure these programs are secure from attacks.
- **Endpoint Security** - Remote access is a necessary part of business, but can also be a weak point for data. Endpoint security is the process of protecting remote access to a company’s network.
- **Data Security** - Inside of networks and applications is data. Protecting company and customer information is a separate layer of security.
- **Identity Management** - Essentially, this is a process of understanding the access every individual has in an organization.
- **Database and Infrastructure Security** - Everything in a network involves databases and physical equipment.

[12] https://digitalguardian.com/blog/what-cyber-security

- **Cloud Security** - Many files are in digital environments or "the cloud". Protecting data in a 100% online environment presents a large amount of challenges.
- **Mobile Security** - Cell phones and tablets involve virtually every type of security challenge in and of themselves.
- **Disaster Recovery/Business Continuity Planning** - In the event of a breach, natural disaster or other event data must be protected and business must go on.

(Source: Digital Guardian, "What is Cyber Security? Definition, Best Practices & More, June 10, 2020, https://digitalguardian.com/blog/what-cyber-security)

Given the changing cybercrime landscape, as highlighted by the COVID-19 pandemic, the diverse array of cyber threats, and the growing number of elements of cyber securities, there are a plethora of emerging technologies to address cyber security. However, just like the dynamic nature of the cyber threats, cyber security technology is also dynamic and is a moving target for many cyber security customers. In essence, there is no one consistent technology or segment. The graphic below from the July 2020 Deloitte article, "Reshaping the Cybersecurity landscape,"[13] highlights cyber security priorities from a financial services industry survey. Notice how over the past three years, the number one cyber security priority has changed year after year.

Top Five Cyber Security Investment Priorities for Financial Institutions

	2018	2019	2020
1	Security continuous monitoring	Protective technology	Access control
2	Access control	Access control	Protective technology
3	Anomalies and events	Anomalies and events	**Data security**
4	Detection processes	**Data security**	Detection processes
5	**Data security**	Detection processes	Anomalies and events

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO Survey Reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis

Need for Cyber Security Classification

The cyber security industry continues to shift and respond to the needs of business, organizations and governments. As a result, we've identified four key reasons why a dynamic cyber security classification process is needed for cyber indexes: rapidly changing cyber threats means that cyber security industry will continue to evolve; the types of threat actors are diverse, so a diverse array of cyber securities solutions and companies must be represented; the market continues to shift investment in different emerging cyber security technologies, meaning that multiple solutions and companies must be represented and classified; and the number of solutions are diverse and range across a large cross-section of sub-sectors and industries.

To meet this need as well as given the lack of an existing generally accepted equity classification scheme identifying and cataloging equity securities of companies involved in the cyber security industry, the ISE Cyber Security® Industry Classification was developed by ISE (acquired by Nasdaq in 2016). The ISE Cyber Security® Industry Classification provides a framework for investment research, portfolio management and asset allocation.

ISE Cyber Security Classification

Eligible companies are publicly listed on exchanges globally and derive all or a "material" proportion of their revenues from cyber security or cyber security-related activities. Nasdaq is responsible for the classification of companies within the ISE Cyber Security® Industry Classification, maintenance of the database of companies comprising the ISE Cyber Security® Industry Classification, including the history of changes, and the timely communication of any updates to licensees of the data.

[13] https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

Nasdaq through its ISE Cyber Security® Industry Classification Committee relies primarily on published audited annual reports and discussions with company investor relations groups, industry participants and experts to vet companies for inclusion and determine their classification. Companies are allocated into a category based on the focus of their business. In cases where a company's business straddles two or more segments, a final category determination will be made based on audited reported revenue segments as well as discussions with that company's investor relations group.

Qualified and newly listed companies are assessed and approved by the Classification Committee for inclusion in the ISE Cyber Security® Industry Classification. As the cyber security industry continues to evolve, the framework of the ISE Cyber Security® Industry Classification will evolve in order to accurately reflect the then current state of the cyber security industry.

Any adjustments to the framework of the ISE Cyber Security® Industry Classification will be based on long-term trends driving the cyber security industry and will be announced in advance of implementation. In the event of a significant change to a company's structure or business, its classification may be reviewed on an ad-hoc basis. Events triggering a review include, but are not limited to: mergers, acquisitions, bankruptcy and delisting.

Companies will also undergo a quarterly review. Companies may not apply, and may not be nominated for inclusion in the ISE Cyber Security® Industry Classification. Additions and deletions to the list of companies eligible for classification may occur on an ad-hoc basis and is dependent wholly on the reported activities of those companies. No changes in the ISE Cyber Security® Index Classification will be based on nonpublic information.

All equities listed on exchanges globally are eligible for review. Companies are classified quantitatively and qualitatively. Each company is assigned to a single category according to its principal business activity based on audited financial reporting including the director's report. ISE uses revenues as a key factor in determining a company's principal business activity. Earnings and market perception are also recognized as important and relevant information for categorization purposes and are taken into account during the review process.

The scope of the definition of cyber security can be quite broad. For the purposes of the ISE Cyber Security® Index Classification, we consider cyber security to be concerned with enabling the protection of and secure communication between unique nodes of the internet from both external and internal threats.

The basic eligibility determinant for inclusion in the ISE Cyber Security® Index Classification is that prospective companies are either those which work to develop hardware and/or software that safeguards access to files, websites and networks from external origins or those that utilize these tools to provide consulting and/or secure cyber based services to their clients.

These two categorizations have been labeled as:

- **Infrastructure Provider** - a company that is a direct provider of hardware or software for cyber security and for which cyber security business activities are the key driver of the business.
- **Service Provider** - a company whose business model is defined by its role in providing secure cyber based services and for which those business activities are a key driver of the business.

Infrastructure Provider

Cyber security infrastructure providers provide hardware and/or software that help route and regulate message traffic in and out of networks. Two key areas of cyber security that fall into the infrastructure category are anti-virus and network security.

- **Anti-Virus** - Companies providing anti-virus solutions fall into the definition of Infrastructure Provider as they provide protection against threats originating from external sources.
- **Network Security** - Examples of the type of network hardware products these companies produce include gateways, routers, bridges and switches. The set of operating instructions and security, referred to as a firewall, is usually bundled with the specific hardware element by the manufacturer although third party software can often be adapted to work outside of its native environment. In the case of firewalls, often times, third-party solutions can provide more robust solutions than those packaged with network hardware.

Service Provider

Cyber security service providers provide services that fall outside the narrow definition of Infrastructure Provider. Service Providers allow for their clients to conduct business securely while Infrastructure Providers are providing security itself. For example, a company may be engaged in domain name management or managing the efficient routing of internet traffic but do not have the responsibility for the security of the domains themselves or the nature of the traffic they are routing. Another example would be companies involved in the manufacture of secure credit cards, network authentication devices and/or electronic identity documents.

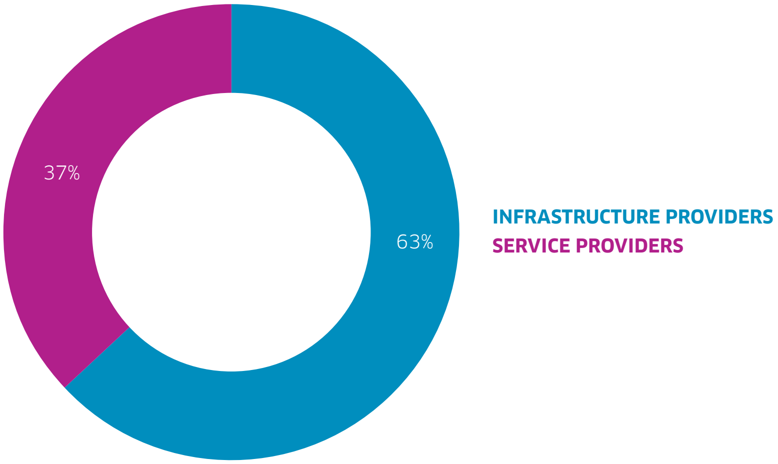
Index Methodology Summary

As a result of the ISE Cyber Security® Index Classification utilized the ISE Cyber Security® UCITS Index (HUR) provides investors with a product allowing them to quickly take advantage of both event-driven news and long term economic trends as the market for cyber security technology continues to evolve. The classification process employed allows the index to include companies that are service providers (hardware/software developers) for cyber security and for which cyber security business activities are a key driver of their business, as well as companies that directly provide cyber security services and for which cyber security business activities are a key driver of their business. Each component in the index must have a float-market capitalization of at least $100 million and a three-month average daily dollar trading volume of at least $1 million.[14] In addition, new adds into the index must also have a minimum five-day rolling average daily value traded over the previous 60 trading days of $750,000.

Index Cyber Security Industry Classification Breakdown

In looking at the ISE Cyber Security® Industry Classification breakdown in HUR, one can see that the index is overweight the Infrastructure Providers with a weighting of 63% while Service Providers account for 37% of the index (as of September 30, 2020).

ISE Cyber Security© UCITS Index: Cyber Security Classification Breakdown



Source: Nasdaq (As of September 30, 2020)

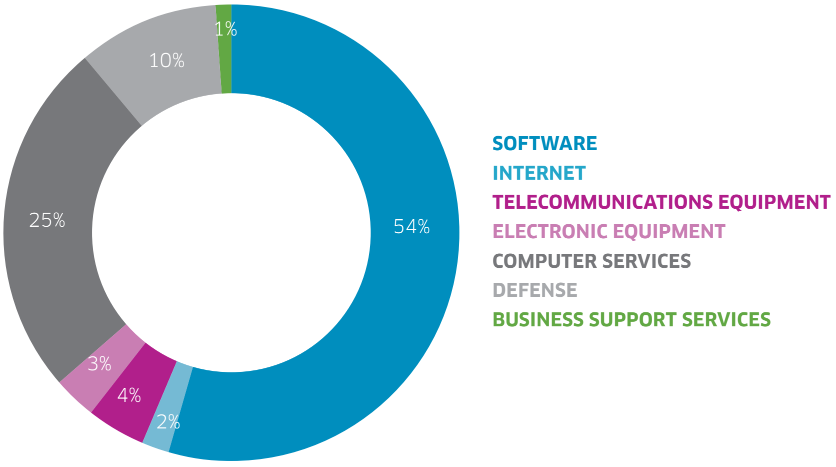
[14] Index Methodology Summary: https://indexes.nasdaqomx.com/docs/Methodology_HUR.pdf

Index Subsector Breakdown

Given the cyber security classification utilized in the index, what does the sub-sector breakdown look like in the index? How does it compare to the broader industry benchmark, such as the Nasdaq Global Benchmark Technology® Index (NQG10). Using ICB sub-sector classifications, when compared to the broader technology benchmark, HUR has a noticeable overweight towards the software and computer services subsectors compared to the technology benchmark.

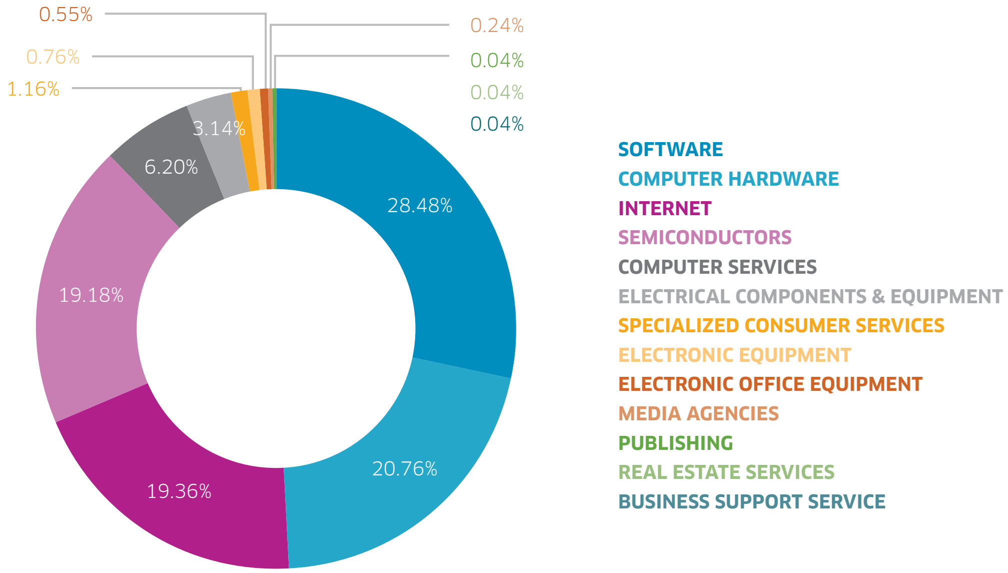
Specifically, as of September 30, 2020, HUR is roughly 54.90% software and 25.10% computer services while NQG10 is 28.48% and 6.20%, respectively. The other key aspect of the cyber security classification story is where HUR is underweight, which is primarily in the following subsectors – internet, semiconductors, and computer hardware. NQG10 is 19.36% internet, 19.18% semiconductors, and 20.76% computer hardware. Meanwhile HUR is only 2.49% internet, and has no semiconductors and computer hardware exposure.

ICB Subsector Exposure: ISE Cyber Security UCITS© Index (HUR)



Source: FactSet and Nasdaq (As of September 30, 2020)

ICB Subsector Exposure: Nasdaq Global Benchmark Technology© Index (NQG10)

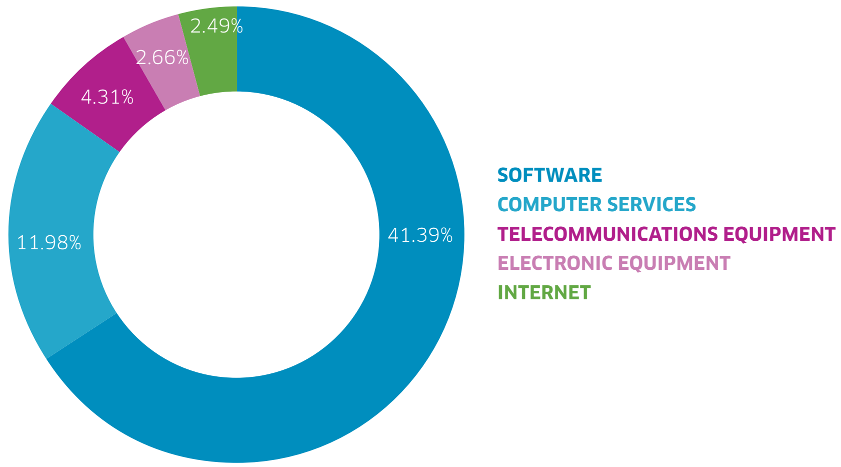


Source: FactSet and Nasdaq (As of September 30, 2020)

Looking at the ICB sub-sector breakdown of the infrastructure and service providers, one can see the differences in the two classifications. Specifically, infrastructure makes up the bulk of software companies present in the index while service providers are spread out among software, computer hardware, and defense. Based on component weighting data through September 30, 2020, out of the 54.05% allocation to software, 41.39% of that is comprised of infrastructure providers. Infrastructure providers make up 11.98% of computer services exposure, followed by 4.31% in telecom equipment, 2.49% in internet, and 2.66% in electronic equipment. The service providers represent a different set of subsectors. For starters, software and computer services subsectors do account for some service providers, with 12.66% and 13.11% allocated to those two subsectors, respectively. However, service providers also account for the defensive and business support services exposure at 10.04% and 1.35%, respectively.

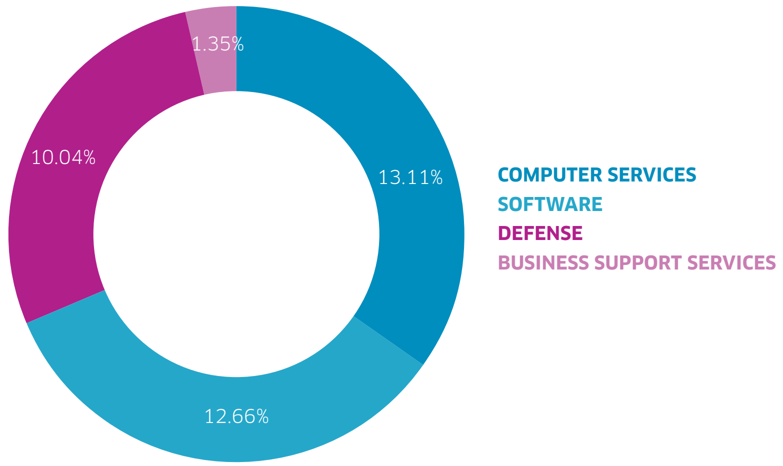
Two important differences between the cyber security infrastructure and service providers that stand out on a subsector level are found in the overweight towards software from the infrastructure provers, and the contribution of defense companies from service providers. (The graphs below display the weights of the each classification's subsector exposure in the HUR and is designed to provide a proportional view of each weighing in the index).

ISE Cyber Security UCITS© Index: Infrastructure Providers



Source: FactSet and Nasdaq (As of September 30, 2020)

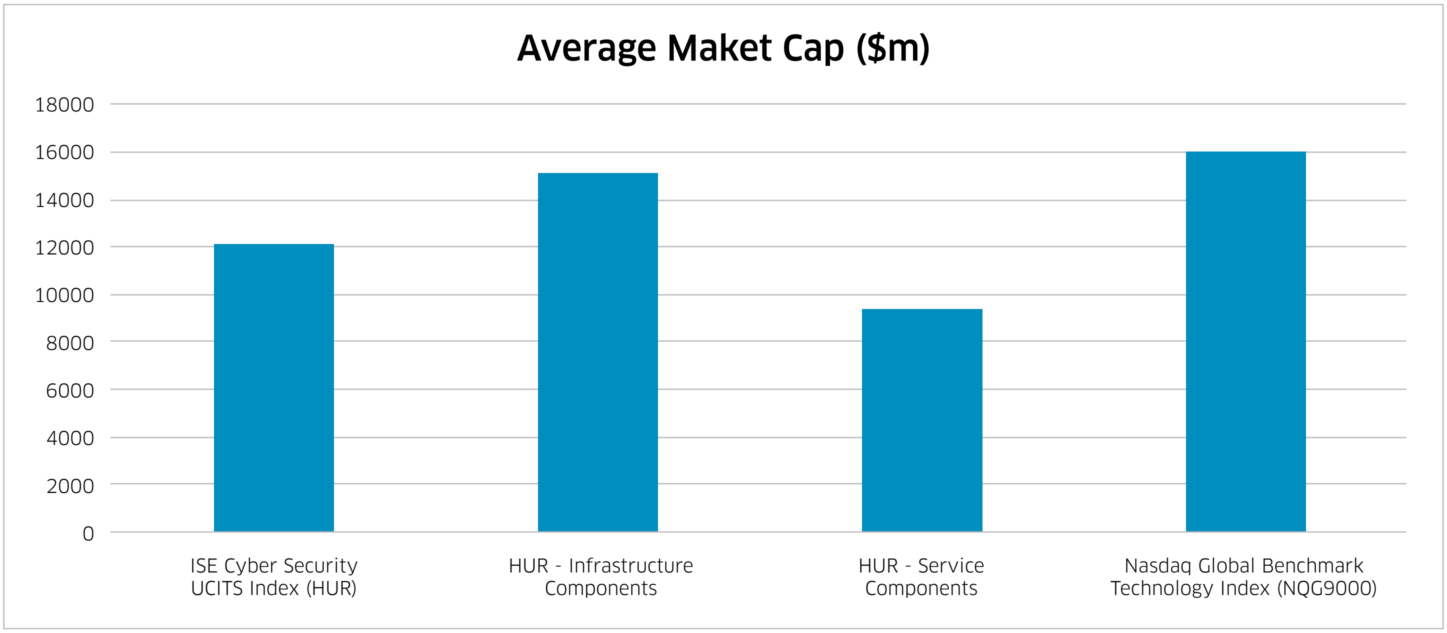
ISE Cyber Security UCITS© Index: Service Providers



Source: FactSet and Nasdaq (As of September 30, 2020)

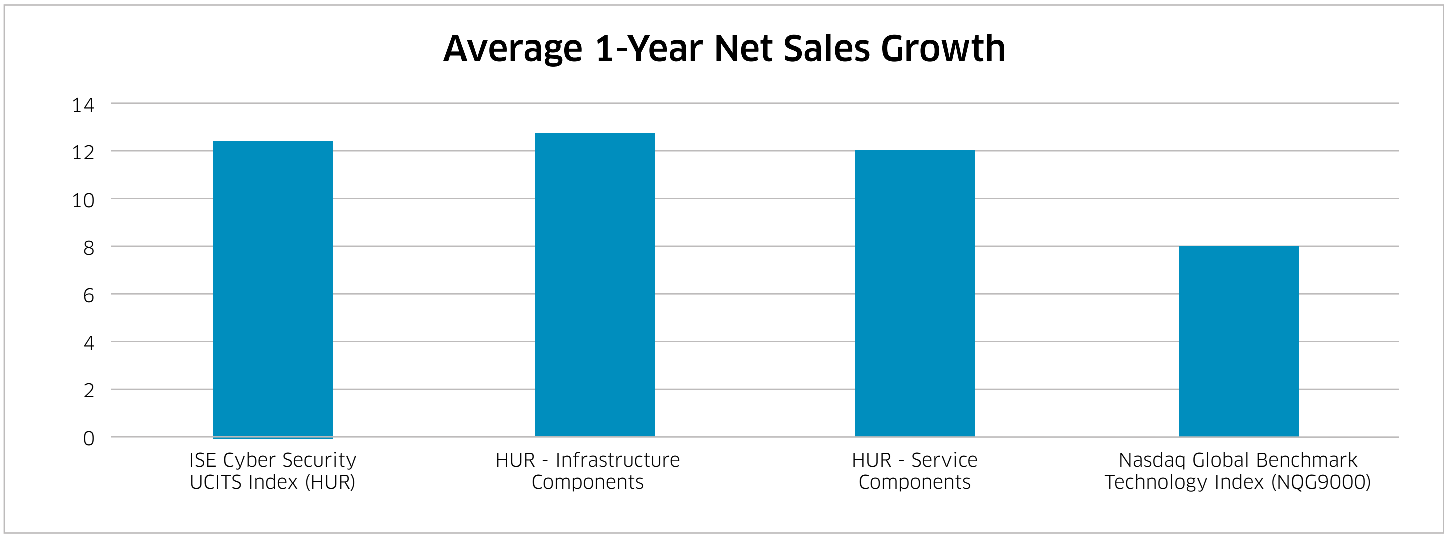
Characteristics of the ISE Cyber Security UCITS© Index Composition

From a size standpoint, the components of HUR are smaller, on average, than the Nasdaq Global Technology Index® (NQG10). That said, the components of the index are still primarily large cap. However, there is a noticeable difference in market capitalizations in the two classifications – infrastructure and service providers. The companies classified as service providers are much smaller on average than the infrastructure providers – just under $10 billion versus slightly over $15 billion, respectively.



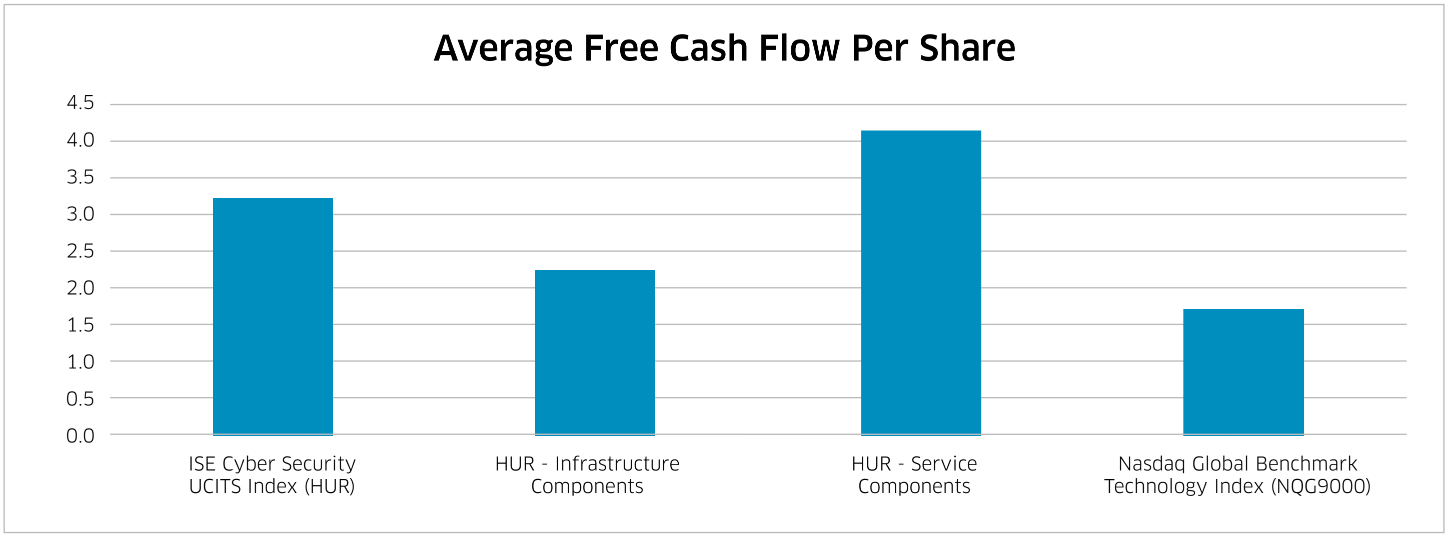
Source: FactSet and Nasdaq (As of September 30, 2020)

While market capitalization measures how large or small a company or industry is, it doesn't provide perspective to whether the area is growing and expanding. To track growth, we compared the one year net sales growth of the index components, which provides a way to measure how quickly and substantially the companies are growing. Both infrastructure and service providers are experiencing greater average sales growth than the technology benchmark. Although the service providers are smaller on average than their peers classified as infrastructure providers, the service providers are exhibiting higher average net sales growth. In fact, both classifications as well as the HUR have higher average net sales growth than the technology benchmark.



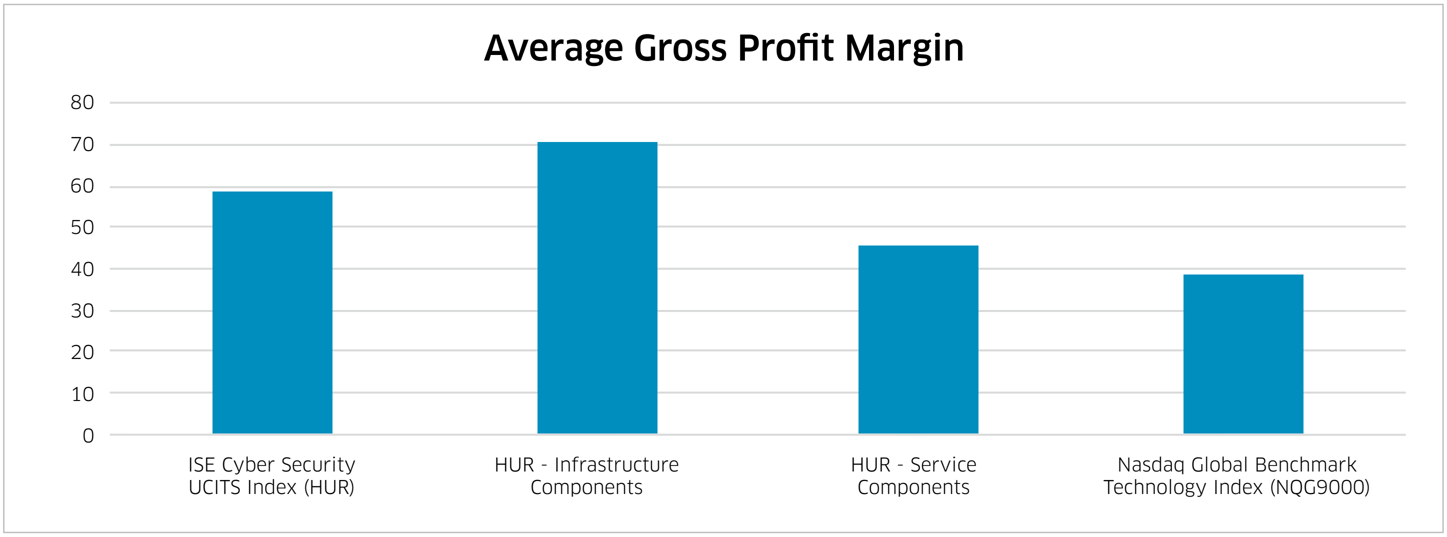
Source: FactSet and Nasdaq (As of September 30, 2020)

Another example of the financial strength present within companies making up the HUR can be found examining cash flow per share, which measures the free cash flow per share on a per-share basis. Within HUR, the service providers have the highest average cash flow per share at 4.18 while infrastructure providers sit at 2.27. So what services providers may lack in sales growth, they make up in free cash flow. For the entire HUR, the average cash flow per share is 3.26 while the benchmark, NQG10, has an average cash flow per share of 1.73 indicating that the cyber security companies present in the index are currently able to generate relatively, healthy cash flow.



Source: FactSet and Nasdaq (As of September 30, 2020)

Examining gross margins provides additional insight into the characteristics of the different cyber security companies within their respective classifications, provides insight into how profitable the different market segments are. As a whole, the HUR has higher average gross margin than the technology benchmark. Meanwhile, the infrastructure providers has a much higher gross margin than their peers in the service providers space, which is primarily driven by lower margins in the larger segments of this classification along with the defense companies.



Source: FactSet and Nasdaq (As of September 30, 2020)

Conclusion

Cyber security is a dynamic theme and is in a constant state of change. The ISE Cyber Security UCITS© Index (HUR), which is designed to measure the performance of cyber security companies, has provided a way of tracking and accessing the cyber security theme. The composition of the index through its classification system of cyber security infrastructure and service providers shows that a number of components possess attractive fundamental qualities, such as high gross profit margins and sales growth, as well as highlighting some of the size and fundamental differences between the theme and the technology benchmark. Thus, the HUR meets the challenges posed by the uniqueness of the cyber security space and paints a complete picture of the theme. Investors can gain exposure to this index through the L&G Cyber Security UCITS ETF (ISPY LN or USPY LN).

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.**