OMBA
ADVISORY & INVESTMENTS

OMBA THEMATIC PUBLICATIONS

Cybersecurity

June 2022

TABLE OF CONTENTS

OVERVIEW

Cybersecurity is becoming increasingly topical as the frequency of high-profile attacks and data breaches continue to rise rapidly, drawing significant attention in media headlines.[1] Russia's recent invasion of Ukraine has also put the topic front of mind as it brings to light the very real threat of state-sponsored cyberattacks and the vulnerability that companies, and countries face in this regard.[2] This is driving both government and private sector budgetary and spending support for the cybersecurity market which should result in continued demand and growth within the sector.

In addition, the continuation of global digitalisation and other technology-led megatrends (such as cloud computing, Work-from-anywhere and the Internet of Things) are driving device connectivity and causing an increase in the attack surface available for malicious actors to access and exploit. In addition, the continued development of these megatrends is increasingly reliant on cybersecurity to address associated threats, further driving demand for cybersecurity products going forward.

The resultant growth in the sector is demonstrated through a conservative estimate of a revenue Compound Annual Growth Rate (CAGR) of 9.5% through to 2030, with certain sub-sectors (such as identity security, network security and cloud security) expected to outperform the market aggregate CAGR over the period.[3]

Cybersecurity is certainly a theme that cannot be ignored and there is no doubt that the sector is growing. Although the fundamentals and drivers of growth indicate that the sector should do well going forward, investment is also about valuations and potential return. Prior to the recent stock market correction, valuations for the sector may have been a concern, with prices at all-time highs and price-to-sales ratios over 100 for certain high growth stocks within the sector. The recent sell-off, particularly in high growth (high duration) stocks, has, however, made valuations in the sector look far more attractive and may offer an appropriate entry point for investment into the sector. Omba is always mindful of valuations when assessing investment viability and when we invest into higher valuation growth sectors, we consider Growth at a Responsible Price "GARP".

CHAPTERS CAN BE READ INDEPENDENTLY:

- To understand more about cybersecurity just read on.
- To jump straight into the **Why Cybersecurity Matters** go to page 4.
- To better understand the **Cybersecurity Market**, look at page 8.
- We look at the **Investment Case** here on page 10.
- To look at **how to invest**, we dissect the **ETF landscape** and thematic expressions on page 14.

WHAT IS CYBERSECURITY?

Cybersecurity is the protection of internet-connected systems including hardware, software, networks, and data from cyberthreats.[4] Protection occurs through the application of technologies, processes, and controls which aim to prevent unauthorised exploitation of systems.[5] Cybersecurity aims to prevent cyberattacks, which include:

- **Denial-of-Service (DoS)** which occurs when an attacker floods servers with traffic to exhaust bandwidth or consume finite resources.
- **Ransomware** which is a type of malware that denies users access to data or systems. The attacker will then demand payment (or ransom) in exchange for the user to regaining access to their system.
- **Injection** which is an attack where a vulnerability in an application allows the attacker to inject code into a program or query to execute remote commands.
- **Phishing** which is the practice of stealing sensitive data by sending fraudulent emails that appear to be from a trustworthy source.
- **Brute Force** which is, simply, trial and error guessing of credentials in order to gain access to systems or data.[6]

DRIVERS: WHY CYBERSECURITY MATTERS?

1 | TECHNOLOGY-LED MEGATRENDS SUPPORT CYBERSECURITY GROWTH

Technology-led megatrends, such as cloud computing, work-from-anywhere, digitalisation and the Internet of Things (to name a few), are intensifying an already heightened cyberthreat backdrop by increasing device connectivity and the associated attack surface for malicious actors to exploit. These megatrends are creating an ever-evolving need for cybersecurity that addresses new cyber concerns as technologies evolve and new technologies emerge.

CLOUD COMPUTING

Cloud computing has increased the demand for cybersecurity by completely disrupting traditional IT environments, changing them from historically closed network environments to IT environments which exist across a collection of network connections, infrastructure resources, users, devices, and business applications. This fundamental change has significantly altered and increased the scope for cyber intrusions, driving new demand for cybersecurity.[7]

WORK FROM ANYWHERE TRENDS

"Work-from-anywhere" (WFA) perks and the expansion and increased speed of connectivity to the internet, via fibre optic cabling or satellite, are further driving cloud adoption and device connectivity via remote access to a company's IT environment and network. This trend was amplified by the COVID-19 crisis which made off-site work no longer a luxury or perk but a necessity for employees in many jurisdictions. The rapid migration to remote and hybrid work environments, necessitated a large migration to the cloud and increased device connectivity, creating a massive expansion of the attack surface for cyber criminals to exploit. According to a report by IBM, remote work was a factor in 17.5% of reported data breaches in 2021.[8] Moving forward, hybrid work environments will likely persist, and enterprises should continue to pursue digital transformation and cloud adoption, resulting in continued complexity and increasing demand for security software.[9]

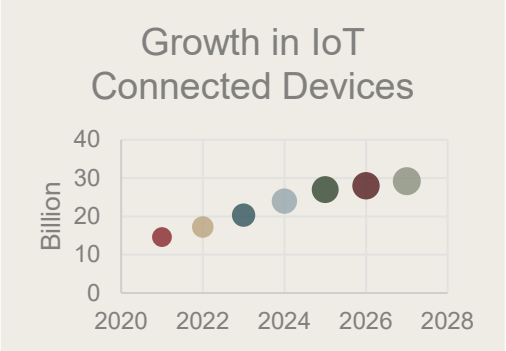
BIG DATA

Huge advances in technology have allowed for a massive increase in the collection and storage of data; the world now creates an estimated 2.5 quintillion bytes (25 000 000 000 000 000 000 bytes) of data every day.[10] This ever-expanding mass of data increases the scope of opportunities for cyber criminals.

Further, the monetisation of data by many companies, who process data into useful and useable insights, has made data even more valuable (represented by the mantra: 'data is the new oil').[11] As such consumers are becoming increasingly sensitive to the exploitation and use of their data as well as to data breaches, and cyber criminals are becoming more incentivised to access and exploit such data as the volume and value of this data increases.

DIGITALISATION & CONNECTIVITY

As digitalisation continues and technology advances so will the need for evolving cybersecurity. This is because each new technology brings about further connectivity and additional access to and collection of data. At the end of 2021, there were 14.6 billion connected devices, this number is predicted to grow by 18% in 2022, and then more than double by 2027.[12] This brings about a new set of vulnerabilities and opportunities for cyber intrusion. Innovative technologies and concepts, which include the continuing development of e-commerce platforms, the growing integration of machine learning, the Internet of Things and the Metaverse, will continue to drive this trend. [13]



**Source: Metrics used in above graph are derived from the IoT device numbers featured in the sources listed in the reference list below (n 13).*

2 | MACRO EVENTS PROVIDE BUDGET SUPPORT

ELEVATED THREAT LEVEL - CYBERATTACKS AS WEAPONS OF WAR

Russia's recent invasion of Ukraine has highlighted the threat of state-sponsored cyberattacks and increased the risk of cyberattacks between not only Russia and Ukraine but also Russia and the West.[14] If the conflict escalates further, either side could resort to malicious cyber activity, which would likely result in significant economic and social costs while avoiding direct military conflict.[15] It is believed that cyberattacks have already occurred during the current war - with the US claiming that Russia was responsible for denial-of-service attacks on the Ukrainian government as well as Ukrainian financial services websites.[16] Private companies have also reported the detection of new malware and note ongoing, elevated cyberattacks.[17] It is also likely that several cyberattacks, particularly those that are not intended to be destructive, are yet to be discovered. IBM notes that last year it took an average of 212 days to identify a data breach and an additional 75 days to contain one, thus the depth and extent of cyber intrusions may yet be determined.[18]

ELEVATED THREAT LEVEL – PUBLIC SECTOR FOCUS

Cybersecurity remains a key focus area of many governments. In the US, the cybersecurity concern is pervasive across government departments with both The Office of the Director of National Intelligence citing cyber threats as the most important strategic threat facing the US, and Federal Reserve Chair testifying that cyber risk is the risk that the Federal Reserve "keep[s its] eyes on the most now".[19] US public spending is also increasing in line with these concerns, with The Infrastructure Investment and Jobs Act having already allocated USD1.9 billion in cybersecurity funding across several programmes.[20] Additional money could be allocated going forward, with estimates of up to USD8 billion potentially

being allocated to the cybersecurity sector between now and 2026.[21] In addition, The White House has also signed a National Security Memorandum (NSM) directed at improving security posture across federal networks. The NSM aims to modernise cybersecurity defences by mandating baseline standards to identify, deter, protect against, detect, and respond to actions and threat actors.[22]

Elsewhere, other governments are also taking note, with the UK government committing to spending GBP2.6 billion on cyber and legacy IT, emphasising a need to improve cybersecurity.[23] Cybersecurity is also a key focus for the Chinese government, who have dedicated an entire section in their 14th Five-Year plan to digitise the nation.[24] China also aims to grow the cyber industry by USD38.7 billion by 2023.[25]

As indicated above, cybersecurity has increasingly become an area of focus for governments across the globe and as such the sector should continue to see budgetary support and growth for the foreseeable future.

ELEVATED THREAT LEVEL – CYBERSECURITY IS A KEY BUSINESS RISK

Following many prevalent and costly attacks in 2021, cybersecurity is front of mind as a key business risk for 2022. The average data breach cost increased from USD3.86 million in 2020 to USD4.24 million in 2021, with serval high-profile attacks making headlines and causing management as well as investors much concern. [26] This trend is likely to continue in 2022, with cyber risks and cybersecurity standing out as the most important business risk for decision makers to address in the next 12 months.[27] This focus on cybersecurity as a key business risk should result in increased spending and budget allocations to the sector, further supporting growth.

THREAT ACCELERATION

Following high profile, successful attacks there is usually an accelerated threat development cycle due to an influx of cash into that market and increased competition between attackers: “every time a threat actor crosses a line, the line gets pushed for all other players and actions today can open the door for incrementally more invasive threats”.[28] The threat environment is thus predicted not to improve but to further deteriorate in 2022.

CHANGING REGULATORY ENVIRONMENT

From a legislative perspective, governments and regulators are starting to incorporate cybersecurity into regulatory requirements. The Securities and Exchange Commission (SEC) has proposed amendments to its rules to enhance and standardise disclosures regarding cybersecurity risk management, strategy, governance as well as incident reporting by public companies.[29] In addition, cybersecurity resilience has been noted as a major ESG priority, as businesses understand their responsibility with respect to data security.[30] Increased regulatory pressure to report on cyber matters, coupled with a focus on ESG and enhanced data security regulations will further enhance companies' prioritisation of and spending on cybersecurity going forward.

3 | CONSOLIDATION WITHIN THE INDUSTRY

There is a trend of accelerated M&A activity and vendor consolidation starting in the cybersecurity industry. This should allow certain companies to offer a more integrated offering which might better serve the ultimate consumer, possibly boosting growth and valuations within the sector.[31]

4| MARKET TRENDS & THE CYBERSECURITY SECTOR

THE CURRENT BUSINESS ENVIRONMENT'S IMPACT ON CYBERSECURITY

The current business cycle may also offer a slight tailwind for the cybersecurity sector. As high inflation persists and the US Federal Reserve proceeds with implementing tighter monetary policy, a slowdown in the economy or even recession is possible. In such scenarios consumer staples are favoured over consumer discretionary. Even in a recession scenario, it is unlikely that individual consumers and companies will reduce their cybersecurity spend significantly, this should offer support to the cybersecurity sector in the current market downturn.

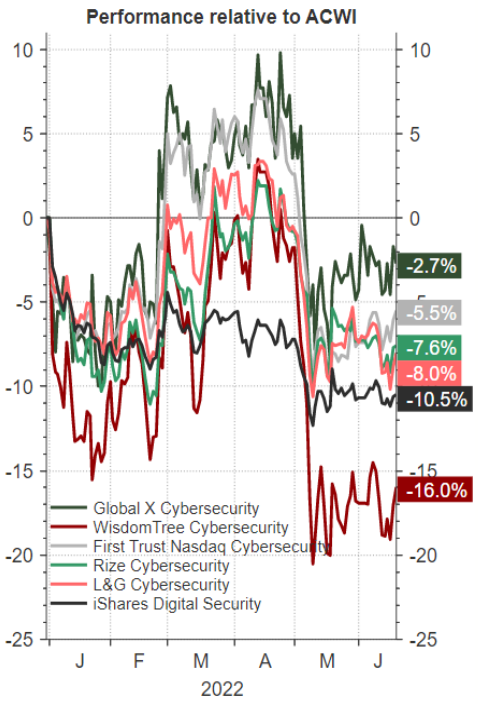
The elevated threat level also suggests that a valuation premium is justified and that the trend of increased spending on cyber defences could be a secular shift, that could outweigh the negative impact of a slowing economy and rising bond yields.[32] This is even more relevant following the recent correction in high growth stocks (which includes many cyber names).

CYBERSECURITY'S IDIOSYNCRATIC PROTECTION IN PORTFOLIOS

In addition, cybersecurity acts as a portfolio "hedge" to some degree during geopolitical tensions.

The graph on the right, which shows the performance of selected cybersecurity ETFs relative to the All-Country World Index (ACWI), depicts the sector's idiosyncratic movement during the initial period of Russia's invasion of Ukraine. An exposure to cybersecurity would have helped manage geopolitical risk within a portfolio acting as a diversifier, with certain cybersecurity ETFs exposures up almost 10% relative to ACWI between 24th February and the end of April 2022.

In addition, cybersecurity exposures have demonstrated other idiosyncratic protection, for example the sector may rally following a high profile cyberattack which could cause another sector-specific or broader market sell-off. The table below shows examples of recent cyber-attacks and demonstrates that cyber stocks (represented by an average performance of selected cyber-ETFs) generally perform better than both the stock of the company that has been attacked and the general market following an attack.



Source: Refinitiv Datastream - 21/06/2022

Table 1: The relative performance of selected stocks after being subject to a cyber attack

Share	Date of announcement of attack (T)	Date of low following attack	Share price prior to announcement (T-1)	Lowest share price in two weeks following the announcement	Performance of share	Performance of ACWI	Performance of S&P	Performance of Nasdaq	Average performance of selected Cyber ETFs
OKTA	22/03/2022	27/03/2022	169.41	138.11	-18.48%	+1.42%	+1.84%	+2.63%	+2.32%
Toyota	28/02/2022	08/03/2022	2104	1811	-13.93%	-6.55%	-4.88%	-6.49%	-2.65%
Nvidia	01/03/2022	07/03/2022	243.85	213.52	-12.44%	-5.78%	-3.95%	-6.45%	-4.97%

Source: Refinitiv

UNDERSTANDING THE CYBERSECURITY MARKET

Understanding the cybersecurity market is important when looking at the investment case for the theme or sector. To give readers a high-level understanding of the market, seven of the key segments or themes within the sector have been highlighted below:

1 | IDENTITY SECURITY

Identity security is concerned with authentication, both initial and continuous, as well as session monitoring and governance. Identity and access management (IAM) focuses on multifactor authentication, privileged access management, password vaulting, and role management.[33] With the recent explosion of remote work, securing access to critical data, resources, and apps is crucial for organisations. Key stocks in the segment include: OKTA Inc; CyberArk Software; Ping Identity; and SailPoint Technologies.

2| NETWORK SECURITY

Network security tools protect against threats traversing the corporate network. Network security products should find, block and alert on threats prior to them reaching endpoints connected to the corporate network.[34] Areas within Network security include Zero Trust Network Access (ZTNA), Software-Defined Networking (SDWAN), Network Detection and Response (NDR), Firewall / NGFW / Unified Threat Management (UTM), and Secure Access Secure Edge (SASE). Key stocks in the segment include: Fortinet; Zscaler; Cloudflare; Palo Alto Networks; Dark Trace; Fastly Inc; and Check Point Software Technologies Ltd.

3 | ENDPOINT SECURITY

Endpoint security is concerned with securing entry points of end-user devices such as desktops, laptops, and mobile devices from attacks. [35] If a device is connected to a network, it is considered an endpoint. Major technology-led megatrends are driving an increase in the type and number of connected devices. These devices include Android devices and iPhones, the latest wearables, all smart devices, voice-controlled digital assistants, as well as all other IoT-enabled smart devices which include network-connected sensors in cars, airplanes, hospitals, and even on the drills of oil rigs. As the different types of endpoints continue to evolve and expand, so the demand for the adaptable security solution in this space continues to grow.[36] Key stocks in the segment include: SentinelOne Inc; Trend Micro; CrowdStrike; NortonLifeLock; Fortinet; Mandiant Inc; AhnLab; and Microsoft (although Microsoft should not be included in any cybersecurity ETFs as it is a multinational corporation that operates across multiple sectors and thus this would not represent purity of revenue for the cyber theme).

4 | CLOUD SECURITY

Cloud security covers security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, data and resource access control, and data privacy protection.[37] Key stocks in the segment include: CrowdStrike; Palo Alto Networks; Cloudflare; Fortinet; Zscaler; SentinelOne Inc; Check Point Software Technologies Ltd; Tenable; and Fastly Inc.

5 | DATA PRIVACY & SECURITY

Data privacy is the protection of personal data from those who should not have access to it.[38] Increasingly, companies are going to be required to comply with data privacy regulations. This will add to the importance of protecting data from malicious attacks and further drive demand for data privacy and security. Key stocks in the segment include: OKTA Inc.; Varonis Systems; and CrowdStrike.

6 | DEVELOPMENT OPERATIONS & APPLICATION SECURITY

Development operations and application security involves addressing vulnerabilities resulting from an insecure development process in the design, coding and publishing of software or a website.[39] Key stocks in the segment include: Datadog; Splunk Inc; Palo Alto Networks; and Cloudflare.

7 | SECURITY ANALYTICS

Security analytics is a proactive approach to cybersecurity that uses data collection, aggregation, and analysis to perform vital security functions that detect and mitigate cyberthreats.[40] Key stocks in the segment include: CrowdStrike; Fortinet; Palo Alto Networks; Splunk; SentinelOne Inc; and Check Point Software Technologies Ltd.

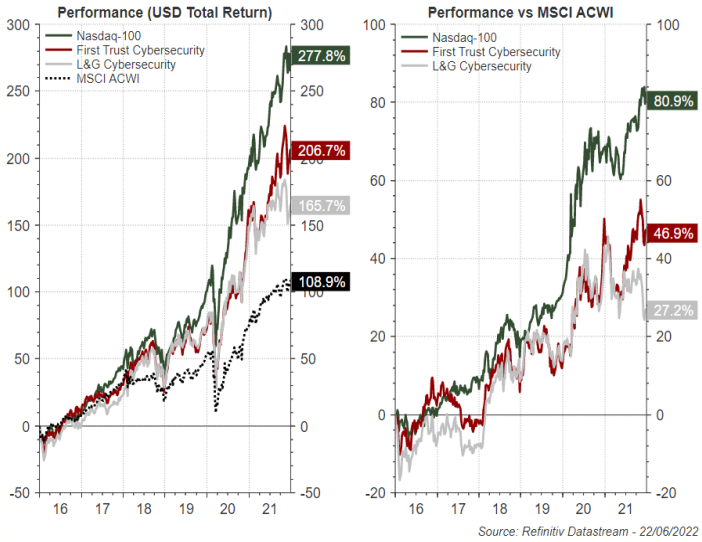
INVESTMENT CASE

This section looks at the investment case for the cybersecurity theme, including expected growth of the market as well as valuations and potential share performance.

1 | UNDERSTANDING MARKET GROWTH

HISTORIC GROWTH AND PERFORMANCE

The cybersecurity market grew at a CAGR of around 9.5% from 2016 to 2021 despite a slight dip in growth in 2020, due to the closure of several organisations during the first and second quarters of 2020.[41] Following this, the market recovered quickly as the COVID-19 pandemic caused security solutions to experience higher than anticipated demand across all regions compared to pre-pandemic levels. During this same period, the value of cybersecurity stocks (depicted using cybersecurity ETFs) increased substantially (refer to the left-hand graph on the right) with cyber stocks outperforming MSCI ACWI by more than 25% over the period (refer to the right-hand graph on the right).

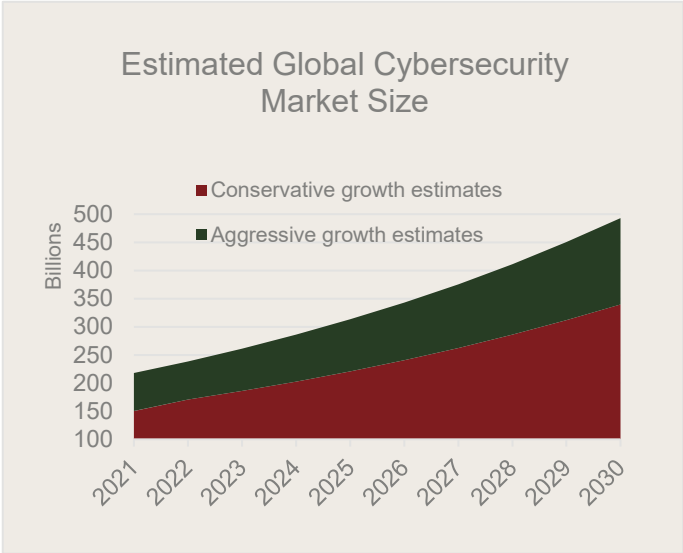


LOOKING FORWARD

Conservative growth estimates for the global cybersecurity market predict that the market will continue to grow at a CAGR of around 9.5% from 2022 to 2030 (while more aggressive forecasts predict the market to grow at a CAGR of between 12% – 14% from 2022 to 2030).[42]

Within the cybersecurity sector, identity security and network security are expected to outperform with an average compound CAGR between 2021 and 2026 of 19% and 24% respectively.[43]

Endpoint security is also highlighted as an area which may experience a higher-than-average revenue CAGR. Endpoint security experienced massive growth in 2020 and 2021 as COVID drove an increase in connectivity of devices, resulting in market growth of 17% and 19%, respectively. In addition, certain cloud-based players in the space delivered a trailing 2-year CAGR of 88%.[44] [45]



**Source: Metrics used in above graph are derived from the market size and growth estimates featured in the sources listed in the reference list below (n 45).*

The continued development and expansion of the IoT should continue to drive growth in this sector of the market, however, the magnitude of this disparity of growth is expected to narrow, with the endpoint market only forecast to grow at around 16% from 2022 – 2024, just above the market aggregate.[46]

Finally, cloud computing is an area that is expected to drive increased growth and budget allocation for the cybersecurity sector, the cloud security market is estimated to grow at around 13% CAGR from 2022 – 2026, with cloud computing expected to be net positive for budget allocations to the sector.[47]

In conclusion, growth is expected to continue at high levels through to 2030, this is in line with expectations based on the drivers of demand set out in the *Why Cybersecurity Matters* section of this piece. Generally, high growth should support valuations and stock performance overtime, however, current valuations (and the degree to which future growth and performance has already been priced into a sector) is also an important consideration in the investment decision making process.

ADOPTION CURVE SUPPORTIVE OF SUSTAINED GROWTH

Another very important aspect to consider when looking at the future growth of a market is the adoption curve. Every new product category and technology has an adoption curve, which is the cumulative rate that a population adopts a product, service, or technology over time.[48] An adoption curve is made up of five different segments of adopters, based on their tendency to adopt new products and technologies. These five segments can be broken down as follows: the innovators, early adopters, early majority, late majority, and laggards. The potential market growth will vary in each segment/stage of adoption, with the high growth tending to occur around the early majority stage as illustrated in Image 1 & 2 below.

Image 1: The five segments of the adoption curve.

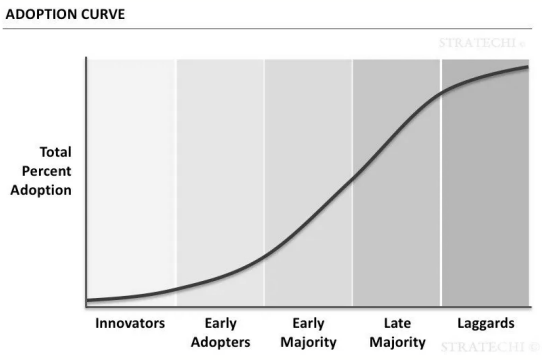
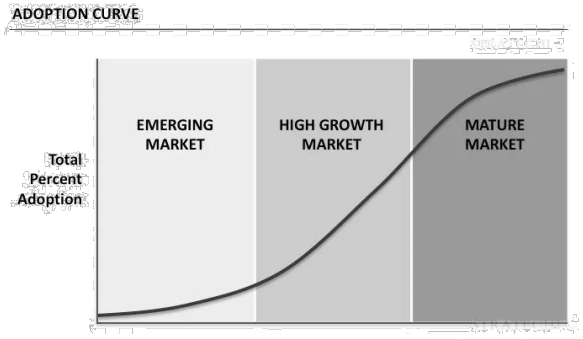


Image 2: Expected growth across the segments/curve.

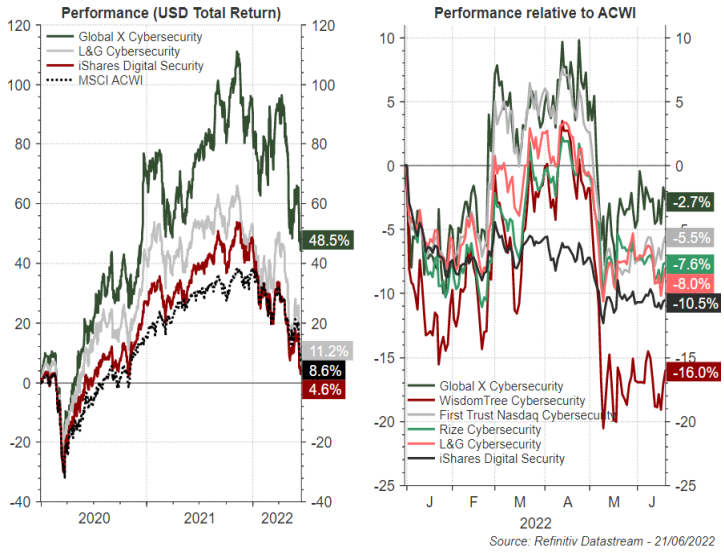


Source: Stratechi – Adoption Curves

Based on the forecast growth of the cybersecurity market, the sector appears to be in the early majority phase of the curve, in a high growth market. This is supported by evidence of increasing adoption rates being driven by the megatrends outlined in the *Why Cybersecurity Matters* section of this piece as well as a heightened threat environment and increasing awareness of cybersecurity threats. The adoption curve, and more importantly where the sector is on the curve, is also supportive of high growth in the cybersecurity market going forward.

2 | VALUATIONS

As depicted in the left-hand graph on the right, valuations for the cybersecurity sector (and the broader market) peaked in late October/early November 2021, following a hot bull market since the March 2020 COVID lows. Loose monetary conditions and pent-up demand drove the broader market higher in late 2020 through to the end of October 2021, with high growth ('high duration') stocks outperforming in the low interest rate environment. In addition, the cybersecurity market grew substantially over this period, with the pandemic acting as a catalyst for increased demand for and adoption of cybersecurity solutions, further driving share performance. The MSCI ACWI was up more than 35% from pre-COVID levels at its peak (end October 2021), all cybersecurity ETFs outperformed ACWI, growing by 50% – 110% from pre-COVID levels (refer to graph on the left-hand side above).



On the contrary, as depicted in the left-hand graph above, 2022 year to date (YTD) has been brutal for all stocks, and cybersecurity has not been spared. Inflation fears and concomitant tightening monetary policy (rising interest rates and bond yields), Russia's war in Ukraine and China's Zero Covid policy have cause a significant and broad market sell-off (excl. energy and commodities), with the S&P 500 and Nasdaq both posting their worst start to a year since 1939 and 1971, respectively. Cybersecurity has not been spared, as the sector contains high-multiple names that are highly sensitive to interest rate movements. The latest, extreme sell-off followed the first 50bps rate hike by the Fed on the 4th of May 2022 (see far right-hand side of right-hand graph above), demonstrating the sector's increased sensitivity to interest rate movements. Volatility has continued into June, following a higher-than-expected inflation print of 8.6% and resultant 75bps point hike by the FED, which has fuelling recession fears. While things remain volatile, the extreme sell-off could, in our view, present an opportunity to add to the sector.

Table 2 below looks at selected performance metrics, namely price, price-to-sales ratios, and revenue growth, for selected stocks in the cybersecurity space. Looking at the selected single stocks within the sector, the valuation story is much the same with the current share price of the majority of the selected stocks well below their October/November 2021 highs. The table also demonstrates a recent decline in the price-to-sales ratios for most of the selected stocks, following the latest sell-off combined with continued revenue growth in the sector.

Of the selected single stocks, there are a few that have outperformed their peers as well as the broader market, namely Checkpoint, SailPoint, Trend Micro, Mandiant and Ahnlab, with some of these stocks up 20 – 30% since October 2021. Generally, the selected stocks that outperformed had lower earnings growth and lower price-to-sales ratios than other stocks in the sector, indicating that these are lower growth stocks. The outperformance of these stocks may suggest that there is strength in the cybersecurity market which could be net positive for medium to high growth cybersecurity stocks should interest rate fears (and the resultant extreme selling pressure on high duration stocks) abate.

Conversely, the stocks with the highest price-to-sales ratios in October 2021, namely Crowdstrike, Zscaler, Sentinelone, Cloudflare and Datadog, are down more than 40% from their October 2021 prices. Sentinelone and Cloudflare, the two stocks with the highest price-to sale-ratios in October 2021 (both over 100) are down significantly, 67% and 71%

respectively, further corroborating that high growth stocks have been subject to higher selling pressure than lower growth stocks in the same sector.

Table 2: Analysis of price action, price to sales ratio and revenue growth for selected Cyber stocks

	Price movements current (9 May 2022) relative to x				Price to Sales ratio				Revenue Growth Year on Year			
	x = 31 Oct 22 (Recent highs)	x = 20 Mar 20 (Covid lows)	x = 31 Dec 19 (Pre-covid)	x = 31 Dec 16	Current	Recent highs	Covid lows	Pre-covid	Latest (T)	Prior year (T-1)	(T-2)	(T-3)
Palo Alto Networks Inc	-9.7%	+220.1%	+98.7%	+267.5%	9.3	11.7	4.3	6.5	+24.9%	+17.5%	+27.5%	+29.5%
Check Point Software Tech	-0.3%	+32.9%	+7.5%	+41.2%	7.0	7.5	6.3	8.5	+4.9%	+3.5%	+4.1%	+3.3%
Fortinet Inc	-27.1%	+188.8%	+129.7%	+714.1%	11.0	18.9	5.8	8.5	+28.8%	+19.9%	+20.1%	+20.5%
Nortonlifelock Inc	-3.5%	+44.9%	+66.6%	+78.0%	5.2	5.6	4.1	3.0	+9.6%	+2.4%	+1.4%	-4.0%
Tenable Holdings Inc	-19.7%	+133.9%	+78.5%	N/A	8.2	11.8	4.1	6.7	+22.9%	+24.2%	+32.6%	+42.4%
Sailpoint Techno	+30.9%	+322.2%	+166.2%	N/A	12.8	11.4	4.2	7.4	+20.2%	+26.6%	+15.9%	+33.8%
Trend Micro Inc	+11.8%	+87.7%	+28.4%	+73.0%	5.3	5.0	3.1	4.8	+9.4%	+5.4%	+3.0%	+7.8%
Crowdstrike Ho-A	-49.0%	+193.2%	+188.1%	N/A	23.0	56.5	14.4	22.0	+66.0%	+81.6%	+92.7%	+110.4%
Mandiant Inc	+24.7%	+121.6%	+31.5%	+82.7%	10.2	9.5	2.3	4.1	+21.0%	+20.6%	-60.1%	+6.6%
Zscaler Inc	-52.0%	+185.4%	+229.2%	N/A	25.1	65.7	N/A	N/A	+56.1%	+42.4%	+59.2%	+51.3%
Rapid7 Inc	-48.4%	+78.8%	+18.7%	+446.3%	6.7	15.7	4.7	8.6	+30.1%	+25.9%	+33.9%	+21.5%
Okta Inc	-64.1%	-23.1%	-23.0%	N/A	10.7	37.5	18.3	24.4	+55.6%	+42.5%	+46.8%	+55.6%
Ping Identity Ho	-29.5%	+9.5%	-17.8%	N/A	5.4	8.7	5.4	8.1	+22.9%	+0.3%	+20.5%	+16.8%
Sentinelone Inc -Class A	-67.0%	N/A	N/A	N/A	29.1	127.9	N/A	N/A	+120.1%	+100.2%	N/A	N/A
Ahnlab Inc	+29.6%	+135.7%	+62.3%	+83.9%	5.1	4.5	N/A	N/A	+16.3%	+6.7%	+4.5%	+6.4%
Cloudflare Inc - Class A	-71.0%	+160.4%	+231.5%	N/A	25.3	118.1	16.8	18.1	+52.3%	+50.2%	+49.0%	+42.8%
Datadog Inc - Class A	-41.6%	+192.2%	+158.2%	N/A	25.7	68.2	18.4	31.8	+70.5%	+66.3%	+83.2%	+96.6%
Splunk Inc	-45.4%	-18.4%	-39.9%	+76.0%	5.4	11.0	6.7	9.9	+19.9%	-5.5%	+30.8%	+37.7%
Fastly Inc - Class A	-76.8%	-33.7%	-41.5%	N/A	3.8	18.4	6.5	9.6	+21.8%	+45.1%	+38.7%	+37.8%

Source: Refinitiv

INVESTMENT CASE SUMMARY

Cybersecurity stocks have not been spared in the latest sell-off, in fact high-growth cyber stocks have been particularly hard hit with many stock prices down more than 50% off October 2021 levels. Despite the large sell-off, the fundamentals and earnings across the sector remain strong driven by increased adoption and awareness of cybersecurity issues as well as technology-led megatrends driving growing demand for cybersecurity products. This recent correction could make this a possible good entry point for investment into the sector.[49] One should, however, remain conscious of the fact the broader stock markets risks (like a hiking cycle in many developed countries to curb inflation) could weigh on growth stocks for the remainder of 2022.

HOW TO INVEST?

ETF LANDSCAPE

ETFs can be a very effective tool to implement a view on a particular theme, and Cybersecurity is a strong example of this. Structurally, there are several players in the industry and while US companies may dominate the space other international companies are equally important especially given the geo-politics and sensitivity around data and privacy. The cyber industry has a relatively close link to the cloud computing industry, and this will increasingly become the case as more data is stored remotely.

ETF REVIEW/SELECTION

Within the European-domiciled ETF universe, there are six cybersecurity ETFs that could be used to gain a cybersecurity exposure:

- First Trust Nasdaq Cybersecurity UCITS ETF (CIBR);
- Global X Cybersecurity UCITS ETF (BUG);
- iShares Digital Security UCITS ETF (LOCK/SHLD);
- L&G Cyber Security UCITS ETF (ISPY);
- Rize Cybersecurity and Data Privacy UCITS ETF (CYBR); and
- WisdomTree Cybersecurity UCITS ETF (WCBR).

Table 3: Summary of key ETF characteristics:

ETF Name	Total Expense Ratio (TER)	No. of holdings	Top 10 stocks as a % of total holdings	Country Exposure (largest)	Performance YTD to 20/06/2022	Performance 1 year to 20/06/2022	Performance 3 year	Performance 2021	High-level Comments
First Trust Nasdaq Cybersecurity ETF (CIBR)	0.60%	41	46%	US=83%	-26.0%	-15.40%	+39.80%	+19.70%	This ETF uses a broader definition to include cyber security ETFs - those that are classified as a Cybersecurity company as deteremined by the Consumer Technology Assocation. This, for example, results in a holding in CISCO of approximately 5%.
Global X Cybersecurity UCITS ETF (BUG)	0.50%	31	58%	US=65%	-23.3%	N/A	N/A	N/A	The ETF holds stocks that generate income from cybersecurity activities in the main (at least 50% of their revenue from cyber security activities).
iShares Digital Security UCITS ETF (LOCK/SHLD)	0.40%	119	18%	US=60%	-29.3%	-23.70%	+13.60%	+16.50%	This ETF is made up of over 80 stocks, that derive more than 50% of their most recent total annual revenue from sectors linked to the digital security trend. The weights are then assigned on an adjusted equal-weight basis.
L&G Cyber Security UCITS ETF (ISPY)	0.69%	44	42%	US=68%	-27.4%	-26.80%	+16.70%	+8.20%	The ETF holds stocks that generate a material proportion of their revenues from the cyber security industry. The weights are then assigned on an adjusted equal-weight basis.
Rize Cybersecurity and Data Privacy UCITS ETF (CYBR)	0.45%	53	34%	US=67%	-27.0%	-23.70%	N/A	+5.00%	The ETF holds stocks that generate income from cybersecurity activities in the main (excluding those with below 20% of revenue/profit, and over-weighting those with greater exposure).
WisdomTree Cybersecurity UCITS ETF (WCBR)	0.45%	29	45%	US=80%	-33.7%	-27.40%	N/A	N/A	The ETF holds stocks that generate income from cybersecurity activities in the main (at least 50% of their revenue from providing primarily cyber security oriented products).

Source: Datastream, Omba, Provider websites

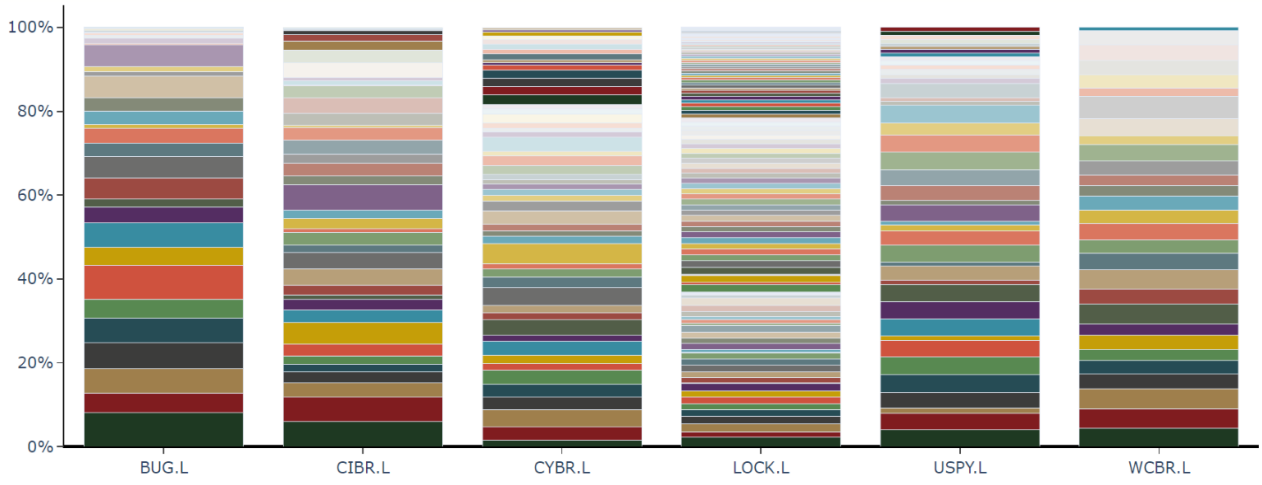
The selection of the most appropriate ETF is highly subjective and requires extensive qualitative and quantitative analysis. This is especially true in the context of thematic ETFs where underlying indices can differ widely in their methodology and exposures. Selection of the most appropriate index can more easily outweigh other factors that may be more important when assessing traditional ETFs. A robust process is needed to identify relevant risks and to assess purity of theme expression and valuations.

- The cost of thematic ETFs can be relatively high compared to traditional ETFs and can vary significantly between issuers. The thematic ETF market is nascent where often the first mover has an advantage and thus charges higher fees. Competition is yet to drive fees lower, and the complexity and differentiation of indices is often used to explain higher fees.
- ETF holdings and composition: it is also important to consider whether the holdings and composition of an ETF adequately express the intended view or tilt. The number and type of holdings as well as the location of the operations of the holdings and the sectors in which the holdings operate, are all relevant factors to consider in the context of the overall portfolio as well as with refence to the intended view that one wishes to express.

  For example, the location of operations could be used to add geographic diversification to the portfolio. Furthermore, specific holdings is relevant - if a cybersecurity ETF was to hold for example Microsoft or CISCO (or any other large, multinational conglomerate), such an ETF may not express a 'pure' cyber play as these companies/holdings do not generate revenue from cybersecurity in the main and cyber is only ancillary. Accenture, a company specialising in information technology services and consulting, is held in some cyber-ETFs, but might not be considered a pure 'cyber' play. This added diversification and sometimes increased liquidity of the stock can however work in favour of the ETF and can sometimes be a valuable inclusion depending on an investor's view and existing portfolio exposures.

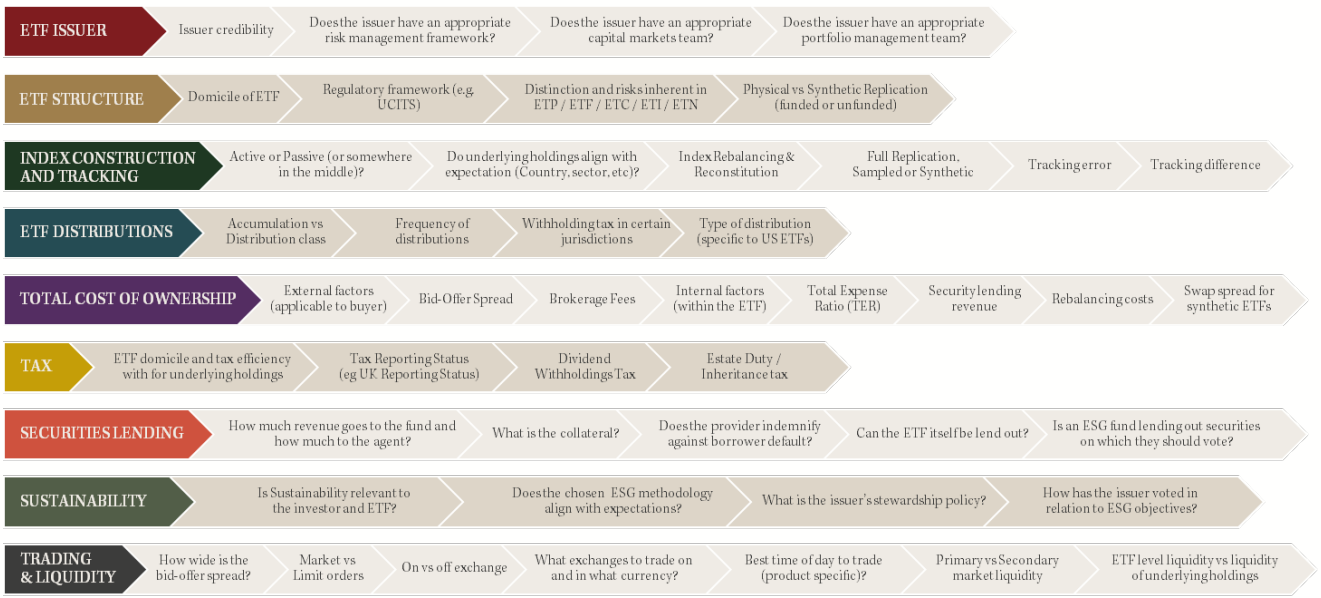
  The underlying holdings per ETF is depicted below, from this it is evident that the iShares Digital Security ETF (LOCK) has far more holdings, each with a smaller relative weighting, than the other ETFs (outlined in table 3 above). Depending on the intended view trying to be expressed, the number and size of holdings is a relevant consideration.

Underlying Holdings per ETF



- ESG consideration: some cybersecurity ETFs may have exposure to aerospace or defence companies which may need to be excluded should a portfolio have ESG requirements or restrictions.
- The index and tracking error: it may be relevant to review the index that the ETF tracks (composition, index provider, any exclusions etc) as well as whether the ETF provider is able to adequately track the index.

- How the ETF is constructed: is the ETF physically backed (i.e. holds the underlying stocks) or is the ETF synthetically replicated (using swap contracts) which comes with additional considerations and can be advantageous in extreme market and banking stress.
- Whether the ETF provider does securities lending and if so to what extent.
- Where the ETF is domiciled: this may be a relevant tax consideration.
- Whether the ETF is accumulating or distributing: this may also be a relevant tax consideration.



The above considerations are not exhaustive and the ultimate selection of an appropriate ETF to express a cybersecurity view will depend on ones' portfolio and other investor specific requirements.

ETF Overlap and Correlation

Due to the different approach followed by each index in defining what a cybersecurity company is and how it is weighted, the overlap in holdings between each of the ETFs should be considered and can be quite low. First Trust CIBR and Global X BUG only have overlapping holdings of 20%. This can also be seen with an overlap in Top Holdings as depicted in the Underlying Holdings per ETF image above. While overlap is low, correlation is a lot higher.

Table 4: Percentage Overlap of the Underlying Holdings

	Global X BUG	First Trust CIBR	Rize CYBR	iShares LOCK	L&G ISPY	WisdomTree WCBR
Global X BUG	100					
First Trust CIBR	20	100				
Rize CYBR	49	29	100			
iShares LOCK	22	14	29	100		
L&G ISPY	43	27	49	29	100	
WisdomTree WCBR	49	25	48	24	51	100

Source: Omba, Issuer websites

Table 5: Correlation

First Trust CIBR	1				
Rize CYBR	0.9435	1			
iShares LOCK	0.8992	0.9094	1		
L&G ISPY	0.9722	0.966	0.9101	1	
WisdomTree WCBR	0.9530	0.9445	0.8851	0.9423	1
	First Trust CIBR	Rize CYBR	iShares LOCK	L&G ISPY	WisdomTree WCBR

Source: Refinitiv, 27/5/2022 (1 year weekly correlation)

Performance of Selected ETFs

The importance of a particular theme can sometimes be outweighed by the macro environment in which the companies operate. 2022 has been a good example of this where higher growth companies and those that performed strongly at the start of the pandemic are now performing more poorly. Cybersecurity is currently facing a number of headwinds but is buoyed by the structural trend and current awareness about the risks relating to cybersecurity. YTD performance of all the cyber-ETFs under consideration has been poor, with all ETFs down about 20%-35% (refer to table 3 above). This is in line with expectations based on market performance YTD as well as single stock performance within the cybersecurity space (where certain high-growth stocks are down more than 50% YTD refer to table 2 above). The three-year performance of the sector has, however, been good with selected ETFs (with a track record of 3 years plus) up more than 20% over the period (even after the recent, large drawdown). This compares with the S&P 500 being up 24.4% over the same 3-year period.

CONCLUSION

Cybersecurity is a sector that will likely experience high and sustained growth over the next 5-10 years, such growth should be supportive of good share performance. Prior to the recent sell-off, it could have been argued that valuations for the sector were stretched (following the bull run into the end of 2021, particularly in high growth names). The recent sell-off has, however, seen certain cyber stocks (especially the high growth stocks) fall over 40% from October 2021 highs. Price-to-sales ratios within the sector are also far more attractive following a significant decrease in price and continued revenue growth within the sector. With strong demand and a robust growth outlook for the sector, the recent sell-off may offer a good entry point for investment into the cybersecurity market.

DISCLAIMER

REFERENCES

[1] CrowdStrike. (2022) 'CrowdStrike's Annual Threat Report Reveals Uptick Around Ransomware and Disruptive Operations; Exposes Evolution of eCrime Ecosystem' *CrowdStrike.*

[2] Walker, R et al. (2022) 'US Economics Analyst: The Economic Impact of Cyberattacks', *Goldman Sachs Economic Research*, page 2.

[3] Boolani, F et al. (2022) 'Global Software Welcome to the Cambrian Explosion of Infrastructure Software', *Citi Research Essentials*, page 12- 13.

[4] Clark, C. *What is cybersecurity?* Available at: https://www.techtarget.com/searchsecurity/definition/cybersecurity (last accessed 05/05/2022).

[5] ITgovernance. *What is Cyber Security? Definition and Best Practices.* Available at: https://www.itgovernance.co.uk/what-is-cybersecurity (last accessed 05/05/2022).

[6] Walker, R (n 2), page 2.

[7] Boolani, F (n 3), page 4.

[8] Essex, B et al. (2022) 'Americas Technology: Security and Analytics: Quick Reads From Security Software Earnings This Season' *Goldman Sachs Equity Research*, page 5.

[9] Essex, B (n 8), page 5.

[10]Palandrani, P et al. (2022) 'Rising Cybersecurity Threats Expected to Continue in 2022', *Global X by Mirae Asset.* Available at: https://globalxetfs.eu/rising-cybersecurity-threats-expected-to-continue-in-2022/ (last accessed 05/05/2022).

[11] WisdomTree Cybersecurity Strategy. (2022) 'WisdomTree Cybersecurity Strategy', *Wisdom Tree, page 5.*

[12] Palandrani, P (n 10).

[13] Metric derived from average number of IoT devices featured in the following sources: Palandrani, P et al. (2022) 'Rising Cybersecurity Threats Expected to Continue in 2022', Global X by Mirae Asset. Available at: https://globalxetfs.eu/rising-cybersecurity-threats-expected-to-continue-in-2022/ (last accessed 05/05/2022) and Hasan, M. (2022) 'State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally', IOT ANALYTICS. Available at: https://iot-analytics.com/number-connected-iot-devices/#:~:text=In%202021%2C%20IoT%20Analytics%20expects,than%2027%20billion%20IoT%20connections (last accessed 20/06/2022).

[14] Walker, R (n 2), page 2.

[15] Walker, R (n 2), page 2.

[16] Walker, R (n 2), page 8.

[17] Walker, R (n 2), page 8.

[18] Walker, R (n 2), page 8.

[19] Walker, R (n 2), page 2.

[20] US. Congress, H.R. 3684, August 10, 2021. BGR Group. (2022) *Infrastructure Investment and Jobs Act – Cyber Security.* Available at: https://bgrdc.com/infrastructure-investment-and-jobs-act-cyber-security/#:~:text=Overview%3A%20The%20Infrastructure%20Investment%20and,and%20state%20and%20local%20governments (last accessed 05/05/2022).

[21] US. Congress (n 19).

[22] Essex, B et al. (2022) 'Americas Technology: Security and Analytics State of Security: PANW, OKTA, FTNT, TENB Top Picks Into 2022', *Goldman Sachs Equity Research*, page 7.

US. Congress, H.R. 3684, August 10, 2021.

[23] Horton, C. (2021), *UK government investing millions to improve its own cybersecurity.* Available at: https://www.thinkdigitalpartners.com/news/2021/10/28/uk-government-investing-millions-to-improve-its-own-cybersecurity/ (last accessed).

[24] Chang, A et al. (2021) 'China Software: FAQs on Cybersecurity demand across government and enterprise; data security and privacy computing product', *Goldman Sachs Equity Research*, page 1 - 8.

[25] Chang, A (n 23), page 1 - 8.

[26] Palandrani, P (n 10).

[27] Allianz Global Corporate & Specialty. (2022) 'Allianz Risk Barometer 2022', *Allianz Global Corporate & Specialty.*

[28] Essex, B et al. (2022) 'Americas Technology: Security and Analytics: Impact of Russian Cyberattacks' *Goldman Sachs Equity Research*, page 2.

[29] SEC. (2022) 'Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies' *SEC Press Release.*

[30] Allianz Global Corporate & Specialty. (2022) 'Allianz Risk Barometer 2022', *Allianz Global Corporate & Specialty*, page 23.

[31] Palandrani, P (n 10).

[32] Bloomberg, (2022) 'Five Things to Start your day Europe Edition', *Bloomberg.*

[33] Canner, B. (2020) *Where Does Endpoint Security Overlap With Identity Management? Available at:* https://solutionsreview.com/endpoint-security/where-does-endpoint-security-overlap-with-identity-management/ (last accessed: 09/05/2022).

[34] Palandrani, P (n 10), page 3-4.

[35] Trellix. (2022) *What Is Endpoint Security?* Available at: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html (last accessed: 09/05/2022).

[36] Trellix (n 34).

[37] CheckPoint. (2022), *What is Cloud Security?* Available at: checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/ (last accessed:09/05/2022).

[38] CloudFlare. (2022) *What is data privacy?* Available at: https://www.cloudflare.com/learning/privacy/what-is-data-privacy/ (last accessed 16/05/2022).

[39] ITgovernance. *What is Cyber Security? Definition and Best Practices.* Available at: https://www.itgovernance.co.uk/what-is-cybersecurity (last accessed 05/05/2022).

[40] Splunk. (2022) *What Is Cybersecurity Analytics?* Available at: https://www.splunk.com/en_us/data-insider/what-is-cybersecurity-analytics.html (last accessed: 09/05/2022).

[41] Global X Market Research.

[42] Allied Market Research. (2022) Cyber Security Market by Component (Solution and Service), Solution (Identity & Access Management, Infrastructure Security, Governance Risk & Compliance, Unified Vulnerability Management Service Offering, Data Security & Privacy Service Offering, and Others), Deployment Model (Cloud and On-Premise),

Enterprise Size (Large Enterprises and SMEs), and Industry Vertical (Telecom, Automotive, BFSI, Public Sector, Retail, Healthcare, IT, Energy & Utilities, Manufacturing, and Others): Global Opportunity Analysis and Industry Forecast, 2021-2030. Available at: https://www.alliedmarketresearch.com/cyber-security-market (last accessed: 06/05/2022).

Markets and Markets. (2022) Cybersecurity Market with COVID-19 Impact Analysis by Component (Software, Hardware, and Services), Software (IAM, Encryption, APT, Firewall), Security Type, Deployment Mode, Organization Size, Vertical, and Region (2022 - 2026). Available at: https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=CjwKCAjwjtOTBhAvEiwASG4bCGqplpSArvTcxNmBzuRZEtDkLR3BPubNJyMiO48nycRsqEf6dDL4mBoCU14QAvD_BwE (lasted accessed: 06/05/2022).

[43] Palandrani, P (n 10) page 4.

[44] Boolani, F (n 3), page 42.

[45] Metrics derived from the forecast market size and growth from the following sources: Mordor Intelligence. *CYBERSECURITY MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2022 - 2027).* Available at: https://www.mordorintelligence.com/industry-reports/cyber-security-market (lasted accessed 21/06/2022). Allied Market Research. *Cyber Security Market by Component (Solution and Service), Solution (Identity & Access Management, Infrastructure Security, Governance Risk & Compliance, Unified Vulnerability Management Service Offering, Data Security & Privacy Service Offering, and Others), Deployment Model (Cloud and On-Premise), Enterprise Size (Large Enterprises and SMEs), and Industry Vertical (Telecom, Automotive, BFSI, Public Sector, Retail, Healthcare, IT, Energy & Utilities, Manufacturing, and Others): Global Opportunity Analysis and Industry Forecast, 2021-2030.* Available at: https://www.alliedmarketresearch.com/cyber-security-market (last accessed: 21/06/2022). Markets and Markets. *Cybersecurity Market by Component (Software, Hardware, and Services), Software (IAM, Encryption, APT, Firewall), Security Type, Deployment Mode, Organization Size, Vertical, and Region (2022 - 2026).* Available at: https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=CjwKCAjwjtOTBhAvEiwASG4bCGqplpSArvTcxNmBzuRZEtDkLR3BPubNJyMiO48nycRsqEf6dDL4mBoCU14QAvD_BwE (last accessed: 21/06/2022).

[46] Boolani, F (n 3), page 42.

[47] Boolani, F (n 3), page 15-25.

[48] Stratechi. *ADOPTION CURVES.* Available at: https://www.stratechi.com/adoption-curves/ (lasted accessed 10/05/2022).

[49] Essex, B t al. (2022) 'Americas Technology: Security and Analytics State of Security: Earnings Recap; Upgrade CRWD to Buy; Downgrade RPD and VRNT to Neutral', *Goldman Sachs*, pages 1-2.

OMBA
ADVISORY & INVESTMENTS

ombainvestments.com | ombafunds.com