IHS Markit®

Cybersecurity: The next frontier for investors?

Understanding the corporate and investment landscape

Introduction: The Cybersecurity Industry

Ensuring safety while working online remains a challenge for businesses and individuals despite growing awareness of online risks. There are various types of on-network threats and cybercriminals have been creative in exploiting vulnerabilities. Many companies and consumers still lack appropriate assessment of their online exposure and have incomplete awareness of the danger. However, with increased knowledge, the demand for cybersecurity solutions is growing and along with it, the hypothesis that the investment case into cybersecurity assets is strong. The enterprise cybersecurity market, currently estimated at ~US$173bn in global spend today, will grow at a CAGR of almost 8% between now and 2025[1].

IHS Markit interviewed industry leaders and investors, including Akamai, Clango, Full Frame Technology and Ibex Investors who all agreed that the hypothesis is correct, and cybersecurity is an increasingly important, high growth industry. The transcripts of these discussions also form part of this report.

Given the current set of business challenges presented by COVID-19, our speakers all pointed out that their clients' main priority was to get as close as possible to the state of business as usual. With their services having to rapidly migrate to predominantly online delivery, this warranted access to their portals for end customers while ensuring their employees can work with all the internal resources they accessed when in the office. Once the available solutions were assured, safety was given paramount importance.

Our points were further validated by data from the IHS Markit Research Signals team, who in collaboration with cybersecurity ratings company BitSight, provide analysis on cyber readiness and rank companies accordingly. We looked at companies with various ranks, compared their financial performance and valuation metrics. The comparison revealed that companies with the highest possible rank offered greater returns to their investors year to date.

Economy vs Infrastructure

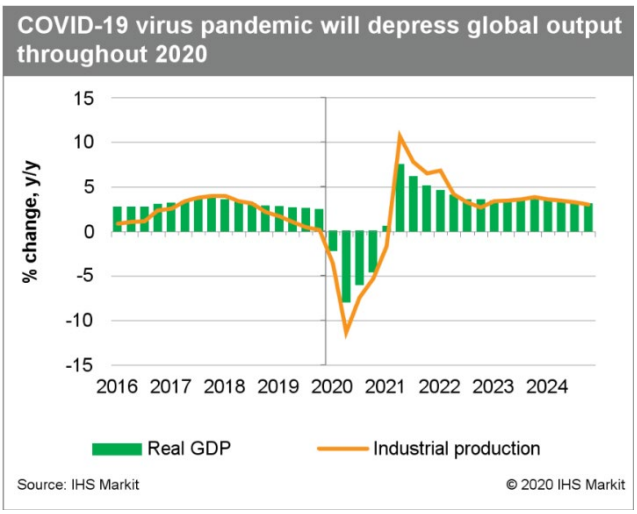
According to the IHS Markit Economics & Country Risk team, the global economy is in the midst of the worst downturn since the 1930s. Although modest recoveries are expected in the second half of 2020, real global GDP is projected to fall 5.5%, more than three times the contraction in the 2009 aftermath of the global financial crisis. The recovery in global economic output to pre-pandemic levels is expected to take two to three years.

IHS Markit predicts real global GDP to fall 5.5% for the calendar year 2020…

…and the corporate IT spending could be cut by a third

IT spend typically exhibits a strong positive correlation to GDP growth and – like previous recessions – it is expected that the overall investment into new IT projects will be reduced. We believe that the IT spend could be reduced even as high as by a third, with many businesses struggling to survive past the pandemic. However, it is also a time where progressive organisations keep migrating their technology to digital. Some will realise their employees' have not been affected while working remotely and the emergence of a hybrid workforce is an opportunity to reduce tangible assets and operational expenses with the extended IT infrastructure.

Figure 1: COVID-19 and global economic recovery



Source: IHS Markit Economics & Country Risk

The continued successes of data-driven companies and innovative industries such as fintech, remote video production, AI automation and autonomous vehicles will support continued demand for cybersecurity. Further progress of these industries is partially dependent on a full-fledged cybersecurity solutions landscape. Cybersecurity is

[1] Source: Forbes: https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#5abbb1de381d

an indispensable component of that commercial success and must be considered as a priority.

Common types of cyber threats

Most organisations and their employees have improved their approach to cybersecurity and recognize that it is a responsibility of all those connected to the network to ensure their actions do not expose their customers and organizations to cyber threats.

With hackers and spammers using advanced and creative ways to hoax users to access internal databases with information on their consumers and employees, continuous investment in training, following security best practices, and deploying cyber solutions is essential for all companies.

There are several ways to group and describe various types of cyber threats. For instance, Cisco considers seven types[2];

- **(Distributed) Denial-of-service (DDoS) attack** – floods systems, servers, or networks with traffic to exhaust resources and bandwidth and as a result, the system is unable to fulfil legitimate requests
- **DNS (Domain Name System) tunneling** – utilizes the DNS protocol to communicate non-DNS traffic over port 53. DNS requests are manipulated to exfiltrate data from a compromised system to the attacker's infrastructure
- **Malware** – malicious software, including spyware, ransomware, viruses, and worms
- **Man-in-the-middle (MitM) (eavesdropping attacks)** – attackers insert themselves into a two-party transaction, e.g. on unsecured public Wi-Fi, attackers can insert themselves between a visitor's device and the network
- **Phishing** – sending fraudulent communications that appear to come from a reputable source in order to obtain personal information
- **Structured Query Language (SQL) injection** – attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not
- **Zero-day exploit** – attack released after a network vulnerability is announced but before a patch or solution is implemented

Breaches have serious consequences

In July 2020, Twitter was the target of a huge cyber-attack. Accounts of Joe Biden, Bill Gates, Elon Musk, Barack Obama and dozens of others were hacked into and a cryptocurrency scam was initiated via the Coinbase exchange. According to Bitcoin.com, cryptocurrency-related scams took in US$381m so far in 2020[3] and according to the Wall Street Journal, over US$4bn in 2019[4]. Just one month earlier, a US$42m ransom demand was issued for stolen legal documents from singer Lady Gaga.

Verizon: In 2019, 86% of breaches were financially motivated

According to Verizon's "2020 Data Breach Investigations Report (DBIR)", 86% of breaches last year were financially motivated and 27% of malware incidents can be attributed to ransomware[5]. In the last decade, billions of users were exposed to various data breaches, including those using the services of Adobe, eBay, Equifax LinkedIn, Marriot, MySpace, Playstation and Yahoo. The breach of Yahoo is considered one of the largest corporate compromise to date, with around 3bn users affected. It also makes it amongst the most harmful, as customer names, dates of birth, email addresses, passwords and security questions for a large percentage of records were stolen.

Individuals, businesses and governmental agencies have been equally targeted. According to The Center for Strategic and International Studies (CSIS) – a bipartisan, non-profit policy research organisation that tracks cybersecurity events, several high-profile attacks occurred since May 2020, including;

- The Australian Prime Minister announced that an unnamed state actor had been targeting businesses and government agencies in Australia as part of a large-scale cyber attack
- COVID-19-themed phishing emails were sent to more than 5 million businesses and individuals in Singapore, Japan, the United States, South Korea, India, and the UK in an attempt to steal personal and financial data, believed to be driven by North Korean hackers
- The NSA announced that Russian hackers associated with the GRU had been exploiting a bug that could allow them to take remote control of U.S. servers
- Ongoing attacks were organized by a Russian group compromised German networks of energy, water, and power companies via its supply chain
- A phishing attack tricked an employee of Norway's state investment fund into transferring money into an account controlled by the hackers

[2] Source: Cisco: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
[3] Source: news.bitcoin.com: https://news.bitcoin.com/crypto-scammers-steal-381-million-in-2020-while-twitter-hackers-direct-funds-to-mixers/
[4] Source: WSJ: https://www.wsj.com/articles/cryptocurrency-scams-took-in-more-than-4-billion-in-2019-11581184800
[5] Source: Verizon: https://enterprise.verizon.com/en-gb/resources/reports/dbir/

- A cyber espionage campaign conducted by an Iranian group, targeting air transportation and government sectors in Kuwait and Saudi Arabia
- Chinese hackers accessed the travel records of nine million customers of UK airline group EasyJet[6]

The time it takes to realise and assess security breaches can be lengthy and some small businesses will never learn that an attack has occurred. According to IBM's "2019 Cost of Data Breach Report", amongst the 507 organizations that reported attack on their businesses, the average time to identify and contain a breach was 279 days with an average cost of a data breach at US$3.86m[7].

Cybersecurity vendors

Cybersecurity is a vast topic and many businesses play significant roles in protecting the safety of organisations and individuals online, providing services that span across cloud, network, IoT, consumer, threat detection, consulting, advisory or awareness. Amongst the most prominent solution providers are large corporations for whom cybersecurity is just one pillar in their rich technology product portfolio. These can be grouped as:

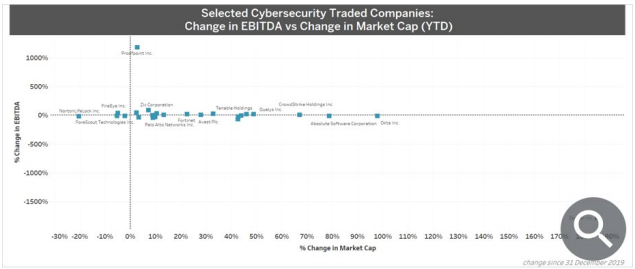
- Traded: e.g.: Accenture, Akamai, AT&T, AWS, BAE Systems, BT, Cisco, IBM, Intel, Lockheed Martin, Northrop Grumman, Microsoft or Verizon;
- Private diversified businesses such as KPMG, and EY;

But many leading cybersecurity specialists remain private. For example:

- Checkmarx, Clango, Cynet, Gigamon, Herjavec Group, Imperva, Optiv, Palantir, SonicWall, SparkCognition, Tanium and Thycotic, TrapX Security

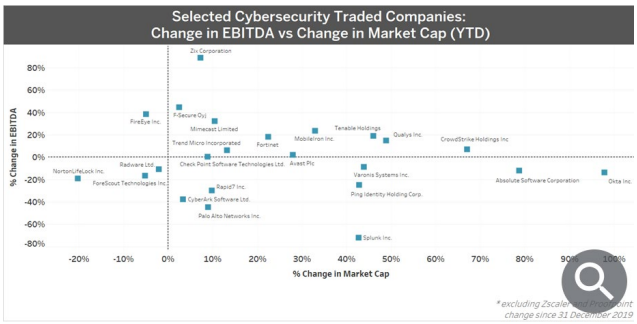
Publicly traded cybersecurity specialists – where all or most of their operational revenues are associated with online security – act as a good proxy for industry performance

- Out of 25 traded cybersecurity companies, 20 increased their share value between 31st December 2019 and 31st July 2020
- The average unweighted return was 41%
- The share price of Zscaler and CrowdStrike increased by 179% and 127% respectively.
- The cumulative market cap for all 25 companies amplified by over US$53bn to reach US$226bn.

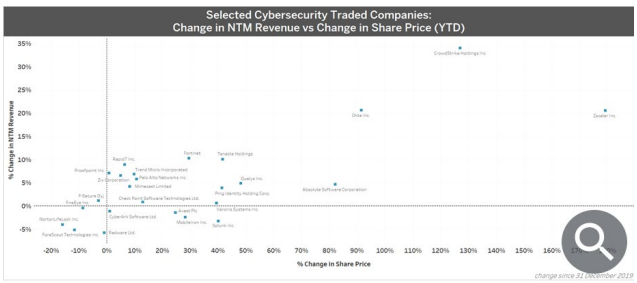


Source: IHS Markit / FactSet

By excluding outliers Zscaler and Proofpoint, we can focus on the variations between the majority of vendors.



Source: IHS Markit / FactSet



Source: IHS Markit / FactSet

Which companies / industries rank higher for cyber protection?

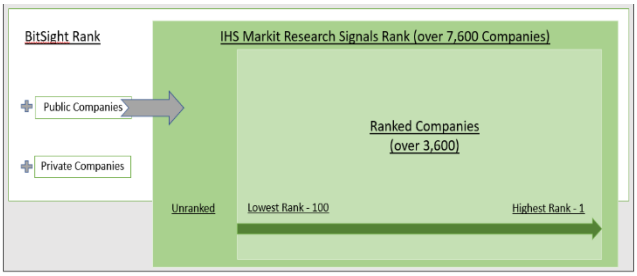
IHS Markit and BitSight partnered to provide asset managers with critical cybersecurity intelligence on traded organizations worldwide. These ratings are used while assessing cyber risk in the companies' ecosystems. Much like credit ratings, this approach offers insight into companies' security, driving stock selection and risk management decisions.

One of the most comprehensive sources for comparing cybersecurity readiness amongst listed companies is a joint

[6] Source: CSIS https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

[7] Source: IBM https://www.ibm.com/security/data-breach

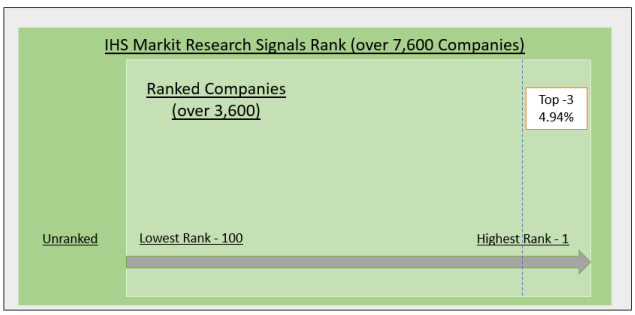
analysis from BitSight and IHS Markit Research Signals. This analysis ranks companies on a scale from 1 (highest) to 100 (lowest).



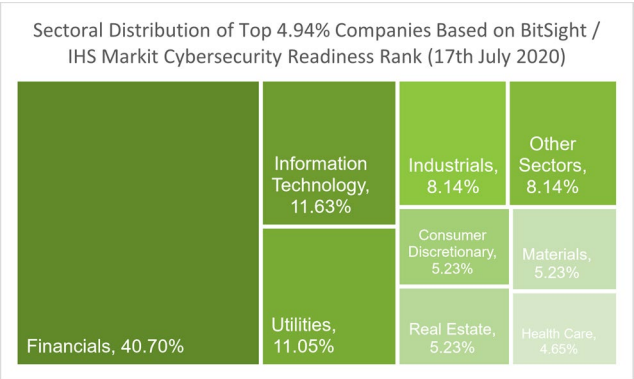
There are currently over 3,600 traded companies that are being analysed daily across 36 cyber metrics. The BitSight analysis shows that for companies with the lowest scores – close to 100 – the likelihood of suffering a data breach is 5 times higher than for top ranked companies. For the purposes of this report, data from 17th July 2020 was extracted, conducting analysis of which businesses and industries were (on average) less likely to be breached due to stronger security measures in place.

Financial Sector scores rank high

Firstly, based on a scale of 1 (highest rank) to 100 (lowest rank) we studied companies with a rank of 1, 2, or 3 (top 4.94% of scorers). Out of the universe of 3,600 businesses, 172 were ranked in this top-scoring segment (sector agnostic).



Within these top-performers, 40.7% belonged within the Financial Industry, which comprises banks, insurance companies and diversified financial service providers. Information Technology companies came second with 11.6%, followed closely by Utilities at 11%. The least represented in these top performers were Communication Services and Energy sectors.



Source: IHS Markit Research Signals

This analysis provides an effective, uniform and hence comparable basis for cross-sectoral analysis. The BitSight / IHS Markit Research Signals data enables various other analyses, including that used to determine supply chain risk, in M&A due diligence and investment prioritisation.

However, different sectors will have varying employee and customer habits, volumes and types of devices in the network, mobility of employees, software updating schedules, supply chain, customers and many other considerations which practitioners could consider.

The framework also enables intra-sector comparison and benchmarking, assessing the difference between the company's current BitSight Rating and the average BitSight Rating for that sector, scaled by the standard deviation of the sector's BitSight Ratings. Hence, ratings are put in context as some sectors/industries have a disproportionately higher/lower rating because of their business priorities. This method accounts for the difference between these, normalising the rating for more detailed comparison.

Companies with the best cybersecurity have had better share price performance (YTD) and have higher valuation multiples

There is a causal relationship between the company's cybersecurity readiness – manifested in a higher BitSight / IHS Markit rank – and their equity performance. The 37 highest performers with a top rank of 1 offered more attractive valuation multiplies than the 35 businesses that were ranked at the bottom. It is worth noting that the top performers also benchmarked very highly against the S&P 500 averages.

Amongst the companies with highest readiness score:

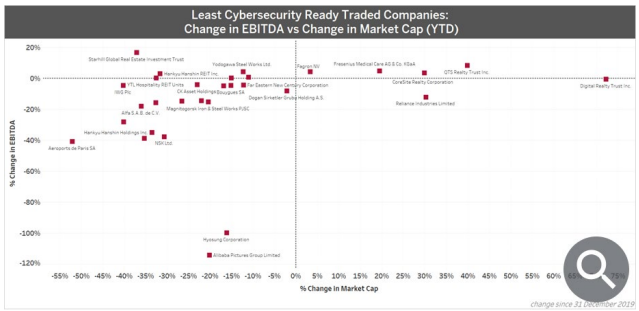
- The unweighted average share price declined by 2% during the period between 31st December 2019 and 31st July 2020
- The cumulative Enterprise Value increased by 13%

- 22 experienced negative NTM Revenue Adjustment with an average unweighted increase of 2.6%

Amongst the companies with lowest readiness score:

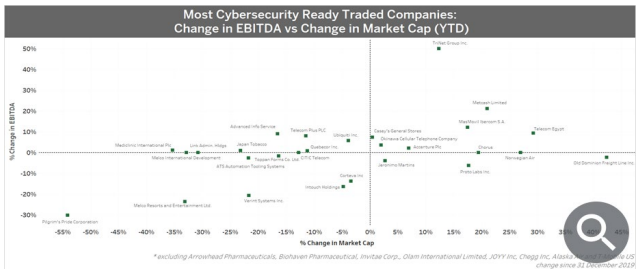
- The unweighted average share price declined by 17%, with five recording a decline at or below 40%
- The cumulative Enterprise Value increased by 6.5%
- 21 experienced negative NTM Revenue Adjustment with an average unweighted increase of -6.1%

Source: IHS Markit / FactSet

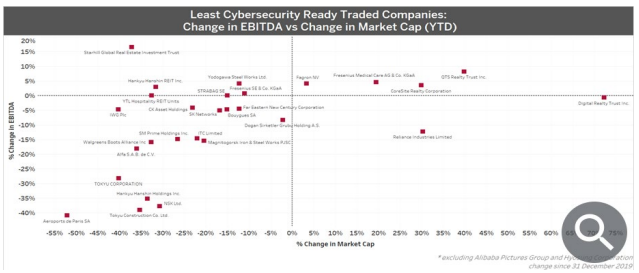


Source: IHS Markit / FactSet

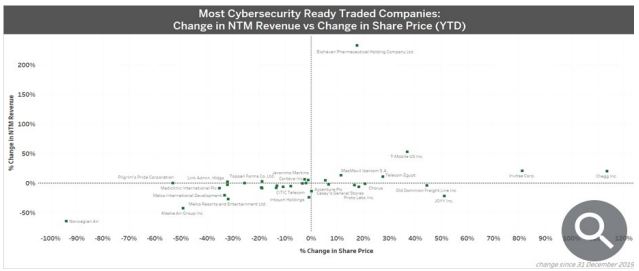
By excluding companies that either outperformed or underperformed others, we can focus on the differences between the remaining group.



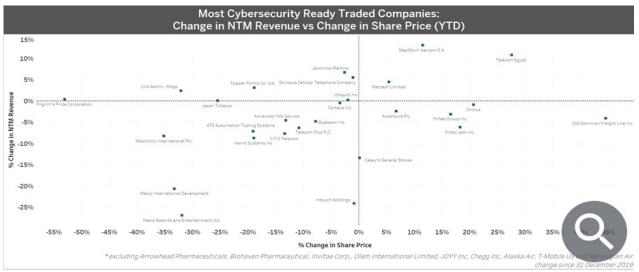
Source: IHS Markit / FactSet



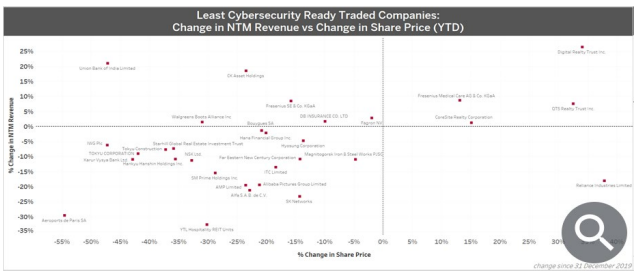
Source: IHS Markit / FactSet



Source: IHS Markit / FactSet



Source: IHS Markit / FactSet



Source: IHS Markit / FactSet

Industry voice

The data from BitSight and IHS Markit Research Signals underlines market sectors and listed companies that are better prepared for dealing with cybersecurity challenges. It also demonstrates a casual relationship between cybersecurity preparedness and better financial performance.

The next hypothesis states that despite financial uncertainty attributed to the outbreak of COVID-19 pandemic and associated lockdown measures, the majority of developed businesses increased their spending on security solutions to enable their employees to work remotely and their customers to access uninterrupted services. We believe that many leading cyber services have never been busier in building safe networks and ensuring their clients' protection.

The following experts were invited to share their views on cybersecurity priorities and opinions on the matter with Przemek Bozek, an IHS Markit Technology Subject Matter Expert:

- **Martin Turner – Founder, Full Frame Technology**, a boutique cybersecurity training provider
- **Gerhard Giese – Cybersecurity Specialist at Akamai**, the largest content delivery network (CDN) and a leading enterprise security provider
- **Arun Kothanath – Chief Security Strategist at Clango**, a leading system integrator specialising in Identity and Asset Management

MARTIN TURNER – FULL FRAME TECHNOLOGY; ON CYBER AWARENESS

Full Frame Technology was set up as a result of the frustrations that founders had working in companies where there was a seemingly unbridgeable gap between those who controlled the technology and those who used it. As well as leading to obvious frustrations on both sides, it meant that projects were over-promised, under-delivered, and over-ran in cost and time. Full Frame viewed cybersecurity as an important element in this because it is of little interest to most people until something awful goes wrong, or they are working on a project that carries a particular risk.

What aspects of cybersecurity is Full Frame Technology addressing?

Most of our clients operate in Media and Content. Cybersecurity has become the central part of our business as we have a deep understanding of how media production works. We know that when a production or a story runs into challenges, people will do whatever is needed to overcome them. Currently, the cybersecurity part of the business is split equally between vulnerability assessments and training. We work with big organisations like the BBC, ITV and NHK, and smaller production companies, many of which face challenges because of how they have grown organically from kitchen-table operations.

We work with trusted partners on specialised issues such as data protection and penetration testing. We believe strongly in the importance of deep expertise in the subjects we are dealing with – and we are dismayed at the plethora of people who, for example, call themselves "GDPR-qualified", when there is really no such thing.

How would you describe the awareness of your clients to cybersecurity?

> *Turner: "Awareness of cybersecurity is mixed. (It) tends to be at the bottom of the to-do list until something happens to make it a priority"*

Awareness of cybersecurity is mixed. It has improved since we set up the company, not least because commissioners impose detailed (and demanding) requirements on production companies. Nevertheless, while its importance may be understood, cybersecurity tends to be at the bottom of the to-do list until something happens to make it a priority.

Not surprisingly, we see an increase in requests for training in the aftermath of security failures, particularly those affecting the media sector. This is a significant motivation for signing staff up to training, but we have seen an increase in companies who have decided training is a worthwhile investment.

What is your advice for production companies?

> *Turner: "embed cybersecurity in the fabric of the organisation, so that it becomes an integral part of everyday life"*

Our main advice is not to ignore it, which is extremely likely because of the pressure on managers and co-ordinators in the media sector. The mobile nature of the media workforce means that people are constantly coming and going, and they are highly likely to bring their own security solutions with them. This carries risks with, for example, cloud computing.

We believe the most important thing is to embed cybersecurity in the fabric of the organisation, so that it becomes an integral part of everyday life. This does not

mean obsessing about it – but it does mean that if someone is using their private Dropbox account to share data, their colleagues will call them out for it.

Do you think the demand for cybersecurity training will keep increasing?

Last year KnowBe4 raised US$300m in a round led by KKR, which shows that there is strong demand for investors to fund companies offering security awareness training. It is a growing market – and profit margins are very attractive. Expertise in products and services is where companies like ours would benefit from the funding. We've tried to develop a couple of solutions (for supply chain security and SIM management) and had tried to fund this internally – but ultimately without success, partly because of costs and partly because of day to day business.

Thank you, Martin.

GERHARD GIESE – AKAMAI; ON MARKET UPTAKE OF CYBERSECURITY SOLUTIONS

Akamai is widely known as a content delivery network (CDN), a system of distributed servers that optimize the delivery of all types of web content to users. Akamai's route to offering cyber protection to customers was a natural extension of the company's core capabilities. As a CDN, Akamai had to learn to protect itself and its platform against attacks from external actors. Since the CDN stands in front of all the customers, Akamai are getting the punch if somebody wants to hit one of them. They had to defend themselves against all sorts of cyber-attacks, such as Distributed Denial of Service (DDoS), and web applications attacks (like SQL injections or cross site scripting). Akamai productised the company's knowledge – with the launch of its first WAF back in 2009. Later, in 2012, it launched its first standalone, integrated DDoS and WAF solution – Kona Site Defender (KSD). KSD had already extended DDoS protection capabilities for web applications. End of 2013, Akamai decided to extend the DDoS part of the solution with the acquisition of Prolexic to protect the full suite of enterprise IP applications – including email, file transfers, and VPN.

What security solutions do you offer?

Akamai has been providing Edge security products and services for over a decade, starting with solutions to protect our customers' websites, applications and data centers against all types of DDoS and Web Applications attacks.

About four years ago, we complemented our Web Application Solution portfolio and introduced a solution to address the increasing challenges and risks associated with bot traffic. Bot Manager employs multi-layered bot detections, and let our customers select between multiple responses and actions to meet their business objectives. Bot Manager can detect and identify the most sophisticated bots—including those seen conducting credential abuse or other web fraud attacks.

With the increased adoption of the Cloud and the evolution of the attack surface, Akamai introduced a new set of "Zero Trust" solutions to protect users, devices, applications, and data that are moving outside of the enterprise perimeter and zone of control. Akamai and its customers use the platform to stop employees from browsing malicious websites (malware protection) or to make sure their internal resources are securely accessed externally without the need for a VPN (cloud-based secure remote access).

The week of June 21, Akamai mitigated the largest packet per second (PPS) distributed denial-of-service (DDoS) attack ever recorded on its platform. The attack generated 809 million packets per second (Mpps), targeting a large European bank.

We also offer a Customer Identity and Access Management tool, which provides a highly secure and resilient environment for collecting and storing sensitive user information. We are the most versatile when it comes to identifying user journey and a multi-faceted approach, like for example, combining customer information from several events, storing it and connecting with all the other business systems based on obtained permissions, rules of GDPR and other regulations.

For organizations that collect credit card data and other sensitive, personal information on their websites – usually within industry verticals like Travel & Hospitality, Retail, and Financial Services – and are susceptible to form-jacking attacks, such as Magecart, Akamai is offering client-side protections via a solution called Page Integrity Manager. It aims to mitigate the risk of a data breach, regulatory non-compliance, and/or financial loss.

Giese: "There are at least two trade-offs with cybersecurity: measuring your ROI before you are attacked and user experience that could be lowered."

What is the market understanding of the importance of cybersecurity?

Almost every person on the planet now understands the importance of cybersecurity and the question is rather if

they embrace it as well. Most will admit that cybersecurity is very important but can be intrusive, so some choose not to implement it. There are at least two trade-offs here.

First is justifying the cost of cybersecurity. It is difficult to measure the ROI until you are attacked. Some may think that if no attack occurs for a year, they are safe, but that is a short-sighted approach. We provide our customers with detailed attack reports on what type of attacks hit them, what we mitigated, we update them on all that's happening around them, other similar-type services have been attacked and so on to keep them aware of the situation.

The second trade-off is that the user experience and performance may worsen. Many security solutions add latency and impact user experience for the customer. We work hard to find the right balance. Because Akamai's security solutions are built on the Akamai distributed platform, performance does not get impacted.

Giese: "A lot of companies were unprepared for a situation where almost 100% of their employees had to suddenly start working from home"

Would you say that some industries are more mature than others?

For instance, the Financial Services market is rather mature compared to most other markets. The Financial Services industry has always been prone to all sorts of attacks and understands the importance of cybersecurity. Banks, for example, must defend their online presence against fraud attacks. The same goes for other asset-depending companies such as retail and streaming media companies.

Can we say the same about employee access to internal resources?

A lot of companies were unprepared for a situation where almost 100% of their employees had to suddenly start working from home. Almost every single business was frantically building up resources to give their employees the opportunity to work from home and stay safe. Once the lockdown occurred, everyone knew that there will be problems and the tolerance level was much higher than usual. We expected things to break from the day we all started working from home and didn't freak out when something was not working.

Since the lockdown and growth of Internet users, did you see an increased demand for cybersecurity solutions?

Absolutely yes. Age groups that were not relying on online banking earlier added to that traffic. From February to March alone – and across all industries – we saw a 30% increase in traffic. In comparison, a typical year-on-year increase would be around 3%, so it was ten times higher. The peak traffic – the highest traffic we have seen on the platform at a given time – more than doubled from slightly over 80 terabits per second to over 160 terabits per second.

From February to March alone – and across all industries – Akamai saw a 30% increase in traffic. In comparison, a typical increase would be around 3%

Since the end of February, we have noticed an increase in Malware attacks. Several large phishing email campaigns were aiming to exploit the fear around COVID-19. For example, emails pretending to be sent from the CDC (The U.S. Centres for Disease Control and Prevention) where people were encouraged to download the latest information for their area via links provided. These emails were highly personalised. In April and May, we also saw high increase in maze malware tripling the number of attempts trying to infiltrate large websites. The week of June 21, Akamai mitigated the largest packet per second (PPS) distributed denial-of-service (DDoS) attack ever recorded on the Akamai platform. The attack generated 809 million packets per second (Mpps), targeting a large European bank.

Did Akamai readjust to respond to the existing situation?

We highlighted – amongst others – our remote access solutions for granting external access to internal resources without a VPN concentrator and without exposing the services more than they necessarily must be. We made sure we had enough capacity and looked at the problem of last and middle mile as the additional traffic also affected the middle mile. For Akamai to not add to this problem, we did two things; first, we diverted traffic away from areas experiencing high levels of congestion. Second, we also worked with leading distributors of software, particularly for the gaming industry, including Microsoft and Sony, to reduce gaming software downloads at peak times and to complete the downloads at the normal fast speeds late at night.

Thank you, Gerd.

ARUN KOTHANATH – CLANGO; ON "IDENTITY CENTRIC" CYBERSECURITY

Clango specialises in cybersecurity and the "identity centric" part of it. Fifteen years ago, when they started to practice the theory, the company noted that every aspect of cybersecurity has an identity component: whether clients were deploying a firewall, anti-virus solutions, data protection solution, or encryption or any identity and access management solution. With every facet of cybersecurity, there is a user and an identity associated with it.

Arun, what security solutions does Clango provide?

Clango provides the authentication services (as part of their Identity Management services portfolio), which will identify who is a threat and who is not based on what they do. Identity has a wide definition. There is a name, a surname, a username, password, computer, browser, location, and a mobile phone to access things. Each of these factors needs to be protected as any of these elements can be compromised. The theory is, if you protect that identity and all the attributes that constitute that identity, then you are much closer to securing your environment. We work with products like Oracle Identity Management, CyberArk and Thycotic. All these individual products solve one piece of the puzzle, so we put it all together to give the larger picture. Blocking a perpetrator is one activity of cybersecurity, but the identity of a bad actor and how to stop them is another.

That sounds both simple and complicated…

There is no one solution that fixes all the problems that large systems have. It is dispersed, very diverse and a very heterogeneous technology landscape, so some clients need more assistance. They also need a robust strategy on how to do that, to visualize what they have and what they need. For better security, you always need to have a vision of what good security means to each organization. If you look at your house, you might say that it is secured because you have a state of art electronic security system and surveillance cameras at every door, but you may forget to lock your front door. You should make sure that even if you do not lock your front door, other measures can be taken to protect it from somebody entering the house. These are all part of the larger strategy for securing your assets that Clango provides.

Do you think that the market understands the importance of cybersecurity?

It is much better compared to what people understood five years ago. And five years ago, they understood much better than they did 10 years ago. However, the scenario I have seen is that some invest in what is en-vogue but does not necessarily provide the fullest security. There are really good technologies out there, but the question is, are they well invested and well-funded?

Since the lockdown and growth in Internet usage, do you see an increased demand for cybersecurity solutions?

Kothanath: "We have been advising customers to think about what is going to happen in six months and what potential scenarios may emerge, including what will happen when thousands of employees get back to their offices after months of working from home."

Absolutely, especially in financial services. One of our banking clients have around 3,800 employees and roughly about 3,200 of them had the habit of getting up in the morning, put their suits on and head to the offices. In the 80 years of the company's history that is how they were used to working. But in March 2020, due to COVID-19, they all had to stay home and work. Most employees did not even know where to start. They did not know what a VPN was, how to log into their systems in the office or how to function without printing because there is no printing at home like you have in your office, there is no concept of data exfiltration because when you print a financial document at home you may be violating some regulations. So, the importance of securing all these things is multi-folded. That is the employee side. On the customer side, everything is happening electronically. So, the demand for creative thinking on cybersecurity is now higher than ever really!

Do you think the interest and investment in cybersecurity solutions will remain high?

I expect that during the first 90 days of lockdown, security is not the absolute top priority for many businesses. At this point, it is still about making systems functional to employees from wherever they are. The primary focus was on making sure that people can access what they need to continue business and make money so that the businesses survive. Once that access is assured, companies will think about how to protect it. The importance of investing in trusted technologies to provide cybersecurity is coming.

In the example described earlier, when thousands of additional employees had to work from home the priority had to be the VPN. The company had about 500 VPN's because usually the VPN's were used by the security people, the support people, and not necessarily financial analysts. With the new situation, this and many similar companies had to increase their VPN capacity by many folds and thousands more devices needed the end point protection. You need to make sure that employees using all

sorts of ISPs have same security level as if they were in the office.

Kothanath: "With the new situation companies had to increase their VPN capacity by many folds and thousands more devices needed the end point protection. (…) you have, instead of your company network, 500 different providers you must deal with and make sure that they all have the same level of security."

We are talking about security, but we have not even come to the point where we see many regulations being broken or abused due to the current situation. Doctors downloading and printing patient information and medical results at home may be a direct violation of pretty much every Healthcare Act in every country. We must protect patients and make sure that the access to data is intended and secured. Most of the time, people are doing things to make sure that they can get their job done, but that sometimes results in an unsecured way of doing things.

Will organisations that have invested in security spend even more?

For many organisations that already invested in cybersecurity, the next step is to focus on monitoring various types of proactive security measures. We have been advising customers to think about what is going to happen in six months and what potential scenarios may emerge, including what will happen when thousands of employees get back to their offices after months of working from home. Many businesses realise that productivity really has not gone down since the lockdown, so we don't need to get all these people back in. It may change the prospect of a hybrid workforce where people don't have to spend hours in tubes and cars, so from a financial perspective, the CFOs may be able to reduce the office bill by about 30% across, and that's huge. We anticipate that many will stick with a hybrid workforce after everything comes back to normal or whatever the new normal is going to be. And they will invest some of the savings back into security.

Kothanath: "There are fascinating cybersecurity companies out there and they share a very innovative way of thinking: increasing the security while increasing the usability and reducing the cost"

Do you think that the lockdown will contribute to the emergence of even more advanced cybersecurity solutions and new, exciting technologies?

Of course. I talked to a very fascinating company this morning. They are based in Israel and have been around for five years. They, and several others, share a very innovative way of thinking: increasing the security while increasing the usability and reducing the cost. We are at the earlier stages of this innovation.

Thank you, Arun.

Investor's voice

Upgrading cybersecurity systems as a response to a higher level of threats across various industries is a constant occurrence for most businesses, especially those operating directly with end consumers. Staying ahead of threats not only shields the company from financial losses but also protects its subscribers, reputation and ultimately long-term revenue streams. The industry's awareness is rising and security projects get funded. The total market opportunity is growing fast and that consequently attracts investors who are searching for most innovative start-ups with a high likelihood to succeed.

Leon Sinclair, Global Head of Private Equity and Debt Services at IHS Markit spoke with Brian Abrams, President of Ibex Investors about their cybersecurity investments and how to increase the chance of selecting most promising companies. In his response, Brian shares Ibex processes and encourages other investors to work together.

BRIAN ABRAMS – IBEX INVESTORS – ON STRATEGY FOR SELECTING CYBERSECURITY COMPANIES

Ibex Investors is a US-based investment firm targeting outsized returns through niche, non-correlated, differentiated strategies. Located in Denver, New York, and Tel Aviv, Ibex has over $600 million in assets under management as of June 30, 2020. Ibex invests across all industries, but one of its key focus subjects is cybersecurity and one of its main focus geographies is Israel. Israel, a country with less than 0.1% of the world's population is now a cybersecurity superpower that had accounted for 20% of the world's cybersecurity investments, including acquisitions last year.

Brian, how in your opinion did Israel gain the status of a cybersecurity superpower?

In Israel, military service is compulsory, and the military works rigorously to recruit top tech talent from high schools. They scout talent at a very young age and then recruit them into units in the Israeli military: one of the best known is unit 8200 (Israeli Intelligence Corps unit or as some say 'cyber spy agency') where they do just incredible stuff on both sides of cyber: defence and offense, learning how to be the best hackers and best cyber defenders in the world. When cadets graduate from units like 8200, they are already amongst the best in the world and many create their own companies with a focus on cyber. These entrepreneurs then have an ability to move fast, learn offense and defence while defending a government and transpose that expertise to defend companies from all the most sophisticated attacks that they have seen. That is the environment that we find incredibly attractive to invest in. We have invested in several cybersecurity companies from early stages through later growth stages and across different aspects of the cyber landscape.

Abrams: "(Investing in Israel) comes down to an incredible pool of skilled entrepreneurs with a tremendous background in terms of what they do in the army, the ability to transfer that know-how from the army into the private sector and then the culture of innovating very quickly as there is no fear of failure."

What is the biggest appeal in investing in Israel's cyber companies?

Israeli companies in our eyes move rapidly and if something does not work, they discard it and they try a new approach. We believe that rapid adaptation is great for any entrepreneur and for any start-up, but it is particularly well suited to cybersecurity where the attackers are moving and adapting very quickly and therefore the defenders at these start-ups and also at more established companies need to move and adapt very quickly. In our view, the Israeli DNA is well suited for that and to date has been very successful, but it is also part of why the VC, PE and M&A landscape is so attractive within cybersecurity. I think staying ahead of the curve is paramount for big companies and in order to stay ahead of the latest attack patterns with the latest approaches and the latest vulnerability they need state-of-the-art technologies. It is often many times easier and cheaper for a big enterprise to acquire a really lean start-up that already has a solution for a new threat. In other words, it is the question of build versus buy that most big enterprises are constantly evaluating.

Do you see any preferential deal pricing due to the entrepreneurism, funding landscape, or economy in Israel?

We focused on Israel because of the talent and the technology and the know-how, but the valuations are incredibly attractive and that supply-demand function in deal economics adds to the attractiveness. There happen to be a huge supply of great talent, great start-ups, great innovation and a relative scarcity of capital proportional to the opportunity. We believe that leads to fundamentally lower valuations at the entry point, which makes it attractive, so when we look at Israeli cybersecurity, we feel like we are getting the best technology in the world at the best prices in the world. On the way into the investment we enter at local deal economics, but then they scale up, mature, and become multinational companies. Roll forward, when they are acquired, they are acquired at international multiples. If a US tech company acquires an Israeli start-up, they are not paying Israeli price at the exit but a standard global price or a standard US price today. So, what we see, is the ability to invest at relatively attractive, possibly low valuations and exit at a relatively high valuation. It is e probably true of many other markets outside of the US as well and I know of really great American cyber companies too, but that's an important factor to the opportunity set in Israel.

We established that there are lots of great start-ups in Israel to invest in, but how do you select the best of the best?

When investing, we generally follow the five Ts. These are:

1. Team
2. Technology
3. Traction
4. Terms/Valuation
5. Total Opportunity

Our view is to not prioritize any element over another. You have to have it all to make it worthwhile and you have got to make sure every investment checks all of the boxes or you wait for a better opportunity. We look at these same criteria within any venture investment across Ibex.

Within cybersecurity we are also looking for an additional three elements.

1. First is a really unique technology, something that doesn't exist elsewhere, is out of the landscape today and therefore it is going to be a very attractive acquisition candidate for the big cyber companies that will be looking to add that capability. Cyber is very much an arms race and the attackers are almost always a step ahead and so there is a constant need for new defence to deal with the latest threat that I don't think will ever change. I think we are in the first innings of cybersecurity globally in terms of the industry and as it continues to evolve, it will continue to be more important, and a need for continuous innovation is going to be critical throughout the

entire lifecycle of cybersecurity for decades ahead. That category of unique new technology is always very attractive if there is nothing else out there.

2. The second category is best-in-breed. Chief Security Officers (CSOs) tell us they do not want to have to manage multiple different vendors. They want to make it simple and make sure all those solutions operate harmoniously with each other. Often that means they want to acquire the best in each category whether that is endpoint or network or cloud or ransomware. Therefore, they look to invest in the leader of whichever aspect of cybersecurity is required. That is an attractive category to Ibex as a lot of the Israeli portfolio companies fit that description.
3. The third category would be comprehensive. If there is a company that can lead the way to provide comprehensive cyber defence across the entire lifecycle, we would put them high on the list.

We invested in companies representing these three categories and that is how we are constantly evaluating them again within the framework of those five Ts that we talked about earlier.

Abrams: "When investing we look for five Ts: Team, Technology, Traction, Terms / Valuations and Total Opportunity"

Has the demand for cybersecurity solutions increased due to COVID-19?

Even before the COVID-19 pandemic started, cybersecurity was a fast-growing space that showed no signs of slowing down. What has changed is that COVID put cyber in the centre of attention. The incredible need for security and the ability of companies to combine all those different work environments whether it is public, private, hybrid cloud or on-prem or whether it is at the headquarters or satellite office or work from home, are now a must to have. Before 2020, many of these elements were viewed as nice to have and now I think they are very much considered as critical to operate and survive.

We are seeing the best cybersecurity companies accelerating out of COVID-19. They are seeing even faster uptake of their solutions and sales accelerating significantly versus budgets. In many ways, the remote work environment makes it easier for companies to sell their solutions remotely. Previously, the buyer and the customer meetings were sometimes very difficult to set up and now buyers find time online. In our view, the best companies are taking advantage of that. We observed some slowdown in the speed of purchasing behaviour on the part of cyber customers earlier in the year – and it may affect Q2 for some companies – but that said we know of other companies that are going to hit into Q3 numbers by the end of Q2. One of our portfolio companies was able to close a few new customers in Italy in March, the epicenter of the outbreak then. On the flip side, other companies that are not as strong or their solutions are not must-have may find it a lot harder. Again, that reinforces that landscape where you really need to be either unique, best of breed or comprehensive. As you would imagine the pandemic is shaping the medium-term winners and losers in the space.

If cybersecurity is an expedited topic for many companies, has your investment strategy been impacted as well? Do you think that the exit strategy or timelines have changed by the increased speed of adoption?

First in terms of speed of adoption I will answer with my favourite quote about two types of companies in this world: those who have been hacked and those who do not know it yet. I think after COVID-19 started, we are seeing a lot of companies move from the second category to the first category. If they were not aware before, they are aware now. This is changing the behaviour of organisations as they are realising that they cannot get away without protecting themselves across a wide range of environments. They must be aware of that and of any gaps in their cyber capabilities. But they are also dealing with constrained budgets so when you look at the landscape of cyber companies, the solutions on offer must appeal to the IT budgets, which are shrinking. I believe companies providing great technology for an affordable price are going to remain and grow their market share. As far as the exit landscape, we have seen buying behaviour among security officers that has led to consolidation and roll-up play in the investment and corporate space. This has created more exit pathways. You either need to be the best of the new breed or do it all. If you are not one of those things, you are not going to succeed. So that leads to consolidation also.

Are there more companies out there than even 6 months ago, which are looking to be acquired rather than going through several rounds of financing?

I think we will continue to see a very active environment in terms of price points that big companies come in and acquire new technology relatively inexpensively and that will almost always be attractive for them. If a big provider of

Abrams: "We try to make successful companies a self-fulfilling process. We go in usually relatively early in their lifecycle and then aim to help them accomplish that big scale up for their crossing over from being Israeli technology-oriented business to an international sales-focused company."

cybersecurity solution has a gap that they need to address or if a gap simply emerged because of the way the threat landscape evolves, they need to go and buy a company that helps them bridge that gap. The top two or three

companies in a niche may be a great way to do that. There are fewer independent companies on the market that can do it all, but a number can act as quick capability fillers and be attractive to the management teams. I believe we will see them continue to go public and if they succeed that way it will keep the big cybersecurity providers on their toes.

How do you build your network in Israel, Academia, incubators, intermediaries and agents?

For Ibex, it is about being embedded in the ecosystem and knowing people in that ecosystem and covering all these channels, whether it is a great talent coming out of the military in Israel or universities or working with incubators and accelerators to identify their most exciting companies. Or in the case of Israel, working with other venture capital firms. We believe Israel is a remarkable environment where venture capital firms work together. It is collegial whereas we have seen Silicon Valley is often very sharp elbows and everyone is competing against each other. This leads to terrific collaboration even amongst investors. We have been working with other investors too. So, it is all those things and it really is about forming a long-term engagement with an ecosystem. I do not think you can drop into an ecosystem like Israeli cyber and expect to get the best companies right away, get the best investments, form the best partnerships that create the best deal channels. You really need to commit to that ecosystem for a multi-year period. In our view, Israel is one of the best ecosystems in the world and we have been visible in the community there for almost a decade now. For Ibex it's really bearing fruit, but other investors could do it too as it is a very welcoming environment. But they really need to be able to commit to it and that means traveling there or, better, have a presence on the ground and engaging with a lot of different stakeholders as described above.

Are there any unexplored places left in the local market, or is it a case of harvesting a decade of commitment to the market?

There are plenty of places that are under explored. For instance, there is a tremendous innovation coming out of Be'er Sheva, a city in the South of Israel and there are really not many people investing there. But we believe there are terrific innovations and big opportunity for any investor looking to find a match.

What is the added value that Ibex brings to its portfolio companies?

We try to make successful companies a self-fulfilling process. We go in usually relatively early in their lifecycle and then aim to help them accomplish that big scale up for their crossing over from being Israeli technology-oriented business to an international sales-focused company. And we get very involved on their Boards of Directors, very active with the founders and management, helping them build up the teams and develop the go-to-market strategy. Our goal is to shift the centre of gravity from Israel to their target markets usually within the US, sometimes the UK or Europe, occasionally Asia. We consider that not just as a huge value that we can provide but also critical to getting the best outcome for all.

How does the DD and investment committee process look like for these early-stage companies far from home?

The five Ts including team, technology, traction, terms/valuation and total opportunity are key. Also, we do thorough due diligence in our companies from all angles. We are making sure the team is top-level and they have great and unique talent. We are checking the backgrounds of people working there and whom they served with in the military. We want to find out what they are all about. We are often leveraging our other portfolio companies or former portfolio companies or just people we know in the cyber ecosystem to vet the technology. If the technology is sound, we expect them to confirm to us "yes, this is tops, this is really a leading-edge technology with lots of promise". We are talking to customers to get their references and make sure that the technology does what it says. It is true of all start-ups but even more so for cyber. We want to develop technology that the market is pulling and demanding rather than something that someone thinks is a great idea and is trying to push to demonstrate its value to the market. We want to test the traction. We often bring a prospective customer to test our prospective investments even before we have invested and it is a win-win situation as start-ups are thrilled to get a prospective customer and we get to watch the process unfold in front of our own eyes and see how the prospective customer receives it, questions it, what their concerns are, what their needs are and we are also looking for independent third-party validations on each point.

Which are the key financial KPIs as you move from early stage development, ACV, ARR?

For any venture capital growth stage company or early stage company, the number one metric we are looking at is growth in recurring revenue on a year-to-year basis and, if possible, preferably a quarter-over-quarter basis. Within that we look at the sales funnel, including lead generation. Key questions are: is the company generating qualified leads and then how many Marketing Qualified Leads (MQLs) are converting to Sales Qualified Leads (SQL), then how many of those are converting into proofs of concept (PoCs), how effective is the salesforce at taking those and then finally how many close and turn into wins. Within deals, we look at whether they are converting upsell revenue or whether it is an additional logo in terms of a prominent customer. Then below that I like to think of it as an hourglass rather than a funnel because after the win, we have to create customer success, keep the churn low to make sure we are not just winning but retaining customers and then ideally upselling to them. We want to see expansion within our customer accounts to make sure that it is a growing and recurring revenue.

You often embed strong preferential terms and liquidation preferences in your agreement. We've seen some great capital structuring in your deals. How important is that for you?

Those terms are very important to us. In Silicon Valley you often see "clean term sheets" and a strong desire for some investors to appear founder friendly. I think it is a mistake on their part. For Ibex, having liquidation preferences is protecting us from the downside, particularly with early stage companies who may not yet be at that steep revenue growth curve and may be taking more of a bet on the team and the technology to gain early traction. We add these preferential terms and attractive liquidation preferences in many of our deals. We like to build in warrants or options that allow us to double down on our winners and protect ourselves from the losers. In many cases we liken it to betting in a horse race and having the flexibility to double down in the homestretch. I think it is a big part of successful venture capital investing. It is not just about finding great entrepreneurs or finding your technology or identifying a great opportunity or have a great investment thesis. It is equally important to invest at attractive valuations and structure attractive terms.

Also, our investees are often happy to give us those terms because they believe so deeply in their companies. We have observed that they do not mind giving up liquidation preferences because they do not believe it will ever come into play. They are also happy to give options because it gives them a pathway to further capital down the road and again, they are very confident in their ability to execute and they know that it will be a step up in the valuation for them as well and so it is a win-win. Since they are very confident and willing to accept those terms, it tells us about their attitude and commitment to the business.

Abrams: "We are seeing the best cybersecurity companies accelerating out of COVID-19. They are seeing even faster uptake of their solutions and sales accelerating significantly versus budgets."

In other words, entrepreneurs should have the conviction that the business can do what they promise to do and therefore, should not have concerns about preferential terms?

That is exactly right. If they do what they say they can do, what they believe they can do, and have the kind of exit that they are targeting that all those preferred classes of shares end up converting to common anyway and so when they are willing to do something like that it is truly standing behind their optimism and confidence.

Are you actively searching for new investments in cybersecurity?

Yes, very much so. We have never stopped. We had a term sheet with one of the companies in early March and we closed it in late March. We met with at least as many companies in the last three months as we have ever met before. We are very active in the space and think it is a terrific time to be an investor in cybersecurity. We think cyber is in the first inning of its lifecycle as a vertical and we are continuing to invest in the space. We are trying to make great investments in great companies right now for over a decade's lifecycle.

Ibex contracted IHS Markit as an independent valuator for your investments. Can you tell us why that independent valuation is so important for Ibex?

We are really enjoying working with IHS Markit on the valuation of the portfolio and it is a great practise to have someone independent go through the portfolio with a fine-tooth comb. It is also valuable for our investors and our portfolio companies. The skills the IHS Markit team demonstrate is second to none we have seen in the industry.

Thank you, Brian

Valuation Considerations for Early-Stage and Innovative Companies

Ibex Investors and hundreds of other equity and debt investors trust IHS Markit's independent valuations. IHS Markit's valuation approach is based on generally accepted industry best practice – the International Private Equity and Venture Capital Valuation Guidelines issues by the IPEV Board, US GAAP and IFRS – incorporating the most widely used methodologies to establish a baseline valuation.

The Private Equity & Debt Services practice – via a broad IHS Markit pool of talent and resources, including Technology, Energy & Chemicals, Healthcare, Economy & Country Risk, Automotive, Agriculture and their subsidiaries – supports pre-deal analysis, growth and buyout stages and provide subject matter expertise to fund managers and start-ups

As an added value to its customers IHS Markit is harnessing the deepest sources of information, analytics and expertise to forge solutions for the industries and markets that drive economies worldwide. Leaders in business, finance and government rely on us to help them see the big picture and interconnected factors that impact their organisations. This knowledge enables them to focus on what really matters.

Given the underlying portfolio companies' stage of development, what should firms consider when preparing performing valuation?

- The change in market and sector pricing conditions;
- The complexity of the capital structure of the company;
- The recent developments in the underlying technology and innovation of the business and the industry; and
- The timeline and exit plan for the investor.

Due to the difficulty of gauging the probability and financial impact of the success or failure of development activities of early stage companies, one should be mindful that traditional valuation techniques may not be appropriate in all cases. It is also worth noting that, given the rate of change for certain early-stage companies, the price paid in a recent transaction may not be reflective of the fair value quicker than is typically the case.

In their latest valuation guidelines, the IPEV and the AICPA recommend the use of more complex valuation methodologies, when necessary. These complex valuation techniques may include:

- Scenario-Based Model (or PWERM);
- Option Pricing Model; or
- Milestone-Based Model (or adjusted price or recent investment).

IPEV Special Valuation Guidance, March 2020

As the impact of COVID-19 continues to ripple across the globe and affect the fundamental outlook of a wide array of sectors, the need to apply additional valuation techniques to estimate the fair value of investments is becoming increasingly necessary. This point was recognised by the International Private Equity and Venture Capital Valuation Guidelines Board (IPEV) who recently issued a Special Valuation Guidance note to assist with 31 March valuations.

Key aspects of the Special Guidance:

- Fair value must capture current market conditions. Fair value does not equal a "fire sale" price.
- Valuation inputs such as performance metrics and/or future cash flows need to be adjusted for the impact of the crisis.
- Greater uncertainty may translate into greater risk, which may translate into greater required returns, which may translate into lower asset values.
- It may no longer be appropriate for recent transaction prices, especially those from before the expansion of the pandemic to receive significant, if any, weight in determining fair value. This will increase the need for mark-to-model valuation techniques.

At IHS Markit, we have developed scenarios for a number of business planning purposes ranging from operational decision making to regulatory strategy and its potential implications to inputs into due diligence valuations. The approach relies on the market-level insights from our economists who provide baseline estimates and assessments of direct economic risks and magnitudes.

The board further highlights the following key aspects with respect to valuing certain types of equity and debt investments which should be considered on an investment by investment basis:

- The impact of the crisis on the portfolio company's revenue/customers, supply chain, and operations must be rigorously considered.
- Adjustments to performance projections and/or metrics are likely to be necessary to reflect current conditions and uncertainty in projections.
- Scenario analysis is likely to be necessary to assess and incorporate the probability of the crisis extending for 3-, 6-, 12-, 18-months or longer.
- Liquidity needs must be evaluated more than ever. What is the likelihood of a loan covenant breach? What is the impact of customers delaying payments or nonpayment and the impact on reduced cash flow? What is the source of working capital required to "restart" the business if impacted by the crisis? A scenario analysis that weighs various potential outcomes (including the risk of default or potential government support) may be appropriate to assist in estimating fair value.
- Par value or face value or cost value is not automatically fair value. Credit spreads have widened for various industries, credit ratings, and terms, which will put downward pressure on fair valuation of debt instruments.

It is important to note that the key difference when dealing with Level 3 assets (and particularly early-stage unlisted equity assets or convertibles) is the heavily analyst-driven approach to valuation. For valuations of such assets, analysts must have the aptitude to understand legal documentation of the deal, corporate finance theory, financial performance and the relevance of milestones and disclosures, as well as the modelling skills to ensure these are appropriately captured at inception and throughout the life of the deal. Due to the heterogeneous nature of investments, this requires significant access to the correct market data, research, model infrastructure, people and control oversights.

In our view, asset owners need to consider the potential impact of COVID-19 in re-evaluating their investments

even if they expect the high levels of market volatility to be short-lived.

The principles of fair value should be kept front of mind as participants construct their valuations, i.e. incorporate market assumptions for the orderly transaction price at the measurement date with known or knowable information.

Whilst a view must be taken as to the length and depth of the anticipated economic downturn and the impact on the specific investment being valued, judgement should be exercised to determine the price of the investment in an orderly transaction at the measurement date.

These insights are combined to develop scenario narratives on the performance of an industry in a particular country. While the narratives themselves can be largely qualitative, there are often clear quantitative economic implications.

These quantitative assessments and judgmental assessments of qualitative impacts are then used as inputs into our proprietary macroeconomic models and associated industry models. This allows us to trace the impacts of the different elements of a scenario at the economy-wide level as well as the industry-level. These macroeconomic and industry observations/impacts, in turn, can inform valuations through providing different trajectories for market size, risk free rates, inflation etc. IHS Markit believes this offers a practical yet sensitive set of frameworks to start viewing the potential impact on any given economic turbulence.

Appendix

List of selected cybersecurity traded vendors and their YTD financial performance (31st July 2020).

Company Name	Share Price LOC 12/31/2019	Share Price LOC 7/31/2020	31-Jul-20 YTD Return	31-Jul-20 Market Cap (US$m)	YTD Change	Enterprise Value (US$m)	YTD Change	Valuation Multiples EV/ Revenue	YTD Change	EV/ EBITDA	YTD Change	P/E	YTD Change	31-Jul-20 NTM Revenue	NTM EBITDA	YTD NTM Revenue Adjustment	YTD NTM EBITDA Adjustment
Absolute Software Corporation	8.7	15.84	82%	502.5	79%	472.9	86%	4.52x	81%	18.14x	112%	47.25x	7%	113.4	25.1	4.6%	10.1%
Avast Plc	4.60	5.745	25%	7,730.0	28%	8,552.0	20%	9.73x	19%	18.37x	18%	34.77x	6%	921.2	517.3	-1.4%	0.2%
Check Point Software Technologies Ltd.	110.96	125.35	13%	17,574.1	9%	16,490.9	14%	8.17x	13%	18.18x	14%	21.12x	6%	2,084.5	1,032.1	0.8%	-3.0%
CrowdStrike Holdings, Inc.	49.87	113.2	127%	17,117.4	67%	23,430.8	149%	41.59x	81%	N/A	N/A	N/A	N/A	889.9	60.3	25.4%	108.3%
CyberArk Software Ltd.	116.58	117.84	1%	4,564.1	3%	3,882.6	-1%	8.61x	-5%	85.56x	59%	134.03x	3%	505.3	110.5	-1.1%	-30.8%
FireEye, Inc.	16.53	15.1	-9%	3,405.4	-5%	3,506.6	-4%	3.83x	-7%	N/A	N/A	N/A	N/A	946.3	135.1	-0.5%	20.8%
ForeScout Technologies, Inc.	32.8	28.99	-12%	1,436.5	-5%	1,395.0	-9%	4.36x	-4%	N/A	N/A	N/A	N/A	366.4	(20.3)	-5.4%	37.8%
Fortinet, Inc.	106.76	138.3	30%	22,356.0	22%	21,018.7	28%	8.93x	17%	43.86x	8%	54.38x	2%	2,724.2	762.4	9.3%	8.1%
F-Secure Oyj	3.045	2.955	-3%	554.9	2%	567.8	1%	2.36x	2%	20.54x	-30%	76.45x	0%	267.4	37.8	1.1%	6.3%
Mimecast Limited	43.38	46.93	8%	2,970.2	10%	3,025.2	10%	6.83x	3%	38.82x	-17%	600.28x	N/A	508.6	103.0	4.0%	11.4%
MobileIron, Inc.	4.86	6.23	28%	728.2	33%	643.4	38%	2.99x	32%	N/A	N/A	N/A	N/A	212.9	(5.3)	-2.5%	270.0%
NortonLifeLock Inc.	25.52	21.45	-16%	12,675.8	-20%	14,736.0	-20%	7.94x	32%	17.32x	-2%	18.08x	2%	2,467.2	1,257.4	-4.2%	19.9%
Okta, Inc.	115.37	220.98	92%	25,663.5	98%	27,230.0	97%	42.30x	63%	N/A	N/A	N/A	N/A	892.7	(10.3)	17.1%	-244.8%
Palo Alto Networks, Inc.	231.25	255.92	11%	24,687.6	9%	24,533.7	16%	7.52x	7%	405.52x	109%	N/A	N/A	3,965.8	888.6	5.4%	2.7%
Ping Identity Holding Corp.	24.3	34.36	41%	2,764.1	43%	2,763.7	43%	11.04x	39%	84.12x	90%	N/A	N/A	276.1	38.1	3.7%	26.5%
Proofpoint, Inc.	114.78	115.67	1%	6,661.2	3%	6,527.4	4%	6.67x	-5%	479.56x	N/A	N/A	N/A	1,135.0	182.2	6.6%	-5.5%
Qualys, Inc.	83.37	123.48	48%	4,810.7	49%	4,572.3	52%	13.35x	43%	37.63x	33%	56.70x	3%	384.8	165.2	4.7%	6.0%
Radware Ltd.	25.78	25.55	-1%	1,184.0	-2%	1,054.2	4%	4.21x	5%	41.99x	17%	57.00x	2%	259.7	38.4	-5.8%	-20.0%
Rapid7 Inc.	56.02	59.57	6%	3,038.4	10%	3,062.7	9%	8.32x	-3%	N/A	N/A	N/A	N/A	433.3	21.3	8.9%	-21.1%
Splunk Inc.	149.77	209.82	40%	33,333.9	43%	33,708.4	49%	14.23x	38%	N/A	N/A	N/A	N/A	2,744.3	166.6	-3.3%	-67.2%
Tenable Holdings, Inc.	23.96	33.93	42%	3,435.9	46%	3,249.7	54%	8.15x	37%	N/A	N/A	N/A	N/A	479.5	17.2	10.1%	N/A
Trend Micro Incorporated	5,600	6,150	10%	8,175.2	13%	6,634.7	20%	4.23x	16%	12.73x	13%	30.04x	4%	1,686.2	497.0	6.9%	9.1%
Varonis Systems, Inc.	77.71	108.35	39%	3,409.6	44%	3,354.2	46%	12.95x	43%	N/A	N/A	N/A	N/A	284.1	(9.9)	0.6%	-29.5%
Zix Corporation	6.78	7.115	5%	405.2	7%	696.5	5%	3.41x	-11%	20.15x	-44%	N/A	N/A	226.6	52.8	6.5%	2.2%
Zscaler, Inc.	46.5	129.85	179%	16,947.8	185%	16,575.1	197%	42.34x	153%	N/A	N/A	N/A	N/A	554.8	64.7	20.6%	47.4%
S&P 500	3230.78	3271.12	1%					2.89x		15.07x		22.77x					
Bottom Quartile			1%					4.36x		18.27x		32.40x				-1.1%	-16.4%
Median			13%					8.15x		37.63x		54.38x				4.2%	4.3%
Top Quartile			41%					11.04x		63.99x		66.73x				7.1%	12.5%

Source: IHS Markit / FactSet

Appendix

List of highest scorers in BitSight / IHS Markit Research Signals Sector rank (17th July 2020) and their YTD financial performance (31st July 2020).

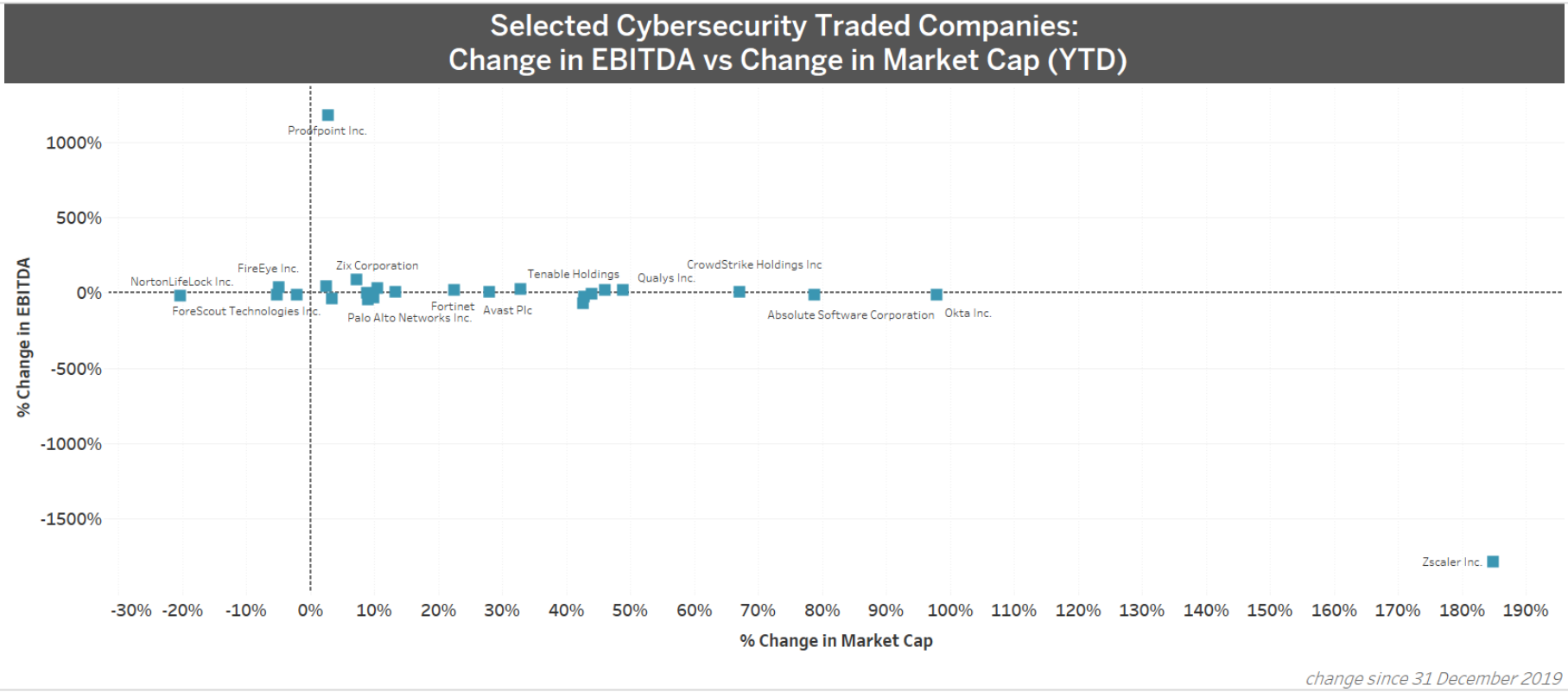
		17-Jul-20	17-Jul-20			31-Jul-20	31-Jul-20										31-Jul-20			
Company Name	Sector	BitSight Rank	BitSight / IHS Markit Sector Rank	Share Price LOC 12/31/2019	Share Price LOC 7/31/2020	YTD Return	Market Cap (US$m)	YTD Change	Enterprise Value (US$m)	YTD Change	Valuation Multiples						NTM Revenue	NTM EBITDA	YTD NTM Revenue Adjustment	YTD NTM EBITDA Adjustment
											EV/ Revenue	YTD Change	EV/ EBITDA	YTD Change	P/E	YTD Change				
T-Mobile US, Inc.	Communication Services	5	1	78.4	107.4	37%	133,022	98%	173,774	60%	51,723	15%	15,933	0.2	2,362	-32%	3.4x	39%	10.9x	32%
Telecom Egypt	Communication Services	21	1	10.2	13.0	28%	1,383	29%	2,374	24%	1,633	6%	387	0.1	200	-6%	1.5x	16%	6.1x	13%
Intouch Holdings Public Company	Communication Services	31	1	57.3	56.8	-1%	5,835	-5%	5,873	-5%	146	-7%	40	(0.2)	353	-1%	40.1x	2%	147.9x	13%
Quebecor Inc.	Communication Services	31	1	33.1	30.6	-8%	5,776	-11%	10,497	-8%	3,180	-2%	1,427	0.0	444	6%	3.3x	-7%	7.4x	-9%
MasMovil Ibercom, S.A.	Communication Services	37	1	20.3	22.7	12%	3,532	17%	5,803	25%	1,975	5%	561	0.1	142	36%	2.9x	19%	10.3x	11%
CITIC Telecom International Holdings Limited	Communication Services	43	1	2.8	2.5	-13%	1,163	-13%	1,873	-11%	1,150	0%	315	0.0	128	0%	1.6x	-11%	6.0x	-11%
Okinawa Cellular Telephone Company	Communication Services	57	1	4,270.0	4,225.0	-1%	1,093	2%	1,088	2%	633	2%	197	0.0	92	1%	1.7x	0%	5.5x	-1%
Advanced Info Service Public Co.	Communication Services	60	1	213.0	185.0	-13%	17,639	-17%	23,919	0%	5,754	-1%	2,756	0.1	954	-5%	4.2x	1%	8.7x	-8%
JOYY, Inc.	Communication Services	60	1	52.8	79.8	51%	5,124	50%	3,080	114%	3,564	-4%	N/A	N/A	164	-67%	0.9x	122%	N/A	N/A
Chorus Limited	Communication Services	77	1	6.2	7.5	21%	2,209	19%	4,430	11%	629	0%	422	0.0	36	0%	7.0x	11%	10.5x	11%
Melco International Development Ltd	Consumer Discretionary	1	1	21.9	14.6	-33%	2,857	-33%	10,260	-13%	3,191	0%	1,402	0.0	88	0%	3.2x	-13%	7.3x	-13%
Melco Resorts and Entertainment Ltd	Consumer Discretionary	1	1	24.2	16.5	-32%	7,848	-33%	11,996	-23%	5,184	-10%	1,072	(0.2)	(107)	-129%	2.3x	-15%	11.2x	0%
Chegg, Inc.	Consumer Discretionary	71	1	37.9	81.0	114%	10,012	118%	10,218	116%	504	23%	86	0.7	2	-117%	20.3x	76%	118.6x	27%
Jeronimo Martins SGPS SA	Consumer Staples	1	1	14.7	14.3	-3%	10,637	3%	13,210	1%	21,056	1%	1,543	(0.0)	366	-16%	0.6x	1%	8.6x	6%
Pilgrim's Pride Corporation	Consumer Staples	1	1	32.7	15.4	-53%	3,746	-54%	6,174	-39%	11,740	3%	704	(0.3)	263	-42%	0.5x	-41%	8.8x	-13%
Casey's General Stores, Inc.	Consumer Staples	3	1	159.0	159.2	0%	5,875	0%	7,207	1%	9,175	-2%	650	0.1	264	12%	0.8x	3%	11.1x	-6%
Japan Tobacco Inc.	Consumer Staples	3	1	2,432.5	1,812.0	-26%	34,276	-23%	38,371	-21%	19,858	-1%	5,888	0.0	2,721	-15%	1.9x	-20%	6.5x	-22%
Metcash Limited	Consumer Staples	3	1	2.6	2.7	5%	1,987	21%	2,516	50%	8,782	-2%	311	0.2	(38)	0%	0.3x	53%	8.1x	24%
Olam International Limited	Consumer Staples	3	1	1.8	1.3	-27%	3,160	-28%	10,593	-9%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
1Life Healthcare, Inc.	Health Care	1	1	N/A	29.6	N/A	3,735	N/A	3,524	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Arrowhead Pharmaceuticals, Inc.	Health Care	1	1	63.4	43.1	-32%	4,383	-31%	4,111	-33%	124	-24%	(28)	(1.6)	(24)	-146%	33.2x	-12%	N/A	N/A
Biohaven Pharmaceutical Holding Company	Health Care	1	1	54.4	64.0	18%	3,748	32%	3,687	38%	11	N/A	N/A	N/A	(609)	15%	339.9x	N/A	N/A	N/A
Invitae Corp.	Health Care	1	1	16.1	29.2	81%	3,848	141%	3,862	168%	233	8%	(368)	0.7	(421)	74%	16.6x	149%	N/A	N/A
Mediclinic International Plc	Health Care	1	1	4.1	2.7	-35%	2,599	-35%	5,611	-22%	3,915	0%	687	0.0	(406)	-353%	1.4x	-23%	8.2x	-23%
Alaska Air Group, Inc.	Industrials	1	1	67.8	34.4	-49%	4,258	-49%	6,025	-40%	6,674	-24%	393	(0.7)	57	-93%	0.9x	-21%	15.3x	135%
ATS Automation Tooling Systems Inc.	Industrials	1	1	21.4	17.3	-19%	1,193	-22%	1,418	-16%	1,052	0%	134	(0.0)	34	-21%	1.3x	-16%	10.6x	-13%
Norwegian Air Shuttle ASA	Industrials	1	1	37.8	2.3	-94%	893	27%	6,001	-18%	4,842	0%	735	0.0	(184)	0%	1.2x	-18%	8.2x	-18%
Old Dominion Freight Line, Inc.	Industrials	1	1	126.5	182.8	44%	21,563	42%	21,139	42%	3,941	-4%	1,076	(0.0)	589	-4%	5.4x	48%	19.7x	45%
Proto Labs, Inc.	Industrials	1	1	101.6	120.1	18%	3,197	18%	3,089	19%	451	-2%	104	(0.1)	59	-8%	6.8x	21%	29.8x	27%
Toppan Forms Co., Ltd.	Industrials	1	1	1,226.0	995.0	-19%	1,082	-16%	628	-19%	2,047	-1%	138	(0.0)	20	-40%	0.3x	-18%	4.6x	-18%
TriNet Group, Inc.	Industrials	1	1	56.6	66.0	17%	4,442	12%	3,757	7%	3,983	3%	471	0.5	320	51%	0.9x	4%	8.0x	-29%
Accenture Plc	Information Technology	1	1	210.6	224.8	7%	143,004	7%	140,488	10%	44,547	1%	7,575	0.0	4,950	2%	3.2x	8%	18.5x	7%
Link Administration Holdings Ltd.	Information Technology	1	1	5.9	4.0	-32%	1,514	-31%	2,157	-17%	913	0%	229	0.0	111	0%	2.4x	-17%	9.4x	-17%
Ubiquiti Inc.	Information Technology	10	1	189.0	185.3	-2%	11,801	-4%	12,442	-3%	1,256	4%	469	0.1	359	4%	9.9x	-7%	26.5x	-8%
Verint Systems Inc.	Information Technology	82	1	55.4	44.9	-19%	2,897	-22%	3,370	-19%	1,276	-1%	162	(0.2)	21	-59%	2.6x	-18%	20.7x	2%
Corteva Inc	Materials	1	1	29.6	28.6	-3%	21,373	-3%	21,891	-9%	14,041	1%	1,885	(0.1)	465	-261%	1.6x	-11%	11.6x	5%
Telecom Plus PLC	Utilities	15	1	15.0	13.4	-11%	1,383	-11%	1,458	-9%	1,112	3%	84	0.1	46	6%	1.3x	-12%	17.3x	-16%
S&P 500				3230.8	3271.1	1%											2.9x	4%	15.1x	7%
Bottom Quartile						-26%											1.3x		8.0x	
Median						-3%											2.3x		10.3x	
Top Quartile						17%											4.8x		16.3x	

Appendix

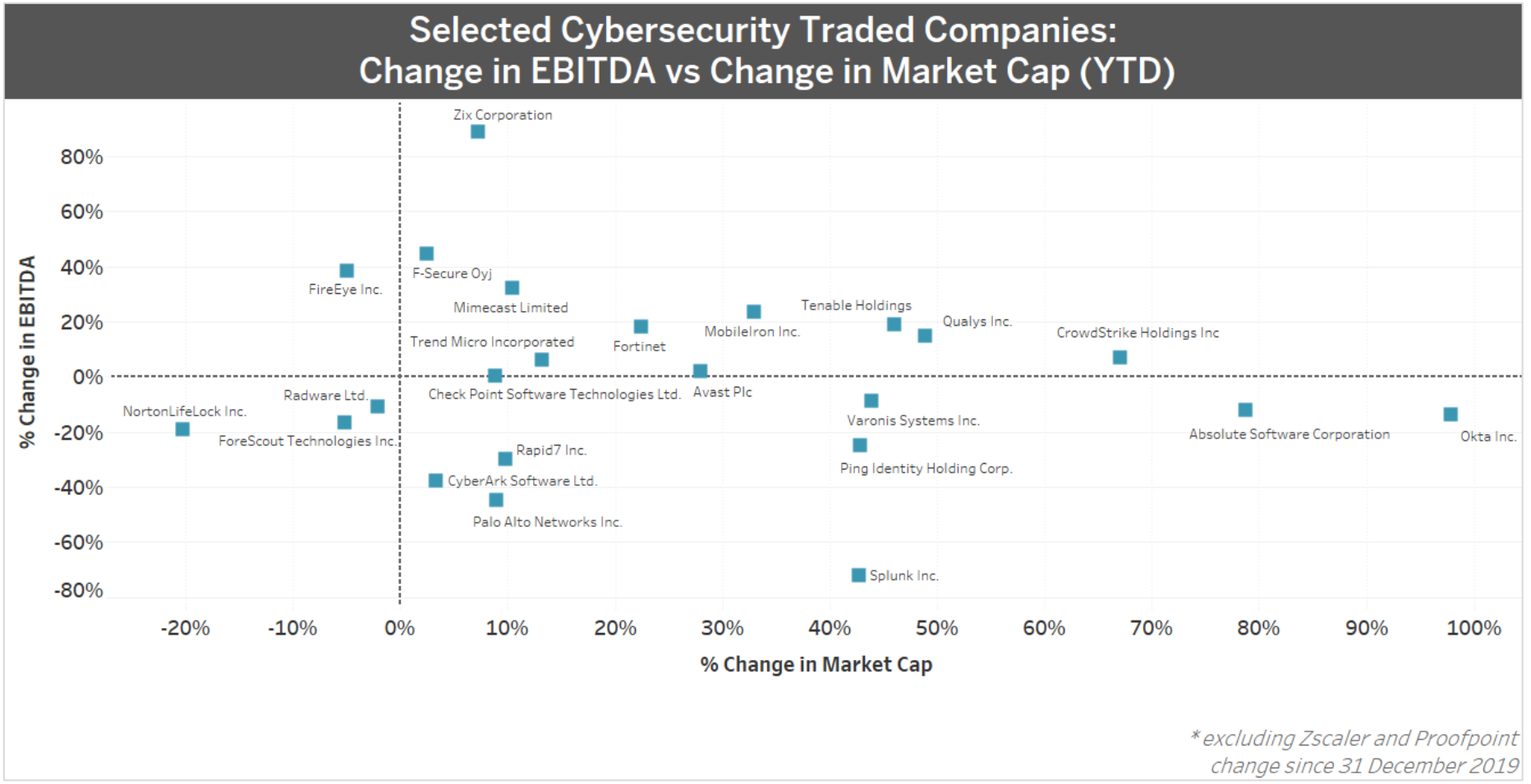
List of lowest scorers in BitSight / IHS Markit Research Signals Sector rank (17th July 2020) and their YTD financial performance (31st July 2020).

		17-Jul-20	17-Jul-20			31-Jul-20	31-Jul-20										31-Jul-20			
Company Name	Sector	BitSight Rank	BitSight / IHS Markit Sector Rank	Share Price LOC 12/31/2019	Share Price LOC 7/31/2020	YTD Return	Market Cap (US$m)	YTD Change	Enterprise Value (US$m)	YTD Change	Valuation Multiples						NTM Revenue	NTM EBITDA	YTD NTM Revenue Adjustment	YTD NTM EBITDA Adjustment
											EV/ Revenue	YTD Change	EV/ EBITDA	YTD Change	P/E	YTD Change				
Alibaba Pictures Group Limited	Communication Services	98	100	1.4	1.08	-21%	3,737.7	-20%	3,036.7	-24%	7.36x	-20%	N/A	N/A	N/A	N/A	522.2	60.1	-19.4%	-52.1%
Walgreens Boots Alliance Inc	Consumer Staples	99	100	59.0	40.71	-31%	35,276.6	-33%	76,844.0	10%	0.55x	9%	13.34x	31%	46.36x	228%	143,111.3	7,320.0	1.4%	-11.2%
ITC Limited	Consumer Staples	100	100	238.0	194.25	-18%	31,901.2	-22%	28,642.5	-26%	4.47x	-17%	12.05x	-13%	15.98x	-17%	6,485.2	2,428.7	-13.6%	-17.6%
Reliance Industries Ltd	Energy	100	100	1,501.6	2070	38%	175,147.6	30%	211,017.2	32%	2.90x	54%	19.04x	51%	29.88x	37%	75,349.8	13,342.7	-18.0%	-16.1%
DB Insurance Co. Ltd	Financials	97	100	52,300	47,100	-10%	2,799.0	-13%	3,266.7	-9%	0.25x	-8%	N/A	N/A	7.24x	-27%	10,715.4	547.5	1.7%	-0.4%
Union Bank of India Limited	Financials	97	100	54.9	29.00	-47%	2,483.5	-5%	4,471.4	41%	0.73x	37%	N/A	N/A	N/A	N/A	2,775.4	N/A	21.0%	N/A
AMP Limited	Financials	99	100	1.9	1.47	-23%	3,610.6	-22%	16,019.4	-7%	2.89x	156%	N/A	N/A	N/A	N/A	311.6	385.1	-19.5%	5.2%
Hana Financial Group Inc.	Financials	99	100	36,900	29,500	-20%	7,434.2	-22%	56,842.0	23%	1.97x	-39%	N/A	N/A	3.51x	-26%	6,734.0	N/A	-2.2%	N/A
Karur Vysya Bank Ltd.	Financials	99	100	60.3	34.40	-43%	373.7	-45%	-50.9	-115%	-0.05x	-115%	N/A	N/A	10.12x	-55%	476.6	N/A	-11.0%	N/A
Fresenius Medical Care AG & Co. KGaA	Health Care	97	100	66.0	74.62	13%	26,878.0	19%	41,905.9	12%	2.10x	10%	9.70x	7%	18.58x	11%	22,583.0	4,848.8	8.7%	11.7%
Fresenius SE & Co. KGaA	Health Care	97	100	50.2	42.27	-16%	27,863.9	-11%	67,964.6	-2%	1.70x	-3%	8.96x	-3%	13.78x	-7%	45,344.6	8,920.3	8.4%	9.2%
Fagron NV	Health Care	98	100	19.3	18.96	-2%	1,618.3	3%	1,937.7	4%	3.14x	1%	15.35x	0%	24.43x	-4%	690.8	151.9	2.8%	4.2%
Hyosung Corporation	Industrials	99	100	79,100	68,300	-14%	1,207.9	-16%	3,364.5	-8%	1.33x	6%	N/A	N/A	28.68x	77%	2,904.5	272.5	-4.7%	-20.0%
Aeroports de Paris SA	Industrials	100	100	176.1	80.00	-55%	9,361.7	-52%	16,383.9	-38%	4.02x	-20%	14.44x	5%	N/A	N/A	3,960.7	1,035.1	-29.6%	-52.3%
Alfa, S.A.B. de C.V.	Industrials	100	100	15.7	12.08	-23%	2,663.4	-36%	10,438.4	-15%	0.66x	-5%	6.30x	4%	13.28x	-4%	15,597.7	1,831.4	-21.3%	-25.9%
Bouygues SA	Industrials	100	100	37.9	30.00	-21%	13,478.5	-15%	20,786.9	-15%	0.50x	-13%	5.09x	-11%	11.68x	-3%	41,764.5	3,720.2	-1.3%	-10.0%
Dogan Sirketler Grubu Holding A.S.	Industrials	100	100	1.8	2.11	15%	791.6	-2%	521.8	-11%	0.28x	10%	4.48x	-3%	6.41x	-14%	N/A	N/A	N/A	N/A
Far Eastern New Century Corporation	Industrials	100	100	29.9	25.60	-14%	4,677.8	-12%	14,833.2	9%	1.90x	13%	12.07x	14%	14.07x	-8%	7,376.7	1,347.0	-10.9%	-1.7%
Hankyu Hanshin Holdings, Inc.	Industrials	100	100	4,680	3,015	-36%	7,251.1	-34%	15,422.1	-15%	2.43x	-2%	15.09x	31%	53.84x	197%	6,525.7	1,058.2	-10.9%	-31.5%
NSK Ltd.	Industrials	100	100	1041	700	-33%	3,649.7	-31%	5,088.7	-14%	0.75x	2%	10.12x	39%	N/A	N/A	7,153.0	588.5	-11.3%	-31.9%
SK Networks Co., Ltd.	Industrials	100	100	5,940	5,090	-14%	1,060.3	-17%	5,122.3	2%	0.52x	17%	6.90x	8%	N/A	N/A	9,399.9	877.6	-23.3%	1.8%
Strabag SE	Industrials	100	100	31.0	24.95	-20%	3,245.4	-15%	1,796.8	-49%	0.10x	-49%	1.91x	-49%	7.80x	-15%	17,346.1	1,185.5	N/A	N/A
Tokyu Construction Co., Ltd.	Industrials	100	100	781.0	490	-37%	494.8	-35%	472.7	-41%	0.18x	-28%	3.41x	-3%	5.28x	5%	2,635.7	N/A	-7.7%	N/A
Tokyu Corporation	Industrials	100	100	2,019	1,172	-42%	6,926.6	-40%	17,505.7	-17%	1.73x	-12%	16.11x	16%	127.75x	478%	10,100.9	1,180.1	-9.0%	-30.4%
Magnitogorsk Iron & Steel Works PJSC	Materials	98	100	42.0	39.96	-5%	6,016.9	-20%	6,060.2	-19%	0.91x	-9%	4.00x	-5%	11.24x	26%	6,467.6	1,480.0	-11.0%	-17.0%
Yodogawa Steel Works, Ltd.	Materials	100	100	2,042	1,738	-15%	589.1	-12%	261.5	-41%	0.19x	-39%	3.02x	-44%	14.91x	10%	N/A	N/A	N/A	N/A
CoreSite Realty Corporation	Real Estate	98	100	112.1	129.05	15%	5,488.9	30%	7,292.3	24%	12.35x	21%	24.00x	20%	73.03x	31%	633.5	336.4	1.3%	0.1%
SM Prime Holdings, Inc.	Real Estate	98	100	42.1	30.00	-29%	17,629.4	-27%	22,010.2	-21%	10.70x	-13%	19.84x	-7%	30.78x	-6%	2,205.5	1,266.7	-15.5%	-13.8%
Digital Realty Trust, Inc.	Real Estate	99	100	119.7	160.54	34%	43,075.0	72%	58,715.7	52%	17.38x	43%	34.00x	53%	61.39x	42%	3,985.8	2,204.6	26.4%	14.0%
QTS Realty Trust, Inc.	Real Estate	99	100	54.3	71.95	33%	4,410.7	40%	6,497.6	27%	12.73x	20%	26.22x	18%	401.34x	199%	571.6	305.9	7.5%	9.0%
CK Asset Holdings Ltd	Real Estate	100	100	56.3	43.05	-23%	20,515.7	-23%	26,156.1	-10%	2.28x	-12%	5.66x	-6%	7.85x	10%	9,661.5	4,244.6	18.5%	0.1%
Hankyu Hanshin REIT,	Real Estate	100	100	171,300	113,600	-34%	746.9	-32%	1,343.1	-20%	8.28x	-11%	19.94x	-23%	17.79x	-34%	55.6	N/A	N/A	N/A
IWG Plc	Real Estate	100	100	4.4	2.31	-47%	3,046.5	-40%	11,502.7	-10%	3.42x	-9%	6.51x	-5%	N/A	N/A	3,474.8	448.2	-6.2%	-20.0%
Starhill Global Real Estate Investment Trust	Real Estate	100	100	0.7	0.47	-36%	740.1	-37%	1,505.8	-23%	11.44x	-13%	19.94x	-34%	N/A	N/A	138.3	94.2	-7.4%	-4.4%
YTL Hospitality REIT Units	Real Estate	100	100	1.4	0.95	-30%	381.9	-33%	811.6	-19%	6.70x	-19%	11.78x	-19%	13.61x	-33%	87.0	N/A	-32.6%	N/A
S&P 500				3230.8	3271.1	1%					2.89x		15.07x		22.77x					
Bottom Quartile						-33%					0.61x		6.14x		10.68x				-14.6%	-20.0%
Median						-21%					1.97x		11.92x		14.91x				-7.7%	-10.6%
Top Quartile						-12%					4.25x		16.84x		30.33x				1.6%	1.4%

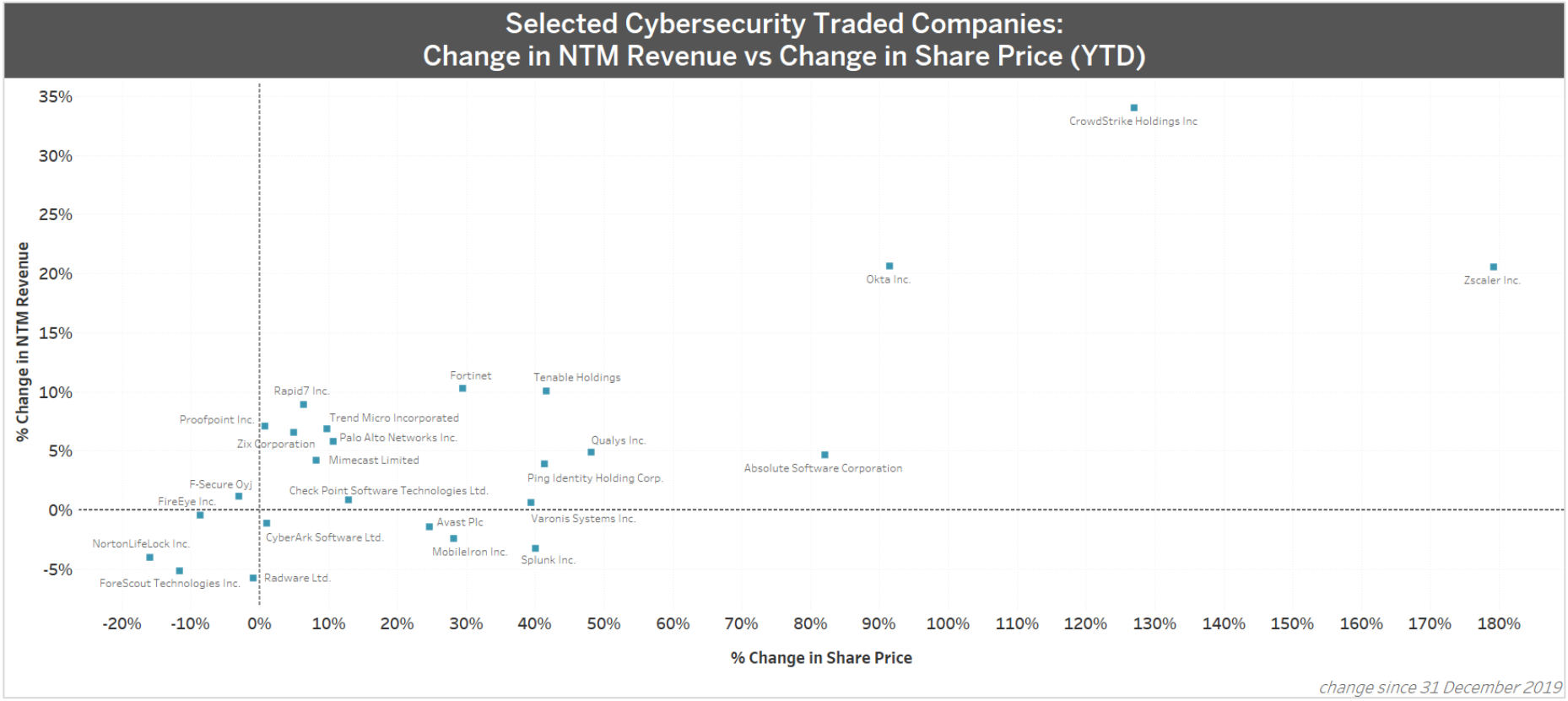
CLOSE GRAPH


Selected Cybersecurity Traded Companies:
Change in EBITDA vs Change in Market Cap (YTD)
% Change in EBITDA
1000%
500%
0%
-500%
-1000%
-1500%
Proofpoint Inc.
NortonLifeLock Inc.
FireEye Inc.
ForeScout Technologies Inc.
Zix Corporation
Palo Alto Networks Inc.
Fortinet
Avast Plc
Tenable Holdings
Qualys Inc.
CrowdStrike Holdings Inc
Absolute Software Corporation
Okta Inc.
Zscaler Inc.
-30% -20% -10% 0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100% 110% 120% 130% 140% 150% 160% 170% 180% 190%
% Change in Market Cap
change since 31 December 2019

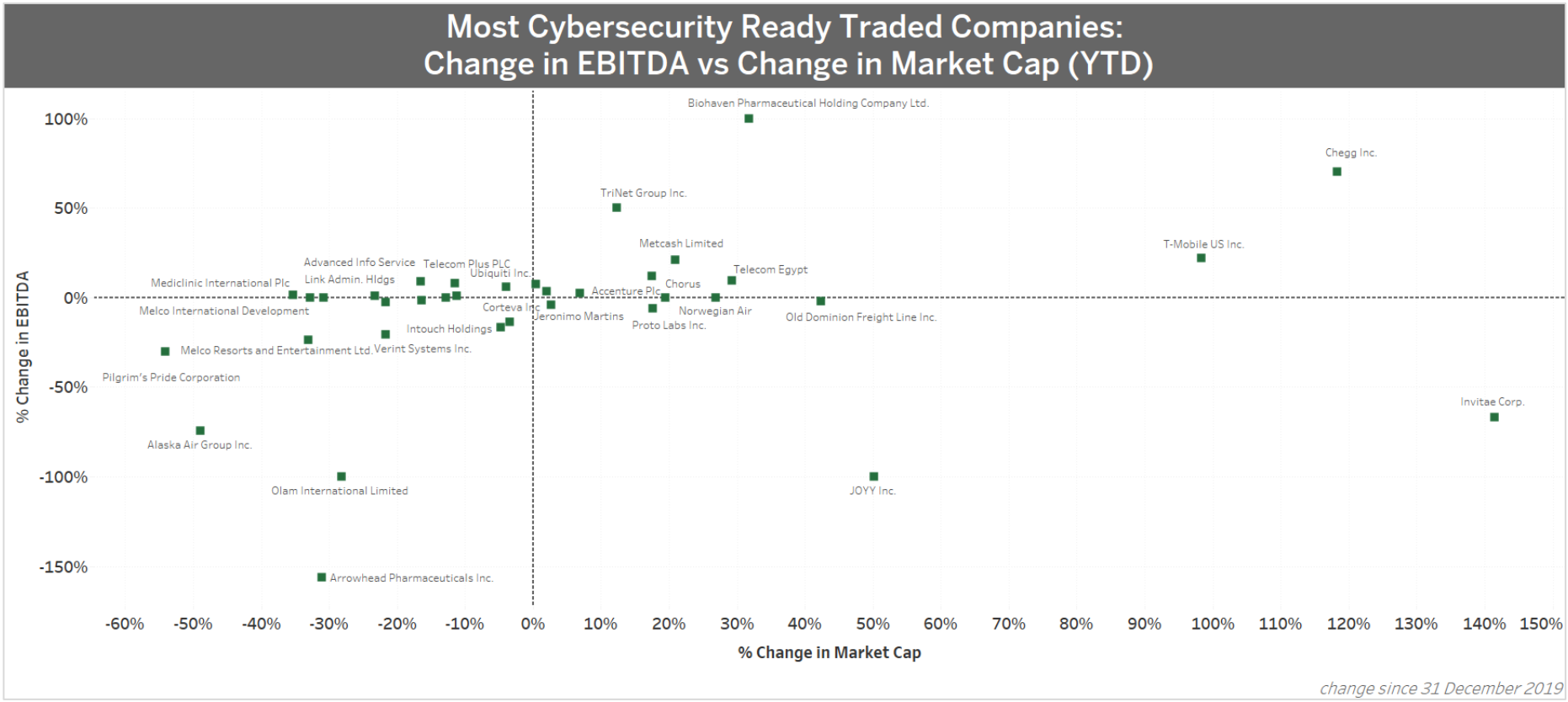
CLOSE GRAPH


Selected Cybersecurity Traded Companies:
Change in EBITDA vs Change in Market Cap (YTD)
% Change in EBITDA
80%
60%
40%
20%
0%
-20%
-40%
-60%
-80%
-20%
-10%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
% Change in Market Cap
Zix Corporation
F-Secure Oyj
FireEye Inc.
Mimecast Limited
Trend Micro Incorporated
Fortinet
MobileIron Inc.
Tenable Holdings
Qualys Inc.
CrowdStrike Holdings Inc
Check Point Software Technologies Ltd.
Avast Plc
Radware Ltd.
NortonLifeLock Inc.
ForeScout Technologies Inc.
Varonis Systems Inc.
Absolute Software Corporation
Okta Inc.
Rapid7 Inc.
Ping Identity Holding Corp.
CyberArk Software Ltd.
Palo Alto Networks Inc.
Splunk Inc.
*excluding Zscaler and Proofpoint
change since 31 December 2019

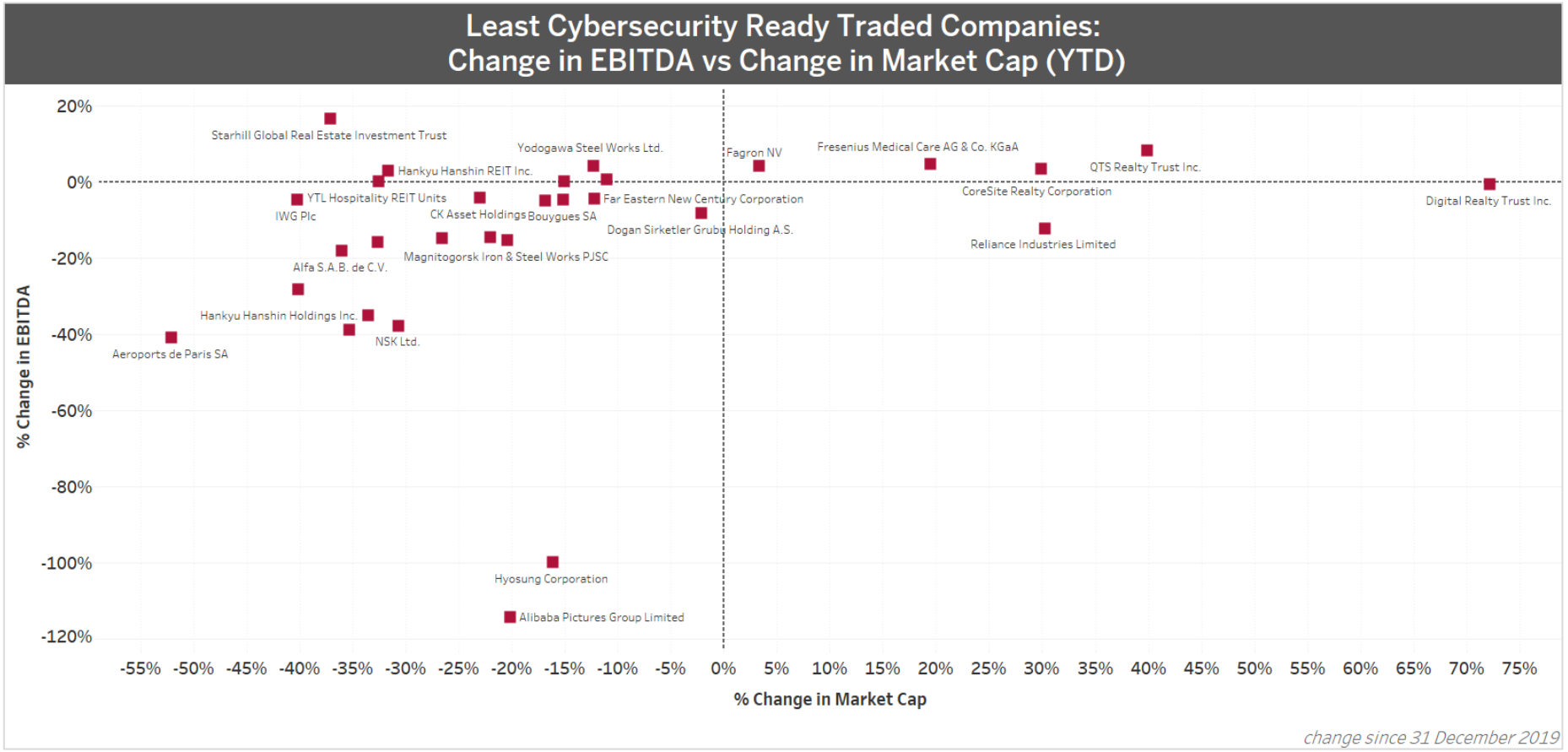
CLOSE GRAPH


Selected Cybersecurity Traded Companies:
Change in NTM Revenue vs Change in Share Price (YTD)
% Change in NTM Revenue
35%
30%
25%
20%
15%
10%
5%
0%
-5%
-20%
-10%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
110%
120%
130%
140%
150%
160%
170%
180%
% Change in Share Price
CrowdStrike Holdings Inc
Okta Inc.
Zscaler Inc.
Fortinet
Tenable Holdings
Rapid7 Inc.
Proofpoint Inc.
Trend Micro Incorporated
Zix Corporation
Palo Alto Networks Inc.
Mimecast Limited
Qualys Inc.
Ping Identity Holding Corp.
Absolute Software Corporation
F-Secure Oyj
FireEye Inc.
Check Point Software Technologies Ltd.
Varonis Systems Inc.
Avast Plc
CyberArk Software Ltd.
NortonLifeLock Inc.
MobileIron Inc.
Splunk Inc.
ForeScout Technologies Inc.
Radware Ltd.
change since 31 December 2019

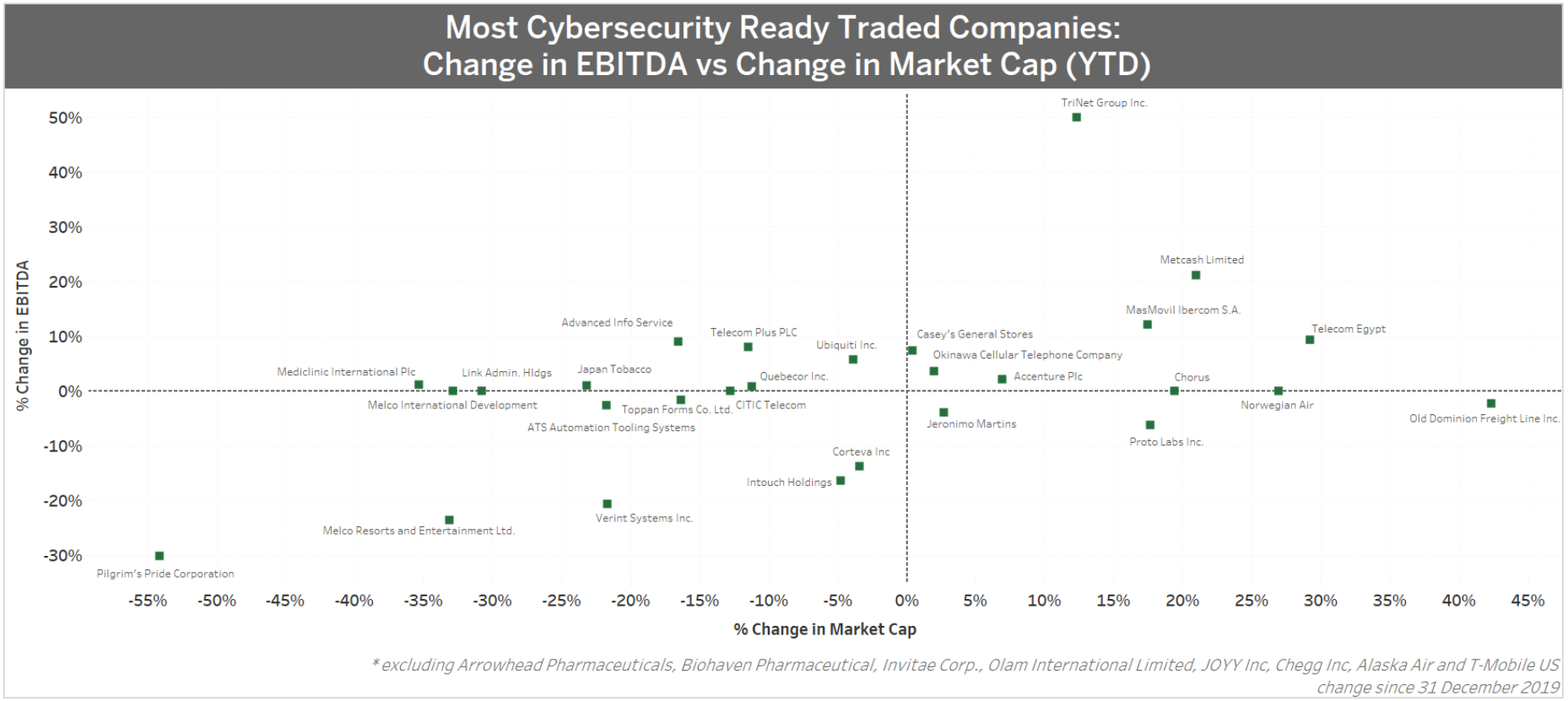
CLOSE GRAPH


Most Cybersecurity Ready Traded Companies:
Change in EBITDA vs Change in Market Cap (YTD)
% Change in EBITDA
100%
50%
0%
-50%
-100%
-150%
-60%
-50%
-40%
-30%
-20%
-10%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
110%
120%
130%
140%
150%
% Change in Market Cap
Biohaven Pharmaceutical Holding Company Ltd.
Chegg Inc.
TriNet Group Inc.
Metcash Limited
T-Mobile US Inc.
Telecom Egypt
Advanced Info Service
Telecom Plus PLC
Ubiquiti Inc.
Mediclinic International Plc
Link Admin. Hldgs
Chorus
Accenture Plc
Melco International Development
Corteva Inc
Jeronimo Martins
Norwegian Air
Old Dominion Freight Line Inc.
Proto Labs Inc.
Intouch Holdings
Melco Resorts and Entertainment Ltd.
Verint Systems Inc.
Pilgrim's Pride Corporation
Invitae Corp.
Alaska Air Group Inc.
Olam International Limited
JOYY Inc.
Arrowhead Pharmaceuticals Inc.
change since 31 December 2019

CLOSE GRAPH

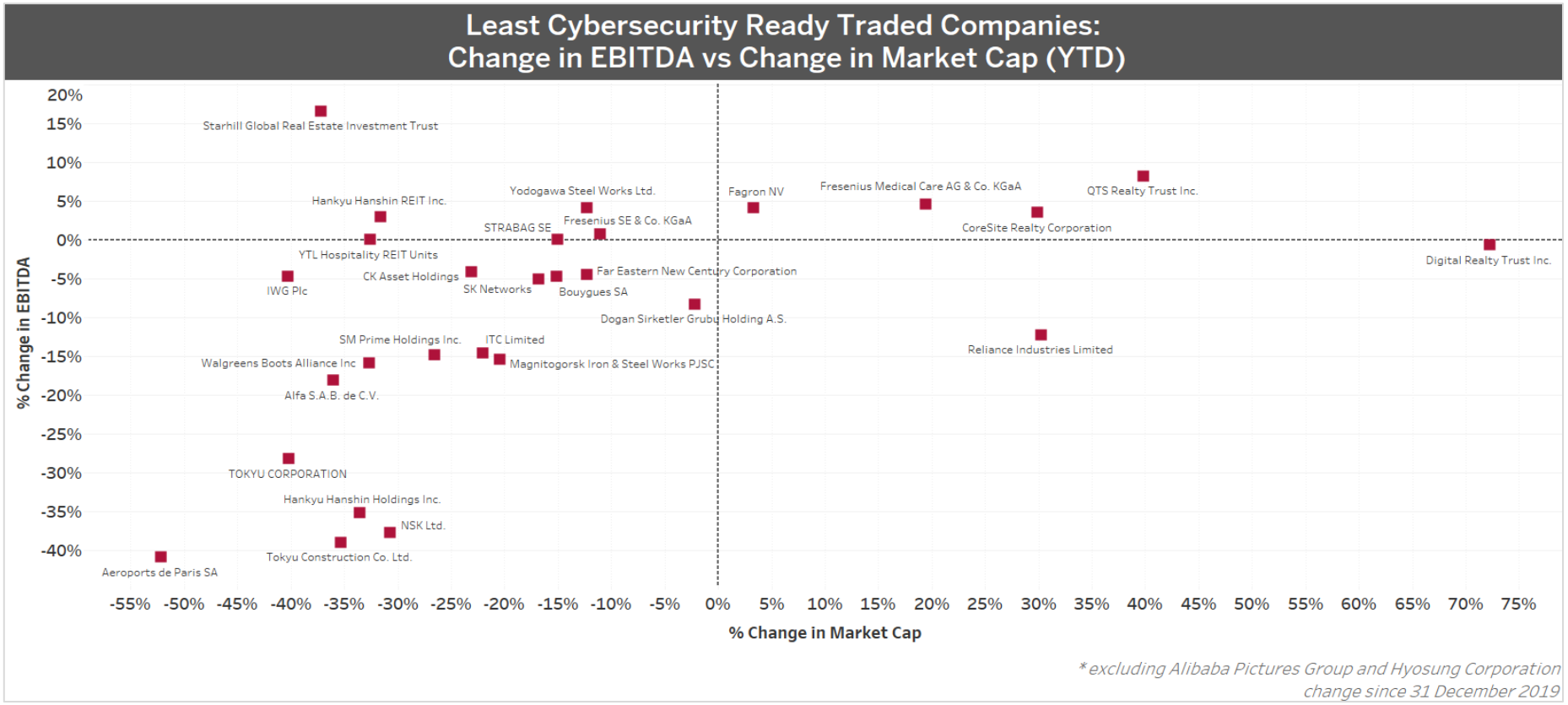

Least Cybersecurity Ready Traded Companies:
Change in EBITDA vs Change in Market Cap (YTD)
% Change in EBITDA
% Change in Market Cap
20%
0%
-20%
-40%
-60%
-80%
-100%
-120%
-55% -50% -45% -40% -35% -30% -25% -20% -15% -10% -5% 0% 5% 10% 15% 20% 25% 30% 35% 40% 45% 50% 55% 60% 65% 70% 75%
Starhill Global Real Estate Investment Trust
Yodogawa Steel Works Ltd.
Fagron NV
Fresenius Medical Care AG & Co. KGaA
QTS Realty Trust Inc.
Hankyu Hanshin REIT Inc.
YTL Hospitality REIT Units
IWG Plc
CK Asset Holdings
Bouygues SA
Far Eastern New Century Corporation
CoreSite Realty Corporation
Digital Realty Trust Inc.
Dogan Sirketler Grubu Holding A.S.
Reliance Industries Limited
Alfa S.A.B. de C.V.
Magnitogorsk Iron & Steel Works PJSC
Hankyu Hanshin Holdings Inc.
NSK Ltd.
Aeroports de Paris SA
Hyosung Corporation
Alibaba Pictures Group Limited
change since 31 December 2019

CLOSE GRAPH

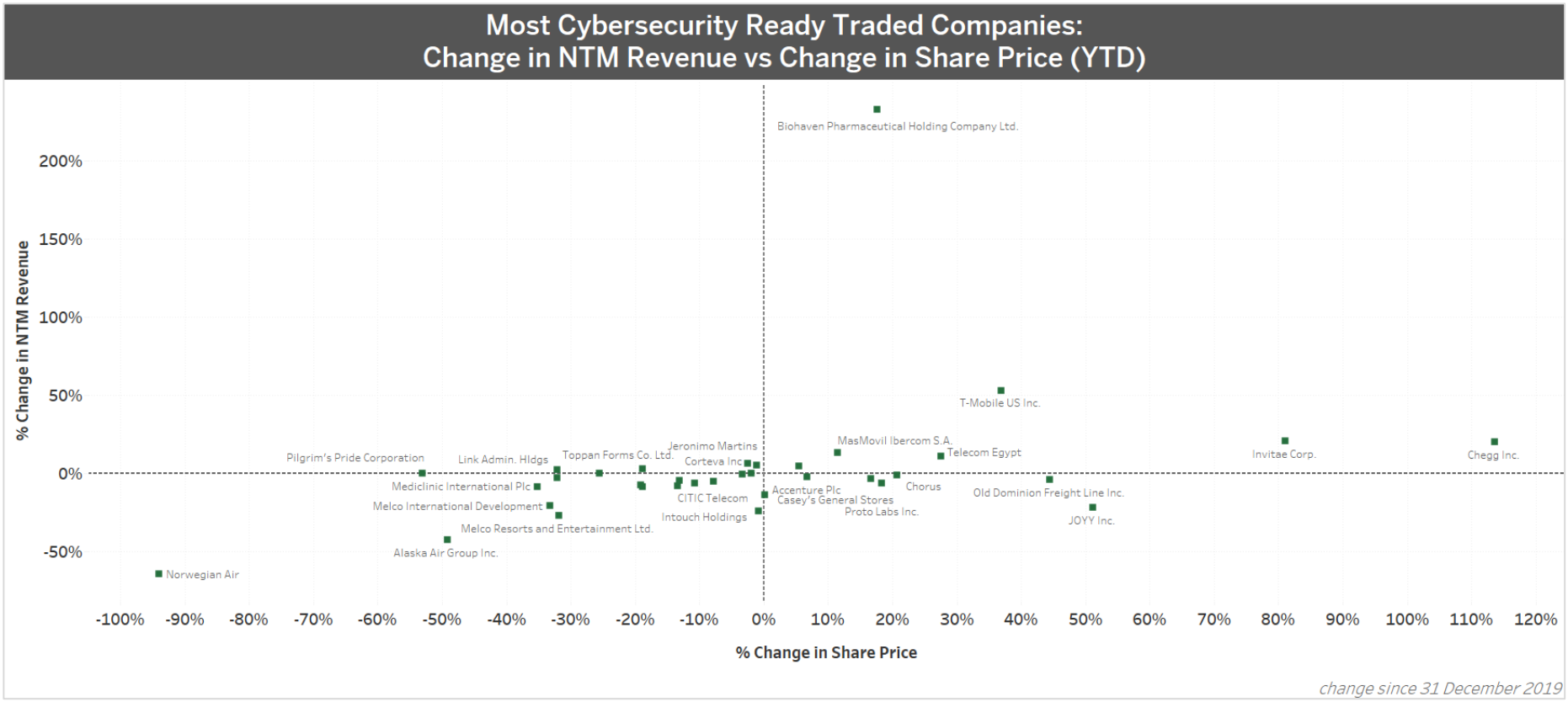


** excluding Arrowhead Pharmaceuticals, Biohaven Pharmaceutical, Invitae Corp., Olam International Limited, JOYY Inc, Chegg Inc, Alaska Air and T-Mobile US change since 31 December 2019*

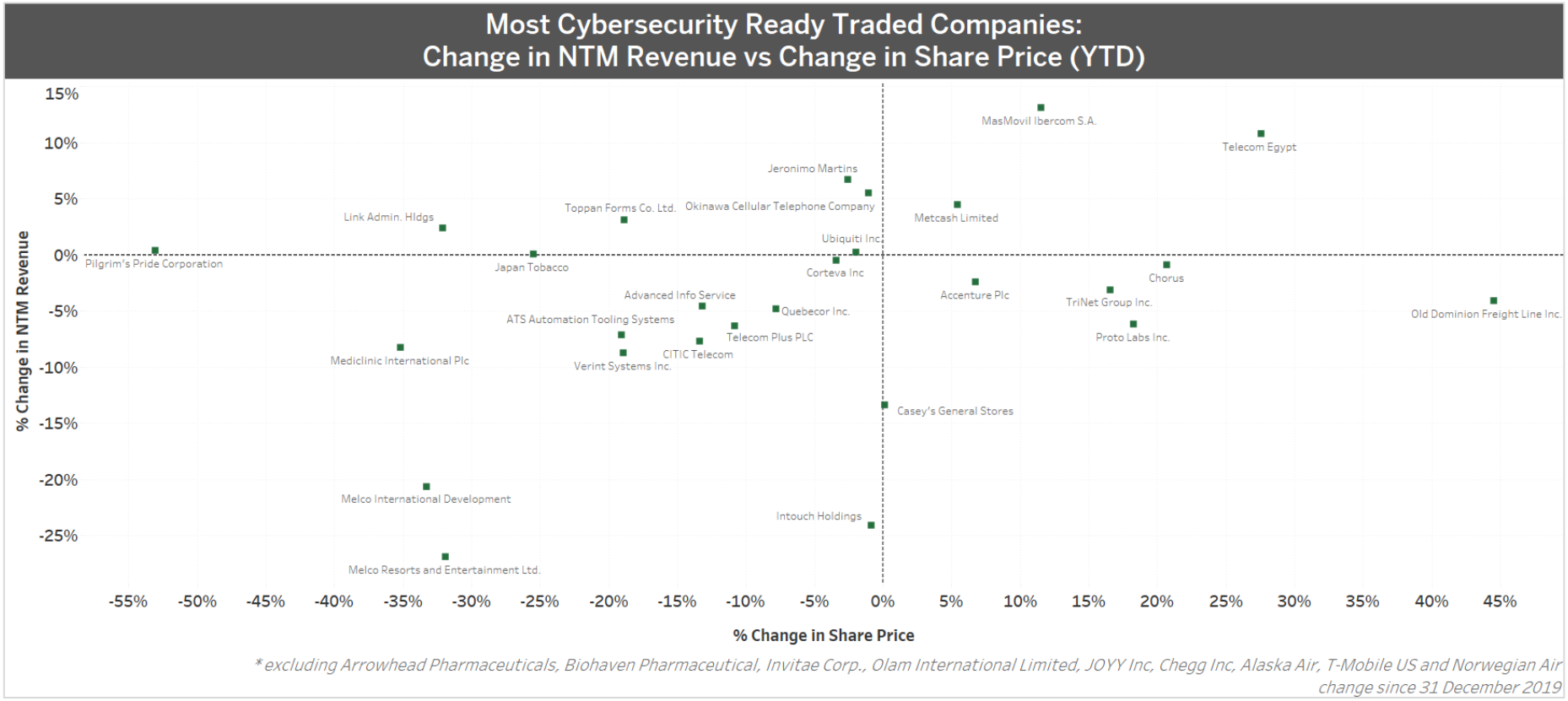
CLOSE GRAPH


Least Cybersecurity Ready Traded Companies:
Change in EBITDA vs Change in Market Cap (YTD)
% Change in EBITDA
% Change in Market Cap
Starhill Global Real Estate Investment Trust
Hankyu Hanshin REIT Inc.
YTL Hospitality REIT Units
IWG Plc
Yodogawa Steel Works Ltd.
STRABAG SE
Fresenius SE & Co. KGaA
CK Asset Holdings
SK Networks
Bouygues SA
Far Eastern New Century Corporation
Dogan Sirketler Grubu Holding A.S.
SM Prime Holdings Inc.
ITC Limited
Walgreens Boots Alliance Inc
Magnitogorsk Iron & Steel Works PJSC
Alfa S.A.B. de C.V.
TOKYU CORPORATION
Hankyu Hanshin Holdings Inc.
NSK Ltd.
Tokyu Construction Co. Ltd.
Aeroports de Paris SA
Fagron NV
Fresenius Medical Care AG & Co. KGaA
CoreSite Realty Corporation
QTS Realty Trust Inc.
Digital Realty Trust Inc.
Reliance Industries Limited
* excluding Alibaba Pictures Group and Hyosung Corporation
change since 31 December 2019

CLOSE GRAPH

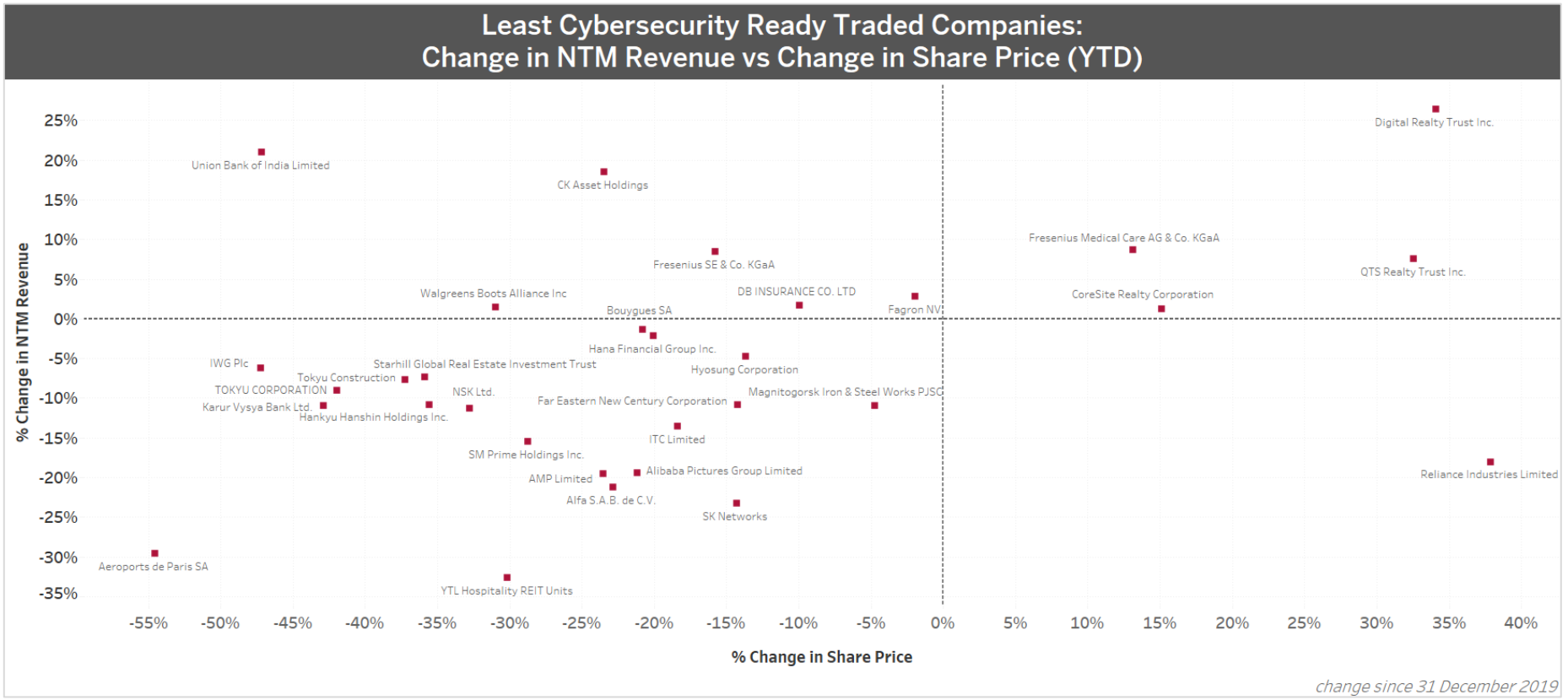

Most Cybersecurity Ready Traded Companies:
Change in NTM Revenue vs Change in Share Price (YTD)
% Change in NTM Revenue
200%
150%
100%
50%
0%
-50%
% Change in Share Price
-100% -90% -80% -70% -60% -50% -40% -30% -20% -10% 0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100% 110% 120%
Biohaven Pharmaceutical Holding Company Ltd.
T-Mobile US Inc.
MasMovil Ibercom S.A.
Telecom Egypt
Invitae Corp.
Chegg Inc.
Jeronimo Martins
Corteva Inc
Pilgrim's Pride Corporation
Link Admin. Hldgs
Toppan Forms Co. Ltd.
Mediclinic International Plc
Melco International Development
Melco Resorts and Entertainment Ltd.
Alaska Air Group Inc.
Norwegian Air
CITIC Telecom
Intouch Holdings
Accenture Plc
Casey's General Stores
Proto Labs Inc.
Chorus
Old Dominion Freight Line Inc.
JOYY Inc.
change since 31 December 2019

CLOSE GRAPH



**excluding Arrowhead Pharmaceuticals, Biohaven Pharmaceutical, Invitae Corp., Olam International Limited, JOYY Inc, Chegg Inc, Alaska Air, T-Mobile US and Norwegian Air*
change since 31 December 2019

CLOSE GRAPH


Least Cybersecurity Ready Traded Companies:
Change in NTM Revenue vs Change in Share Price (YTD)
% Change in NTM Revenue
% Change in Share Price
change since 31 December 2019
Digital Realty Trust Inc.
Union Bank of India Limited
CK Asset Holdings
Fresenius Medical Care AG & Co. KGaA
Fresenius SE & Co. KGaA
QTS Realty Trust Inc.
Walgreens Boots Alliance Inc
DB INSURANCE CO. LTD
CoreSite Realty Corporation
Bouygues SA
Fagron NV
Hana Financial Group Inc.
Hyosung Corporation
IWG Plc
Starhill Global Real Estate Investment Trust
Tokyu Construction
TOKYU CORPORATION
NSK Ltd.
Magnitogorsk Iron & Steel Works PJSC
Karur Vysya Bank Ltd.
Hankyu Hanshin Holdings Inc.
Far Eastern New Century Corporation
ITC Limited
SM Prime Holdings Inc.
Reliance Industries Limited
AMP Limited
Alibaba Pictures Group Limited
Alfa S.A.B. de C.V.
SK Networks
Aeroports de Paris SA
YTL Hospitality REIT Units

Author contact details

Leon Sinclair
Global Head
Private Equity & Debt Services, IHS Markit
Leon.Sinclair@ihsmarkit.com

Przemek Bozek
Consulting & Advisory
Private Equity & Debt Services, IHS Markit
Przemek.Bozek@ihsmarkit.com

Disclaimer Statement

For more information ihsmarkit.com

CUSTOMER CARE AMERICAS
T +1 800 447 2273
+1 303 858 6187 (Outside US/Canada)

CUSTOMER CARE EUROPE, MIDDLE EAST, AFRICA
T +44 1344 328 300

CUSTOMER CARE ASIA PACIFIC
T +604 291 3600

E CustomerCare@ihsmarkit.com

About IHS Markit

IHS Markit (S&P: INFO) is a world leader in critical information, analytics and solutions for the major industries and markets that drive economies worldwide. The company delivers next-generation information, analytics and solutions to customers in business, finance and government, improving their operational efficiency and providing deep insights that lead to well-informed, confident decisions. IHS Markit has more than 50,000 key business and government customers, including 80 percent of the Fortune Global 500 and the world's leading financial institutions. Headquartered in London, IHS Markit is committed to sustainable, profitable growth.