Cybersecurity

Update

by Przemek Bozek przemek.bozek@ihsmarkit.com

In July 2020, we looked at Cybersecurity as the new frontier for investors. We said that the security of data and information must be paramount for all businesses and individuals. We claimed that there was still a lack of understanding of how easy it is to breach an unsecured environment. We made the case that cybersecurity will be amongst the fastest growing industries, expected to see high investments in online security and further M&A activity. Our thoughts were supported by a panel of experts from Akamai, Clango, Ibex Investors, and IHS Markit colleagues.

2020 was declared the worst year ever for cyberattacks by the US Department of Justice. That same department created a Ransomware Task Force in April 2021 as the number of attacks kept increasing and we can confidently say that 2021 is already worse than the previous year. The European Commission announced plans to build a Joint Cyber Unit, run by a dedicated team of multinational experts that can be rapidly deployed to European countries in case of serious attacks, as the number of major incidents in Europe rose from 432 in 2019 to 756 in 2020[1].

During the last 12 months, we witnessed numerous attacks on schools, hospitals, local and federal agencies, watchdogs, restaurant chains, travel companies, gaming companies and many more. Recent well-known attacks include:

- Ongoing attacks on the Irish health service are causing major disruptions to many hospitals; the Health Service Executive (HSE) said it would cost as much as €100m (£85m) to recover but – more important – will also have high "human costs"[2];
- The attack on Colonial Pipeline took the US fuel pipeline offline for several days causing resource shortages in the East-Coast of the country; the Colonial Pipeline decided to pay US$4.4m in ransom; since then, most of the money had been recovered;
- An attack on US IT firm Kaseya that provides managed service systems for thousands of large and small businesses worldwide; a group responsible for the attack demanded US$70m in Bitcoin; there are similarities between the Kaseya attack and the biggest cyber breach in the XXI century – the case of SolarWinds;
- JBS, the world's largest meat processing company, paid US$11m in ransom to resolve a cyberattack;
- An attack on EA, the second largest game publisher in the world, delivering to PlayStation and Xbox amongst other platforms; in November 2020, another game-maker, Capcom, announced that its internal networks had been suspended due to unauthorised access;
- Data of about 4.5m customers was stolen during the attack on Air India where;
- 30,000 organisations globally were affected during the attack on Microsoft Exchange servers;

Unfortunately, it is expected that the number of cyber-attacks and their scale will grow over time and will continue to affect companies, supply chains and consumers. There are no industries that are immune from this risk. However, we all must do our utmost to make it harder to breach our systems, steal our identities, and compromise our passwords.

Recent Investments

According to Preqin, between July 2020 and end of June 2021, over US$32.5bn was invested in companies that either focus solely on cybersecurity services or for whom cybersecurity is a core product. The most notable deal involved Proofpoint, a cloud-based email security, discovery and compliance solution provider bought by

[1] https://www.bbc.co.uk/news/technology-57583158

[2] https://www.bbc.co.uk/news/technology-57583158

Thoma Bravo in April 2021 for US$12.3bn. In January 2021, Thoma Bravo acquired a provider of machine identity management software Venafi for US$1.15bn. In May 2021, Veritas Capital announced the acquisition of Perspecta for US$7.1bn. Perspecta was an add-on to Peraton, which acquired Northrop Grumman's IT business in February 2021. In June 2021, FireEye announced the sale of its FireEye product business to Symphony Technology Group for US$1.2bn.

The list below provides a summary of deals over US$200m:

Company	Region	Most Recent Deal Type	Most Recent Deal Date	Most Recent Deal Size (US$ m)
Arctic Wolf Networks, Inc.	North America	Series E/Round 5	22-Oct-2020	200.00
ExtraHop Networks, Inc.	North America	Buyout	08-Jun-2021	900.00
FireEye, Inc.	North America	Buyout	29-May-2021	1,200.00
FireEye, Inc.	North America	PIPE	19-Nov-2020	400.00
Illumio, Inc.	North America	Series F/Round 6	24-Jun-2021	225.00
Lacework, Inc.	North America	Series C/Round 3	18-Dec-2020	514.69
MobileIron, Inc.	North America	Add-on	28-Sep-2020	872.00
Netskope, Inc.	North America	Unspecified Round	09-Jul-2021	300.00
OneTrust LLC	North America	Series C/Round 3	01-Apr-2021	210.00
Perspecta Inc.	North America	Add-on	27-Jan-2021	7,100.00
Proofpoint, Inc.	North America	Public To Private	25-Apr-2021	12,300.00
ReliaQuest, LLC	North America	Growth Capital	25-Aug-2020	300.00
SentinelOne, Inc.	North America	Series F/Round 6	11-Nov-2020	267.00
The Citadel Group Limited	Australasia	Public To Private	14-Sep-2020	326.43
Trulioo Information Services Inc.	North America	Series D/Round 4	07-Jun-2021	393.81
Venafi, Inc.	North America	Buyout	10-Dec-2020	1,150.00

Source: Preqin

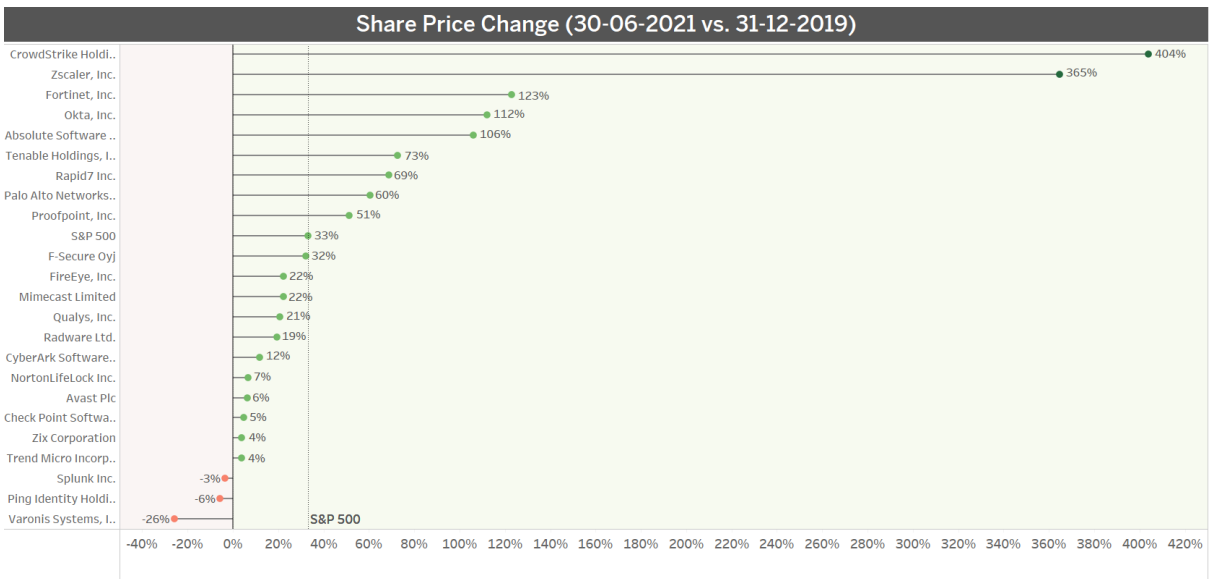
Traded company performance

Looking at the same group of twenty-five publicly listed cybersecurity companies as used in our earlier report, we noticed two had been taken private since then. During the 18 months between 31 Dec 2019 and 30 June 2021, nine companies achieved a share price growth higher

than the S&P Index, and the share price for three stocks decreased.

The two companies taken private were MobileIron and ForeScout Technologies. Advent International acquired the latter for $29 per share (~US$1.7bn) in August 2020.

Between 31 December 2019 and 30 June 2021, the unweighted change in average share price for the remaining twenty-three businesses was 64%, a healthy gain over S&P's 33% recorded growth in the same period. That share price growth is highly skewed by sizeable increases in share prices for CrowdStrike (404%), Zscaler (365%), Okta (112%) and Absolut Software (106%). On the downside, Varonis Systems (-26%), Ping Identity (-6%) and Splunk (-3%) all saw declines in value.

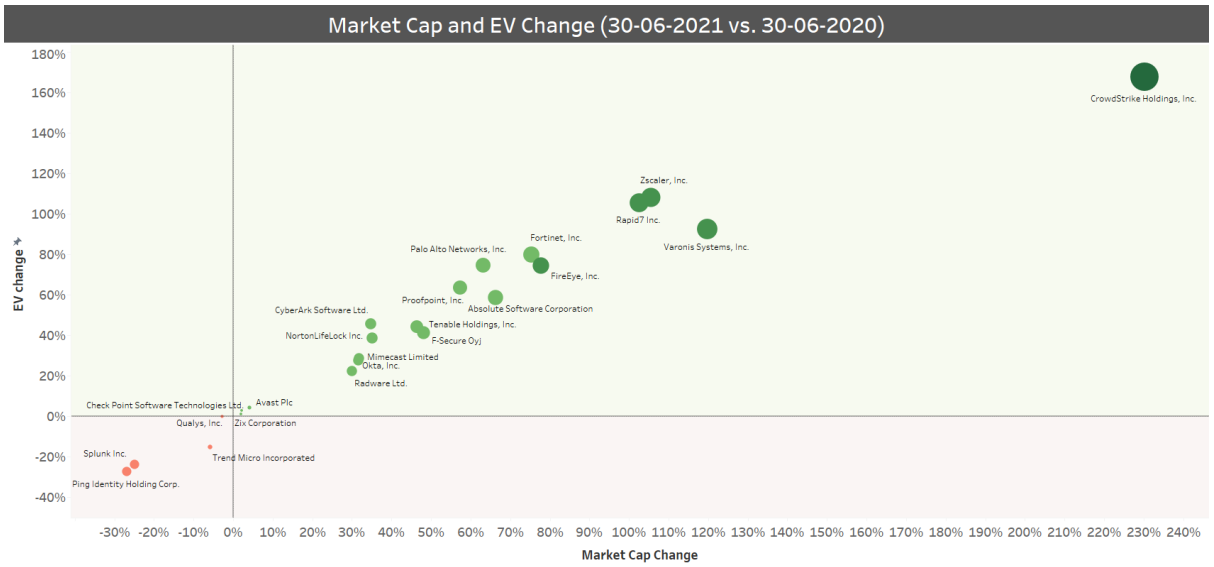


Source: IHS Markit, S&P Capital IQ

Consequently, the combined Market Cap of these firms has increased by roughly US$100bn during the last 12 months, with CrowdStrike more than tripling its value (to US$50bn), followed by Varonis Systems, Zscaler and Rapid7 that all doubled.

Recorded LTM revenues for these twenty-three companies were higher than during the same period ending on 30 June 2020. Only two firms logged small decreases while thirteen businesses achieved double-digit growth, with CrowdStrike again leading with a 77% increase, followed by Zscaler (54%) and Okta (40%). Fifteen out of twenty-five companies recorded negative LTM income; while the entire group's reported losses were over US$400m, driven by Splunk (US$-1.07bn), Palo Alto (US$-439m) and Okta (US$-317m). On the positive side were Check Point Software (US$+851m), NortonLifeLock (US$+696m) and Fortinet (US$+492m).

Eleven out of twenty-five reported negative LTM EBITDA, including Splunk (-149% YoY bringing it to US$-801m) and Zscaler (-119% YoY and US$-71m). Firms showing positive LTM EBITDA were Palo Alto with 442% YoY increase, Proofpoint with 429% YoY increase (moving from the negative side to positive), and Tenable with 90% YoY but which remained on the negative side. Despite a very large increase in sales, CrowdStrike also remains loss making, although with an LTM increase of 68% YoY, the company is close to changing that.



Source: IHS Markit, S&P Capital IQ

SPACs activity

Two pending mergers with cybersecurity companies have been announced this calendar year.

Tailwind Acquisition Corp. Class A aims to combine with QOMPLX, a cloud-native risk management company. QOMPLX supports organisations in risk management through its proprietary analytics platform by ingesting, contextualising and merging various data sources. The pro-forma enterprise value post-merger is expected to be US$1.2bn, based on 5.6x 2022E pro-forma revenue of US$210m and a pro-forma equity value of US$1.448bn. Up to US$200m of the proceeds will be used to complete two already announced add-ons: Sentar, operating in the national security sector and Tyche, an insurance software modelling firm.

The other opportunity is LGL Systems Acquisition which aims to merge with IronNet Cybersecurity. IronNet, in its prospectus, announced a pro-forma enterprise value of US$927m, representing 17.1x FY22E and 8.4x FY23E revenue and an implied pro-forma equity value of US$1.2bn. IronNet offers AI-driven behavioural analytics that identifies attack patterns that have penetrated the first line of network defence and which automatically and in real-time shares findings with its ecosystem, creating a network of fast responders.

The Future

When discussing cybersecurity, one must mention quantum computing. The principles of quantum physics are used to perform data operations. But instead of traditional bits resulting in either 0 or 1, quantum bits (qubits) can take the superposition of 0 and 1, holding and processing a lot more information. Quantum computing is a holy grail for advanced AI and cybersecurity. Since photons cannot be separated or even duplicated, it is considered as potentially the most reliable and secure way of transmitting data. This allows the receiver and sender to know whether the signal transmission has been viewed during transmission in real time. It is believed that quantum computing will shape the future of cybersecurity and companies that emerge on top of that development will become households' names in no time.

Adding up, the financial opportunities associated with cybersecurity investments remain high due to permanent migration to a partial working from home environment in much of the developed world, shifting consumer behaviour to digital and the intensification of cybercrime. As awareness increases and to shield from cybersecurity threats, organisations and individuals will keep upgrading to the most established prevention and mitigation tools. The market is vast yet offers space for new entrants as well as additional growth opportunities for already existing vendors. There will be further consolidation and new partnerships announced. There are still very

interesting offerings that remain in private hands and will look at public markets in the foreseeable future.

Valuation considerations

Below we take a look at some of the implications for valuation of SPAC PIPEs and warrants.

Considerations for PIPE valuation

Once a target company is identified and a merger is announced, market participants have enough information to consider the transaction more fundamentally. As such, the public share price of the SPAC will incorporate market views on the business combination, structure, and likelihood of consummation. Consequently, during this stage the valuation approach generally becomes similar to other PIPE investments, where a discount for lack of marketability (DLOM) is considered. In determining an appropriate DLOM, the first question to consider is 'what is the expected time to exit'? In case of a SPAC PIPE, the exit timeline is generally based on the expected merger closing date, combined with the time required to complete the registration process. It is common to consider multiple exit scenarios within the valuation, weighting the likely outcomes. Another aspect to take into consideration is volatility. How do we appropriately measure future volatility? There are several items to consider here, including the use of implied versus historical volatility, volatility time horizons, and whether it is more appropriate to use the volatility of the underlying security in a basket of comparables.

Consideration for Founder shares and Sponsors

This revolves around determining the potential exit dates for shareholders based on various price hurdles and timing restrictions. The movement of stock prices is unpredictable and countless potential outcomes exist; this indicates one should simulate thousands of scenarios or price paths when price hurdles could be hit, or conditional restrictions could be relaxed. These dates are then utilised as inputs into two valuation approaches, a discount for lack of marketability approach and discounted cash flow approach / cost of capital approach. Sponsor shares are generally convertible into common shares. Thus, similar to a PIPE, publicly traded common shares of the SPAC should provide a starting point for a valuation. However, sponsor shares generally include layers of additional price-based hurdles and time-oriented lockup periods applied to distinct blocks of shares that could be released upon contingent completion. How should a provider incorporate the various restrictive layers into a valuation methodology? A robust valuation methodology should adequately simulate the potential paths to liquidity based on the mechanics of the sponsor share lockups and determine a restriction period based on a probability weighted expected outcome. The resulting restriction period can then be utilised as inputs into other valuation approaches, such as DLOM and discounted cash flow approach / cost of capital approach.

Consideration for Warrants valuation

The valuation of warrants should consider the issuance price or, if prices are not specifically detailed in agreements, employ similar strategies as the Sponsor and Founder Shares. Given the presence of a price hurdle, liquidity restrictions, and expiration, it is prudent to generate a wide array of potential price paths over numerous simulations in order to encompass an exhaustive list of scenarios. Once the price paths are determined, the lifting of liquidity restrictions can be incorporated and either a theoretical exercise can be implemented when appropriate, or an option pricing model could be employed.

Written by:

Przemek Bozek, Advisory & Consulting, Private Equity & Debt Services, IHS Markit