LUMINII CONSULTING

Spotlight on Cyber Security and Cybercrime in 2020

2020 M&A Outlook

Lushani Kodituwakku
Managing Director

Ioana Nobel
Associate Director

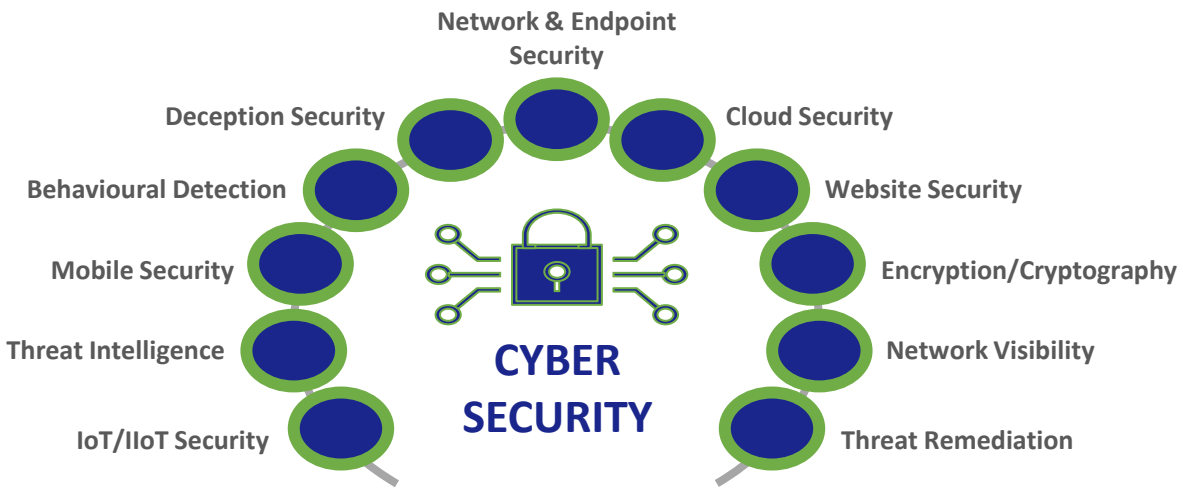
Sam Thompson
Senior Consultant

A search for "cyber security" in the Financial Times reveals 29 articles over a four-week period, involving as targets; the UK & US Government, high-profile Twitter users such as the Dutch prime minister, Amazon's CEO, LinkedIn, Morgan Stanley and Capital One, as well as retail investors and a variety of cyber-crimes from state-sponsored election interference and stealing coronavirus research to financial fraud or online espionage and personal data theft. This illustrates that cyber security is a broad term describing different distinct threats yet remains a very topical issue. Hence, Luminii Consulting's decision to explore the topic, exploring the attractiveness of investment opportunities in cyber security technology.

Cyber Security Market Map

In a market characterised by strong technical and capability overlap, Luminii Consulting believe there are presently eleven key segments of the worldwide cyber security market, covering the five stages of the cyber security value chain; **identification, protection, detection, response and recovery**.

FIGURE 1: Cyber Security Market Map



An increasingly complex and fragmented ecosystem has resulted in the emergence of cyber security consultancies, system integrators and managed service providers. Throughout the same period, Luminii have also witnessed a marked increase in the number of system integrators adopting a 'land and expand' business model, with cyber security system integrators increasingly offering internally developed add-on software elements to their customers.

The 11 key segments of cyber security are:

1. Threat intelligence: information used to understand the threats that have, could, or are currently targeting an organization. Examples of leading vendors within this space include Anomali, Recorded Future, FireEye, CrowdStrike and ThreatConnect.
2. Behavioural detection: the use of software tools to detect patterns of data transmissions in a network that are out of the norm. Examples of leading vendors within this space include RedScan, Cisco and StealthWatch.
3. Deception security: decoy technology to misdirect and prevent a cybercriminal that has managed to infiltrate a network from doing any significant damage. Examples of leading vendors within this space include Rapid7, LogRhythm, ForeScout and Attivo Networks.
4. Network & endpoint security: the securing of endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by cybercriminals. Examples of leading vendors within this space include Microsoft, Palo Alto Networks, RSA and SentinelOne.
5. Cloud security: the protection of virtualised IP, data, applications, services, and the associated infrastructure of cloud computing. Examples of leading vendors within this space include LaceWork, Qualys, Tenable and CloudPassage.
6. Website security: the protection of website data. Examples of leading vendors within this space include WordFence, cWatch, Sucuri and SiteLock.
7. Mobile security: the protection of mobile or portable computing devices, and the networks they connect to from threats and vulnerabilities. Examples of leading vendors within this space include Lookout, Strikeforce, Fortinet and CyberArk.
8. IoT/IIoT security: technology concerned with safeguarding connected devices and networks in the internet of things (IoT). Examples of leading vendors within this space include Armis, Simplisafe, Rapid7 and Bastille.
9. Network visibility: The ability to collect and directly analyse individual traffic packets as they flow through a network. Examples of leading vendors within this space include Dynatrace, LogicMonitor, Plixer and SolarWinds.
10. Encryption/cryptography: the process of encrypting data. Examples of leading vendors within this space include Craxel, CryptoMove, Spyrus and Echoworx.
11. Threat remediation: the tactics, techniques and procedures used to address and eliminate cyberattacks and data breaches. Examples of leading vendors within this space include Mimecast, Proofpoint, Barracuda Networks and SolarWinds.

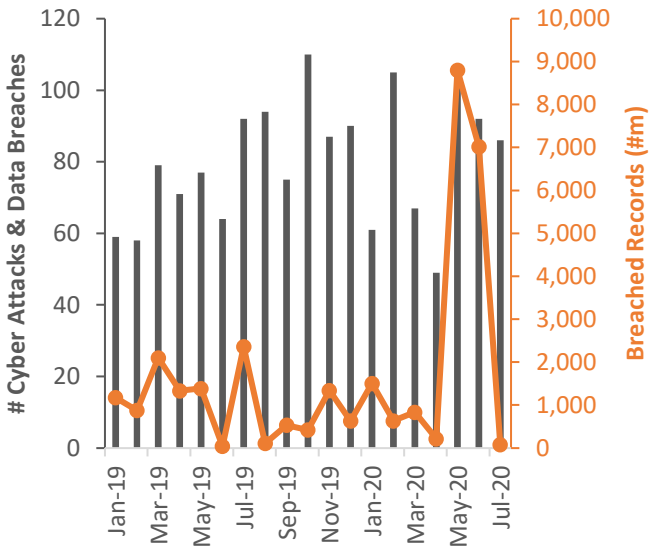
Strong Tailwinds for Cyber Security

The digitalisation of consumers and businesses has resulted in an explosion in cybercrimes from ransomware attacks to state-sponsored hacks. For consumers, this can be explained by the rate of people coming online using non-secure public Wi-Fi or adopting IoT devices. While in themselves connected devices do not store sensitive data, they communicate with others that do and can thus be points of access for cyber criminals.

According to a 2019 study by the World Economic Forum (WEF), cyberattacks were perceived as the #2 global risk of concern to business leaders in advanced economies, second only to fiscal crises. Even though since this WEF study, the COVID-19 pandemic may have become the main risk that Governments and companies must tackle, cyber security is probably still high on leaders' agendas given the operational, financial and reputational implications and the proliferation of attacks against individuals and businesses at a time when we are more reliant on digital for many aspects of our life from work to schooling and shopping for essentials.

With 565 cyber attacks and data breaches in the first half of 2020 and 19bn records breached, this year has already surpassed the 12.3bn records breached throughout the entire of 2019 and is also on-track to surpass the 956 cyber attacks recorded in 2019. May and June 2020 saw a significant rise in the number of cyber attacks and documents breached than at least the last 16 previous months. Covid-19 has clearly boosted the prevalence of cybercrime in recent months and the resultant social and economic volatility derived from the current global pandemic has led to Interpol issuing a stark warning;

FIGURE 2: Number of Cyber Attacks and Data Breaches, Worldwide (Jan 2019-Jul 2020)



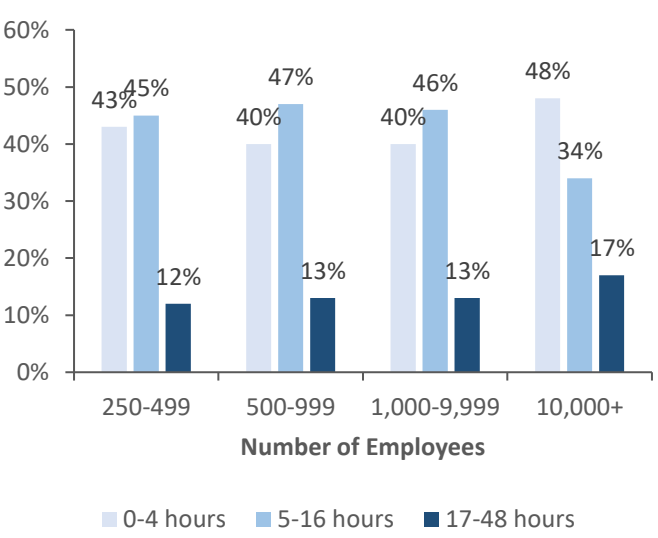
Source: IT Governance UK [Source]

"Cyber criminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by Covid-19." - **Interpol secretary general Jürgen Stock**

However, whilst cybercrime numbers in July seem to have reverted to the historic mean, it bears noting that most breaches take 100 days or more to be discovered and reported. It is clear that the rapid transition to remote working has strained the IT infrastructures and digital security of many organisations.

According to a study conducted by IBM[1], the average cost of a data breach in 2020 averaged $3.86m, with the average time to identify and contain a data breach being 280 days. Moreover, a 2020 Cisco survey with Chief Information Security Officers (CISOs) measured the downtime following severe data breaches and found that except for very large companies who have more resources, the recovery timespan tends to be 5-16 hours. However, interestingly, a higher proportion of cyberattacks on large enterprises vs. smaller organisations result in 17-48 hours downtime (17% for large organisations vs. 13% for medium sized organisations).

FIGURE 3: CISCO Study: Downtime Following Severe Data Breaches

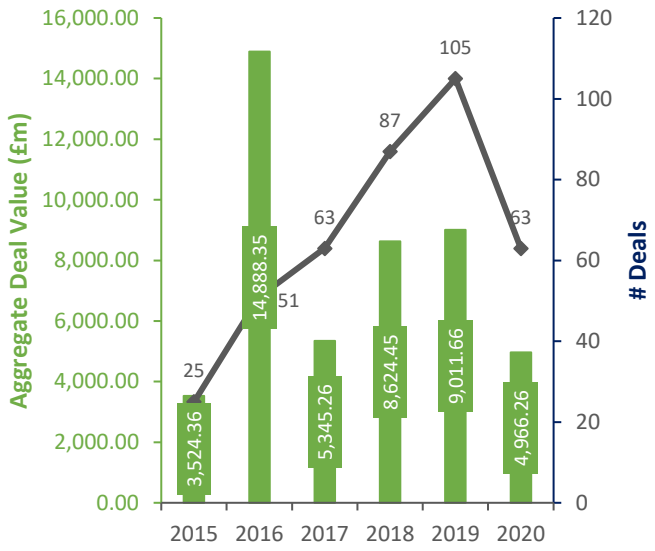


Source: Cisco 2020 CISO Benchmark Survey

[1]IBM analysed 524 breaches that occurred between August 2019 and April 2020, in organizations of all sizes, across 17 geographies and 17 industries. [Source here]

M&A within Cyber Security

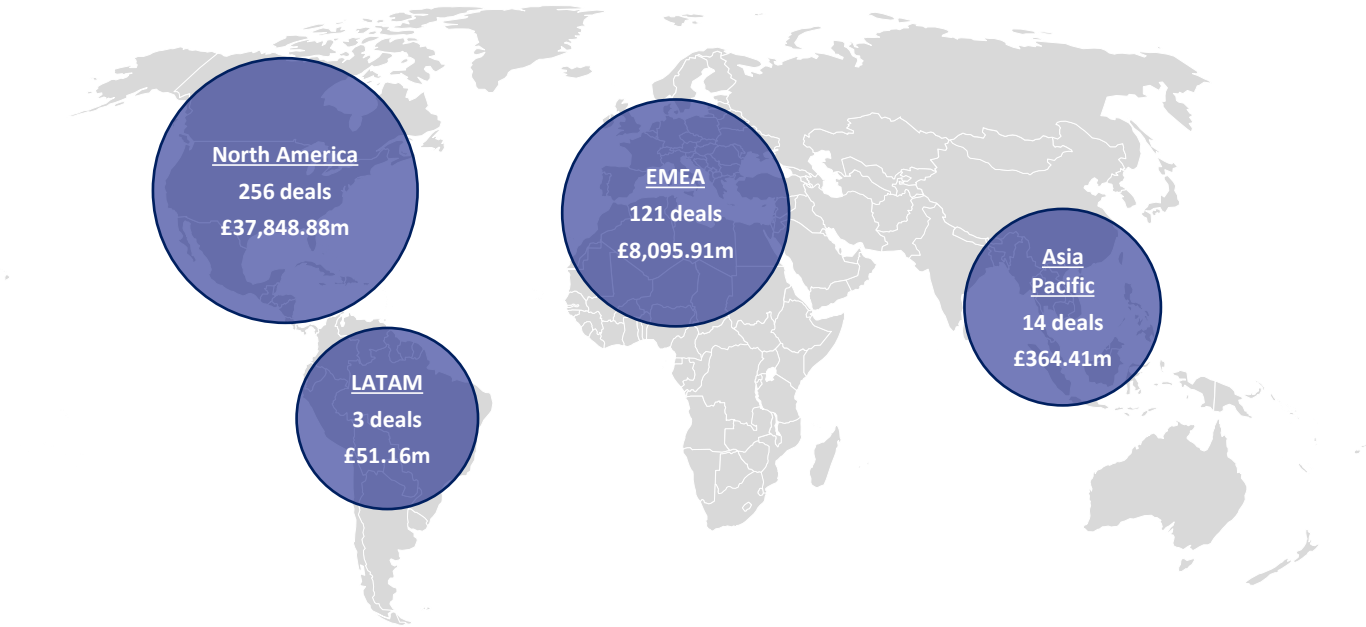
FIGURE 4: Cyber Security M&A Deals (Worldwide; 2016 - H12020)



Having established a strong presence within the TMT sector, Luminii Consulting has experienced a marked interest in UK and European-based cyber security assets in H1 2020. In an increasingly attractive market, the volume of deals within cyber security has grown by a CAGR of 20% over the last four years, resulting in over 100 deals completed within the space in 2019 and 63 deals already announced so far this year.

With 256 deals completed with an aggregate deal value of £37.8bn since the beginning of 2016, North America represents the largest M&A market for cyber security. With 24 deals completed with an aggregate deal value of £3.5bn since 2016, the UK is the second highest country, following the USA.

FIGURE 5: Cyber Security M&A Deals by Region (Worldwide; 2016 - H12020)



Moreover, at present cyber security assets appear to offer great value for investors compared to other fast-growing and resilient sectors. The average deal multiple within cyber security currently stands at 3.2x revenue (based on 173 deals worldwide with disclosed deal values between 2015 and H1 2020). In comparison, the average revenue multiple for SaaS businesses currently stands at 4.9x [Source]. Therefore, Luminii expect deal valuations for cyber security assets to rise in the next 12-24 months as cyber security players continue to demonstrate their scalability and validate their products and business models.

With mounting cyber pressures, fuelled by geopolitical conflicts and the current global pandemic, this year is likely to present a turning point in organisations' digital strategies and offers a significant opportunity to develop a more secure, robust and trusted digital world coupled with more resilient businesses. Although faced with turbulent times, Luminii believe these market tailwinds, coupled by the relatively attractive sector valuations, should result in cyber security assets continuing to represent a strong potential for investors.

About Luminii Consulting

Luminii Consulting is a consulting firm specialising in Commercial Due Diligence and Growth Strategy. It provides corporates, private equity and their portfolio companies with strategic advice and pragmatic solutions to grow their business, make well-informed investment decisions and manage risk. Luminii has extensive experience within the technology, media, telecoms, retail/e-commerce, B2B products & services and healthcare sectors.

To find out more about Luminii Consulting, please visit https://www.luminiiconsulting.com/

LUMINII CONSULTING

Specialists in Commercial Due Diligence, Strategy & Value Creation

Lushani Kodituwakku
Managing Director

Ioana Nobel
Associate Director

Sam Thompson
Senior Consultant

1 Paris Garden, London, SE1 8ND

+ 44 (0) 203 105 0569

www.luminiiconsulting.com