CYBER SECURITY

THE DIGITAL TRANSFORMATION IN A FAST-MOVING SECTOR

The global pandemic has changed the way we work, forever.

Our increased dependency on technology is driving the cyber security market, as investors seek high-growth assets in this red-hot space.

COOPER PARRY CORPORATE FINANCE

GLOBAL M&A PARTNERS

THE ESSENTIALS OF CYBER SECURITY

REPORT

Protection should be easy to report on. Cloud technologies offer many portals and dashboards around this.

Many offer a secure score that will give you a clear indication of security to your organisation as well as comparing it against organisations of similar size and business type.

IDENTITY

MFA (Multi Factor authentication) and the latest way of deploying this technology, conditional access, are the base line that any organisation should have.

By far the easiest system to implement, it offers the best value for money in the fight against cybercrime.

ENCRYPT

The modern approach with regards to protecting data is to have it encrypted at rest as well as in transit.

Data should be labelled with a set of rules around that data as to what encryption and permissions there should be.

PROJECT

Anti-phishing and next generation anti-virus are essential.

Newer generation of antivirus run on the file protection levels and work by looking at activity on the files, making them more intelligent and adaptive to threats.

THE IMPACT OF COVID-19

SHIFT IN WORKING PATTERNS

The COVID-19 pandemic has completely altered the landscape of cyber security. With remote-working now the new normal, businesses all over the world are adjusting to the challenge. Businesses know they must rapidly innovate, take advantage of new digital tools and leverage cloud services to emerge from the crisis.

AWARENESS OF THE CYBER SECURITY SECTOR

A now digitalised work force has created an overnight increase in exposure to data fraud and cyber attacks.

In the unprecedented world we now live in, a cyber attack that deprives organizations of access to their data or the internet could be devastating, potentially causing widespread infrastructure failures that take entire data centres offline, obstructing healthcare providers, public systems and networks.

Great importance is now being put onto cyber security in our current climate, fuelling investment in a hot tech sector.

DIGITAL TRANSFORMATION OF BUSINESSES

Digital transformation will continue at an alarming rate well beyond the pandemic. The challenge for industries is creating business models that are agile and adaptive to the threats. For example, this is evident in two sectors heavily reliant on security:

VIRTUAL RETAIL – Retailers are looking to invest in advanced tech like augmented reality to create a 'no contact' experience for customers, further fuelling the need for increased cyber security.

ROBOTICS & HEALTHCARE – Robotics in healthcare are disinfecting hospitals, handling lab samples and removing biological waste autonomously, however cyber vulnerabilities are creating uncertainty about the reliability of these ground-breaking technologies at such a critical time in global health.

MAJOR DRIVER OF M&A DEALS

With swathes of firms in a variety of sectors forced to digitally transform their operations in the context of cyber security, some of the most active M&A buyers in the UK have seen the opportunity to invest in innovative, high-growth companies.
Cyber security transaction volume rose by 15% in the second-half of 2019 pre-Covid, compared to the second half of 2017 (source: info-security magazine). Valuations have also remained healthy, with revenue multiples consistently trading around 5x for the past four years – significantly above the 3x valuations seen in the wider enterprise software space.

MARKET DRIVERS

UK COMPLACENCY

Security complacency amongst UK firms pre-Covid being replaced with an urge to act now.

RISE IN MALWARE AND PHISHING

There were a total of 875 major cyber security incidents related to Phishing in the first three quarters of 2019/20.

GROWING DEMAND FOR CLOUD-BASED SOLUTIONS

Innovative cloud-based networks are a growing trend which is creating a need for increased cyber security.

NETWORK AND INFORMATION SECURITY (NIS) REQUIREMENTS IN UK LAW

UK law prompted cyber security improvements in many organisations, but more guidance would help organisations further address the cyber risks they face.

EXPECTED SPENDING CHANGE IN THE NEXT 12 MONTHS BY INDUSTRY

As a result of both the impact of Covid-19 and a demand-driven market, the expected spending on cyber security in the next 12 months varies by industry. Industries hardest hit by the pandemic such as travel and retail are expected to slash budgets. However, healthcare and tech should see increased investment in cyber security across the sector; demonstration of the adaptiveness of the sectors and the opportunities available from an M&A perspective within the mid-market cap.

	LARGE ENTERPRISES[1]	SMALL AND MEDIUM-SIZE BUSINESSES[2]	OVERALL
Healthcare systems and services	Increase	Small Increase	Increase
Banking and financial services	Increase	Small Increase	Small Increase
Technology, media and telecommunications	Increase	Small Increase	Small Increase
Public and social sectors	Increase	No Change	Small Increase
Insurance	Small Increase	No Change	Small Increase
Professional services	No Change	No Change	No Change
Consumer and retail	Small Increase	Decrease	Decrease
Advanced industries	No Change	Decrease	Decrease
Global energy and materials	Decrease	Decrease	Decrease
Travel, transport and leisure	Decrease	Decrease	Decrease

SOURCE, McKinsey & Company

CYBER RESILIENCE

CURRENT CHALLENGES

ARTIFICIAL INTELLIGENCE IN CYBER ATTACK	AI provides multiple opportunities for cyber attacks – such as increasing the speed and volume of attacks, to the sophisticated, such as making attribution and detection harder, impersonating trusted users and deep fakes.
TECHNICAL SKILLS GAP	A recent report found that around 48% of organisations in the UK are unable to carry out basic security functions such as setting up a firewall, storing data etc (DCMS). Furthermore, the labour market is not providing cyber security professionals at the same speed at which the vulnerabilities are arising, with a predicted 3.5 million unfilled cybers security jobs by 2021.
THE INTERNET OF THINGS ATTACKS	With the number of devices connected to the IoT expected to reach 75 billion by 2025, IoT networks are now more vulnerable to cyber attack – often overloading networks or locking down equipment for financial gain.
RANSOMWARE THREATS	Ransomware encrypts files and blocks access to systems, with cyber criminals demanding money on the criticality of the data – by far the biggest threat in terms of potential financial losses.
CLOUD RISKS	With a significant number of companies moving sensitive data into the cloud, the technology and procedures needed to quell external threats changes.

SOURCES, New York Times, Department for Digital Culture, Media & Sport (DCMS)

Investing in and putting emphasis on the speed of detecting a cyber breach, quickly mobilising responses and returning to operational normality as quickly as possible.

Leaders scale more, train more and collaborate with the best firms to increase the value from innovative technology.

While firms feel there is low risk of cyber attack, budgets on security and infrastructure may be reduced – industry leaders sustain investments, get the basics right and de-risk.

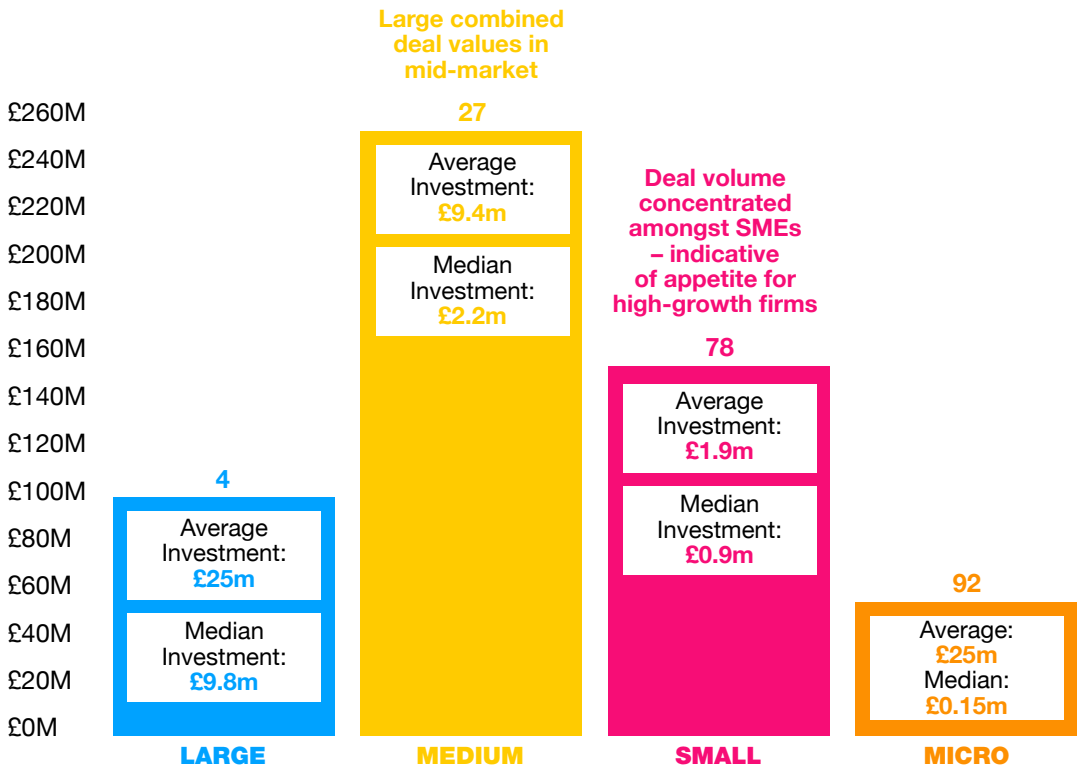
M&A IN THE CYBER SECURITY SPACE

An increasing appetite for UK-based assets is fuelling M&A activity. Security consulting, network and infrastructure providers as well as managed service providers are attracting the most interest.

'Highly scalable with a higher growth margin' type business models in the space are pushing multiples up. Many tech-enabled businesses are valued on revenue multiples instead of EBITDA due to rapid growth and sticky, predictable revenue streams.

Strategic buyers and vendors make up c.80% of deal activity by value globally, many targeting software providers and newly developed tech that presents potential competition. PE appetite is focussed on services due to recurring revenues, however many are seeing a shortage of good-quality mid-market assets.

SOURCE, Department for Digital Culture, Media & Sport(DCMS)



UK Deal value and volume 2007-2017 Source: DCMS, 2017

CONTACT US

BEN ROOKES

Ben joined Cooper Parry in 2002 and has over 14 years Corporate Finance experience. He has vast experience of advising business owners and management teams across a variety of sectors including both cross-border and domestic company disposals and private equity transactions

Ben is a member of the Global M&A Board.

benr@cooperparry.com

LAURA CLARKE

Laura joined Cooper Parry in 2005 and has a wealth of experience in both advising business owners and deal origination.

Laura organises networking events for Healthcare Leaders and provides regular sector commentary and market news for our entrepreneurial contacts.

Laura is a Chartered Accountant, having trained at Deloitte.

laurac@cooperparry.com

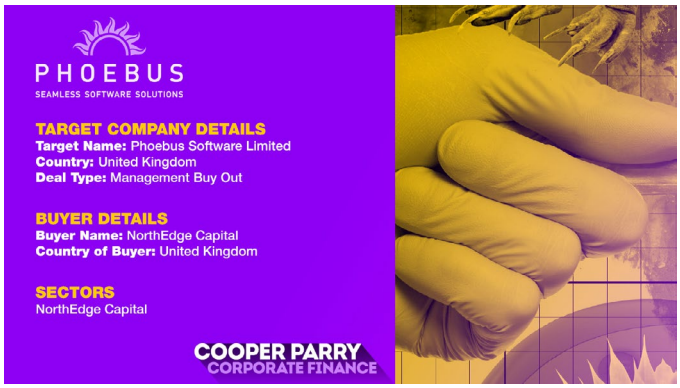
LOREN DOCKSEY

Loren joined Cooper Parry Corporate Finance in 2020 as an analyst, assisting the team with deal origination and market research.

He holds a BA (Hons) in Economics from The University of Derby.

lorend@cooperparry.com

OUR RECENT COMPLETED DEALS IN THE TECHNOLOGY SPACE



To read more about our recent deals, **CLICK HERE**.