TECHNOLOGY M&A INSIGHTS PAPER: A SPOTLIGHT ON CYBERSECURITY AND CYBER SERVICES

Introduction

The explosive growth in cyberattacks and major technical shifts introduced by AI and cloud technologies are just a few of the drivers fueling sustained demand for cybersecurity services in recent years.

These disruptive forces have made assets in the space highly attractive to financial and corporate buyers, who are drawn by the strong long-term growth prospects and clear opportunities for value realisation these businesses provide. M&A activity in the UK involving cybersecurity businesses has reflected this interest, showing resilience in 2024 even if overall dealmaking has seen a slowdown.

In this article, we consider the key themes shaping the cybersecurity landscape and discuss the major drivers behind dealmaking, with a focused lens on cyber services companies.

Cybersecurity market overview: key themes

- Rising, persistent and more sophisticated threats
- Pressure on cyber governance is increasing
- Cyber warfare and infra-focused attacks on the rise
- Shift to zero-trust security models
- AI, ML and automation emerging as powerful tools
- Skills gaps are one of the biggest risks in building cybersecurity resilience

Cybersecurity market overview: key themes

The cybersecurity landscape has grown increasingly complex, with several mega-trends driving transformation in the industry as organisations seek more robust, adaptive and integrated cybersecurity strategies.

1. Rising, persistent and more sophisticated threats

- Global cyberattacks climbed by almost a third year-on-year in Q2 2024, reaching an average of 1,636 attacks per organisation each week[1].
- In the UK, the number of severe attacks has tripled in the past 12 months[2], with several high-profile incidents affecting institutions such the British Library and London hospitals.
- Ransomware, especially those aimed at data recovery systems, and phishing are the most prominent threats.

2. Cyber warfare and infra-focused attacks on the rise

- Nation-state activities have increasingly targeted critical infrastructure, leveraging sophisticated cyber tactics to disrupt essential services.
- Rising geopolitical tensions and conflicts like the Russia-Ukraine war have intensified this trend, with significant growth in the frequency and scale of infrastructure-focused attacks.

3. Cloud and hybrid work heightening risks

- The shift to cloud-based infrastructure has significantly expanded attack surfaces, introducing security vulnerabilities and risks.
- Similarly, the rise of remote working has increased reliance on cloud services and underscored the urgency of protecting hybrid IT environments and critical systems.
- New vendors have emerged to address these fresh demands, while incumbents have had to adapt their offerings, driving disruption and consolidation in the industry.

4. AI, ML and automation emerge as powerful tool

- Artificial intelligence, machine learning and automation are revolutionising threat detection and response. For example, AI tools can enable real-time anomaly detection and automate incident management, making defences more adaptive.
- The global market for AI-based cybersecurity products is expected to surge to $135 billion by 2030, from $15 billion in 2021[3].

5. Pressure on cyber governance is increasing

- Regulatory compliance requirements are becoming increasingly stringent, as governments and regulators recognize the complexity of the cybersecurity landscape and demand more comprehensive protection measures.
- As a result, companies must ramp up efforts to meet compliance mandates in areas such as data protection, cross-border data transfer and supply chain security, among others.

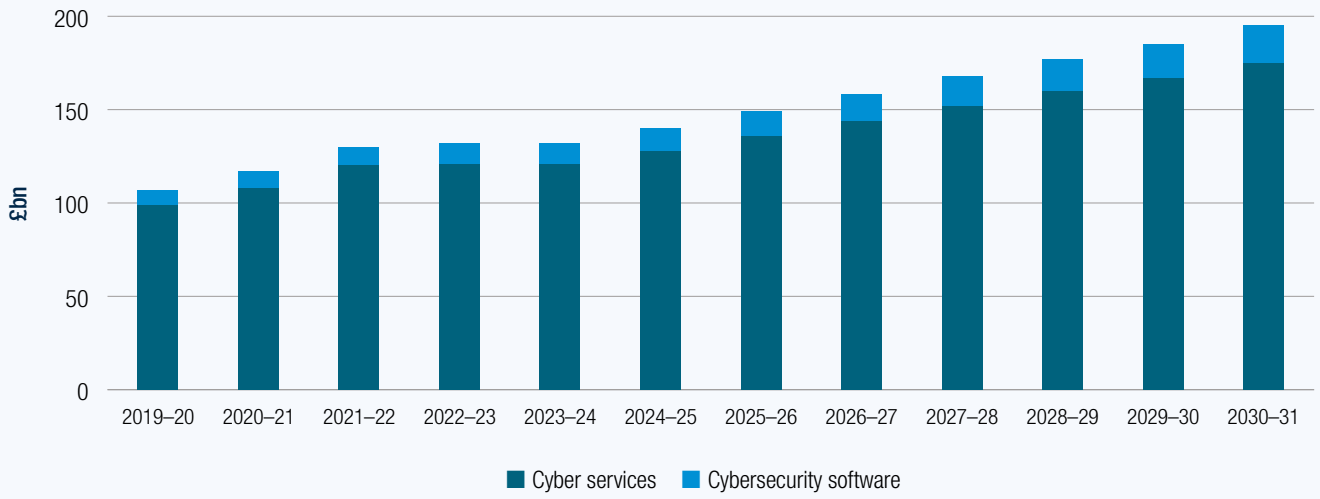
6. Shift to zero-trust security models

- Organisations are shifting from a traditional perimeter-based security paradigm to a model of continuous verification of users and devices, irrespective of location, also known as the zero trust model.
- This approach is supported by new technologies such as multi-factor authentication (MFA), micro-segmentation and real-time monitoring.

7. Talent shortages

- At a time when attacks grow increasingly sophisticated and defence strategies become more intricate, the industry faces a tremendous skills gap, with 95% of organisations reporting difficulty finding qualified professionals.
- The deficit of experts is a major factor driving investment in the cyber services market, which is expected to grow faster than the other security segments.

Fig. 1 – Cybersecurity market – UK (£bn) 2020 to 2031)



Sources: A&M insights, Megabuyte, CapIQ

1 https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

2 https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024

3 https://www.acumenresearchandconsulting.com/artificial-intelligence-in-cybersecurity-market

Cybersecurity M&A: Transaction catalysts and investors

With revenues of nearly £12 billion[1] in the 2023-2024 financial year period and growing at a healthy CAGR rates of near 10% in the past four years, the UK cybersecurity market is large and growing, providing an attractive investment opportunity for trade and financial buyers alike. Common features of M&A activity in the space include:

1. Increasing scale and capability

2. Value realisation

3. Access to funding for future growth

4. Expansion into new, resilient end-markets

5. Attract or incentivise talent

6. Higher valuations for unique IP

More than 2,000 firms are currently active within the UK providing cybersecurity products and services. Cyber services companies dominate the market. These businesses are projected to growth at accelerated rates, spurred by the demand for security consulting and professional services to address the skills gap in the industry.

Many financial buyers have increased their focus on cybersecurity services opportunities rather than software in recent years, taking a step back from frontline technology development that can carry more binary risks of obsolescence.

Meanwhile strategic acquirers have sought smaller firms to scale, secure talent in key technologies, diversify services or expand geographically.

Some of the areas being most targeted within cyber services include:

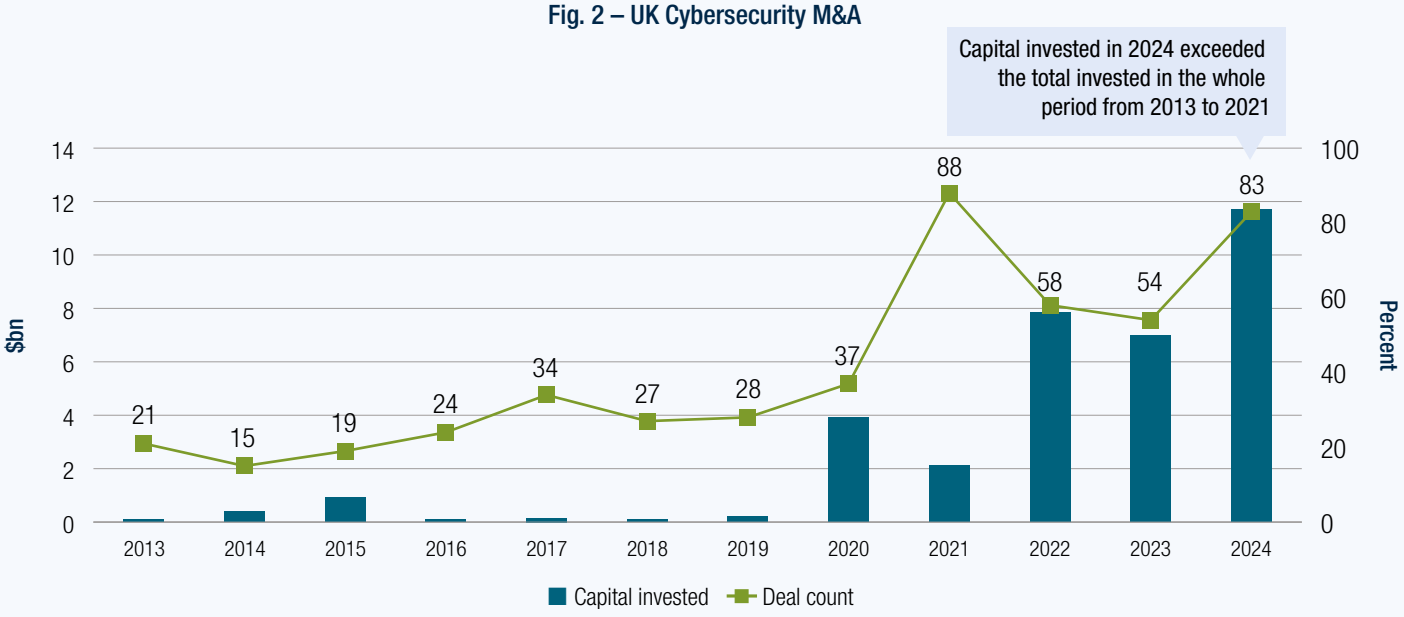
Managed security service providers (MSSPs): third-party providers offering a variety of security services to an organisation, such as monitoring, detection and response to incidents, alongside tools such as security information and event management (SIEM), endpoint detection and response (EDR), and vulnerability management platforms.

Security consultancies: providers of advisory services on risk assessments, compliance frameworks, and defence strategies, often through tools like penetration testing suites, risk platforms, and security awareness training programmes.

Value-added resellers: third-parties which enhance cybersecurity products by integrating them with additional features or services before reselling them to end-users. These enhancements can include customised security solutions, implementation services, and ongoing support tailored to the specific cybersecurity needs of their clients.

In the UK, capital invested and deal count both show a pronounced upward trajectory over the years, reaching a peak in 2024.

Fig. 2 – UK Cybersecurity M&A



Sources: A&M insights, Megabuyte, CapIQ, PitchBook Data, Inc.

1 https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2024/cyber-security-sectoral-analysis-2024

Sector Outlook

Government investment and regulatory frameworks will drive market growth

The UK government, through initiatives such as the National Cyber Strategy and the work of the National Cyber Security Centre (NCSC), is steadily increasing funding and introducing more stringent standards to protect critical infrastructure. This creates a significant opportunity for cybersecurity vendors capable of offering both technical solutions and compliance expertise, as new regulations (e.g., expanded requirements under the Network and Information Systems (NIS) Directive) generate consistent demand for advisory services.

Continued consolidation across European markets and among UK-based providers

The drive for scale and wider geographical reach will likely spur further M&A activity, mirroring trends seen in other tech-driven segments. Larger players, such as global Managed Security Service Providers (MSSPs) and established UK firms, may look to acquire smaller niche specialists in AI-driven threat detection or IoT security. Cross-border mergers are also on the rise, reflecting a broader European push for platform-building to capture synergies in R&D and customer reach.

Emerging technologies will help close the security gap—albeit gradually

Innovations in AI, Zero Trust architecture, and quantum-resistant cryptography promise to elevate detection and prevention capabilities. However, as with many rapidly evolving fields, widespread deployment faces obstacles: lengthy certification processes, limited real-world validation of new tools, and complex integration with legacy systems.

Despite these near and mid-term challenges, analysts agree the UK market's long-term potential remains robust, underpinned by both public and private investment in next-generation cybersecurity solutions.

Technology and Cyber M&A

Sell-side Advisory

Exit strategy

Identify the optimal exit option for shareholders

Prepare for exit

Ready the business for exit, preparing marketing documents

Engage buyers

Organise approach through our global technology network

Execution

End-to-end support throughout the transaction

Buy-side Advisory

Unlock the targets

Engage with global network and relationships to start the dialogue with targets

Evaluation

Financial and opportunity-assessment – transact at the right valuation

Execution

End-to-end support throughout the transaction

Deal strategy

Maximise long-term shareholder returns

Cyber Due Diligences and Maturity Assessments

Due Diligences and Maturity Assessments are conducted for a wide range of Global Private Equity funds. The team frequently conducts NIST Cybersecurity Framework based assessments, to identify the cyber risks which placed the company below sector benchmark

Cyber SOC Design and Implementation

A global Private Equity backed company, faced significant operational disruption and delivery delays due to a cyber attack, resulting in estimated financial losses in the millions.

In response, A&M Cyber conducted a thorough cyber risk evaluation, highlighting critical security gaps in relation to business risks. This assessment justified a €3 million investment in cyber technology, personnel, and processes. Additionally, a 16-month, 2-phase Security Program was developed and implemented groupwide.

About A&M

Alvarez & Marsal is a global consultancy that, for more than four decades, has set the standard for helping organisations tackle complex business issues, boost operating performance, and maximise stakeholder value.

We bring operating and management expertise combined with top-tier consulting and specialised industry experience to meet the changing needs of companies and investors.

KEY CONTACTS – CORPORATE FINANCE M&A

Ian Birch
Managing Director,
Head of Technology M&A
ibirch@alvarezandmarsal.com

Richard Day
Director, Cyber M&A
rday@alvarezandmarsal.com

Afsor Miah
Director, Technology M&A
amiah@alvarezandmarsal.com

KEY CONTACTS – GLOBAL CYBER RISK SERVICES

Lorenzo Grillo
Managing Director
Head of Cyber Risk Services EMEA
lgrillo@alvarezandmarsal.com

Libero Marconi
Senior Director
lmarconi@alvarezandmarsal.com

Bogdan Chirila
Senior Manager
bchirila@alvarezandmarsal.com

Disclaimer

Follow A&M on:

ABOUT ALVAREZ & MARSAL

Founded in 1983, Alvarez & Marsal is a leading global professional services firm. Renowned for its leadership, action and results, Alvarez & Marsal provides advisory, business performance improvement and turnaround management services, delivering practical solutions to address clients' unique challenges. With a world-wide network of experienced operators, world-class consultants, former regulators and industry authorities, Alvarez & Marsal helps corporates, boards, private equity firms, law firms and government agencies drive transformation, mitigate risk and unlock value at every stage of growth.

To learn more, visit: AlvarezandMarsal.com

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.℠