



Cybersecurity:

A fast-growing market
that's tackling evolving
threats

September 2026

+44 2031 264907

info@princelet.com

www.princelet.com



Overview

\$353bn

Projected size of the global cybersecurity market by 2030, growing at roughly 10% a year¹

153

M&A transactions tracked in H1 2026 alone - the highest pace on record¹

The cybersecurity market has evolved into a fragmented ecosystem of businesses tackling **increasingly complex threats**. Attacks haven't necessarily become more frequent - surveyed breach rates among UK businesses have eased slightly since 2023/24 - but they have become more severe. The National Cyber Security Centre now manages over 200 nationally significant incidents a year, more than triple the figure from two years earlier, and recent attacks on M&S, Co-op and Jaguar Land Rover are a reminder of the scale of disruption a single breach can cause.

It is therefore unsurprising that the market is growing quickly with Kroll estimating it to be over \$200bn today, expanding at roughly 10% a year to reach \$353bn by 2030. Global deal activity is running at its highest pace recorded as Kroll tracked 153 M&A transactions in H1 2026 alone. Regulation is also trying to keep pace: the UK's Cyber Security and Resilience (CSR) 2026 Bill will be the most significant UK regulatory update since the Network and Information Systems (NIS) Regulations in 2018.

Even for a market accustomed to fast-paced change, today feels like an **unusually challenging yet exciting moment**. Join us as we explore the cyber ecosystem, the areas with heightened M&A activity, a deep dive into one particularly promising part of the market, and much more.



¹Kroll, 2026. Cybersecurity M&A Industry Insights – Summer 2026.



How to segment the market

The cybersecurity industry is highly fragmented and dense with acronyms and technical vocabulary, making it difficult to navigate.

The former UK Department for Science, Innovation and Technology's (DSIT) Cyber Security Sectoral Analysis segments the market three ways²:



By delivery model – 72% of firms are service-led generating £8.4bn in revenue, versus £6.4bn from the 28% that are product-led



By specialism – 69% are dedicated cyber security providers, rather than offering a service alongside other lines



By solution category – "Information Risk Assessment & Management" and "Cyber Professional Services" are the most common, each offered by around 80% of firms

This is useful for market sizing and describing what a business does, but it doesn't explain where a business sits in the ecosystem or why its proposition is valuable. Here, many in the industry refer to the Cyber Defence Matrix, a 5x5 strategic framework that plots the five NIST functions³ against the five assets a business needs to defend.

The matrix shows how different cyber businesses can be positioned across functions and what they protect against. Beneath, outlines the degree of dependency on technology, people and process based on where a business is in the matrix. This shows how technology plays a greater role in **IDENTIFY** and **PROTECT**, and how the dependency on **PEOPLE** grows moving towards **DETECT**, **RESPOND**, and **RECOVER**. Throughout all five functions, there's a consistent level of dependency on **PROCESS**.

²Department for Science, Innovation & Technology (DSIT), 2026. Cyber security sectoral analysis 2026.

³The NIST functions (from the NIST Cybersecurity Framework) describe how an organisation manages cyber risk - covering the full lifecycle from preparation through to recovery.

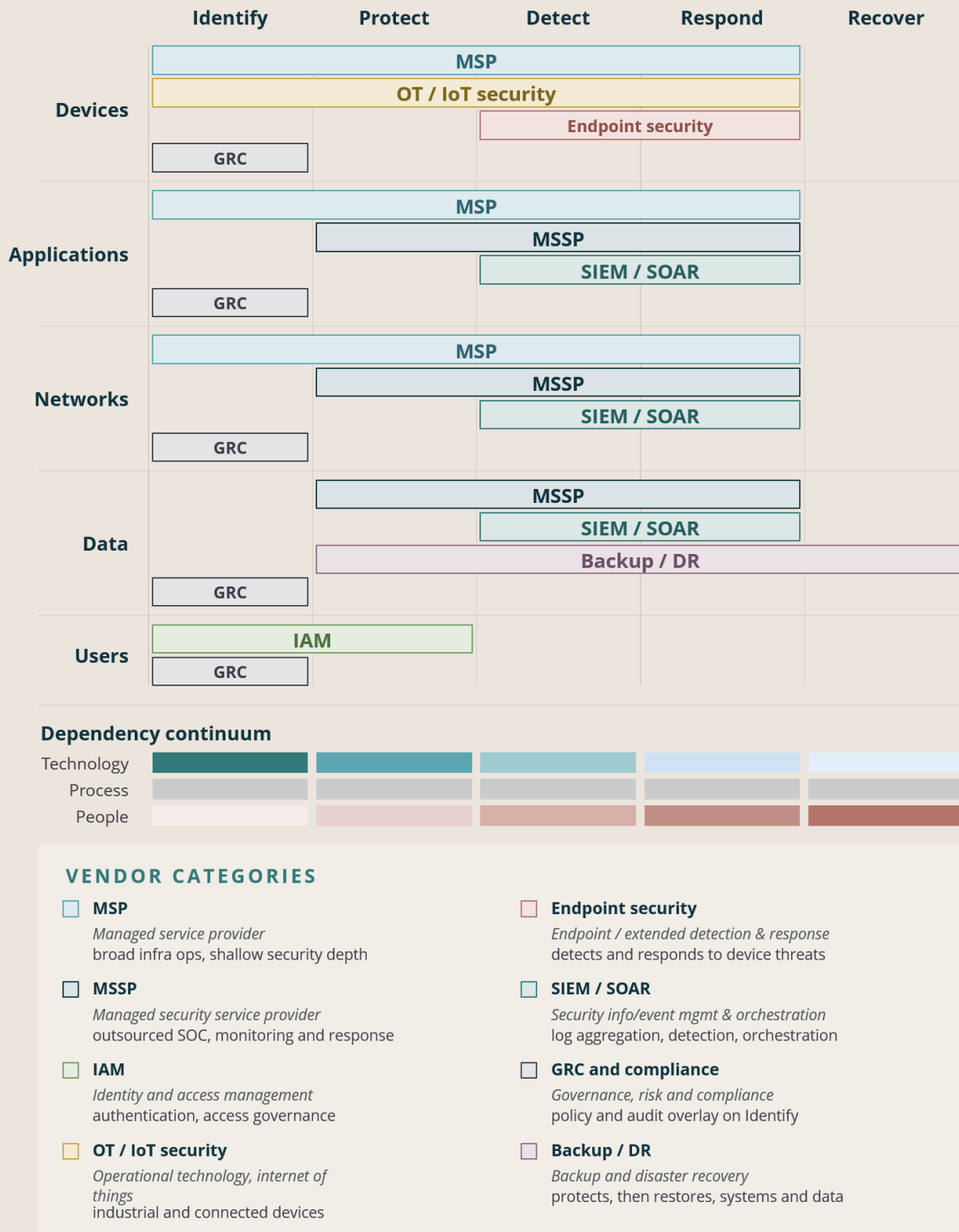


Figure 1. The Cyber Defence Matrix⁴

A fully comprehensive segmentation of the market is tricky, but together, these give a workable starting point for understanding what a business does and its value proposition.

⁴The Cyber Defense Matrix, a framework created by Sounil Yu. Available at: <https://cyberdefensematrix.com/>

Where is M&A activity taking place?

In terms of deal count, cybersecurity M&A activity is trending upwards in recent years with high deal count reported in H1 2026, suggesting that 2026 could be a record-breaking year for deal activity (deal value each year is more irregular).

Global Cybersecurity M&A Activity:

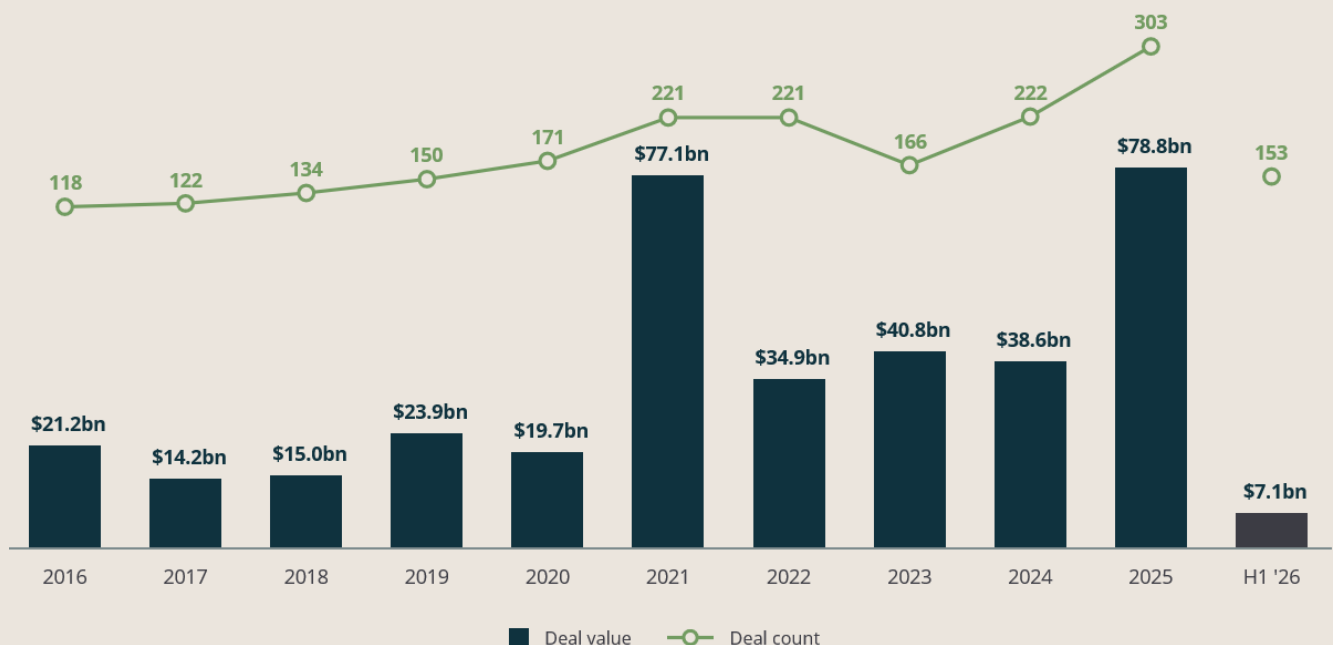


Figure 2. Kroll shows the trend of Global Cybersecurity M&A Activity by deal value and deal count¹

The rationale behind many deals can perhaps be explained by acquirers buying capabilities they cannot quickly build themselves.



Check Point reportedly paid \$300m for **Lakera**, a 70-person Swiss firm⁵, that builds runtime guardrails for AI apps, for its rare security expertise and real-world tuning data.

LAKERA

SOPHOS

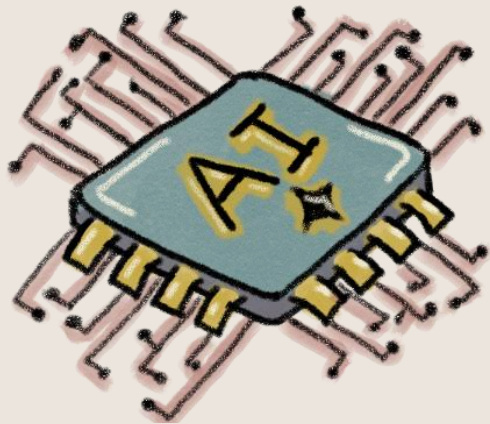
On the established technology end of the market, **Sophos** acquired **Secureworks** for \$859m⁶, buying Secureworks' MDR delivery scale and market leadership.

Secureworks®

¹Kroll, 2026. Cybersecurity M&A Industry Insights – Summer 2026.

⁵Globes, 2025. Check Point buys Swiss AI security co Lakera.

⁶Sophos, 2025. Sophos Completes Secureworks Acquisition.



Artificial intelligence is also steering M&A activity. AI is being used by cyber businesses to identify threats with greater accuracy, as organisations running AI-driven security tools achieve 95% detection accuracy versus 85% with traditional tools⁷. This may provide operational leverage that is feeding through into valuation, with AI-native security platforms sometimes commanding 20x to 30x revenue multiples, far above the broader sector's median⁸.

In addition, funding is flowing to businesses that protect against emerging AI risks like agentic AI. Agentic processes, whereby employees can query data from several locations and perform actions like writing to a database, need governance to ensure these tools have the appropriate level of access and permissions and can't be maliciously exploited.

⁷AllAboutAI, 2025. AI Cyberattack Statistics 2026: What the Data Warns Us About.

⁸Windsor Drake, 2026. AI in Cybersecurity Valuations: Q2 2026.



Deep dive: OT/IoT Security

A particularly interesting cybersecurity area is OT/IoT Security.

Operational Technology (OT) security protects the industrial systems controlling physical processes (Industrial Control Systems (ICS), SCADA systems, controllers running factories amongst other things), distinct from the IT systems that handle data and communications. Internet of Things (IoT) security then covers the connected physical devices, from smart meters to industrial sensors, increasingly linking these operational environments to the internet.

WHY NOW?

Factory owners are turning to tools like predictive maintenance that use sensor data to flag potential asset failures before they happen, cutting downtime and repair costs while extending equipment life. This level of connectivity is what exposes previously isolated OT environments to attack, and OT/IoT Security has emerged as a vertical because these industrial systems were built for reliability and safety first, not cyber resilience - IT/OT convergence and rising industrial IoT adoption have widened the surface available to attack.

The threat landscape has grown in tandem. Nation-state actors are now positioning themselves inside critical national infrastructure (CNI) alongside rising ransomware, industrial espionage, and cyber-physical threats to ICS and SCADA systems.

\$27.4bn → \$58.9bn

OT Security market, 2026 to 2031 - a 16.6% CAGR, ahead of the c.10% growth rate of cybersecurity broadly⁹



This has led to a fast-growing yet fragmented OT/IoT market. OT Security is estimated at c.\$27.4bn in 2026, growing to \$58.9bn by 2031 (16.6% CAGR), ahead of the ~10% growth rate of cybersecurity broadly. Buyers are responding by building full "xOT" platforms spanning asset visibility, threat detection, vulnerability management and secure remote access.

⁹MarketsandMarkets, 2026. OT Security Market worth \$58.94 billion by 2031.

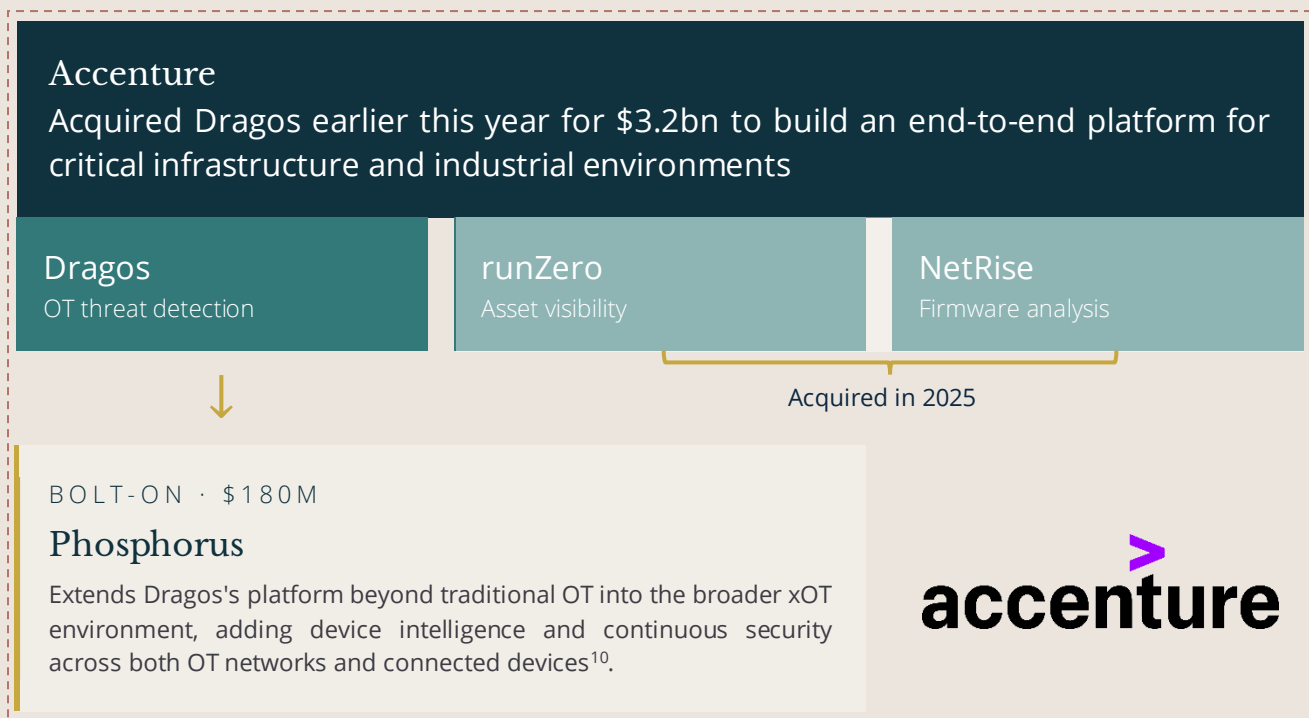


Figure 3. Accenture is an example of a platform build in OT/IoT security

At the lower mid-market end, there are:

- **OT consultancies** specialising in Cyber Assessment Framework advice, where compliance work generates sticky, recurring revenue
- **Regional MSSPs** with a genuine industrial practice
- **Vertical specialists in water, rail and maritime**, whose products are woven into how clients meet sector-specific regulation
- **Businesses ensuring secure remote access for OT**, letting engineers and contractors connect safely into ICS environments

MID-MARKET M&A

Ekco, a Dublin-based MSSP acquired OT security firm Datalogix earlier this year, following a busy 2025 in which it also acquired Predatch, Adapt IT and Solsoft.



The OT/IoT market is still working out how to respond to a rapidly evolving threat and regulatory landscape. Businesses that build ahead of that curve are best placed to become tomorrow's market leaders.

¹⁰Dragos, 2026. Dragos Acquires Phosphorus to Bring OT-Native Cybersecurity to the Full xOT Environment.



The UK cybersecurity landscape

The UK cybersecurity market generated £14.7bn of revenue in 2025 across 2,603 firms, which is 20% higher in company count than the year before. **The emerging trend of AI security can also be seen in DSIT's data:** the number of UK firms offering AI-specific cyber security products or services grew 68% year-on-year to 111 in 2026².

£14.7bn

UK cybersecurity revenue in 2025

2,603

UK cyber firms, 20% more than the year before

111

UK firms offering AI-specific cyber products, up 68% year-on-year

Regulation

On the regulation front, the Cyber Security and Resilience Bill 2026 aims to protect businesses in a threat landscape far different from the last major regulatory overhaul in 2018. Data centres come into scope for the first time, as do an estimated 900-1,100 managed service providers, and regulators gain new powers to scrutinise individual suppliers they deem critical, meaning even SMEs can face stringent protocols¹¹. Notably, food, retail and manufacturing remain outside scope despite significant OT/ICS risk, in contrast to the EU's NIS2 cybersecurity directive, which does cover manufacturing. The minister's defence was that manufacturing supply chains are too fragmented to regulate the same way as energy or water¹². **Overall, the remit of regulated cybersecurity is expanding.**

Demand-side

On the demand-side, **cybersecurity has become the main brake on SME digitisation**, as research by Be Certified found 42% of SME owners named cyber fears as their single largest obstacle, ahead of skills shortages and budget constraints combined¹³. The UK Government has committed £90m over three years to improving SME cyber resilience, but the specialist skills gap is acute in areas SMEs need; AI security, penetration testing and advanced threat detection remain the hardest roles in the sector to fill.

42%

of SME owners name cyber fears as their single largest obstacle to digitisation, ahead of skills shortages and budget constraints combined

²Department for Science, Innovation & Technology (DSIT), 2026. Cyber security sectoral analysis 2026.

¹¹UK Parliament, 2026. Cyber Security and Resilience (Network and Information Systems) Bill.

¹²Travers Smith, 2025. The UK's new Cyber Security and Resilience Bill.

¹³Be Certified, 2026. The SME Digitalisation Report: How Small Businesses Are Approaching DT in 2026.



Supply-side

On the supply-side, investment into dedicated UK cyber firms fell from £206m across 59 deals to £184m across 47 deals in 2025. Of the £184m, 46% went to companies with 10-49 staff, up from 17%². This may point to how it has become easier to start a UK cyber business and harder to scale one.

Taken together, the UK cybersecurity market is one whose scope and complexity are expanding faster than its funding and skills base can keep pace, leaving a widening gap between what regulation and customers now demand and what early-stage capital can supply. For strategic acquirers and financial sponsors, this dynamic increasingly positions M&A as a key route to scale UK cyber businesses.





Valuation drivers

Certain factors help drive value within cyber businesses:

FACTOR	HOW IS IT DRIVING VALUE
Recurring revenue	MSSPs are trading at higher multiples than MSPs, with the former bringing in more recurring revenue as security monitoring is a continuous, always-on service.
AI-driven operating leverage	AI that lifts the volume of endpoints or alerts a single analyst can handle cuts cost-to-serve directly, improving gross margin without adding headcount.
Regulatory stickiness	Where a vendor is embedded in a customer's compliance workflow, displacement is expensive and disruptive.
Accreditation and clearance	Certifications, cleared personnel and approved-supplier status are costly and take time to earn, making accreditation a competitive moat.
Proprietary data	Threat intelligence, telemetry or behavioural data that improves a product is hard to replicate by a new entrant.
Proven vertical depth	Sanctioned deployments inside CNI, defence or industrial customers gives credibility that generalist firms cannot claim in regulated sectors.



Industry headwinds

While the case for growth is strong, the following are challenges for cyber businesses:

Multiple compression

Median EV/NTM revenue multiples across Kroll's cybersecurity index fell 26% in a single quarter in early 2026¹.

Talent scarcity, acutely in OT/IoT Security

The pool of people who understand both industrial engineering and cybersecurity is small, creating retention risk in transactions.

Vendor concentration risk

Small managed providers typically build their service on a narrow set of underlying vendor platforms, creating margin risk from vendor pricing changes, product risk if a vendor is acquired and folded into a wider suite, and channel risk if the vendor moves to sell direct.

Regulatory fragmentation

The UK's CSR Bill, the EU's NIS2 and the EU Cyber Resilience Act are moving at different speeds with different levels of scope, complicating cross-border operations.

Procurement structurally favouring incumbents

Enterprise and public-sector procurement continue to shut out small suppliers.

¹Kroll, 2026. Cybersecurity M&A Industry Insights – Summer 2026.



Princelet's view

The cybersecurity market is moving at pace, and M&A activity shows how strategic acquirers and financial sponsors are backing businesses that solve a clear, well-defined problem.

OT/IoT Security is one vertical where that pattern is playing out, but similar dynamics are visible across other parts of the market.

In the lower mid-market specifically, we meet many cybersecurity businesses, which has previously led us to work with the likes of Creativity Software and iStorage. If you're a founder of a cybersecurity business, we'd be happy to talk through how you might start thinking about an exit, and how a potential investor may currently view your business. And if you're simply wondering how cyber risk might affect your business more broadly, we've developed a checklist Princelet uses to probe into cyber-related diligence areas - please do get in touch and we'd be glad to share it.



2010
Founded

£10m-£50m
Deals specialists

+£3 billion
Aggregated deal value

38 deals
Completed since 2012



Our Team

We're a team of experienced advisors, former investors, and sector specialists.

Each of us brings a different perspective, but we're united by a shared belief in hard work, thoughtful approach, and seeing the deal through.



Stephen Moore

Managing Director



Mitchell Upama

Vice President



Megan Hall

Vice President



Alex Ioannou

Associate, M&A



Harry Brown

Analyst, M&A



Chirag Guha

Origination Manager



+44 2031 264907



info@princelet.com



www.princelet.com