Who controls your technology vendors?

Record M&A is changing who owns the systems you run on. Most firms find out too late.

THE PROBLEM

You signed with one company. Today it may belong to someone else.

Vendors get bought, taken private or folded into foreign groups. Your contract stays the same. Your risk does not. Most firms find out at renewal, after an incident, or when the regulator asks.

Can you answer these today?

If not, you have exposure you cannot see.

01 Who ultimately owns each of your critical vendors today?

02 Which of them has changed owner since you signed?

03 Which are owned by private equity, and when will that owner sell?

04 Which countries' laws can reach the data your vendors hold?

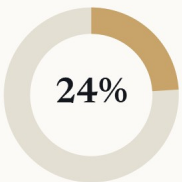
05 Who controls the vendors with privileged access to your systems?

06 Could you show your regulator the ultimate parent of every critical vendor?

WHY NOW

$2.85 trillion of deals in the first half of 2026, a record. Technology was the biggest sector. Governments are watching too: the US reviewed 347 foreign investment filings in 2025, and the UK received 1,324 national security notifications in 2025–26.

Technology's share of global M&A value, H1 2026

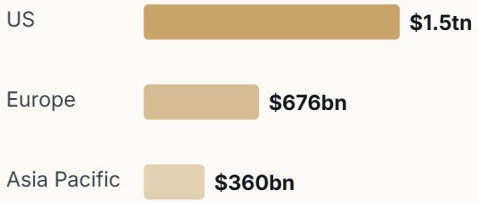


Technology, the largest sector

All other sectors

Tech deal value up 90% year on year

Deal value by target region, H1 2026



US targets: 54% of the global total. Europe more than doubled.

Sources: LSEG Data & Analytics, H1 2026; CFIUS Annual Report 2025; UK National Security and Investment Act

WHAT IS AT STAKE

A new owner inherits your contract, not your priorities. It can raise prices, retire products, move your data abroad and bring sanctions questions to your door.

15% of UK businesses review the cyber risk posed by their immediate suppliers

Attackers go through suppliers. US cybercrime losses hit $20.9 billion in 2025, up 26% (FBI). A new owner means merged systems and new hands on your access.

WHY TODAY'S APPROACH FALLS SHORT

Regulators in the US, EU, UK and Australia expect you to know who owns your vendors. Most firms check once, at onboarding, on the vendor's word. Then nobody looks again.

A BETTER WAY

Verify who really controls each vendor. Focus on the ones you cannot afford to lose. Decide in advance what a change of owner triggers.

How Vendor Exposure helps

See who really controls it
Ultimate owner, jurisdiction and data locations for every vendor, traced and sourced.

Weighted to your business
Exposure judged by how critical each vendor is to you and whether it holds your sensitive data.

Eight risk areas, one view
Sanctions, ownership, jurisdiction, resilience, cyber hygiene, supply chain, financial stability, regulatory alignment.

Evidence you can use
Dated, sourced findings for your board, auditors and regulator.

Start with the vendors you can least afford to lose.

Send your vendor list. Answer two questions per vendor. See where you are exposed.

[CONTACT EMAIL] [SAMPLE REPORT LINK]

Sources: UK Cyber Security Breaches Survey 2025/26; FBI Internet Crime Report 2025; ENISA Threat Landscape 2026; US Interagency Guidance on Third-Party Relationships (2023).