March 11, 2026

Safeguarding the Portfolio: Incident Readiness and the Cyber Landscape in 2026

Authors: Edward Machin

Last week, Ropes & Gray's Data, Privacy and Cybersecurity team partnered with FTI Consulting to host a roundtable breakfast in London for privacy, compliance and IT leads from across the private equity industry. The conversation centred on a simple question: how ready are PE firms and their portfolio companies for the cyber threats heading their way in 2026?

The short answer: it depends on who you ask. The longer answer follows below.

PE is in the Crosshairs

Threat actors like portfolio companies because private equity-backed businesses often sit at the intersection of high-value transactions, sensitive deal data and operationally critical sectors where even modest disruption carries a serious price tag. And the numbers bear it out: 54% of respondents to a recent survey of 300 risk managers and CISOs at PE firms reported that up to one quarter of their portfolio companies had suffered a cyber incident in the past year. That is because the qualities that make a business attractive to private capital — speed, complexity and growth — also increa the number of risk points that attackers can look to exploit.

What emerged from the discussion is that threat actors are watching the market with the attentiveness of a deal team. Public deal rumours and valuation chatter act as signals; fresh capital may be flowing in, management attention is divided, and documentation is moving between advisors, bidders and lenders. Ransomware gangs in particular are timing their campaigns around these moments of transition, when

everyone involved has one eye on the closing timetable and the other on any number of competing priorities.

A change of ownership can compound the risks, with access rights getting reassigned, systems becoming connected and legacy environments being integrated or — in theory — decommissioned. When that process is not handled well, the result is orphaned accounts and hastily configured links between old and new networks, among other things; the kind of gaps that attackers are trained to find. For sponsors, every transaction should be understood not just as a change in corporate ownership, but as a — potentially material — change in the company's cyber risk profile

AI is Supercharging the Adversary

Artificial intelligence cut across every part of the discussion. The UK National Cyber Security Centre and the European Union Agency for Cybersecurity have each flagged that AI is lowering the barrier to entry for threat actors, and the roundtable participants had seen those effects first-hand. Most notably, generative AI models are removing some of the traditional warning signs that users have been taught to look for: the clumsy phrasing, the inconsistent tone and the formatting that does not quite look right. Phishing emails and social engineering attempts now land with a polish and credibility that would have been difficult to achieve at scale even 18 months ago.

In the PE context, attackers can now generate highly tailored approaches using public and semi-public data about funds, portfolio companies, advisors and transaction timelines — and can do so at a volume that would previously have required significant manual effort. AI-driven tools are also accelerating vulnerability discovery, by enabling threat actors to map exposed services far more quickly than before. Once inside a network, automation can support lateral movement and privilege escalation, compressing the window in which an intrusion might be detected and contained.

The corollary is that traditional controls are under strain. Firms and their portfolios

need to invest in advanced detection capabilities, stronger identity and access management, and training programmes that reflect the quality of what AI-enabled attacks look like today, and not what phishing looked like in 2019.

Keeping Cybersecurity in the Conversation

The last part of the discussion centred on what sounds like a simple governance question that is often much more difficult in practice: where does cybersecurity sit in the conversation between incidents? The answers varied more than you might expect. Some firms have made cyber a standing board agenda item, reported on alongside financial and operational KPIs as a matter of course. Others treat it as an annual deep dive, or something that surfaces mainly in response to an external trigger, such as a headline breach, a regulatory development or a near-miss.

It was clear that there is a real challenge of integrating cyber insights into deal and portfolio company board discussions without being perceived as overstepping or slowing things down. Clarity on ownership — whether responsibility sits with the CISO, the COO, the portfolio operations team, or some combination — was seen as essential to keeping cybersecurity alive between formal milestones, rather than letting it drift to the margins until something goes wrong.

Exit scenarios drew particular attention. Handling serious vulnerabilities or breaches that come to light during a sale process remains a perennial challenge, and for good reason. There is a tension between transparency that may depress valuation in the short term and the longer-term risks of under-disclosure, particularly where a future buyer or regulator may revisit past incidents with the benefit of hindsight. But when it is done well, cyber diligence can turn a potential red flag into a documented part of the equity story, rather than a lingering risk that resurfaces later down the line.

The Bottom Line

The morning's discussion pointed to three concrete priorities: first, incident response plans should be stress-tested regularly through tabletop exercises that include deal

leads, portfolio operations, legal counsel and the security function; second, cyber diligence should carry the same weight as financial and commercial diligence at every stage of the deal lifecycle, from pre-acquisition scoping through hold-period monitoring to exit preparation; and third, sponsors need consistent, quantifiable reporting frameworks across their portfolios so that cyber risk can be measured, compared and escalated in a way that the investment committee can understand.

None of this is costless, but the expense of preparedness is predictable, whereas the cost of a serious breach is not.

Subscribe to Ropes & Gray Viewpoints by topic here.