Hilco Global
AN ORIX COMPANY

SMARTER PERSPECTIVE: CYBERSECURITY

Cyber Risk Is Deal Risk: Embedding Security Into PE Diligence an Portfolio Governance

By Jason Koehn

March 2026

For private equity, cyber risk is no longer an operational IT issue. It is a material investment consideration. As cyber incidents grow in scope and severity, firms are seeing tangible valuation adjustments and deal disruptions after cyber weaknesses are uncovered. Yet many funds, especially small and mid-sized firms, still lack consistent cyber diligence and portfolio-wide baselines, leaving them exposed to both immediate incident costs and longer-term effects that can undermine deal certainty and exit value.

Financial Impact of Cybersecurity Risk

A survey of 325 portfolio leaders found that the average cost of deal disruption linked to cyber incidents is $2.1 million, and larger losses are not uncommon. The most visible costs of a cyber incident arise immediately after an incident: incident response support, legal fees, forensics, and remediation of affected systems. But direct response costs represent only a portion of the total financial impact. The remainder tends to accumulate over time and can affect long-term valuation. These long-term financial impacts include:

- Costs associated with extended remediation and control uplift
- Higher insurance premiums or reduced coverage
- Contractual friction with customers and vendors, including audits and new security requirements as well as damaged relationships and lost trust
- Heightened regulatory scrutiny and added compliance obligations that become recurring costs
- Reputational damage resulting in loss of existing and potential new clients

Over time, the cumulative costs of weak cyber governance can ultimately reduce valuation and exit pricing. For smaller PE firms, valuation risk is even higher, as 44% of firms with under $500mn in assets under management reported valuation reductions due to cybersecurity risks. Given the material impact of cyber risk on valuation, private equity should view managing cyber risk as a lever to de-risk their portfolio and minimize unexpected impacts across the investment lifecycle.

Diligence Blind Spots

Cyber risk should be considered from the outset, as part of the diligence phase. Without sufficient pre-close cyber diligence, PE firms can inherit risk that is not priced or accounted for in deal terms. Lack of robust cyber diligence can translate into avoidable post-close outcomes, including:

- Unbudgeted control uplift to meet customer, regulator, or insurer expectations
- Delays to integration as remediation competes with business priorities
- Increased breach likelihood during the post-close period
- Reputational and commercial impact that extends to the fund

Many smaller and mid-market PE firms lack formal cyber diligence processes altogether. Given the significant short- and long-term implications of weak cyber governance, each entity involved in a transaction should be thoroughly evaluated. Cyber risk needs to be assessed in deal diligence either by pricing in the cost to remediate and improve capabilities or by adjusting terms to account for any residual or unmitigated risk.

Cyber as Portfolio Risk

In addition to rigorous diligence, effective cyber governance requires visibility into cybersecurity practices across the portfolio. Without clear benchmarks and minimum requirements across the portfolio, firms lack visibility into where cyber risk is concentrated and where it may surface as a valuation issue. For funds of all sizes, establishing a portfolio-wide approach is critical to ensure that cyber risk is benchmarked and minimum standards are enforced. A portfolio-wide baseline also helps prioritize security investments and, in some cases, enables shared security resources across portfolio companies. Such opportunities to operationalize cyber services across a portfolio via fund-level support, shared cyber services, and vendor contract bundles provide opportunities for companies to reduce aggregate costs and maximize impact.

The Road Ahead

With accelerating technology adoption and a threat landscape increasingly shaped by AI-enabled adversaries, cyber risk will increasingly threaten private equity firms. The differentiator will be whether PE firms govern cybersecurity with clear accountability and repeatable benchmarks across the portfolio. Practically, that means:

- Establish portfolio-wide minimum standards and measurable baselines
- Create visibility through reporting and risk scoring
- Prioritize controls that deliver the highest risk reduction per dollar spent
- Embed cybersecurity into diligence so risk is priced pre-close

Hilco Global Cyber Advisors (HCA) supports private equity firms with a tailored approach to portfolio cyber risk management aligned to each firm's operating model. HCA helps select the right mix of technology, processes, and policies for each operating environment, ensuring investments produce measurable risk reduction.

HCA also provides cyber due diligence for M&A transactions and PE investments, helping identify and incorporate risks into decision-making before a deal is signed. By governing cyber risk across portfolio companies and integrating it into dealmaking, PE firms can reduce costly disruptions and protect exit value. Moving forward, the strongest firms will treat cybersecurity not as a checklist item, but as a lever to create and defend value across portfolios.

JASON KOEHN
MANAGER
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Jason can be reached directly at jkoehn@hilcoglobal.com or 406.830.7750.

Hilco Global
Asset Smarter

Find Additional Smarter Perspectives at hilcoglobal.com