



Beyond Traditional Risk: Why Resilience May Become the Next Source of Investment Alpha

For generations, institutional investors have become increasingly sophisticated at measuring financial risk. We model interest rates, credit spreads, volatility, leverage, liquidity, correlations, drawdowns and default probabilities. Private-market investors supplement those tools with operational due diligence, manager selection, covenant analysis and increasingly sophisticated portfolio analytics. Those capabilities remain essential. But they are no longer sufficient.

The investment threats emerging in the second half of this decade increasingly come from outside traditional financial models: cyberattacks, artificial intelligence, geopolitical fragmentation, technology concentration, supply-chain disruption, critical infrastructure constraints, third-party dependencies and organizations' ability — or inability — to make sound decisions under pressure. The challenge is not that these risks are individually new. The challenge is that they are becoming interconnected.

At Opal Group's Alternative Investing Summit in Dana Point this December, our panel, “Beyond Traditional Risk: Identifying the Next Generation of Investment Threats,” examined this changing risk architecture and what it means for institutional investors.

We Are Moving From Individual Risks to Risk Networks

The World Economic Forum's *Global Risks Report 2026* provides an important snapshot of this transition. Geoeconomic confrontation is ranked as the leading global risk for 2026 and over the next two years. Cyber insecurity ranks sixth over the two-year horizon. And adverse outcomes of artificial intelligence rise dramatically — from 30th over two years to fifth over ten years.ⁱ The important insight is not the ranking. It is the interconnection.

A conflict can create export controls. Export controls can interrupt semiconductor supplies. Semiconductor shortages can delay data-center construction. Data-center delays can constrain an AI company's growth. That can reduce portfolio-company revenues, weaken debt-service coverage and ultimately affect private-equity and private-credit valuations. A cyberattack can shut down a supplier. The supplier disruption can halt production. Production problems can breach customer contracts, impair liquidity and trigger covenant pressure. A risk that begins as geopolitical can end as credit risk. A risk that begins as technology can become valuation risk. The next generation of investment risk therefore requires us to look beyond individual assets and ask: What systems must remain functioning for our investment thesis to work?

Cybersecurity Has Become an Enterprise-Value Issue

Cybersecurity illustrates the change particularly well. For many years, cyber risk was largely treated as the responsibility of IT departments. Today, it belongs in investment due diligence, portfolio monitoring and exit planning. Kroll's 2026 research into private-equity cybersecurity found that cyber incidents are increasingly disrupting investments across the deal lifecycle. Its survey of 325 PE executives found an average financial impact of approximately **\$2.1 million** from cyber-related deal disruptions, while 13% reported losses exceeding \$5 million. Larger private-equity firms were also substantially more likely than smaller firms to incorporate cybersecurity into standardized diligence and portfolio-company governance.ⁱⁱ PwC similarly recommends integrating cyber analysis throughout the deal lifecycle and benchmarking portfolio-company cyber readiness rather than treating cybersecurity as an isolated technical review. The implications for private markets are significant.

- When acquiring a company, investors increasingly need to ask: What digital vulnerabilities are we buying?
- During the hold period: What cyber remediation belongs in the value-creation plan?
- Before exit: Could deficiencies reduce valuation or delay the transaction?

Cybersecurity therefore moves from being merely a defensive expenditure toward something closer to enterprise-value preservation.

AI Creates Both Opportunity and a New Risk Surface

Artificial intelligence creates an even more complicated problem because it sits on both sides of the risk equation. AI can increase productivity, automate processes, enhance cybersecurity, improve investment research and transform portfolio companies. But AI also introduces model risk, hallucinations, data leakage,

intellectual-property exposure, algorithmic bias, autonomous decision-making and new cyberattack capabilities.

NIST's AI Risk Management Framework emphasizes managing these risks throughout the AI lifecycle. Its emerging Cyber AI framework separates the problem into three useful areas: securing AI systems, using AI for cyber defense and thwarting AI-enabled attacks.ⁱⁱⁱ

For an investment committee, the key AI governance question should therefore not be simply: *Are our portfolio companies using AI?* It should be: Where can AI materially affect customers, revenues, operations, financial reporting or investment value — and what controls exist around those decisions? The greater the economic consequence of an AI-generated decision, the greater the need for accountability, validation and human oversight.

Geopolitics Must Enter the Cash-Flow Model

Geopolitics presents a similar challenge. For years, investors discussed geopolitical risk largely through country-risk scores and macroeconomic outlooks. That framework is increasingly inadequate. The IMF has documented growing evidence that trade and foreign investment are becoming more concentrated among geopolitically aligned economies, particularly in strategic industries.

The World Economic Forum goes further, ranking geoeconomic confrontation as the most significant near-term global risk. Its analysis identifies supply-chain disruptions and concentration in strategic technologies and resources among the likely consequences. Investors therefore need to move from country risk to dependency mapping. Consider a portfolio company with operations in the United States but: semiconductors from Taiwan; critical minerals processed in China; software from a European vendor; manufacturing in Mexico; cloud infrastructure concentrated with one provider; financing in U.S. dollars; and customers across several political blocs. What is the company's "country risk"? There isn't one.

It has a network of geopolitical dependencies. Those exposures should ultimately enter underwriting through revenues, margins, working capital, capex, financing costs, discount rates and potential exit multiples. If geopolitical risk never reaches the cash-flow model, investors may be discussing it without actually pricing it.^{iv}

Resilience Requires Rethinking the Supply Chain

The post-pandemic response to supply-chain risk initially emphasized reshoring. The emerging picture is more nuanced. The OECD's *Supply Chain Resilience Review 2025* finds that sourcing patterns tend to evolve slowly because existing supply chains reflect accumulated infrastructure, expertise and commercial relationships. Evidence instead suggests that firms may reduce geopolitical concentration while maintaining diversified global production networks.

This leads to an important capital-allocation concept: risk-adjusted efficiency. The cheapest supply chain is not necessarily the most valuable one. Dual sourcing, additional inventory, regional redundancy or alternative transportation may appear inefficient under normal conditions. But the economically relevant comparison is

not: *lowest operating cost versus higher operating cost*. It is: the incremental cost of resilience versus the expected financial impact of disruption. That calculation belongs in investment underwriting.^v

Diversified Portfolios Can Still Contain Hidden Concentration

Technology creates another paradox. An investor may own dozens of companies across different industries, geographies and strategies and appear highly diversified. But those companies may depend on: the same cloud provider; the same cybersecurity platform; the same fund administrator; the same payment infrastructure; the same semiconductor supply chain; or the same critical energy system. That is hidden systemic concentration.

The Financial Stability Board has highlighted the growing reliance of financial institutions on third-party service providers and warns that disruption at critical providers can threaten individual organizations and, in sufficiently concentrated cases, financial stability.^{vi} The Basel Committee's 2025 principles similarly broaden risk management beyond traditional outsourcing to encompass increasingly complex third-party relationships. This suggests an additional level of portfolio analytics: dependency-adjusted diversification. Investment committees should increasingly understand not only correlations among asset prices, but correlations among the underlying infrastructure upon which those assets depend.

Scenario Planning Must Move Beyond the Spreadsheet

These risks also change how institutions should conduct stress testing. Traditional stress tests often ask: *What happens if equities decline 25%? What happens if rates rise 200 basis points?*

Those are valuable questions. But next-generation risks require operational scenarios. Consider:

Taiwan disruption → semiconductor shortage → cyber escalation → equity-market selloff → currency volatility → portfolio-company production interruption → liquidity demands.

The critical questions become:

- What breaks first?
- Which operations must remain functioning?
- How much liquidity do we require?
- Who has authority to act?
- What information may become unreliable?
- What decision cannot wait until certainty arrives?

Tabletop exercises are particularly useful because they expose something quantitative models often miss: organizational capability.

The Most Important Risk Control May Be Decision Architecture

Ultimately, sophisticated risk systems cannot compensate for poor decision-making. Organizations navigating uncertainty successfully tend to establish several things before crises: clear decision rights; risk thresholds; escalation procedures; reliable information channels; liquidity triggers; communication responsibilities; and the ability to challenge prevailing assumptions.

That means translating abstract risk-appetite statements into operational thresholds. “Low cyber risk tolerance” is difficult to act upon. “Critical vulnerabilities must be remediated within X days” is actionable. “Maintain adequate liquidity” is ambiguous. Maintain X months of operating liquidity under identified stress conditions” creates a trigger. The distinction matters because resilience depends on acting before perfect information is available.

One useful crisis discipline is to separate three questions: What do we know? What do we believe? What must we decide before we know more? Those questions create decision clarity during uncertainty.

Resilience May Become a Source of Alpha

This leads to what may be the most important investment implication. We normally think of resilience as protection against downside risk. But resilience may increasingly create upside. Companies with diversified suppliers may continue serving customers when competitors cannot. Companies with stronger cyber controls may avoid disruption. Infrastructure with greater climate and physical resilience may command premium valuations. Organizations with stronger AI governance may deploy the technology faster because they have established guardrails. Companies with more robust liquidity may acquire assets during crises rather than sell them. And investment organizations with faster, higher-quality decision processes may reallocate capital while competitors remain paralyzed. In other words: resilience can create optionality. And optionality has economic value.

From Risk Register to Resilience Architecture

The next generation of institutional risk management therefore requires more than expanding the risk register. Investors should consider three actions.

First, map critical dependencies. Identify the technology, suppliers, infrastructure, jurisdictions, counterparties, financing and personnel required for each important investment thesis to succeed.

Second, incorporate emerging risks directly into underwriting. Translate cyber, AI, geopolitical, operational and supply-chain vulnerabilities into cash flow, capex, liquidity, leverage, valuation and exit assumptions.

Third, test the organization — not just the portfolio. Run combined-risk scenarios and determine who decides what, what information is required, what thresholds trigger intervention and how quickly the institution can act.

Traditional risk management asks: How much could we lose?

Next-generation risk management adds: What could stop the investment from functioning? Where are our hidden dependencies? How quickly would we recognize that our assumptions were wrong? And most importantly: Can our organization adapt before the market forces us to?

The institutions best positioned for the coming decade will probably not be those that correctly predict every cyberattack, geopolitical conflict, technological disruption or supply-chain shock. They will be those that build portfolios and organizations capable of functioning across multiple futures. That is not merely risk management. Increasingly, it may be a source of investment alpha.

ⁱ <https://www.weforum.org/publications/global-risks-report-2026/>

ⁱⁱ <https://www.kroll.com/en/publications/cyber/portfolio-cybersecurity-in-private-equity> and <https://www.pwc.com/us/en/services/consulting/deals/library/understanding-cyber-due-diligence.html>

ⁱⁱⁱ <https://www.nist.gov/itl/ai-risk-management-framework>

^{iv} <https://www.imf.org/en/publications/weo/issues/2026/07/08/world-economic-outlook-update-july-2026?cid=ca-com-homepage-WEOET2026004> and <https://www.weforum.org/publications/global-risks-report-2026/>

^v https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/oecd-supply-chain-resilience-review_9930d256/94e3a8ea-en.pdf

^{vi} <https://www.fsb.org/2023/12/fsb-publishes-toolkit-for-enhancing-third-party-risk-management-and-oversight> and <https://www.bis.org/bcbs/publ/d605.htm>