Fail cyber risk, lose capital: 7 questions GPs need to answer

Cybersecurity is no longer just a hygiene factor for private markets firms; it is becoming a potential red line in LP due diligence. According to the Private Funds CFO Insights Survey 2026, 90% of respondents said cybersecurity was the most heavily scrutinized back-office function in LP due diligence questionnaires, making it a critical priority for CFOs, COOs and boards to get right. Following Aztec Group and Drawbridge's joint webinar, ***Fail cyber, lose capital: the new reality for GPs****, cybersecurity specialists* ***Steve Pikett****, CISO at Aztec Group, and* ***Simon Eyre****, CISO at Drawbridge, joined* ***Tobias Cook****, Deputy Chief Risk Officer, to answer the key cyber questions operational leaders should be asking today.*

1. Why has cybersecurity become a boardroom issue rather than an IT issue?

Cybersecurity has become a boardroom issue because the consequences of an incident now extend far beyond technology. A successful attack can damage investor confidence, disrupt operations, impact employee morale and even affect portfolio company valuations. With 90% of CFOs identifying cybersecurity as the most heavily scrutinized back-office function in LP due diligence questionnaires, cyber resilience has also become a critical component of fundraising and investor relations. Perhaps most importantly, regulators expect senior leadership to oversee cyber risk. Firms can no longer delegate responsibility entirely to IT teams; boards and management teams need to be actively engaged in governance, oversight and risk management.

2. What are LPs really looking for during cyber due diligence?

LPs are no longer satisfied with policies sitting on a shelf, they want evidence of a cybersecurity programme.

Investors want evidence that cybersecurity is actively managed, tested and governed across the organization before they commit their capital. That means demonstrating risk assessments, employee training programmes, vendor

oversight, governance processes and remediation activities. One of the biggest red flags across the industry is when cyber resilience is treated as an IT-only issue. The strongest responses come from firms where leadership can clearly explain how cyber risks are continuously assessed, prioritized and managed across the business.

3. Within this context of increased LP scrutiny and cyber risk how should fund managers approach AI adoption?

The first question should not be *"How do we use AI?"* but *"Why are we using AI?"* Before approving AI-enabled tools or processes, CFOs and COOs should understand what problem the technology is trying to solve, whether conventional automation could achieve the same outcome, what data the model relies on, and how outputs will be validated. While AI can create significant efficiencies, it won't without the right scaffolding to support it. What is of paramount importance is putting governance and guardrails in place before scaling adoption. Policies, training, risk assessments and clear accountability frameworks are how CFOs can actively ensure AI delivers value without creating new, potentially unforeseen, vulnerabilities.

4. How is AI changing the cyber threat landscape?

AI is making attackers more effective as well as helping firms become more efficient. GPs are facing sophisticated impersonation attacks that mimic routine business interactions whether by email, through calendars, messaging platforms or capital call processes. These attacks exploit trusted relationships between GPs, LPs, portfolio companies, advisors and service providers. What makes these attacks particularly dangerous is that they often unfold gradually. Rather than relying on obvious phishing emails, attackers build familiarity and trust over time, making fraudulent requests appear legitimate. What AI has enabled is allowing cyber risks to look like normal business activity.

5. How can CFOs separate genuine cyber risks from industry hype?

CFOs do not need to become cybersecurity experts, but they do need to become better risk evaluators. When presented with a new threat, technology or investment proposal, leaders should ask simple questions:

- Has this threat been observed in the real world?
- How could it affect our business?
- What evidence supports the proposed solution?
- What measurable risk reduction does this investment deliver?

Frameworks such as the U.S. National Institute of Standards and Technology (NIST) and industry benchmarking can also help firms move from intuition to evidence when assessing cyber maturity and prioritizing investment. It's also important to make cyber investment decisions based on risk assessment, evidence and business impact rather than headlines.

6. What should fund managers look for when assessing cyber risk among vendors and service providers?

Cyber resilience extends beyond the fund manager's own organization. When firms choose to outsource critical functions or adopt AI-enabled services, they need to understand the third-party and downstream risks those decisions create, and ensure outsourced functions are governed by resilient cyber controls. Vendor assessments should look well beyond security questionnaires to examine how services are delivered, where data is processed, what dependencies exist, and whether providers meet the same standards expected internally. If a provider is handling a critical business function, its cyber standards should meet, or rather exceed, your own. GPs should also consider the growing importance of concentration risk and third-party dependencies as firms become more reliant on a smaller number of technology platforms.

7. What should fund managers do next to ensure they are tackling cyber risk upfront?

The best place to start is with risk. GPs need to understand their firm's cyber exposure, assess key vendors and portfolio companies, and ensure cybersecurity is regularly discussed at leadership level. From there, invest in meaningful employee awareness training and continuously test controls rather than simply checking compliance boxes. Strong cyber hygiene is fast becoming a differentiator in investor conversations and firms that can demonstrate operational maturity, robust governance and resilience in managing cyber risk are much better positioned to build confidence with LPs and protect value across their portfolios. Cybersecurity cannot be treated as a defensive function, instead

for today's fund managers, it's becoming a key indicator of business capability. And the complexities of keeping up with, and getting ahead of, these threats is only going to expand.

To watch the full webinar recording, **'Fail Cyber, Lose Capital: The New Reality for GPs',** click here.

As a leading global fund administrator Aztec delivers exceptional service, powered by best-of-breed technology. Across our client base we support fund managers and their investors throughout their fund's lifecycle, using intentional automation coupled with our expert teams to help them deliver results.

Drawbridge: Drawbridge combines technology and human expertise to help alternative investment firms raise their guard and lower their cyber risk. Trusted by hedge funds, private equity managers, portfolio companies, investors, LPs and other entities to protect their finances – and reputation – Drawbridge identifies vulnerabilities, mitigates risk and ensures business continuity.



Click here to talk to us