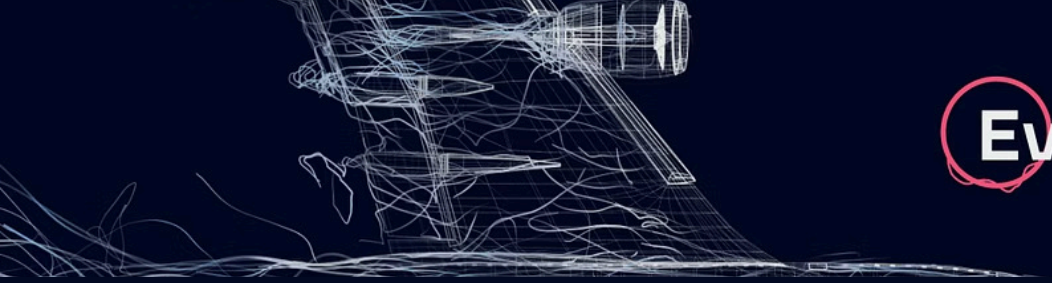


EveryCloud

VALUE IN TRUST

Cybersecurity as a foundation for PE value creation

Key Takeaways

Cybersecurity is seen more as a symbol of trust than a value driver

A quarter to recognise the value of cybersecurity in efficiency and innovation

Firms prefer company-level cybersecurity value creation over fund level

- **39% of firms view cybersecurity as a strategic foundation for business resilience and trust.**
- **43% of firms say it simply enhances investor confidence in governance.**

In private equity, cybersecurity often functions more as a symbol of confidence than an operational driver. Our Q1 2026 survey data shows that 39% of firms consider it a strategic foundation for business resilience and trust.

Additionally, 35% view it as a defensive imperative, essential for managing operational risk and preserving value. The critical question remains: Can robust cybersecurity do more than just preserve value? Can it actively facilitate growth?

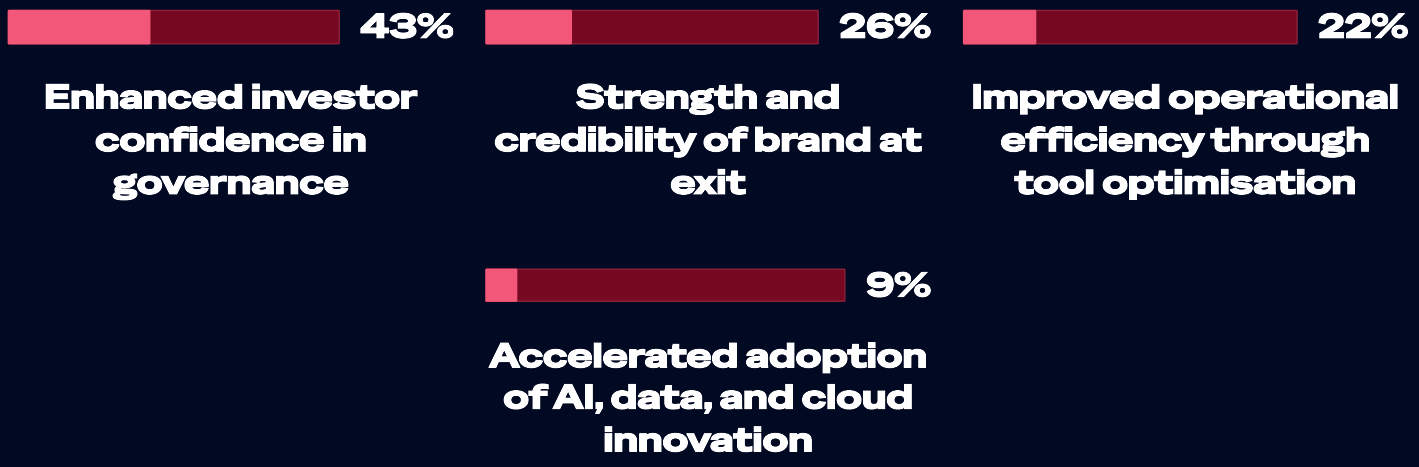
Currently, only 17% of firms see cybersecurity as a strategic enabler for tech investment returns. However, this perspective is likely to shift, largely driven by the rapid advancement of AI, a key lever for value creation across all sectors.

While AI offers exponential operational efficiency gains, its rapid pace introduces new risks. Establishing clear cybersecurity guardrails is crucial for AI-based transformations. Firms struggle to strike the right balance, either underinvesting or over-engineering protection. This tension presents significant opportunity for value creation.

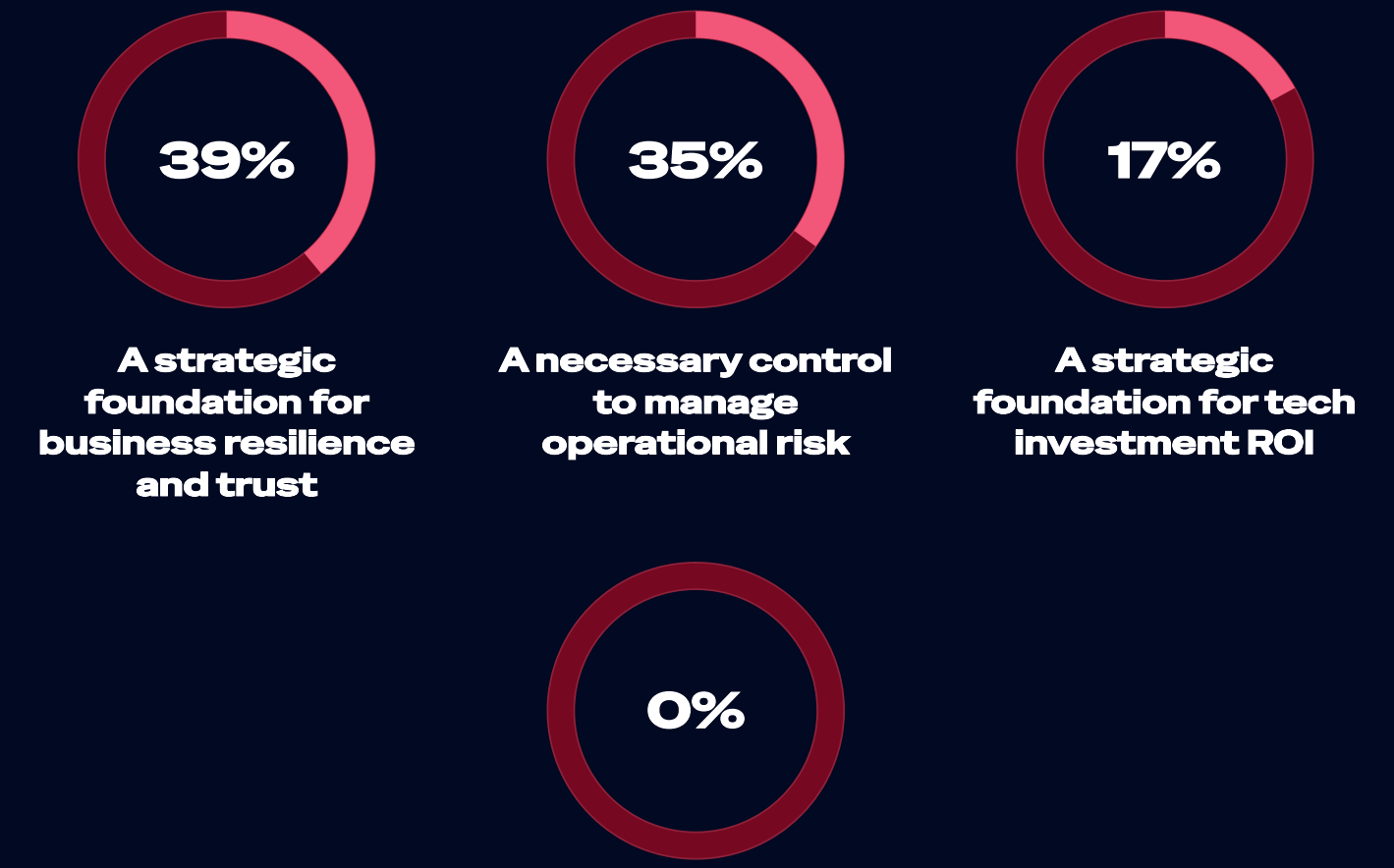
When asked about cybersecurity as a value lever, 43% of firms believe it enhances investor confidence in governance, and another 22% say it builds brand strength at exit. Both are largely symbolic benefits.

More proactively, 26% acknowledge that focusing on cybersecurity can improve operational efficiency through tool optimisation. Still, only 9% currently see cybersecurity as a springboard for innovation in AI, data, and cloud technologies.

How cybersecurity contributes to value creation



Perceptions of cybersecurity in PE portfolios



Implementation Approaches

Given the unique operations and security risks of each portfolio company, a top-down approach to cybersecurity has its limitations. This divergence in needs leads to varied implementation preferences:

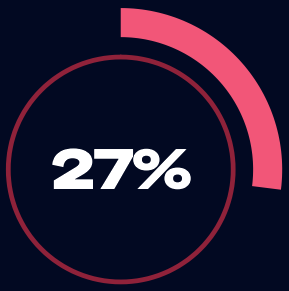
- **30%** of firms believe individual cybersecurity implementation plans per company are most effective for value creation.
- **26%** prefer centralising standards and frameworks at the fund level.
- Only **17%** would opt for a shared security operation or "centre of excellence" model at the fund level.

These choices often reflect firms' broader perceptions of cybersecurity: defensive-minded organisations tend to favour common standards, while those more proactive lean towards innovation or tailored, per-company solutions. Additionally, more than a quarter (**27%**) of firms would ideally partner with an external service provider to ensure ongoing cyber resilience.

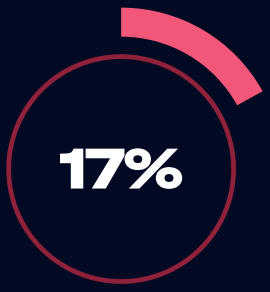
Ideal implementation models for cybersecurity across PE portfolios

Cyber value creation plans per company

Fund-level cyber framework and standards



Partnering with a managed provider for ongoing resilience



Shared security operations or "centre of excellence" model