

Cyber Resilience in Fund Administration: Built for What's Next



BY THE NUMBERS

01 The Threat Landscape



\$5.56M

Average Breach Cost

For financial services firms, making prevention a business imperative

IBM, 2025



105%

DDoS Attack Surge

Year-over-year increase in attacks targeting financial institutions

2026



30%

Third-Party Breaches

Of 2025 breaches involved a vendor, double the prior year

2025



PILLARS

02 What Resilient Looks Like



Visibility

Know where investor data lives, who touches it, and how it moves at all times



Third-Party Risk

Due diligence before onboarding. Contractual controls. Regular vendor reviews



Incident Response

Rehearsed response beats a documented plan every time. Speed reduces cost



Identity & MFA

Credential attacks are the #1 entry vector. MFA and access audits are baseline



REGULATORY

03 The 2026 Compliance Picture



LARGER ADVISERS

Required to comply with amended Reg S-P by December 2025



SMALLER ENTITIES

Required to comply with amended Reg S-P by June 2026



2026 EXAM FOCUS

Governance quality, incident response rigor, and AI-driven attack readiness



EVALUATION

04 Ask Your Administrator



Incident Response

Is your plan documented, tested, and recently exercised?



Access Controls

How is investor data access managed and regularly reviewed?



Vendor Oversight

What controls govern your vendors' cybersecurity practices?



Reg S-P Readiness

Are you ready to support SEC breach notification requirements?



Phishing Defense

Do you run regular simulations and staff security training?



Wire Fraud Protection

How do you guard wire instructions against business email compromise?



Business Continuity

What is your posture if key systems go down in a ransomware attack?



THE TAKEAWAY

Security is no longer about being unhackable. It's about being able to keep operating when disruption arrives.