Innovation Growth Partners Specialty®

CONTACT US

Dave Perkins, RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

Cyber Claim Examples for Asset Managers

Applicable to Investment Managers, Hedge Funds, Venture Capital Funds, Private Equity Funds, Family Offices, and Registered Investment Advisors (RIAs)

Asset managers face a unique cyber risk profile due to their custody of sensitive investor information, access to capital movement systems, portfolio company data, and reliance on third-party service providers. Below are twelve realistic cyber claim scenarios that frequently drive losses and insurance claims in the asset management sector.

1. Ransomware Attack on Investment Advisor

Scenario
A registered investment advisor experiences a ransomware attack that encrypts trading systems, CRM databases, investor records, and compliance files.

Potential Losses
- Incident response and forensic costs
- Data restoration expenses
- Business interruption losses
- Ransom payment (where legally permitted)
- Regulatory investigations

Cyber Coverage Triggered
- Incident Response
- Cyber Extortion
- Data Recovery
- Business Interruption

2. Social Engineering Wire Transfer Fraud

Scenario
An accounts payable employee receives an email appearing to come from a managing partner requesting an urgent capital transfer to support a portfolio company acquisition. The request is fraudulent, and $750,000 is wired to criminals.

Potential Losses
- Direct financial loss
- Investigation costs
- Recovery expenses

Cyber Coverage Triggered
- Social Engineering Fraud
- Funds Transfer Fraud

3. Investor Personally Identifiable Information (PII) Breach

Scenario
A cybercriminal gains access to a cloud-based investor portal containing Social Security numbers, tax information, banking details, and investor subscription documents.

Potential Losses
- Privacy breach notification expenses
- Credit monitoring services
- Legal defense costs
- Regulatory fines and penalties
- Class action litigation

Cyber Coverage Triggered
- Privacy Liability
- Regulatory Defense
- Breach Response Services

4. Business Email Compromise During Capital Call

Scenario
Hackers infiltrate email accounts and alter wiring instructions distributed to limited partners during a capital call. Investors unknowingly send funds to fraudulent accounts.

Potential Losses
- Investor reimbursement demands
- Legal defense
- Reputation management
- Regulatory scrutiny

Cyber Coverage Triggered
- Cyber Liability
- Social Engineering Coverage
- Errors & Omissions (potential overlap)

5. Vendor-Dependent Business Interruption

Scenario
A fund administrator experiences a significant cyberattack that renders accounting and investor reporting systems unavailable for several weeks. As a result, the fund cannot complete NAV calculations, investor reporting, or capital activity processing.

Potential Losses
- Delayed investor reporting
- Increased operating costs
- Lost management fee revenue
- Investor relations expenses

Cyber Coverage Triggered
- Dependent Business Interruption
- Contingent Business Interruption

6. SEC Cybersecurity Investigation

Scenario
Following a cyber incident, regulators investigate whether the advisor maintained reasonable cybersecurity controls and adequately protected client information.

Potential Losses
- Legal counsel costs
- Regulatory response expenses
- Fines and penalties (where insurable)
- Compliance remediation costs

Cyber Coverage Triggered
- Regulatory Defense Coverage
- Privacy Liability Coverage

7. Portfolio Company Data Exposure

Scenario
A private equity firm's internal systems containing confidential portfolio company financial information and acquisition plans are compromised prior to a transaction announcement.

Potential Losses
- Confidential information disclosure
- Transaction disruption
- Litigation from affected stakeholders
- Crisis communications costs

Cyber Coverage Triggered
- Network Security Liability
- Privacy Liability
- Crisis Management

8. Third-Party Lawsuit Following Data Breach

Scenario
Investors allege that an asset manager failed to adequately secure personal and financial information after a cyber breach compromises investor records.

Potential Losses
- Defense costs
- Settlements or judgments
- Expert witness expenses

Cyber Coverage Triggered
- Privacy Liability
- Network Security Liability

9. Deepfake Executive Impersonation Fraud

Scenario
Criminals use artificial intelligence to create a convincing voice deepfake impersonating the Chief Investment Officer during an acquisition closing. The finance team receives fraudulent instructions to transfer funds.

Potential Losses
- Misdirected transaction funds
- Investigation costs
- Recovery efforts

Cyber Coverage Triggered
- Social Engineering Fraud
- Funds Transfer Fraud

10. Cloud Service Provider Outage

Scenario
A major cloud provider supporting investor portals and fund management systems suffers a cyber event, resulting in several days of downtime.

Potential Losses
- Inability to access investor reporting systems
- Delayed subscriptions and redemptions
- Lost productivity
- Extra operating expenses

Cyber Coverage Triggered
- Dependent Business Interruption
- Extra Expense Coverage

11. Theft of Proprietary Investment Research

Scenario

A threat actor steals proprietary quantitative models, investment strategies, deal sourcing information, and confidential research from a hedge fund.

Potential Losses

- Competitive disadvantage
- Revenue loss
- Litigation costs
- Crisis management expenses

Cyber Coverage Triggered

- Network Security Liability
- Digital Asset Recovery
- Crisis Management Coverage

12. Distributed Denial of Service (DDoS) Attack During Fundraising

Scenario

A VC fund launches a fundraising campaign while its investor portal is targeted by a DDoS attack, preventing prospective investors from accessing offering materials and subscription documents.

Potential Losses

- Business interruption
- Lost fundraising opportunities
- Incident response expenses
- Reputation damage

Cyber Coverage Triggered

- Network Interruption
- Business Interruption
- Incident Response Services

Key Takeaways for Asset Managers

The most significant cyber exposures for asset managers generally fall into four categories:

1. **Investor Data Breaches** involving PII, financial information, and tax records.
2. **Fraudulent Fund Transfers** arising from business email compromise, social engineering, and deepfake attacks.
3. **Operational Disruption** caused by ransomware, cloud outages, and critical vendor incidents.
4. **Regulatory and Litigation Exposure** stemming from SEC investigations, investor lawsuits, and privacy claims.

Given the increasing sophistication of threat actors and the substantial volumes of confidential investor and transaction data held by asset managers, cyber insurance has become a critical component of enterprise risk management for investment advisors, hedge funds, venture capital firms, and private equity managers. Coverage should be carefully reviewed to ensure adequate limits for business interruption, social engineering fraud, privacy liability, ransomware, regulatory defense, and dependent business interruption exposures.

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com