

Cybersecurity: A Strategic Imperative in Private Markets



Kathleen Schau
Vice President,
Investment Strategy
and Risk Management

Alejandra Lesch
Partner,
Investment Strategy
and Risk Management

Craig Goesel
Senior Vice President
& Regional Leader,
Alliant Insurance
Services

KEY TAKEAWAYS

- Cybersecurity is a strategic imperative for private markets firms amid escalating threats that target sensitive investor data, confidential deal details, and interconnected systems across funds, portfolio companies, and vendors
- An adaptive multilayered cybersecurity framework combining governance, technology, training, third-party oversight, and incident response is generally seen as essential to mitigate risk and protect against the potential for financial and reputational harm
- Cyber liability insurance is a key complement to robust internal controls, providing financial safeguards and rapid expert response that can maintain operational continuity, preserve investor trust, and support long-term enterprise value

As cyber threats escalate in frequency, scale, and sophistication, financial services firms must take deliberate and comprehensive steps to mitigate risks. For private markets managers, the stakes are particularly high. Positioned at the intersection of capital and innovation, these firms are often prime targets for cybercriminals seeking to exploit sensitive investor data, confidential deal information, and proprietary insights.

The interconnected nature of the private markets ecosystem amplifies exposure. In addition to safeguarding internal networks, firms also depend on portfolio companies, fund administrators, and third-party technology providers—each representing potential points of entry for malicious actors. A breach can jeopardize deal flow, compromise investor confidence, and trigger regulatory scrutiny or costly litigation.

Most industry experts believe the optimal way to address these challenges is to implement a comprehensive, multilayered cybersecurity framework that anticipates, prevents, detects, and responds to threats. The framework should be regularly reviewed and updated to align with emerging risks, regulatory expectations, and evolving operational dependencies. A well-structured cyber defense program strengthens resilience across business functions and helps protect against diverse attack vectors¹—the methods cybercriminals use to infiltrate a network.

Core Cybersecurity Components

Strategic governance, technical safeguards, and awareness of the organization's standard operating controls and protocols are essential ingredients in a mature cybersecurity framework. Institutional-grade cyber resilience should include:

- **Training and Awareness:** Regular, role-specific education that empowers employees to recognize and respond to threats such as phishing, credential harvesting, and social engineering;
- **Internal Cash Controls:** Implementation of dual authorization, segregation of duties, and out-of-band verification for all wire transfers to reduce the risk of business email compromise (BEC) and fraudulent payments;
- **Information Technology and Access Controls:** Continuous system monitoring, endpoint protection, identity and access management, encryption, and patch management to detect and block unauthorized access attempts;
- **Vendor and Third-Party Risk Management:** Comprehensive due diligence and ongoing monitoring of fund administrators, cloud providers, and software vendors to mitigate vulnerabilities within the extended enterprise;
- **Portfolio Company Oversight:** Cyber due diligence during acquisition, followed by the establishment of baseline security standards and incident response protocols across portfolio holdings, particularly for early-stage or technology-driven companies;
- **Incident Response Planning and Testing:** Clear incident response playbooks, escalation protocols, and regular tabletop exercises to ensure coordinated and timely action in the event of a breach; and
- **Cyber Insurance Coverage:** Adequate insurance policies that provide financial protection against residual risk, including business interruption, ransom payments, and data recovery expenses.

Strategic Benefits

Implementing a holistic cybersecurity strategy provides value far beyond compliance by enabling operational resilience and strategic differentiation. Key advantages include:

- **Protection of Sensitive Data:** Encryption, strict access controls, and proactive monitoring are designed to safeguard investor, deal, and firm data against unauthorized access or theft;
- **Regulatory Alignment:** Strengthens adherence to industry regulations and emerging cybersecurity standards, reducing the risk of penalties, sanctions, or reputational harm;
- **Financial Risk Mitigation:** Preventive measures minimize direct financial losses and indirect costs associated with cyber incidents, including downtime and recovery expenses;
- **Operational Continuity:** Enhances a firm's ability to maintain critical functions during and after an attack, reducing business interruption;
- **Reputation and Trust Preservation:** Demonstrates a tangible commitment to data stewardship, investor protection, and corporate governance;
- **Adaptive Defense Against Emerging Threats:** Periodic learning, threat intelligence integration, and employee engagement help to ensure defenses evolve alongside adversaries' tactics;
- **Cultural Resilience and Accountability:** Promotes organization-wide awareness and responsibility for cybersecurity, which seeks to address human error, the leading cause of data breaches; and
- **Long-Term Cost Efficiency:** Early investment in cybersecurity infrastructure and training generates long-term savings by potentially avoiding the exponential costs of remediation, litigation, and reputational repair.



In today's private markets, cybersecurity is a strategic pillar of operational excellence and fiduciary governance. A robust, layered cybersecurity framework allows firms to better safeguard assets and investors, and to strengthen their reputation as disciplined and forward-thinking stewards of capital. Cyber resilience is now seen as a marker of institutional maturity—one that differentiates leading investment firms in an increasingly digital and interconnected world.

Escalating Cyber Risk Landscape

Global private equity deals reached an estimated \$2 trillion in 2024,² excluding \$600 billion in capital calls and \$700 billion in distributions during the first half of the year.³ This illustrates the value of capital moving through interconnected fund, investor, and portfolio company systems—each a potential entry point for cyber exploitation. Even limited vulnerabilities in cash controls or data security, whether at the fund, general partner (GP), limited partner (LP), or portfolio company level, can be leveraged by bad actors to inflict significant financial and reputational harm.

The FBI's 2024 Internet Crime Report reveals that phishing, extortion, and personal data breaches remain among the most prevalent and costly forms of cybercrime.⁴ Within the financial sector, investment-related fraud and BEC rank highest in reported losses, totaling approximately \$6.5 billion and \$2.7 billion respectively.⁵ Similarly, Travelers Insurance identified social engineering fraud and BEC as two of the top three drivers of cyber insurance claims,⁶ illustrating the persistence and financial impact of these attack vectors across industries.



Accenture reports that 68% of private equity clients experience a measurable increase in cyber incidents during the month of a deal closure,⁷ with the average ransom demand exceeding \$1 million for mid-sized firms.⁸

The threat intensifies during key transactional periods. Accenture reports that 68% of private equity clients experience a measurable increase in cyber incidents during the month of a deal closure,⁷ with the average ransom demand exceeding \$1 million for mid-sized firms.⁸ Adversaries are aware that deal teams often operate under tight deadlines, heightened information exchange, and reduced operational bandwidth, conditions that can increase vulnerability.

The data also reveal a clear advantage for firms with advanced cybersecurity frameworks. Among organizations that strengthened their cyber posture, 55% were able to detect breaches in under 24 hours, only one in six attacks successfully penetrated defenses, and 72% of breaches resulted in zero operational impact.⁹ In other words, disciplined cybersecurity investments yield measurable resilience and risk reduction.

Unique Private Markets Cyber Exposures

Private markets firms face cyber risk from multiple, interrelated dimensions:

- **LP Data and Communications:** LP information often resides on cloud platforms and third-party investor portals, increasing potential exposure to unauthorized access or data leakage;
- **Deal Data and Material Nonpublic Information:** Confidential documents and non-disclosure agreements can contain market-sensitive information which, if compromised, could result in insider trading or reputational damage;
- **Portfolio Company Oversight:** Fund managers are indirectly exposed to downstream cyber events at portfolio companies, especially in early-stage or high-growth businesses that may lack mature security controls; and
- **Third-Party Dependencies:** Reliance on fund administrators, customer relationship management systems, and technology vendors expands the attack surface—the sum of all possible security risk exposures in an organization's environment—across the firm's operational network.

A Growing Strategic Imperative

For private markets firms, these risks highlight an urgent operational and fiduciary reality: cybersecurity is a significant component of institutional excellence. As the private markets industry continues its rapid digitization and data integration, the potential for financial loss, regulatory exposure, and reputational damage due to cybercrime is significantly increased.

In this evolving landscape, firms that invest in comprehensive cybersecurity frameworks and proactive governance structures are better positioned to safeguard sensitive assets and strengthen investor trust, operational continuity, and long-term enterprise value.

Building a Framework to Combat Emerging Risks

Proactive, adaptive cybersecurity frameworks that are deeply integrated into business operations help mitigate exposure to potential attacks while addressing the unique data, communication, and third-party risks inherent to private markets. A robust defense strategy should:

- **Establish Strong Governance and Risk Oversight:** Define accountability, leadership, and alignment between cybersecurity and business strategy;
- **Conduct Comprehensive Risk Assessments:** Identify vulnerabilities across people, processes, technology, and third-party connections;
- **Strengthen Internal Technical and Operational Controls:** Prevent and detect unauthorized access, data exfiltration, and operational disruptions;
- **Elevate Human Defenses Through Training and Awareness:** Reduce human error, the leading cause of cyber breaches;
- **Strengthen Third Party and Portfolio Company Oversight:** Manage downstream risks;
- **Develop and Test Incident Response Plans:** Prepare to respond swiftly and effectively to minimize disruption and damage;
- **Integrate Cyber Insurance as a Risk Transfer Mechanism:** Complement operational defenses with financial protection; and
- **Commit to Regular, Ongoing Improvement and Industry Collaboration:** Maintain an adaptive, defensive, and dynamic cybersecurity posture.

Cyber Liability Insurance: A Risk Management Tool

Cyber liability insurance is a key component of a modern risk management strategy. Beyond reimbursing losses, comprehensive policies can provide immediate access to breach response teams, forensic investigators, legal counsel, ransomware negotiators, and crisis communication specialists. These can be indispensable resources when time and reputation are on the line.

Cyber liability insurance enhances organizational resilience by supporting financial recovery, validating regulatory and investor readiness, and reinforcing a firm's overall cyber posture. However, coverage is not a substitute for strong internal controls—it must complement robust cybersecurity governance, training, and oversight.

Craig Goesel, a Senior Vice President & Regional Leader with Alliant Insurance Services, shares the example of a mid-sized registered investment advisor that was the victim of a ransomware attack that encrypted trading systems and exposed sensitive client data.

The firm contacted its cyber insurance broker, which immediately engaged the insurance carrier and helped to deploy a breach coach and a forensic investigation team. Forensics identified the attack as credible and determined the compromise stemmed from a phishing email but confirmed only limited data exfiltration.



Resource-constrained firms are more vulnerable to cyber risks, as only 28% of managers with less than \$1 billion in AUM have cyber coverage, compared with 52% of managers with over \$1 billion in assets, according to our data

The quick assessment helped negotiators to reduce the ransom demand to \$75,000 from \$250,000, and the carrier handled payment and decryption. The insurer covered system restoration, including rebuilding servers and securing endpoints, and helped legal counsel to manage notifications to the U.S. Securities & Exchange Commission as well as investor communications. The carrier also paid required client notification costs and funded appropriate credit monitoring. Lastly, business interruption coverage reimbursed lost advisory fees and temporary manual trading costs. The insurance carrier coordinated the entire response, from containment through recovery, and total covered losses exceeded \$400,000. This was paid upon a \$2 million insurance policy that had an annual premium of about \$12,000.

Adams Street regularly reviews managers' cybersecurity programs and requests insurance details when available, recommending adoption where appropriate. As of July 2025, roughly half of our managers maintain active cyber insurance policies, aligning with industry norms but lagging adoption rates for other coverage types such as general liability, errors and omissions, directors and officers, crime bond, and fiduciary insurance. Resource-constrained firms are more vulnerable to cyber risks, as only 28% of managers with less than \$1 billion in AUM have cyber coverage, compared with 52% of managers with over \$1 billion in assets, according to our data.

Cyber policies typically support costs related to:

- Regulatory fines and legal defense;
- Ransomware or extortion payments;
- Data breach notification and credit monitoring;
- Business interruption and data restoration; and
- Third-party liability from LPs, vendors, or portfolio companies.

Given the complexity and variability of coverage terms, firms should engage brokers and legal counsel to ensure policies are comprehensive, tailored, and defensible within their operational and regulatory context. Ultimately, cyber liability insurance is a strategic safeguard. Firms that combine strong internal controls, verified coverage, and ongoing vigilance are best positioned to withstand and recover from today's fast-evolving cyber threats.

Practical Next Steps

To effectively safeguard sensitive information and maintain operational integrity, a comprehensive and proactive cybersecurity strategy should combine strong internal controls with expert external support in the form of a layered defense strategy. This includes implementing employee cybersecurity training, conducting regular phishing simulations, performing third-party risk assessments, enforcing cybersecurity standards across portfolio companies, and developing and testing a formal incident response plan through tabletop exercises.

These internal processes, coupled with comprehensive cyber liability insurance coverage, increase firms' resilience, allowing them to mitigate exposure, accelerate response, and ensure business continuity in the event of a breach.

Cyber insurance and robust internal cybersecurity frameworks are strategic assets that:

- Activate expert response networks when time is critical;
- Protect against financial and reputational losses;
- Demonstrate readiness to regulators and limited partners; and
- Reinforce a firm's commitment to operational excellence

In a risk landscape defined by complexity, interconnectivity, and speed, the cost of inaction can far exceed the investment in preparation.

As private markets firms continue their digital evolution, cybersecurity posture and readiness must evolve in parallel. The convergence of high transaction volumes, sensitive data, and interconnected systems amplifies risk and opportunity. Firms that invest in comprehensive, forward-looking cybersecurity frameworks can better protect their operations and strengthen their credibility, resilience, and long-term value in an increasingly complex digital economy. ■

1. CrowdStrike, Attack Vectors: What They Are and How They Are Exploited, January 17, 2025
2. McKinsey Global Private Markets Report 2025, Page 8, May 20, 2025
3. Id., Exhibit 14, Page 24
4. Federal Bureau of Investigation’s Internet Crime Report 2024
5. Ibid., Page 10
6. Travelers Insurance Q2 2025 Cyber Threat Report, September 22, 2025
7. Accenture: Private equity and the rising cost of cyberattacks, Page 7, March 5, 2023
8. Ibid., Page 3
9. Ibid., Page 10

LEADING WITH FORESIGHT™

Adams Street Partners is a global investment firm managing a comprehensive suite of private markets investment solutions. The firm provides private equity and private credit strategies to institutional investors, growth capital to innovative companies, and evergreen funds that offer access to multiple strategies through a single, investor-friendly commitment. The firm also supports wealth advisors with private markets solutions structured to be more flexible and accessible than traditional closed-end funds. With over 50 years of experience, Adams Street leverages deep market insights, global relationships, and proprietary data as it seeks to help investors achieve long-term investment goals. The firm is 100% employee-owned, manages \$65 billion in assets, and operates out of 15 offices globally. Visit adamsstreetpartners.com

Important Considerations: This information (the “Paper”) is provided for educational purposes only and is not investment advice or an offer or sale of any security or investment product or investment advice. Offerings are made only pursuant to a private offering memorandum containing important information. Statements in this Paper are made as of the date of this Paper unless stated otherwise, and there is no implication that the information contained herein is correct as of any time subsequent to such date. All information has been obtained from sources believed to be reliable and current, but accuracy cannot be guaranteed. References herein to specific sectors, general partners, companies, or investments are not to be considered a recommendation or solicitation for any such sector, general partner, company, or investment. This Paper is not intended to be relied upon as investment advice as the investment situation of individuals is highly dependent on circumstances, which necessarily differ and are subject to change. The contents herein are not to be construed as legal, business, or tax advice, and individuals should consult their own attorney, business advisor, and tax advisor as to legal, business, and tax advice. Past performance is not a guarantee of future results and there can be no guarantee against a loss, including a complete loss, of capital. Certain information contained herein constitutes “forward-looking statements” that may be identified by the use of forward-looking terminology such as “may,” “will,” “should,” “expect,” “anticipate,” “estimate,” “intend,” “continue,” or “believe” or the negatives thereof or other variations thereon or comparable terminology. Any forward-looking statements included herein are based on Adams Street’s current opinions, assumptions, expectations, beliefs, intentions, estimates or strategies regarding future events, are subject to risks and uncertainties, and are provided for informational purposes only. Actual and future results and trends could differ materially, positively or negatively, from those described or contemplated in such forward-looking statements. Moreover, actual events are difficult to project and often depend upon factors that are beyond the control of Adams Street. No forward-looking statements contained herein constitute a guarantee, promise, projection, forecast or prediction of, or representation as to, the future and actual events may differ materially. Adams Street neither (i) assumes responsibility for the accuracy or completeness of any forward-looking statements, nor (ii) undertakes any obligation to update or revise any forward-looking statements for any reason after the date hereof. Also, general economic factors, which are not predictable, can have a material impact on the reliability of projections or forward-looking statements. Adams Street Partners, LLC is a US investment adviser governed by applicable US laws, which differ from laws in other jurisdictions.