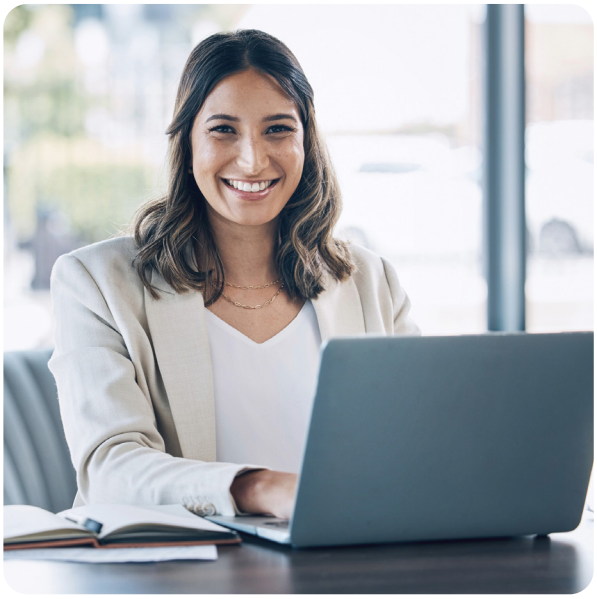
Securing Private Equity Portfolios: An MSP Partner that Leads with Cybersecurity

By John Kochvar



Cyber risk has become one of the most urgent and financially-impactful issues facing Private Equity firms today. With portfolio companies increasingly targeted by ransomware, phishing, and supply-chain attacks, cybersecurity has shifted from an IT concern to a board-level priority. These digital moats are now a major factor in each firm's valuation, deal execution, and investor confidence.

Yet most portfolio companies, especially in the middle market, lack the internal resources to maintain modern security standards across networks, applications, and data environments. For PE operating teams, this creates inconsistent risk exposure and significant operational drag.

According to the 2025 IBM Cost of a Data Breach Report[1], the average breach now costs **$4.45 million**, the highest in the report's 19-year history, with mid-market companies among the fastest-growing targets. Meanwhile, EY's latest Global Private Equity Pulse Survey[2] shows that **cybersecurity has entered the top three concerns** of PE leaders for three consecutive years.

Partnering with a Managed Service Provider (MSP) that leads with cybersecurity and data protection – such as **Access One** – offers an immediate, scalable, and cost-efficient way to bring all holdings to a defensible security baseline.

Keeping our perspective on the M&A process, I'll highlight the five most important reasons for selecting a cyber-focused IT partner, and additional points of consideration for each:

1. Standardizing Cybersecurity Posture Across the Portfolio

One of the biggest challenges PE firms face post-acquisition is cybersecurity inconsistency. Each company arrives with different tools, policies, and maturity levels – creating blind spots across the firm's ecosystem.

A cybersecurity-first MSP delivers:

- Uniform security policies
- Standardized endpoint protection
- Centralized monitoring and alerting
- Consistent compliance reporting
- Documented playbooks and incident response plans

This standardization not only reduces risk but also lowers cost through consolidation, eliminating duplicate tools and unmanaged technologies.

The 2024 Deloitte Future of Cyber Survey[3] found that organizations adopting standardized cybersecurity frameworks reduced incident frequency by **up to 30%** within the first year.

2. Rapid Detection and Response to Minimize Business Interruption

Because threat actors operate around the clock to disrupt mid-market companies, the defenses of your Portfolio need to do the same.

A security-led MSP provides 24/7 Security Operations Center (SOC) services, threat hunting, and continuous monitoring that most mid-market companies cannot staff internally.

This allows for:

- Real-time detection of suspicious behavior
- Containment of threats before spread
- Reduced dwell time (the time attackers go unnoticed)
- Faster remediation and recovery

The IBM Data Breach Report notes that organizations with managed detection and response capabilities reduce breach lifecycles by **over 80 days** on average – saving more than **$1.7M** per incident.

PE firms are taking note of the costs of such incidents and now leverage threat detection as a true protector of portfolio value as they near exit.

3. Enhancing Compliance and Reducing Regulatory Exposure

Portfolio companies often face diverse regulatory environments – HIPAA, PCI-DSS, NIST, SOC 2, GDPR – and the complexity multiplies with each new acquisition or industry vertical.

A cybersecurity-led MSP ensures portfolio companies meet and maintain compliance through:

- Automated compliance monitoring
- Policy management
- Audit documentation
- Ongoing gap assessments
- Staff training and phishing simulation

According to a 2024 Thomson Reuters Regulatory Intelligence Report, compliance failure costs have risen **over 45%** in five years due to increased fines and mandatory disclosure requirements.

Having an MSP partner in place from entry through exit sharply reduces that exposure.

4. Strengthening IT Due Diligence and Reducing Deal Risk

Cyber risk is now a critical part of deal valuation and investment committee approval. Yet many target companies – especially founder-led businesses – lag significantly in cybersecurity maturity.

An MSP that specializes in cybersecurity enhances the deal process by providing:

- Pre-acquisition IT and security assessments
- Inventory of vulnerabilities and legacy systems
- Estimated remediation costs
- Risk scoring aligned to industry standards
- Insights for negotiation and post-close planning

In KPMG's 2025 M&A Deal Market Study, 54% of deal leaders cited cybersecurity issues uncovered during diligence as a reason they reduced valuation, and 27% said it caused them to walk away from a deal entirely.

"Time kills all deals" as they say, but a strong MSP partner gives PE firms the confidence to make faster, clearer, and safer investment decisions.

5. Improving Exit Readiness Through Documented and Mature Cyber Programs

Buyers today place increased scrutiny on cybersecurity posture during exit, often requesting detailed documentation of tools, policies, monitoring, and historical incident reports.

Portfolio companies that demonstrate mature security programs:

- Achieve smoother due diligence
- Inspire higher buyer confidence
- Face fewer contractual demands (e.g., reps & warranties)
- Command higher valuations

According to PitchBook's PE Value Creation Report from Q3 2025, businesses that show "strong cybersecurity maturity" achieve **8–12% higher** exit multiples on average across all industries.

An IT partner that is present from acquisition through exit ensures that cybersecurity readiness is a built-in advantage from day one.

Conclusion: Cybersecurity Is Now a Value-Creation Imperative

For Private Equity firms, cybersecurity is a strategic necessity that impacts valuation, integration, compliance, and just as importantly – their reputation within the market.

By partnering with a cybersecurity-first Managed Service Provider like **Access One**, PE firms gain:

- Portfolio-wide standardization
- Continuous threat protection
- Reduced regulatory exposure
- Stronger due diligence insights
- Enhanced exit readiness

In a landscape where cyber risk is accelerating and attack vectors are expanding, a proactive MSP partnership is one of the most cost-effective ways to safeguard both operational and financial outcomes.

Cybersecurity doesn't just protect value – market participants themselves tell us it is an essential value creation tool.

References
1 - IBM's 2025 Cost of a Data Breach Report, https://www.ibm.com/reports/data-breach

2 - EY's 2025 Global Private Equity Pulse Survey https://www.ey.com/en_gl/insights/private-equity/pulse

3 - 2024 Deloitte Future of Cyber Survey, https://www.deloitte.com/global/en/services/consulting-risk/research/global-future-of-cyber.html

4 - 2024 Thomson Reuters Regulatory Intelligence Report, https://www.thomsonreuters.com/en-us/posts/corporates/global-compliance-report-2024/

5 - KPMG's 2025 M&A Deal Market Study, https://kpmg.com/us/en/articles/2025/2025-ma-deal-market-study.html

6 - PitchBook's PE Value Creation Report from Q3 2025, https://pitchbook.com/news/reports/q3-2025-us-pe-breakdown