Clearwater

Reshaping Private Equity Decisions

Why Cybersecurity Diligence is Core to Value Creation

A Playbook for PE Firms

Leading Healthcare Private Equity (PE) firms increasingly view cyber risk and compliance exposure as high-priority concerns. Not just operational risks, but they are moving their understanding of exposure earlier in the process to inform investment decisions and accelerate value creation plans to align with business and growth objectives.

With sustained and growing threats to the industry, combined with the increasing digitization of businesses—which expands the overall risk footprint—there has been a fundamental shift in how cybersecurity and compliance are viewed. The changes:

- **Cybersecurity is no longer seen as a "nice to have"** or a post-acquisition upgrade — it's now a gating factor in due diligence.
- **Privacy compliance** landmines related to HIPAA, HITECH, 42 CFR Part 2, and state privacy laws like the California Consumer Privacy Act can result in breach notifications, fines, class-action lawsuits, and reputational damage risk and significantly derail ROI.
- **As competition grows with fewer targets, cybersecurity maturity is now a value lever**; companies with mature cybersecurity programs become more attractive at exit, especially for strategic buyers that require strong governance.
- Growing skepticism about cyber insurance is making it clear: rising premiums, policy exclusions, and sub-limits mean **organizations can no longer rely on insurance alone to manage cyber risk**.
- There is a growing objective to **elevate cybersecurity oversight to the board level** within portfolio companies, ensuring alignment with investor expectations, industry benchmarks, and transparent reporting on cyber posture and breach readiness.

Based on these changes, standard IT due diligence is no longer sufficient to understand cyber risk that may impact a deal, value creation plans, and the organization's ability to execute against those plans.

Proactive investors include cybersecurity, privacy, and compliance assessments as an integral component in every stage, and not just at the beginning of the M&A process, to secure investments and provide sustainable value creation. Not knowing these risks can significantly impact valuation, liability, regulatory compliance, and exit potential.

Clearwater experts partner with private equity firms helping them to address the nuanced risk that healthcare organizations face, regardless of market segment or stage of investment.

Recommended Risk-Management Playbook

Healthcare Cyber Risk Due Diligence

An effective Cyber Risk Due Diligence assessment is structured to take into account the healthcare market segment the target operates in and the ecosystem of partners and third-party vendors that can impact the business. This due diligence should be an actual assessment of current cyber risk, identifying gaps and delivering a plan of action for elevating the overall security risk posture to required benchmark standards.

The Pre-Acquisition Cyber Risk Gap Assessments

Taking a deep-dive assessment of a target should include:

- Security posture (e.g., 405(d) HICP, NIST CSF or ISO 27001 baseline maturity)
- Vulnerability and patch management practices
- Incident history and disclosure practices
- Regulatory exposures (e.g., HIPAA, CCPA, GDPR)
- Third-party/vendor risk management (Compliance and Business Associate Agreement Requirements)
- Cloud security controls (especially for SaaS and PaaS platforms)
- Data and Privacy Protections
- Cyber Resiliency and Business Impact Analysis
- Policy and Procedures for Security and Compliance

Cyber Risk Due Diligence goes beyond IT, giving Investors the visibility needed to understand risk and action-oriented reporting to support remediation.

The Clearwater Cyber Risk Benchmark report for Private Equity highlights how key market segments with strong private investment are progressing toward 405(d) HICP standards—and where they may be falling short. For example, here is a summary across all of the organizations where improvements could be made for Data Protection & Loss Prevention:

Data Protection & Loss Prevention

- Weak data classification and handling policies increase exposure to breaches.
- Inconsistent encryption practices leave sensitive data vulnerable in transit and at rest.
- Limited insider threat monitoring fails to prevent accidental or malicious data loss

- Find the full report at: **Clearwatersecurity.com/Healthcare-PE-Cyber-Risk-Report**

Post-Acquisition Cybersecurity and Compliance Action Plans

After close, many PE firms apply a standard cyber uplift program addressing the cyber risk gaps, or elevating the cyber maturity of the organization to meet desired security or compliance goals tied to the acquisition investment plan.

Post-Acquisition Action Plans May Include:

- 30–60–90-day remediation plans based on cyber gap assessments
- Enhanced security control implementation (MFA, endpoint, logging, IR) and ongoing management.
- Consolidation and security efficiency program if acquisition is a roll-up investment with other like organizations.
- Risk management and remediation tracking along with board reporting and oversight
- Compliance readiness: HIPAA, SOC 2, HITRUST, PCI DSS, etc.

Delivered by industry-leading healthcare experts, Clearwater's Security and Compliance programs can assist in every aspect of the post-acquisition action plan:

- Managed endpoint security, log management, vulnerability scanning and remediation support, 24/7 threat detection and response
- Cloud migration and management in Azure with M365 services and 24/7 security and compliance management, and cloud security posture management with remediation response
- vCISO, Privacy and Compliance staff assistance or training
- Clearwater Certified Assessments for HITRUST, HIPAA, PCI-DSS, NIST 800-171, SOC2
- Technical security services including penetration testing, web and application testing

Another risk that comes with mergers and acquisitions is losing key cybersecurity talent. KPMG research[1] shows employee turnover almost doubles after an acquisition is announced. Being in high demand, those responsible for the security of these companies, even CISOs, may swiftly exit, leaving organizations without the necessary security leadership or talent to perform security management.

Cybersecurity KPIs for Portfolio Monitoring

Operational KPIs should align to unique organizations but also roll-up so there is a consistent view of current security posture and cyber risk across all of the PE portfolio companies.

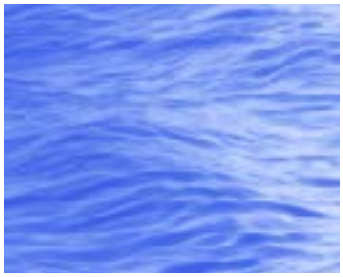
Cybersecurity KPIs:

- Percentage of assets with MDR/EDR coverage
- Incident detection/response SLAs
- Tracking of high/critical findings from vulnerability scans & pen tests
- Patch management timelines
- Privileged access & identity control logging
- Ransomware resilience/readiness score
- Incident Response testing
- Phishing simulation results

(1) https://assets.kpmg.com/content/dam/kpmgsites/dk/pdf/2023/dk-talent-flight-overlooked-risks-during-m-a.pdf.coredownload.inline.pdf

Cyber maturity is often reported quarterly to the board, investment committee, and partners. However, these KPIs are not necessarily the best metrics to understand the overall cyber risk to an organization, especially in healthcare as the number of cyberattacks continues to grow.

Clearwater can customize the appropriate security and risk metrics across multiple portfolio companies, so you have a unified view of the current state and the risk remediation plan for improvements. Leveraging our 405(d) Assessment services and our ClearAdvantage managed services program, you can customize the resources and reporting needed to instill confidence in the security maturity across your portfolio companies.

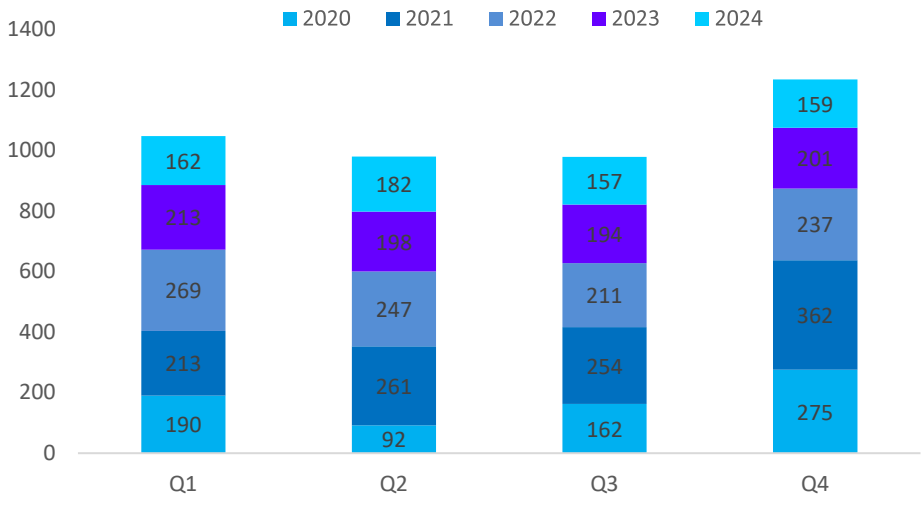


Cybersecurity as a Value Differentiator for Exit Strategies

As markets cool, both buyers and sellers face a shrinking pool of high-quality assets and partners. This increased competition is driving greater emphasis on identifying cyber risk gaps and strengthening cybersecurity maturity—factors that can significantly enhance a company's valuation and deal outcomes during due diligence. Investors and operators are hyper-focused on when they are preparing to exit, to ensure there is no unforeseen risk or uncertainty that could slow down or kill a deal. Firms are moving toward outsourcing assessments to experts to either identify gaps earlier on before launching a process to allow for time for remediation or at least identifying the gaps upfront for prospective buyers.

The Extended Healthcare Investor Challenge

With the hope of better economic conditions as well as reduced industry headwinds, increased M&A may be on the horizon. The graph to the right shows the last five years of healthcare deals from 2020-2024 organized by quarters. The data from Pitchbook, shows deal trend pick-up during Q4 and Q1 then settling down the rest of the quarters.



Whether buying or selling, cybersecurity and risk are now key factors in private equity decisions—shaping strategy, due diligence, integration, and long-term value creation.

Common Actions that PE Firms Are Taking for their Healthcare Investments

- **Hiring specialized healthcare third-party cyber due diligence advisors**, ensuring nothing is missed when it comes to this complex and highly regulated industry.
- Requiring a **standardized security assessment framework** (405(d) HICP, NIST 800-171) across their healthcare companies with ability to view benchmarks against industry standards to assess current security maturity.
- Implementing **cybersecurity improvement plans** post-acquisition and active 24/7 threat detection.
- Mandating **incident response testing** and tabletop exercises.
- Holding **CISO-level reviews** with management teams and board members on cyber risk analysis and remediation.

Clearwater is the leader in healthcare cybersecurity, compliance and resiliency with services that go beyond cyber risk due diligence. We know the industry and have been integral partners with PE firms as they consider their investment strategies and value protection across their diverse healthcare portfolio companies.

To learn more about how a customized PE Playbook for Healthcare Cybersecurity Diligence might look for your organization, please contact info@clearwatersecurity.com

Clearwater helps organizations across the healthcare ecosystem move to a more secure, compliant, and resilient state so they can achieve their missions. The company provides a deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains, purpose-built software that enables efficient identification and management of cybersecurity and compliance risks, managed cloud services, and a 24/7 Security Operations Center with managed threat detection and response capabilities.