Clearwater

Standardizing Cyber Risk Across a Healthcare Portfolio

Introduction

Across a healthcare portfolio, cyber risk rarely presents itself in a consistent or easily measurable way.

Each organization operates independently. Technology environments evolve at different speeds. Security investments are often shaped by local priorities rather than enterprise visibility. For investors and portfolio company leadership, this creates a familiar challenge. Cyber risk exists across the portfolio, but it is difficult to quantify, compare, or manage as a unified concern.

Understanding that returns are asymmetric, with downside events having an outsized impact on IRR, this leading middle market healthcare private equity firm recognized the need for a more consistent approach. Not because cybersecurity had been ignored, but because it had not yet been standardized or consistently incorporated into their value creation strategy.

> “We were investing in infrastructure and technology to support our portfolio companies. But we needed a way to understand how those investments were being protected and how to measure that consistently across the portfolio.”

Leadership was looking for a shared language. One that could bring together technical teams, operators, and investors around a common understanding of risk, progress, and priorities.

To do that, the firm partnered with Clearwater.

Establishing a Common Framework for Measurement

With the need for a consistent, portfolio-wide view of cyber risk clearly defined, the next step was selecting a framework that could support that level of visibility.

The firm chose to anchor its approach in the 405(d) Health Industry Cybersecurity Practices framework.

405(d) offered a healthcare-specific model aligned to NIST standards, with clearly defined practices that could be applied consistently across organizations with varying levels of maturity. Just as important, it provided a structure that could translate technical implementation into something measurable and comparable at the portfolio level and provided a prioritized remediation roadmap for each company.

"We wanted an approach that was measurable and could be applied across our portfolio. It needed to be something that both technical and non technical stakeholders could understand and use."

This introduced a shared foundation for evaluating cyber risk across the portfolio. It allowed leadership to move beyond individual assessments and begin establishing a consistent way to measure progress, compare maturity, and align priorities across organizations.

Building a Portfolio Wide Baseline

With a common framework in place, the focus shifted to establishing a clear baseline across the portfolio.

Clearwater conducted comprehensive 405(d) assessments across a dozen portfolio companies, applying the same methodology to each organization to ensure consistency in how results were measured and interpreted.

Each company was evaluated against 142 controls spanning 10 cybersecurity practice areas, providing a detailed view of both technical implementation and policy maturity.

This established a portfolio-wide view of cyber risk grounded in a single standard.

Security Domain	Portco 1	Portco 2	Portco 3	Portco 4	Portco 5	Portco 6	Portco 7	Portco 8	Portco 9	Portco 10
Email Protection Systems	100%	100%	100%	83%	92%	100%	50%	100%	100%	100%
Endpoint Protection Systems	88%	60%	100%	61%	89%	100%	89%	100%	100%	78%
Identity and Access Management	100%	88%	100%	88%	100%	100%	100%	100%	100%	100%
Data Protection and Loss Prevention	88%	82%	92%	59%	82%	100%	18%	100%	80%	95%
Asset Management	88%	75%	100%	83%	100%	100%	100%	100%	100%	88%
Network Management	89%	64%	89%	93%	67%	94%	56%	100%	83%	100%
Vulnerability Management	100%	80%	83%	100%	100%	83%	33%	100%	100%	100%
Security Ops Center and Incident Response	86%	79%	86%	57%	93%	86%	50%	100%	100%	93%
Medical Device Security	N/A	17%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Cybersecurity Governance	83%	83%	100%	100%	100%	83%	50%	100%	83%	100%
Total Score	91%	73%	94%	81%	91%	94%	61%	100%	94%	95%

Score Legend: 90–100% 80–89% 70–79% 50–69% <50% N/A

“Each company is at a different point in their maturity. This gave us a consistent way to understand where they were and what steps were needed to move forward.”

The firm could now see how maturity varied across organizations, where gaps were concentrated, and how each company compared against the broader portfolio.

For portfolio companies, the assessments provided clarity and direction. Rather than navigating cyber risk in isolation, each organization had a defined starting point and a structured path forward.

Defining Targets and Driving Alignment

With a portfolio-wide baseline established, the next step was to define what meaningful progress looked like.

The firm introduced a clear benchmark of **85 percent alignment** across the 10 practices.

> “By setting a clear benchmark, it created an objective measure that boards and management teams could understand and work toward.”

This allowed cyber risk to be discussed in terms of measurable progress, with a common reference point across the portfolio.

At the portfolio company level, the benchmark helped shape prioritization. Early assessment findings highlighted areas where targeted improvements could have an immediate impact, allowing teams to focus on practical steps that would strengthen their overall posture while building toward broader maturity.

Over time, this approach supported steady, programmatic improvement across the portfolio.

Source: *HHS 405(d) Health Industry Cybersecurity Practices (HICP), 2023*

Measuring Progress Across the Portfolio

Across successive assessment cycles, the portfolio demonstrated measurable improvement in both technical implementation and overall alignment to the 405(d) practices.

+18%

Increase in protection against top threats

50%+

of portfolio companies at or above 85% maturity

Across successive assessment cycles, the portfolio demonstrated measurable improvement in both technical implementation and alignment to the 405(d) practices.

Key results include:

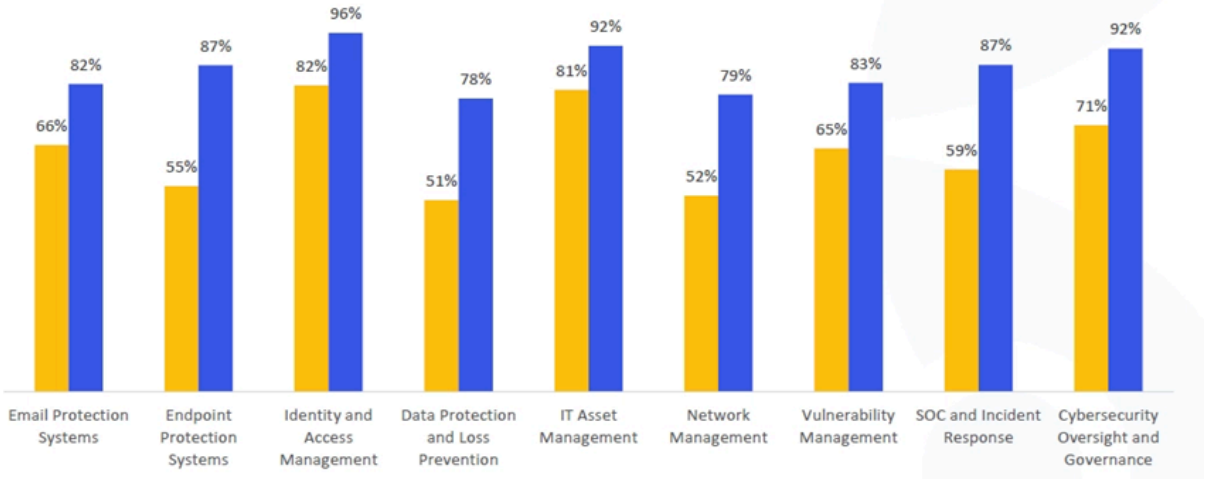
- Threat protection improved from 73% to 91%
- Essential cybersecurity performance goals increased from 84% to 96%
- Enhanced performance goals increased from 75% to 93%
- Half of portfolio companies now meet or exceed the 85% benchmark

Improvement was observed across core domains including endpoint protection, data protection, and network management.

91%

Threat protection achieved across portfolio

The improvement is reflected across all ten 405(d) practice areas, with consistent gains year over year. The data shows particularly strong advancement in identity and access management, data protection, and incident response, while more foundational areas like endpoint and network management continue to trend upward across the portfolio.



“This progress reflects a coordinated and measured approach to achieving what we see as a minimum acceptable level of sustained cyber risk management.”

This provided a clearer view into how risk was evolving across the portfolio and how targeted efforts were contributing to meaningful improvement.

Performance goals are a good way to monitor and measure progress. Reporting performance can include details such as indicators identified, data collected and SDG-related activities accomplished. Clear and concrete performance goals make it easier to generate relevant, consistent and comparable data over time, in formats that your audience can understand and appreciate.

A More Measurable Approach to Cyber Risk

Over time, this program has reshaped how cyber risk is understood across the portfolio.

What began as an effort to create consistency has developed into a more structured, measurable approach to managing risk at the enterprise level. Cyber risk is now evaluated alongside other operational and financial considerations, supported by data that enables clearer visibility into performance and progress.

“Attention to cyber risk is not an option. Being prepared for a cyber event is as essential as conducting an annual financial audit.”

As the program continues to mature, the approach is becoming more targeted. Organizations that have reached the benchmark are shifting toward ongoing validation, technical testing, and periodic check-ins to ensure controls remain effective as environments change. Others continue to build toward that level, supported by structured assessments and remediation planning.

At the same time, the firm is expanding its focus on incident response readiness and regulatory alignment, ensuring that portfolio companies are prepared not only to reduce risk, but to respond effectively when events occur.

The foundation remains consistent. Establish a clear standard, measure consistently, and support ongoing progress over time.

Clearwater partners with healthcare organizations and investors to bring structure, visibility, and measurable progress to cyber risk management.