Atumcell

Driving Portfolio-wide Value with Cybersecurity

A Roadmap for Middle-market Private Equity Firms

Contact

David E. Williams, CEO

d@atumcell.com

(617) 671-8810

atumcell.com

February 2025

Introduction

Middle-market private equity firms are poised to boost their focus on cybersecurity in 2025. LPs demand it, portfolio companies are being pressed by customers and insurers, and ev- eryone wants to avoid expensive incidents. Still, PE firms are hesitant: they're worried about being too prescriptive with portcos or are conscious that prior efforts generated friction but didn't deliver lasting impact.

PE firms can achieve a high ROI on cybersecurity spending. To do so they need a pragmatic, measurable, and sustained approach. This paper explains how to make it happen.

Atumcell

1

Start strong: Integrate Cybersecurity into Due Diligence

Cybersecurity should be emphasized throughout the investment lifecycle. It's best to identify and begin to mitigate risks during due diligence, while alerting new management teams that ongoing attention to cyber will be a priority.

Cyber risks increase as soon as a company announces an investment. That's because criminals target deep-pocketed investors. Newly acquired companies are especially vulnerable to phishing attacks, particularly when they receive messages from seemingly legitimate new contacts in the transition to new management and investors. A recent Atumcell study of 2700+ middle market PE firms and portfolio companies demonstrated that 55 percent are susceptible to phishing due to incorrect DNS configurations.

Action steps:

- Screen all platform and tuck-in acquisition targets with a quick scan to check for phishing and ransomware susceptibility, system vulnerability, and supply chain risks. Atumcell's AtumScreen is a self-service tool for this purpose.
- If the screening provides concerning results, conduct a more thorough Hacker's Perspective Assessment, including a full external vulnerability scan and comprehensive hunt for leaked credentials.
- Condition closing on mitigation of the most critical vulnerabilities, which is usually straightforward. It's important to do this before telling the world a new, deep-pocketed financial partner has arrived.

2

Onboard with a Cyber Lens

PE firms set clear, baseline expectations for financial reporting, e.g., closing the books within a set timeframe. They should strive for analogous standards with cybersecurity.

Admittedly, cyber is a little more complicated. A templated cybersecurity roadmap for the initial cyber maturity journey can help. A roadmap tool enables portfolio companies to make measurable progress and lets PE firms compare cybersecurity performance across the portfolio.

This is simpler for PE firms that invest within a single industry with a standard certification framework, such as HITRUST or ISO27001. It's harder for multi-sector investors, whose companies may encounter many frameworks. However, frameworks have common, core attributes. All start with compiling an asset inventory, for example.

Action steps:

- Establish clear baselines for cybersecurity, e.g., patching critical vulnerabilities. within 72 hours, fixing domain settings to eliminate spoofing.
- Institute quarterly reporting on key metrics.
- Introduce a roadmap tool, such as the one offered by Atumcell.
- Set an expectation for when the initial maturity roadmap must be completed.

3

Make Cyber Metrics Part of the Value Creation Plan

PE firms should integrate cyber performance into value creation plans, ensuring cyber is treated as an important priority alongside product, finance, and operations. In addition to preventing ransomware and enhancing business continuity, strong cybersecurity enables portfolio companies to land and retain larger, more sophisticated customers, build partnerships, and lower insurance premiums. The value can be quantified and measured against cyber investments.

Cybersecurity must be embedded into every aspect of digital transformation, ensuring systems and processes are secure by design. This is particularly critical when developing new web applications or adopting cloud-based systems, both of which are typical initiatives for portfolio companies in the middle market.

Action steps:

- Set measurable goals, such as reducing turnaround time for patching vulnerabilities or achieving compliance with a specific standard.
- Implement secure development lifecycles (SDLC) that prioritize encryption, input validation, access control, and regular penetration testing.
- Present cybersecurity updates in a consistent framework and slide format at every board meeting. This ensures comparability and accountability across the portfolio.
- Use benchmarking data to identify and learn from top-performing portfolio companies.

4

Boost Exit Premiums With Strong Cyber Performance

Strategic and financial buyers increasingly prioritize cybersecurity during due diligence. PE firms should perform diligence on their own portfolio companies before exit, just as they would when acquiring a new business. This is an opportunity to identify and fix vulnerabilities before they slow down or kill the sale.

Action steps:

- Document and present cybersecurity improvements as part of the value creation story, especially for attracting new customers.
- Showcase certifications, compliance achievements, and incident-free records.
- Conduct a Hacker's Assessment of the company to pre-emptively identify issues likely to be uncovered during diligence.

5

Lead by Example: Secure the PE Firm Itself

PE firms that subject themselves to the same or higher cybersecurity standards as portfolio companies set a strong example, gain insights that can be applied across the portfolio, and become more attractive partners for LPs and companies. This includes regular external and internal vulnerability scanning, penetration testing, and progress on the security maturity roadmap.

Action steps:

- Conduct regular assessments of the firm's own systems, focusing on areas like vulnerability detection and mitigation, domain spoofing, and third-party vendor risk.
- Compare results with portfolio companies and industry peers to uncover insights and opportunities for improvement.
- Share performance with portfolio companies to demonstrate accountability and reinforce the importance of cybersecurity.

Take the Next Step:

Secure Your Firm and Portfolio

2025 is the year to move beyond awareness and take effective action to build value through cybersecurity. Contact Atumcell CEO, David Williams d@atumcell.com to learn how we can help your firm and portfolio companies achieve impressive results.

(617) 671-8810

atumcell.com