Hilco Global
Asset Smarter

SMARTER PERSPECTIVE: CYBERSECURITY

The Cybersecurity Imperative: Table Stakes and Competitive Advantage in Distressed Lending

By Robert Gorin, Alexander Niejelow, and James Wolf

February 2026

Can your credit survive a cyberattack?

For distressed companies, the answer increasingly determines whether a turnaround succeeds or fails. According to the National Bureau of Economic Research, cyberattacks involving theft of personal or financial information correlate with negative stock-market reactions, decreased sales growth, increased leverage, downgraded credit ratings, elevated bankruptcy probability, higher cash-flow volatility, and decreased firm value.[1] Meanwhile, Moody's has established that cyber-risk profile now constitutes a core input to credit analysis.[2]

For companies already navigating financial challenges, these consequences can prove catastrophic. When you're operating on thin margins, managing strained vendor relationships, and working to maintain customer confidence, a significant cyber incident may be the last straw.

Yet cybersecurity due diligence and monitoring in private credit remains inconsistent, presenting both a significant risk and a missed opportunity for lenders working with distressed companies. Let's talk about how to change that.

Why Distressed Companies Face Heightened Risk

When companies experience financial

distress, their challenges often become public—bankruptcy filings, workforce reductions, and statements about the current state of affairs. This visibility puts a target on their backs, making attacks more likely to occur at the worst possible time: when resource constraints and budget cuts leave them with the least capacity to respond effectively.

The data bears this out. Many distressed companies face circumstances similar to what researchers call "high uncertainty" environments—fluctuating demand, supply chain disruptions, macroeconomic volatility. According to PYMNTS Intelligence's 2025 Certainty Project, mid-market companies in such environments experience severe consequences as the result of cyber impacts: 81% saw stalled innovation, 38% suffered revenue losses, 31% had difficulty fulfilling client orders, and 19% struggled to maintain profit margins.[3]

The Cost of Cutting Cyber Budgets

Here's where things get particularly problematic. Despite these risks, IT and cybersecurity expenses are often first on the chopping block when companies need to cut costs. It's understandable—these expenses aren't seen as immediate revenue generators, and cash is tight. But this decision creates a stressful spin cycle: with limited resources, technical teams become consumed with reactive measures rather than proactive initiatives, keeping companies stuck—or worse.

The Petersen Health Care case illustrates this dynamic. The nursing home operator, already facing long-standing financial difficulties, filed for Chapter 11 bankruptcy in March 2024. A 2023 ransomware attack that disrupted its billing systems, making it "incredibly difficult" to bill customers and insurers, created a cash flow crisis that contributed directly to pushing the

company over the edge into bankruptcy.[4]

For lenders, this creates a troubling dynamic: the very cost-cutting measures meant to preserve cash may inadvertently increase the risk of cyber incidents that destroy the value you're protecting.

But here's the good news: Forward-thinking lenders are finding that thoughtful cyber program management doesn't just mitigate risk—it can actually accelerate turnarounds by freeing up resources for growth rather than crisis management.

Cybersecurity as Turnaround Enabler

Let's flip the script for a moment. Instead of thinking about cybersecurity as just a defensive measure, consider its potential as a turnaround enabler.

The numbers tell a compelling story. The global average cost of a data breach in 2024 reached $4.88 million—the highest ever recorded. It takes an average of 258 days to detect and contain a breach. That's nine months of exposure. Companies with no formal incident response plan pay 58% more per breach than those with structured protocols. Yet only 35% of businesses run cybersecurity tabletop exercises, even though simulations significantly improve response times.[5]

Think about what nine months of dealing with the fallout of a cyber incident means, from operational disruption to customer communication and compliance burdens, for a distressed company racing to execute a turnaround strategy. It could be the difference between recovery and liquidation. The additional 58% cost premium for companies without response plans represents funds that could otherwise finance critical operational improvements or debt service.
But strong cyber programs do more than just prevent these losses. They build stakeholder trust—the currency that keeps distressed companies alive during difficult transitions. Trust translates into tangible benefits: customers feel that their data is secure, partners don’t need to worry about business continuity, and creditors can feel safe about their capital. Companies with robust cyber foundations can move decisively on new products, technology partnerships, transactions, and critical decisions without getting bogged down in vendor security assessments or lengthy due diligence processes, all of which are critical to a smooth restructuring.

This means that when you're evaluating a borrower's cyber posture—whether during initial due diligence or ongoing portfolio monitoring—you're not just checking a box on risk management. You're assessing whether the company can actually execute on the growth strategies that your capital is meant to enable.

Smart Covenants: What Forward-Thinking Lenders Consider

So how do you actually incorporate these insights into your lending practice? You have several tools at your disposal—from enhanced due diligence processes to ongoing portfolio monitoring and active engagement with portfolio companies on their cyber programs. For new deals, covenant structures offer another lever. While cyber-focused covenants aren't yet standard in private credit agreements, they represent sophisticated risk management for distressed lending situations, where every risk factor compounds and margins for error are razor-thin.

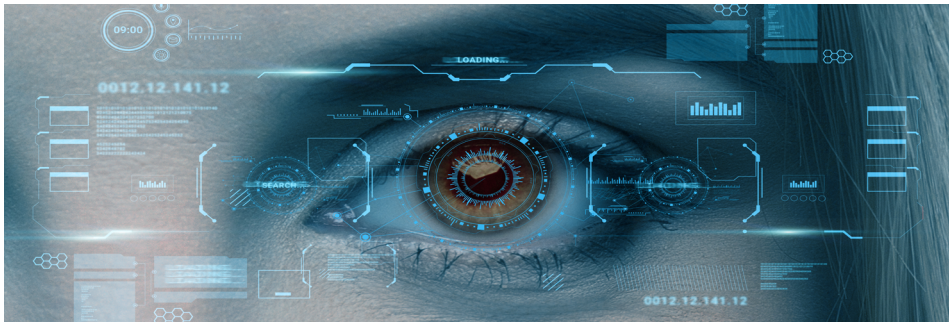
The business case is straightforward. First, the cost of cyber incidents for distressed companies far exceeds the cost of implementing basic protections. Second, distressed companies often cut cyber budgets precisely when cash tightens—exactly the moment when maintaining these protections matters most. Third, in an increasingly competitive fundraising environment, demonstrating sophisticated risk management that doesn't add excessive friction to deal flow could become a meaningful differentiator.

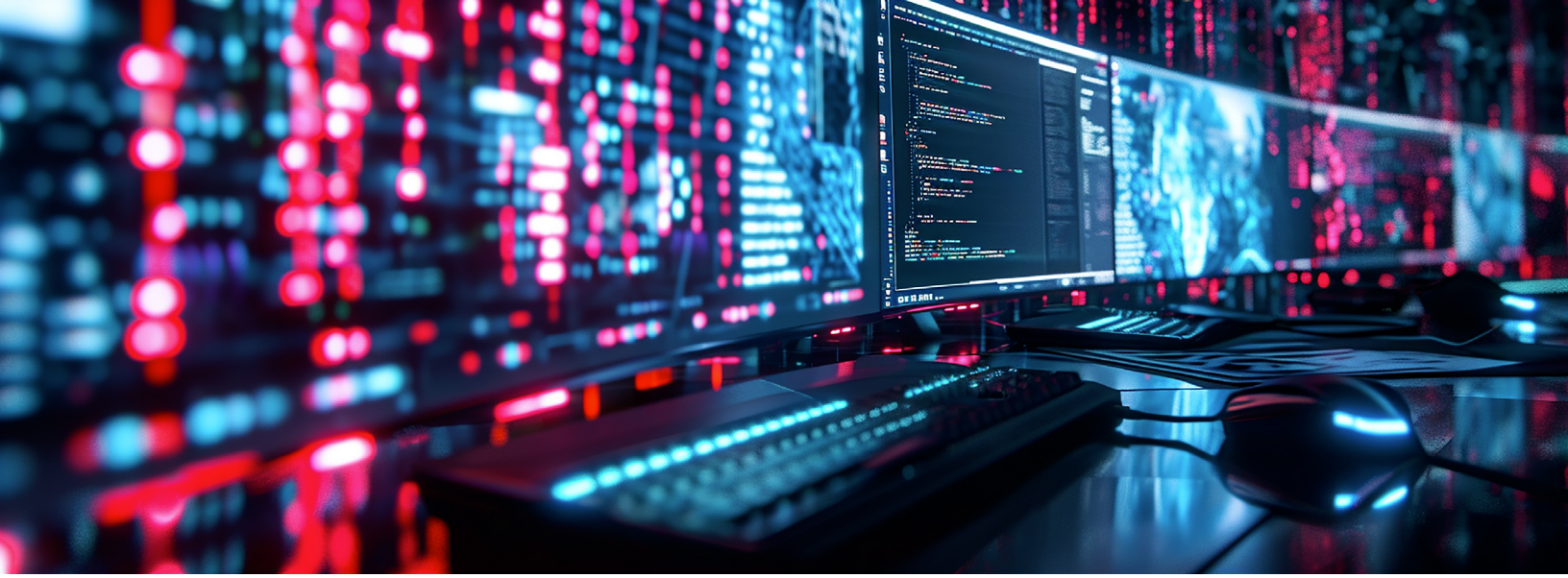
Most importantly, cyber requirements align with a broader principle you already understand: distressed companies require strategic investment to recover successfully—whether in people, processes, partnerships, or technologies. This is exactly why Chief Restructuring Officers are often mandated by lenders in turnaround situations. Cyber should be viewed through the same lens: as a business enabler with demonstrable return on investment, not merely as a cost center to be minimized.

What Comprehensive Covenants Might Include

What would a thoughtful cyber covenant actually look like? Here are the key elements to consider:

- Annual Security Program Review: Requiring borrowers to document and share annual security assessments ensures ongoing attention to cyber risk rather than treating it as a one-time compliance checkbox.
- Comprehensive Cyber Insurance: Mandating appropriate cyber insurance coverage helps ensure that if incidents do occur, the borrower has resources to respond effectively without further compromising their already stressed financial position.
- Tested Incident Response Plans: Requiring tested incident response plans can dramatically reduce both the cost and duration of breaches when they occur.
- Third-Party Vendor Oversight: Given that many breaches occur through vendor relationships rather than direct attacks, requiring borrowers to maintain oversight of their vendors' cyber practices helps protect against supply chain vulnerabilities.
- No Material Weakening of Security





Controls: This covenant prevents borrowers from reducing cyber protections during the loan period—directly addressing the common and problematic tendency for distressed companies to slash cyber budgets when cash becomes tight.

The Minimum Viable Program

A common objection to cyber covenants is that distressed companies simply can't afford robust cybersecurity programs. But this perspective fundamentally misunderstands both the costs involved and the benefits gained.

The risks incurred by inadequate cybersecurity programs cost far more than implementing basic protections: cyber insurance, periodic assessments, and tabletop exercises. Much of cyber resilience actually centers on following strict procedures and policies—measures that don't require significant capital investment but dramatically reduce risk.

What does a "minimum viable" cyber program look like for a distressed borrower? It should include basic access controls (including multi-factor authentication), a documented incident response plan, regular employee training, appropriate cyber insurance coverage, and clear governance structures that establish who owns cyber responsibility at the leadership level.

These measures don't require massive capital outlays, but they dramatically reduce both the likelihood of incidents occurring and the costs when they do. That's a return on investment that makes sense even—especially—for companies operating under financial constraints.

Critical Indicators for Due Diligence and Ongoing Monitoring

What should you actually be looking for when conducting cyber due diligence on a distressed company—and when monitoring your existing portfolio? These indicators reveal whether a company has adequate cyber foundations to protect both their assets and your investment. These components can change as business situations evolve, making it imperative to keep an eye on them for borrowers both before and after capital has been deployed:

- Governance & Oversight: Is there a clear assignment of cyber responsibility at the C-level, with cyber treated as a strategic business issue rather than just an IT function? Or does the company lack a formal program or leadership accountability for cyber issues?
- Incident Transparency: Companies that openly disclose past or active cyber events demonstrate both honesty and organizational maturity around security issues. On the flipside, discovering undisclosed incidents during diligence or portfolio review raises serious questions about both security posture and management transparency.
- Access Controls: Strong foundations include multi-factor authentication, regular password updates, and least-privilege principles consistently applied. Meanwhile, fundamental weaknesses like absent password policies or lack of basic access controls leave the company vulnerable even to unsophisticated attacks.
- Risk Management: Regular security assessments and tabletop exercises demonstrate active, ongoing improvement rather than static compliance. Missing incident response plans, disaster recovery procedures, or any evidence of testing and preparation represents real risk.
- Financial Protection: Cyber insurance should be aligned with the company's specific risk profile, providing adequate coverage for realistic threat scenarios. On the other hand, having no financial backstop in place means any significant incident will compound the company's financial distress.
- Recovery Capability: Tested backup procedures enable recovery from incidents without paying ransoms or losing critical data, whereas untested or nonexistent backup systems mean a ransomware attack could be catastrophic.
- Human Factors: Regular security awareness training helps reduce the human error that causes many breaches. Untrained staff remain vulnerable to phishing, social engineering, and other common attack vectors.

For distressed companies specifically, pay particular attention to whether cyber practices have been maintained despite cost-cutting pressures. If a company has preserved these protections even

during financial stress, it signals that management understands the strategic importance of cyber resilience—and that's a positive indicator of their overall business judgment. Conversely, if you notice deterioration in these areas during ongoing monitoring of portfolio companies, it may signal broader operational challenges that warrant closer attention.

The Path Forward

The broader context here matters. The regulatory landscape is actively shifting. The SEC's 2025 Exam Priorities established information security and operational resiliency as critical themes requiring attention beyond simple compliance checkboxes. The Regulation S-P amendments introduced specific requirements for safeguarding data and responding to cyber incidents.[6]

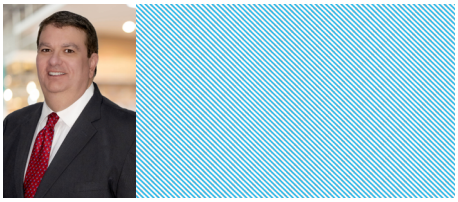
These regulatory pressures increasingly affect private fund managers. While Limited Partners don't currently mandate cyber-risk oriented covenants in deals, the writing is on the wall. More importantly, thoughtful covenant crafting around cyber resilience simply represents best practices for protecting your credit, regardless of whether LPs eventually require it.

For distressed lending specifically, incorporating cyber considerations into your due diligence processes and ongoing monitoring just makes practical business sense. The credit managers reading this likely have businesses in their portfolios to whom they've already loaned money—companies they may be actively supporting through turnarounds. Understanding and monitoring these companies' cyber programs matters just as much now as it would have during the initial diligence phase, perhaps even more so as financial pressures mount.

The lenders who effectively incorporate cyber hygiene into their practice will achieve several competitive advantages. This isn't just about risk management, though that alone would justify the effort. It's about competitive advantage in an increasingly crowded market.
The question for distressed lenders isn't whether cyber considerations matter—it's abundantly clear that they do. The real question is whether you'll proactively incorporate these considerations into your due diligence and turnaround planning now, while it still represents a differentiator, or wait until a cyber incident at one of your portfolio companies forces the issue in the most expensive way possible.

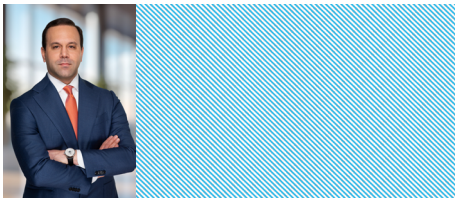
Sources:

[1] *National Bureau of Economic Research*
[2] *Moody's Investors Service*
[3] *PYMNTS Intelligence*
[4] *In re Petersen Health Operations, LLC*
[5] *JumpCloud*
[6] *Silver Regulatory Associates*



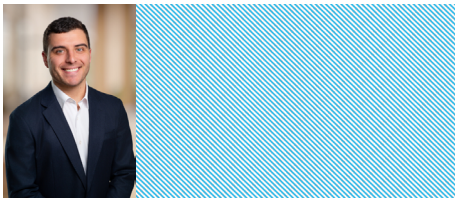
ROBERT GORIN
EXECUTIVE DIRECTOR - RESTRUCTURING
PROFESSIONAL SERVICES

Robert can be reached directly at rgorin@getzlerhenrich.com



ALEXANDER NIEJELOW
EXECUTIVE DIRECTOR
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Alexander can be reached directly at ANiejelow@hilcoglobal.com



JAMES WOLF
DIRECTOR
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

James can be reached directly at JWolf@hilcoglobal.com