TRENDS IN CYBER

Protecting Collateral Liquidity Through Cyber Operational Resilience

BY ALEXANDER N.M. NIEJELOW AND DOUG JUNG

Asset-based lending (ABL) is built on the premise that if a borrower is unable to repay its loan, the cash conversion of the collateral is there. But in a cyber incident, collateral may remain "there" but visibility to the lender's collateral and its quality disappears. If a borrower can't ship, can't invoice, or can't produce a trustworthy borrowing base for even a few days, collateral proceeds and AR/ inventory mix will change significantly, with the resultant impact on the borrowing base leaving the Lender in the dark as to their collateral vis-à-vis their loan exposure

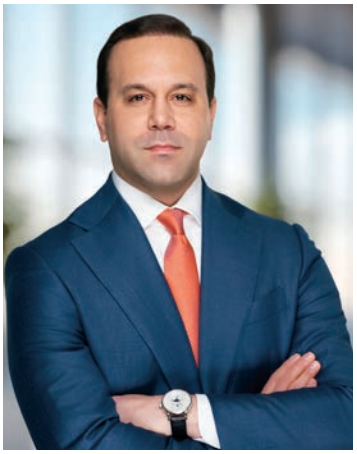
As a result, cybersecurity incidents are no longer peripheral technology problems, they are increasingly the fastest path to major operational issues, losing visibility to collateral details, impairment and liquidity stress.

Axiomatic to ABL is the lender's collateral. And possession or unfettered access to collateral is 9/10th of the law. The field exam, or collateral diligence has traditionally been the cornerstone of ABL underwriting and portfolio management, designed to diligence a variety of areas, including:

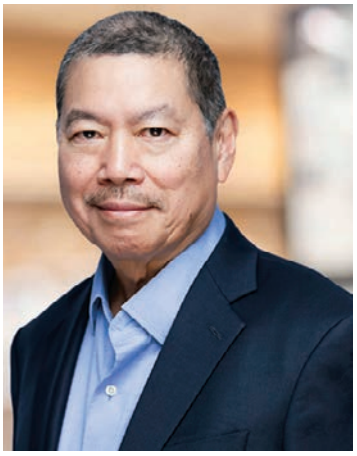
- Determine that the borrower's working capital management is commercially reasonable
- Assess whether bookkeeping and accounting for the collateral and items affecting collateral are accurate and reasonably reflect economic reality
- Identify practical issues to successful cash conversion, substance over form
- Ensure that the borrowing base reflects the lender's collateral with all the agreed upon calculations for ineligibles, reserves and advance rates. And importantly that no other ineligibles or reserves should be in place.

What has changed, however, is the operating environment that underpins that collateral. Today's borrowing base is increasingly digitally dependent, relying significantly on a variety of technologies to manage a business e.g., manufacturing, customer fulfillment activities, inbound and outbound logistics, electronic invoicing, cash application tools, key reporting inputs such as AR agings and inventory perpetuals, third-party service providers that sit between the borrower and its customers.

While many of the risks field exams evaluate remain the same, those risks now coexist with a new category of exposure that can rapidly disrupt collateral integrity: operational interruption driven by cyber events. For lenders, this shift has important implications: a cyber risk assessment performed in conjunction with the field exam should no longer be an optional enhancement; it is an essential evolution of collateral due diligence.



ALEXANDER NIEJELOW
Hilco Global



DOUG JUNG
Hilco Diligence Services

Why Cyber Risk Is Fundamentally an ABL Liquidity Risk

ABL structures, and borrowing bases, in particular, are designed to flex with working capital. But they also assume that the working capital cycle, with competent and proper management, can continue to function, even under pressure. Ransomware, destructive malware, credential compromise, IP theft, and third party outages do not have to permanently destroy data to substantially impact collateral. A few days of disruption during a peak shipping cycle can stall invoicing, increase disputes, delay collections, and materially weaken the borrowing base often before financial statements show any deterioration. Cyber incidents break that assumption in predictable ways:

Inventory exists, but can't move: Production shutdowns, warehouse system failures, or logistics outages can cause fast turn inventory to stock out and slow-moving inventory to further age out. From a lender's perspective, inventory that cannot be processed or shipped cannot be converted into AR and ultimately, cash.

Invoicing and receivables formation slow down: If systems required to pick customer orders and ship goods or generate invoices are unavailable, or if data integrity is in doubt borrowing base integrity collapses, eligible receivables simply stop forming, even if demand remains strong. Service levels drop, increased mis-picks and mis-ships with the resultant customer dissatisfaction or worse permanent or long-term loss of customers– affecting AR dilution, cash collection timing/levels and sales lasting well beyond the remediation of the

cyber issue.

Emergency spending accelerates: Incident response costs, expedited freight, system rebuilds, legal and regulatory expenses, often create immediate and unplanned cash drains. And customer remediation efforts will increase both dilution and past dues thereby deteriorating collateral quality.

Operational Resilience: The Missing Link Between Cyber and Credit

Cybersecurity discussions often focus on prevention: firewalls, endpoint protection, training, and patching. Those controls matter, but for lenders, operational resilience matters more. Resilience is the borrower's demonstrated ability to continue or rapidly restore critical operations during disruption.

In ABL terms, operational resilience answers practical questions lenders care about:

- How quickly can the borrower resume shipping and invoicing?
- Can the borrower produce reliable AR Agings and inventory perpetuals and related reports during an outage, even manually?
- Are backups tested and prioritized for critical functions?
- What third party dependencies exist?
- Has the borrower's transactional accounting and finance team been meaningfully involved in incident response planning?

A borrower with strong cyber hygiene but weak recovery capabilities may still experience a prolonged liquidity event. Conversely, a borrower with well tested recovery processes and clear operational fallbacks may sustain collateral performance even through a significant incident. The difference is resilience, and it is measurable!

A Competitive Advantage for ABL Lenders

ABL has long delivered strong loss performance because of its discipline: constant collateral monitoring including field exams, early warning signals, and rapid intervention when metrics deviate. In a market where operational disruption is increasingly the catalyst for financial distress, lenders that can evaluate and price collateral resilience, not just collateral value, will make better credit decisions, intervene earlier, and preserve capital more effectively.

Conclusion

Cyber risk has become a first order driver of borrowing base reliability because it directly threatens the systems and processes that create, operationalize, and monetize collateral.

Conducting a cyber risk assessment in conjunction with the field exam, focused on operational resilience and collateral to cash continuity, allows lenders to see liquidity risk before it materializes—and to structure accordingly. In today's environment, that is not merely prudent. It is the next standard of care for sophisticated ABL platforms.

Alexander Niejelow is executive director of Cyber Security in the Professional Services division at Hilco Global, where he advises clients on cybersecurity risk, fintech, and digital policy. He previously served as Deputy Superintendent for Innovation Policy at the New York Department of Financial Services, leading initiatives on artificial intelligence and emerging financial technologies.

Alex has also held senior leadership roles at Mastercard, including senior vice president for Cybersecurity Coordination and Advocacy, and served in multiple federal government positions, including on the White House National Security Council. He began his career at Paul, Weiss, Rifkind, Wharton & Garrison LLP. Alex holds a JD from the University of Pennsylvania and a BA from Duke University.

Doug Jung is the CEO and senior managing director of Hilco Diligence Services, a division of Hilco Global. With over 35 years of experience in asset-based lending, Doug is a seasoned financial professional with deep expertise in diligence, field exams, audit, credit, advisory, and forensic investigations.

Doug founded and built the Diligence Services team at Hilco, which now includes professionals in both the U.S. and the UK. His team performs ABL field exams, fraud and forensic reviews, and deal-specific diligence for lenders, private equity firms, and advisors. He is widely recognized for his leadership in the field and was inducted into the Secured Finance Network's Hall of Fame in 2022.

Examples of Cyber Incidents Relevant to the ABL Space.

- **The Clorox Company (August 2023):** Manufacturing and distribution operations crippled for nearly a month with $380M in total losses.
- **Marks & Spencer (April 2025):** Cyberattack shutdown online orders and Click & Collect services across 1,000+ stores. Significant financial losses estimated at $360 million and substantial inventory disruption.
- **65% of manufacturing organizations were hit by ransomware in 2024**, with mean recovery costs of $1.67M per incident and that's before accounting for borrowing base impairment, covenant stress, or lender notification obligations. Global ransomware attacks on critical sectors surged 34% in 2025, with manufacturing seeing the sharpest growth at 61% year-over-year.