Del. Blackbaud Ruling Signals A New Era For Cyberinsurance

By **Steven Teppler and Jade Davis** (March 30, 2026)

Steven Teppler

Jade Davis

What happens when your third-party vendor gets hacked, and you end up footing the bill for the cleanup?

A Feb. 13 Delaware Supreme Court ruling just sent a powerful message to the cyberinsurance industry and its customers. In the landmark case Travelers Casualty and Surety Co. of America v. Blackbaud Inc., the court revived a $2.1 million subrogation lawsuit involving 97 cyberinsurance policyholders.[1]

The February decision does not look, at first glance, like a landmark ruling. It reads like a procedural correction — an appellate court reminding a trial court that Delaware remains a notice-pleading jurisdiction, not a federal plausibility forum.

But to view the decision as merely a pleading case is to miss the far more consequential signal embedded in its reasoning: Cyberinsurance is moving into a second maturity phase, one in which insurers will increasingly attempt to recover their payments from vendors, and in which insureds will face new pressure to justify, defend and sometimes litigate the scope of their cyber incident reimbursement.

Background

The case arose from Blackbaud's 2020 ransomware event. In 2020, a cyberattacker accessed software and data hosting firm Blackbaud's system for months, exfiltrating confidential customer data containing sensitive personal and financial records from nearly a hundred nonprofits and educational institutions. The attacker threatened to publish the data unless Blackbaud paid a ransom.

Blackbaud initially downplayed the incident, only later admitting in a September 2020 Form 8-K filing that "the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords."

The fallout was severe. In 2023, Blackbaud paid $3 million to the U.S. Securities and Exchange Commission, $49.5 million to resolve state law claims from 49 states and the District of Columbia, and $6.75 million to resolve claims from California.

The insured nonprofit and educational entities responded with forensics, legal analysis, notification, customer communications, credit monitoring and compliance-driven remediation. Their insurers paid substantial amounts for these costs and then sought recovery through subrogation and assignment claims against Blackbaud.

Four cyber insurers provided coverage to 97 of Blackbaud's educational and nonprofit clients. Philadelphia Indemnity paid more than $600,000; Travelers Casualty paid more than $1.5 million. After compensating insureds, the carriers exercised their subrogation rights to pursue recovery from Blackbaud.

A Procedural Decision With Structural Consequences

The insurers sued as subrogees and assignees of 97 insured clients under Blackbaud's solutions agreements, governed by New York law. These agreements contained commitments to: maintain administrative, physical and technical safeguards; protect against unauthorized access; maintain commercially reasonable information security procedures; implement written policies and breach response planning; mitigate negative consequences from breaches; and provide timely notice.[2]

The Delaware Supreme Court held that the insurers met Delaware's notice-pleading standard by identifying the affected policyholders, pointing to materially identical service agreements, and alleging specific security and breach-response failures. The insurers alleged that Blackbaud failed its obligations by: ignoring warnings about vulnerabilities in remote desktop access; maintaining unencrypted sensitive data on obsolete servers; failing to patch systems; disregarding internal security warnings; failing to implement multifactor authentication; and retaining data longer than necessary.

The court emphasized that liability and damages are questions for trial, not grounds for early dismissal.

This signals to carriers that pleading-stage gatekeeping mechanisms many defendants rely on — particularly "individualization" demands and "proximate cause is too attenuated" arguments — may not reliably kill subrogation claims before discovery.

And in cyber litigation, discovery is the battlefield.

Why Subrogation Has Been a Cyber Backwater

Historically, equitable subrogation has been underutilized in cyberinsurance for practical reasons. Losses are distributed across many insureds with different systems, regulatory footprints and response strategies. Even when stemming from a single vendor breach, defendants argue that causation and damages are too individualized to litigate collectively.

The Delaware Superior Court attempted to require individualized identification of harmed parties, drawing on cases involving healthcare entities recovering costs from tobacco defendants. The Delaware Supreme Court rejected that analogy, distinguishing those cases as involving amorphous claimant groups and individualized harms, whereas Blackbaud involved a defined set of insureds, identical contracts and shared breach allegations from a single event.

This distinction effectively tells carriers: If you can identify your insureds, tie them to a common contract and allege common breach conduct, you need not plead every individualized data element and response decision at the complaint stage. That detail can wait for discovery. For insurers, that makes subrogation economically feasible as a repeatable strategy.

The True Stakes: Response Costs Are Heart of Cyberinsurance

The insurers sought to recover forensics expenses, outside counsel fees to determine breach notification laws, drafting and mailing notifications, vendor communications, and credit monitoring costs — the core of modern cyber claims.

These expenses routinely dominate cyber claims and are often disputed in adjustment

because they can balloon quickly and their reasonableness is subjective. A ransomware incident can generate six-figure forensic bills before determining whether data was exfiltrated. Legal analysis may require jurisdiction-by-jurisdiction assessment. Notification and credit monitoring obligations vary dramatically depending on data elements and triggered state laws.

If courts treat these expenses as foreseeable contractual damages in vendor agreements promising "commercially reasonable" cybersecurity, then cyber insurers can argue these losses should be shifted outward rather than remaining on the carrier's balance sheet.

This ruling reinforces that cyber resilience is only as strong as the weakest vendor. Even if insurers later recover losses through subrogation, insureds and carriers absorb the immediate operational and financial shock following a breach. Vendor contracts deserve the same scrutiny as insurance policies. Explicit security obligations, breach-notification timelines, cooperation requirements and insurance mandates are foundational risk controls.

From Coverage Litigation to Recovery Litigation

The last decade of cyberinsurance has been defined by coverage fights. Those fights have been particularly intense where cyber incidents overlapped with traditional lines of insurance. The NotPetya litigation wave illustrates this vividly.[3]

Merck's coverage dispute with ACE became emblematic when insurers attempted to deny coverage by framing the NotPetya cyberattack as "war" under traditional exclusions. In 2023, Merck succeeded in convincing the Superior Court of New Jersey, Appellate Division, that the exclusion did not apply. Mondelez's dispute with Zurich, ultimately settled in 2022, similarly exposed the reputational risk of insurers stretching war language to cyber incidents that did not fit traditional warfare paradigms.

These cases resulted in a market correction. Carriers rewrote war exclusions, introduced state-sponsored attack endorsements and tightened systemic event language. But more importantly, they showed insurers that coverage litigation is expensive, unpredictable and can produce precedent undermining underwriting assumptions.

Blackbaud points toward a different strategy: Instead of denying coverage broadly and risking backlash, insurers may pay claims surgically and then seek vendor recovery. The insurer becomes a litigation finance mechanism, paying first and recouping later.

If insurers believe recovery litigation is viable, they gain leverage in claims adjustment. They can take a harder line on reasonableness, pay narrower amounts, insist on documentation and causation narratives, and refuse to subsidize "over-response" expenditures by forcing insureds to justify each cost. Claims adjustment becomes negotiation, not service.

The Coming Vendor Reckoning

Perhaps the most immediate audience for Blackbaud should be software-as-a-service vendors and managed service providers. The court may have clarified insurers' rights, but it has also raised the stakes for vendors. As subrogation becomes more credible, service providers will respond through contract language, pricing and risk-transfer strategies designed to push exposure back onto customers and their insurers.

Vendor security failures are no longer just reputational events. Vendors will likely respond

through tighter limitation-of-liability provisions, often capping exposure at modest multiples of contract fees — even where downstream breach costs dwarf the agreement's value. Blackbaud shows that even where damages caps exist, carriers can survive dismissal and push into discovery, which is expensive enough to reshape settlement posture regardless of ultimate liability limits.

Subrogation waivers are becoming a focal point. As insurers view recovery rights as essential, vendors may press for clauses waiving those rights entirely, shifting losses back to customers and carriers even when vendor security failures are alleged.

Some vendors may reprice cybersecurity commitments, offering faster notification or forensic cooperation only at higher service tiers, while others may narrow contractual security representations to softer, standards-based language more difficult to enforce.

The cyberinsurance industry has long worried about systemic risk: a single widely used vendor triggering thousands of insured losses. That systemic risk creates the incentive for insurers to pursue vendor recovery. If systemic vendor incidents remain unrecoverable, insurers must price premiums accordingly, exclude more risk and narrow coverage. But if insurers can shift systemic loss outward through litigation, their models change — the vendor becomes the de facto reinsurer.

These dynamics underscore that vendor risk allocation is no longer boilerplate. Contract negotiations will increasingly determine whether cyberinsurance functions as true risk transfer or merely as a short-term liquidity bridge after third-party failures.

Cyberinsurance Versus Reps and Warranties: A Crucial Distinction for Private Equity Risk Leaders

The Blackbaud ruling also highlights a critical contrast between cyberinsurance and representations and warranties insurance. In cyberinsurance, subrogation is a core enforcement mechanism tied directly to operational accountability. In private merger and acquisition transactions, by contrast, subrogation against sellers is typically waived except in cases of fraud, preserving deal certainty rather than policing ongoing performance.

Risk leaders who conflate these models may underestimate vendor exposure. Cyberinsurance and R&W insurance both transfer risk — but they allocate accountability very differently.

Private equity sponsors should require operational, time-bound vendor commitments (including rapid breach notice), push back on broad subrogation waivers and refuse fee-multiple liability caps that don't match real incident costs. Then align cyberinsurance to those contractual recovery rights.

Why This Will Resonate — and With Whom

This ruling will resonate with stakeholders who understand that cyber risk is financial and contractual, not merely technical.

Cyberinsurance executives, underwriters and coverage counsel will recognize the importance of aggregated pleading survival. Brokers will recognize the underwriting implications and coming shift in claims scrutiny. Corporate information security officers and corporate counsel will recognize the operational consequence: more documentation demands and disputes about reasonableness. Boards and audit committees will recognize

that cyber incidents are litigation multipliers, generating evidence that determines whether carriers pay in full or sue vendors, or whether vendors blame insureds for contributory failures.

Enterprise general counsel and vendor counsel — the architects of "commercially reasonable" security clauses — will recognize that provisions once treated as boilerplate now function as litigation triggers. If vendors promise to maintain safeguards and breach response plans, and a breach occurs, insurers will use those promises as the foundation for recovery.

Conclusion: The Canary's Warning

The Blackbaud ruling clarifies that even when a breach begins with a vendor, consequences land first on the organization and its insurer. Cyberinsurance remains essential, but is no substitute for disciplined vendor governance.

The Delaware Supreme Court reduced the procedural friction that has kept cyber subrogation litigation from scaling by permitting aggregated pleading where the insured group is defined, contracts are common and breach allegations are shared. It signaled that foreseeable breach response costs — legal analysis, notification, forensics and remediation — are not too remote to be treated as contract damages when cybersecurity promises are broken.

Blackbaud signals a shift toward a cyberinsurance market defined by recovery fights and governance scrutiny. Insurers may now treat vendor-caused losses as recoverable. Vendors may find the true cost lies in discovery pressure and aggregated litigation. And insureds — caught between carriers tightening reimbursement standards and vendors resisting responsibility — may face a more adversarial claims environment where governance decisions, including AI adoption practices, become central to coverage and reimbursement outcomes.

As organizations increasingly integrate AI tools into workflows touching regulated data and critical systems, insurers will treat AI governance as part of the insured's duty to maintain reasonable safeguards, creating new grounds for coverage disputes and subrogation claims.

Risk leaders should immediately reassess vendor contracts, subrogation waivers, limitation-of-liability provisions and cyberinsurance alignment. If vendor agreements were negotiated before subrogation risk became real, they are almost certainly outdated. The next era will be defined not solely by whether policies cover cyber events, but by who ultimately pays — and how aggressively each player uses litigation, contract drafting and governance to avoid being left holding the bill.

Steven Teppler is a partner at Mandelbaum Barrett PC.

Jade Davis is a partner at Shumaker Loop & Kendrick LLP.

[1] Travelers Cas. & Sur. Co. of Am. v. Blackbaud, Inc., 2026 WL 410048 (Del. Feb. 13, 2026).

[2] Id. at 1-2.

[3] Merck & Co., Inc. v. ACE American Insurance Co., No. UNN-L-2682-18 (N.J. Super. Ct. Law Div. Jan. 13, 2022).