Shumaker

MARCH 11, 2026 | PUBLICATION

Delaware Supreme Court Expands Cyber Liability Exposure for SaaS & Managed Service Providers

What the Blackbaud decision means for managed service providers (MSPs) and the clients who rely on them

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

A recent decision by the Delaware Supreme Court in *Travelers Casualty and Surety Company of America v. Blackbaud, Inc.* materially shifts the litigation landscape for cybersecurity incidents involving Software as a Service (SaaS) providers and MSPs.

Key takeaways:

- Lower pleading burden for plaintiffs (including insurers)
- Less emphasis on proximate cause at early stages
- Aggregated claims allowed across multiple customers
- Higher litigation costs and increased settlement pressure
- Expanded expectations around what constitutes "commercially reasonable" cybersecurity

Bottom line: Cyber incidents are now significantly more likely to survive early dismissal and proceed into expensive discovery.

What Happened

Blackbaud, a SaaS provider hosting sensitive donor data, experienced a ransomware attack exposing highly sensitive personal and financial information.

Its customers (nonprofits and educational institutions):

- Conducted their own investigations
- Incurred legal, forensic, and notification costs
- Submitted claims to their insurers

The insurers then:

- Paid millions in claims
- Sued Blackbaud as subrogees and assignees

The trial court dismissed the claims twice.

The Delaware Supreme Court reversed, holding that the insurers had adequately pled a breach of contract claim and could proceed.

1. Why This Case Matters (Especially for MSPs)

This decision is not just about Blackbaud—it is about how courts will treat cyber risk allocation across vendors and customers going forward.

Aggregated Claims Are Now Fair Game

What the Court Said

The Court allowed insurers to:

- Bring claims on behalf of 97 customers
- Use common allegations
- Avoid individualized pleadings at the outset

Why This Matters

For MSPs and SaaS providers, a single incident can now result in:

- Consolidated litigation

For Customers

The easier path to recovery is through:

- Insurance
- Coordinated litigation

This significantly increases claim scale and leverage.

2. Proximate Cause Is No Longer a Barrier at the Pleading Stage

The Critical Shift

The lower court dismissed the case for failure to tightly link:

- Specific contract provisions specific damages

The Supreme Court rejected that approach.

The New Standard

The Court held:

- Proximate cause is typically a fact question

- Plaintiffs only need to show a reasonable inference of causation
- Detailed causation analysis can wait until discovery or trial

Why This Is a Big Deal

This is one of the most important aspects of the decision:

Plaintiffs no longer need to prove exactly how each failure caused each dollar loss at the motion to dismiss stage. Instead, they can allege, "Your security failures led to our response costs."

Practical Impact

- More cases survive dismissal
- Discovery costs increase significantly
- Settlement pressure rises earlier

For MSPs: You will be forced into fact-intensive litigation sooner

For customers: Lower barrier to pursue recovery

3. "Commercially Reasonable Security" is Getting Defined—by Courts

The Court relied heavily on alleged failures that are increasingly viewed as baseline cybersecurity expectations.

The opinion highlights failures such as:

- Not storing sensitive data on obsolete, unpatched servers
- Lack of multi-factor authentication (MFA)
- Failure to encrypt sensitive data
- Ignoring internal security warnings
- Weak access controls enabling lateral movement
- Excessive data retention
- Failure to implement security patches
- Inadequate incident response planning

Emerging Legal Standard for MSPs & SaaS Providers

Courts are implicitly defining "commercially reasonable security" to include the following baseline expectations:

- MFA (especially for remote/admin access)
- Encryption of sensitive data (at rest and in transit)
- Patch management and vulnerability remediation
- Network segmentation and access controls
- Logging, monitoring, and detection capabilities
- Formal incident response plans
- Data minimization and retention controls

These are no longer "best practices"—they are becoming litigation benchmarks.

4. Litigation Costs Will Increase—Significantly

Because of this decision:

Cases Will:

- Survive motions to dismiss
- Move into expensive discovery
- Require:
    - Forensic analysis
    - Expert testimony
    - Contract-by-contract evaluation

For MSPs:

- Defense costs increase, even in weak cases
- Insurance carriers more likely to:
    - Subrogate
    - Aggressively pursue recovery

For Customers:

- Greater leverage in:
    - Vendor disputes
    - Contract renegotiations
    - Claims recovery

5. Courts Are Rejecting "Burden Shifting" to Customers

A key factual theme:

Blackbaud:

- Provided a "toolkit"
- Instructed customers to:
    - Investigate
    - Notify
    - Remediate on their own

The Court viewed this negatively.

Implication

MSPs and SaaS providers cannot simply push incident response downstream.

If your contracts or practices:

- Shift responsibility without support
- Delay disclosure
- Provide incomplete information

You may:

- Strengthen causation arguments against you
- Increase liability exposure

6. What This Means for Contracts

For MSPs / SaaS Providers

You should revisit:

Security Commitments

- Avoid vague "commercially reasonable" language without definition
- Align contractual obligations with actual capabilities

Limitation of Liability

- Ensure:
    - Clear caps
    - Cyber-specific carve-outs
    - Exclusions for consequential damages

Incident Response Obligations

- Clearly define:
    - Roles
    - Timelines
    - Responsibilities

Data Retention

- Limit retention to:
    - Necessary business purposes
    - Defined timeframes

For Customers of MSPs

You should:

- Demand:
    - Specific security controls (MFA, encryption, etc.)

Final Takeaways

The Blackbaud decision signals a clear trend:

Courts are:

- Lowering procedural barriers
- Increasing scrutiny of cybersecurity practices
- Allowing claims to proceed based on systemic failures

The New Reality

For MSPs and SaaS providers:

"If you experience a breach, expect to litigate—deeply and expensively."

For customers:

"You have stronger legal footing to recover costs from your vendors."

Key Risk Themes Moving Forward

- Aggregated, multi-customer litigation
- Reduced importance of proximate cause at early stages
- Expansion of "reasonable security" expectations
- Increased insurer-driven recovery actions
- Higher litigation and settlement costs

How We Can Help

We work with:

- Managed service providers
- SaaS platforms
- Enterprise customers

To:

- Align contracts with evolving legal standards
- Build defensible cybersecurity frameworks
- Navigate breach response and litigation risk
- Proactively reduce exposure before an incident occurs

If you have questions about how this decision may affect your organization or would like assistance reviewing cybersecurity-related contracts, assessing breach exposure, or aligning security practices with evolving legal expectations, please contact Jade Davis, Enisha Smith, or a member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line.

Shumaker