MEALEY'S®
Data Privacy Law Report

# Shifting Cyber Risk: The Critical Role Of Indemnification In Vendor Contracts

*By*
*Latosha M. Ellis*
*Washington, D.C.*

*and*

*Veronica P. Adams*
*Miami, FL*

*Hunton Andrews Kurth LLP*

**A commentary reprinted from the August 2025 issue of Mealey's Data Privacy Law Report**

LexisNexis®

# Commentary

## Shifting Cyber Risk: The Critical Role Of Indemnification In Vendor Contracts

**By**
**Latosha M. Ellis**
**and**
**Veronica P. Adams**

*[Editor's Note: Latosha M. Ellis (lellis@Hunton.com) is a partner in Hunton Andrews Kurth LLP's Insurance Coverage group in the firm's Washington D.C. office. She helps policyholders maximize insurance recoveries and helps clients with all of their insurance coverage needs from policy procurement and analysis to claims resolution and payment to, if necessary, alternative dispute resolution or litigation. Veronica P. Adams (vadams@Hunton.com) is an associate in Hunton's Insurance Coverage group in the firm's Miami office. Her practice focuses on complex insurance litigation and advising policyholders in insurance coverage matters. Any commentary or opinions do not reflect the opinions of Hunton Andrews Kurth LLP or LexisNexis®, Mealey Publications™.*  *Responses are welcome.]*

In today's digital world, data breaches due to vendor failures are becoming increasingly common, often resulting in costly fallout. While insurance can provide a safety net, the interaction between cyber insurance and vendor contracts is crucial for effective recovery and risk management. Vendor contracts should not be treated as mere formalities but as vital frameworks that contain specific, detailed provisions regarding data security obligations to ensure accountability and minimize vulnerabilities.

### The Consequences of Weak Vendor Contracts

Attempts to recoup costs from vendors, following cybersecurity events, increasingly underscore the critical importance of detailed contracts that clearly define cybersecurity obligations and responsibilities. This issue is also becoming a focal point during cyber insurance policy renewals. Weak subrogation cases, where insurers have covered policyholders for incidents caused by vendors but later struggle to recover those costs, have prompted insurers to adopt more aggressive underwriting practices and heightened scrutiny during renewals. Insurers are now asking about contracts between policyholders and their third-party vendors as part of the underwriting process, making inquiries to assess potential exposure. Consequently, policyholders must prioritize precise and enforceable contractual provisions with vendors—not only to enhance their chances of recovering costs after an incident but also to facilitate smoother cyber insurance renewals and potentially secure more favorable policy terms.

The Blackbaud 2020 ransomware incident illustrates the significant challenges policyholders may face in cyber incident disputes when vendor contracts are vague or poorly defined, limitations that can severely restrict recovery options and hinder efforts to recoup losses. In *Travelers Cas. & Sur. Co. of Am. v. Blackbaud, Inc.,* No. N22C-12-130 KMM (Del. Super. Ct., filed December 13, 2022) and *Philadelphia Indem. Ins. Co. v. Blackbaud,* No. N22C-12-141 KMM (Del. Super. Ct., filed December 13, 2022), several nonprofit and higher education organizations insured by Travelers and Philadelphia Indemnity incurred substantial costs related to investigating and mitigating the incident. While the insurers initially covered these expenses,

they later filed lawsuits against Blackbaud to recover the amounts paid, alleging breach of contract and negligence in an effort to recover their payments.

Ultimately, the insurers were unable to recover from Blackbaud. The court dismissed their claims, finding that the insurers failed to provide sufficient factual detail to support allegations of breach of contract or negligence. Specifically, the court noted that the insurers did not clearly identify the contractual provisions within the vendor contracts that would establish a direct link between the ransomware incident and Blackbaud's obligation to indemnify the policyholders for their incurred costs. This case highlights the serious consequences of weak or vague vendor contracts, which can leave organizations, and perhaps their insurers, without legal recourse or financial recovery in the aftermath of a cyber incident.

To proactively manage cyber risk and enhance recovery after an incident, policyholders should focus on several key measures. ***Contract review*** is essential to ensure vendor agreements include specific, enforceable cybersecurity standards that reflect the sensitivity and scope of the services provided. ***Breach notification provisions*** should establish clear timelines, cooperation requirements and audit rights to ensure that vendors promptly report incidents and provide necessary support. ***Cyber insurance alignment*** is equally important. Policyholders should consult with insurance professionals to confirm that the scope of their cyber coverage aligns with vendor obligations, and that there are no gaps or ambiguities in coverage language.

While each of these protections plays an important role, a carefully negotiated indemnification provision often serves as the contractual backbone of risk allocation, ensuring that the party best positioned to prevent or manage a cyber incident bears the financial consequences.

## Indemnification Provisions in Vendor Contracts

Indemnification provisions are a key contractual tool that allocate risk and ensure that vendors, rather than the company, are responsible for covering certain costs related to a breach or other specified event. One of the primary benefits of indemnification provisions is that they allow the contracting parties to define and tailor the scope of risk each is willing to assume in the relationship.

For example, in a relationship between a company and a third-party cloud service provider, it is more efficient and appropriate for the cloud provider to bear the risk of a cyber event affecting its own systems. This is because the provider maintains primary control over the security measures and infrastructure supporting the service, whereas the company's role may be limited to paying for and using the service. Since the provider is in a better position to implement and maintain safeguards, it is also better positioned to manage and mitigate potential losses.

Indemnification provisions play a key role in allocating these types of risks. Typically, they cover events such as breach of contract, negligence, bodily injury or death, and non-compliance with applicable laws. These provisions help protect a contracting party from damages, liabilities and legal actions that are more appropriately borne by the counterparty. Common categories of recoverable losses include judgments, settlements, attorneys' fees, costs and other related expenses. Covered liabilities may include debts or legal obligations, while "claims" often refer to third-party lawsuits. "Causes of action" encompass a broader range of legal grounds, including any claim for damages or a right to relief.

A well-drafted indemnification provision benefits both parties. For the indemnified party, it may allow recovery of losses, such as attorneys' fees, that may not be recoverable under common law causes of action. For the indemnifying party, the provision can help contain liability by incorporating risk-mitigation terms such as liability caps, materiality qualifiers and liability baskets.

Importantly, the indemnifying party's obligations are generally limited to damages that are recoverable under the contract and that arise from events expressly covered by the clause. Both the scope of recoverable damages and the definition of "covered events" can and should be negotiated and tailored to the nature of the transaction and the relative bargaining power of the parties.

## Common Pitfalls

### Understanding the Distinction Between the Duty to Defend and the Duty to Indemnify

A common mistake in negotiating indemnification provisions is failing to appreciate the distinction between the duty to defend and the duty to indemnify, two related but legally distinct obligations.

The duty to defend is typically broader. It is triggered by the allegations in a third-party claim, regardless of whether those claims have merit. In contrast, the duty to indemnify generally requires the indemnifying party to reimburse the indemnified party for actual losses, damages or other costs incurred as a result of a claim—usually after those costs have been incurred and depending on the notice and procedural requirements of the indemnification clause.

From the indemnified party's perspective, a broad defense obligation is critical. It helps avoid out-of-pocket legal expenses in responding to third-party claims arising from the acts or omissions of the indemnifying party, even if those claims are ultimately found to be unsubstantiated.

On the other hand, indemnifying parties may seek to limit or exclude the duty to defend. However, doing so typically comes at a cost: By refusing to undertake the defense, the indemnifying party may forfeit its right to assume control of the litigation. Alternatively, indemnifying parties may attempt to limit their defense obligations only to claims that are ultimately proven to have merit, a narrower and riskier position for the indemnified party.

Careful attention to these distinctions, and strategic drafting around them, is essential to ensuring the indemnification clause operates as intended.

### Inadequately Defining the Scope of Indemnification

When negotiating indemnification provisions, parties often overlook critical nuances that can significantly impact risk allocation, such as inadequately defining the scope of the provision. Most indemnification provisions require the indemnifying party to "indemnify and hold harmless" the indemnified party for specified liabilities. While these terms are often paired and interpreted together as "indemnify," the "hold harmless" obligation is distinct. It not only requires reimbursement of the indemnified party's costs but also protects the indemnified party from liability for the underlying claim, even if it arises from the indemnified party's own negligence or fault. However, some states prohibit indemnification for a party's own negligence unless explicitly stated in the contract.

Additionally, in certain states, "hold harmless" may require the indemnifying party to advance payment for covered but unpaid costs and expenses, even when recoverable damages are limited to losses. Without a "hold harmless" clause, the indemnifying party's obligation to pay typically does not arise until the indemnified party has made payment. The "hold harmless" obligation may also release the indemnified party from any related claims or causes of action brought by the indemnifying party.

### Insufficiently Defining the Indemnification Provisions

Another common pitfall is failing to clearly define the procedures for when and how parties exercise their indemnification rights and obligations. Since indemnification clauses tend to allocate risk between the parties in allowing a party to pursue certain rights, which may otherwise not be available, against another party, it is essential that it clearly describe the requisite process for indemnification. Establishing these processes brings predictability and clarity, outlining how and when an indemnified party may bring a claim and the timeframe for doing so.

For instance, indemnification clauses should clearly define the circumstances under which one party must compensate the other in connection with a cyber breach. This includes specifying the events that trigger the indemnifying party's obligations, the types of claims covered and the procedure for seeking compensation. The provision should also address any caps or limitations on liability. Typically, the indemnifying party will seek to narrow the scope of coverage, while the indemnified party will negotiate for broader language to maximize potential recovery.

Regardless of intent, both parties should ensure that the indemnification language includes clearly defined terms to avoid ambiguity and future disputes. The provision should eliminate vague phrasing and specify the conditions that trigger indemnity. For instance, if indemnification is triggered by a "loss," the contract should clearly define what constitutes a "loss" to avoid uncertainty about when the obligation to indemnify arises. Clear definitions and precise drafting help ensure that the provision functions as intended, requiring the indemnifying party to compensate the indemnified party under the appropriate, agreed-upon circumstances.

### Failure to Consider How Indemnity Might Interact With Other Contract Provisions

It is not uncommon for other provisions in a commercial contract to affect, or be affected by, the indemnification clause. Just as indemnification provisions in vendor contracts should be aligned with the language of any applicable cyber insurance policy, they must also be consistent with other provisions within the same contract. Poor drafting can result in certain rights and obligations being granted in one section of the contract, only to be contradicted or limited in another. A thorough, holistic review of the contract is essential to ensure that any right to recovery is not only clearly stated but also enforceable in light of the agreement as a whole. Accordingly, parties should closely examine related provisions to confirm they do not conflict with, or unintentionally undermine, the agreed-upon allocation of risk.

## Conclusion

Cyber risk is a shared responsibility between insurance coverage and third-party contracts, but indemnification provisions are one of the most critical tools for shifting and managing that risk. While cyber policies offer important protection, the legal system does not always hold third parties accountable, and relying solely on vendors or insurance can leave policyholders exposed. Robust indemnification clauses, paired with thoughtful contract terms and appropriate proactive and reactive risk management steps, help ensure that risk is appropriately allocated and that the insured is in the strongest possible position—both to recover losses and to secure coverage after incidents occur. ■

**MEALEY'S DATA PRIVACY LAW REPORT**
*edited by Mark Rogers*
**The Report** is produced monthly by

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: lexisnexis.com/mealeys
ISSN 2378-6892