The final fortification: using indemnification to shield your M&A investment from cyber risks

By Anjali Das, Esq., and Gregory Parker, Esq., Wilson Elser

FEBRUARY 5, 2025

In the complex landscape of mergers and acquisitions (M&A), cybersecurity and data privacy have become pivotal concerns. Cyber threats can significantly impact the value and success of a deal, leading to financial losses, legal liabilities, and reputational damage. To mitigate these risks, indemnification provisions have emerged as powerful tools in M&A agreements, offering buyers a layer of protection against unforeseen cybersecurity and privacy-related issues.

Despite thorough due diligence and comprehensive representations and warranties, some cyber risks may remain hidden or emerge after the deal closes.

This is the third article in a three-part series on cybersecurity in M&A and navigating hidden risks. The first article discussed the importance of cybersecurity due diligence (https://reut.rs/42nv3g4), and the second focused on representations and warranties (https://reut.rs/4hlq5if).

Understanding indemnification in M&A

Indemnification is a contractual mechanism where one party agrees to compensate another for any losses or damages incurred due to specific breaches or liabilities. In the context of M&A, indemnification provisions allocate risk between the buyer and seller, ensuring that the buyer is protected against certain post-closing liabilities that were not accounted for during the transaction.

When it comes to cybersecurity and data privacy, indemnification can be particularly valuable. Despite thorough due diligence and comprehensive representations and warranties, some cyber risks may remain hidden or emerge after the deal closes. Indemnification clauses tailored to address these risks can provide the buyer with recourse, should undisclosed issues surface.

Why indemnification is essential for cybersecurity risks

- Mitigating unknown threats: Cybersecurity threats are often complex and evolving. Indemnification protects the buyer from unknown vulnerabilities or breaches that were not detected during due diligence.
- Allocating financial responsibility: It ensures that the seller bears financial responsibility for certain cyber incidents, especially those arising from pre-closing activities or negligence.
- Encouraging full disclosure: The possibility of indemnification claims incentivizes sellers to disclose all known cybersecurity issues.
- Providing legal recourse: In the event of a breach or data loss post-closing, the buyer has a contractual basis to seek compensation for losses incurred.

Key considerations for drafting cybersecurity indemnification provisions

Specific versus general indemnities

A general indemnity is a broad provision that covers losses arising from breaches of representations and warranties or other general obligations in the purchase agreement. It typically applies to a wide range of potential issues but it may not address particular risks in depth. In contrast, a specific indemnity is a targeted provision that addresses particular known risks or liabilities that are typically identified during due diligence.

By proactively addressing cybersecurity risks through well-crafted indemnification provisions, buyers can protect their investments and ensure they are not unduly burdened by liabilities arising from undisclosed or unforeseen cyber incidents.

While general indemnities are useful for overall protection, they may not sufficiently address specific cybersecurity risks, which can be complex and have significant impacts. Tailored indemnities, on the other hand, may more precisely protect against particular known risks or liabilities. This is especially important when due diligence reveals specific issues that are unique or significant enough to warrant individual attention.

Defining the scope of indemnification

- Fundamental representations: Fundamental representations are essential statements in a purchase agreement that are considered so critical to the transaction that any breach is treated more severely than breaches of other representations. Buyers may insist that cybersecurity representations be treated as fundamental representations. This classification often results in longer survival periods and may not be subject to standard caps or deductibles.
- Survival periods: The survival period refers to the length of time after closing during which the representations and warranties remain in effect, and during which claims for breaches can be made. Establishing extended survival periods for cybersecurity indemnities recognizes that cyber issues may not become apparent until well after closing.
- Caps and baskets: A cap is a contractual limit on the amount of liability one party has to the other — essentially the maximum amount the seller would be liable to indemnify the buyer for breaches. A basket, on the other hand, is a threshold amount that losses must exceed before indemnification obligations are triggered. Negotiating higher caps or excluding cybersecurity indemnities from aggregate liability caps increases protections for the buyer.

Addressing known risks

- Specific risks identified during due diligence: For vulnerabilities uncovered during due diligence, buyers can request specific indemnities with distinct limitations and recovery methods.
- Holdbacks and escrows: Setting aside a portion of the purchase price can secure funds for potential indemnification claims related to cybersecurity.

Exclusions and limitations

- Materiality and knowledge qualifiers: Sellers may seek to limit indemnification obligations through qualifiers. Buyers should aim to minimize these to ensure robust protection.
- Time limits: Clearly define the time frame within which indemnification claims can be made, considering the latent nature of some cyber threats.

Conclusion

In an era when cyber threats are increasingly sophisticated and damaging, indemnification serves as the final fortification in M&A transactions. By proactively addressing cybersecurity risks through well-crafted indemnification provisions, buyers can protect their investments and ensure they are not unduly burdened by liabilities arising from undisclosed or unforeseen cyber incidents.

Indemnification is not just a contractual formality but a strategic tool that can significantly impact the dynamics of an M&A deal. Anticipating additional costs for cybersecurity enhancements post-closing may influence the purchase price, prompting adjustments to account for necessary investments in security infrastructure.

Robust indemnification provisions can affect other deal terms, such as warranties, covenants, and conditions precedent (an event or state of affairs that must occur before a contract or other obligation can take effect), as parties negotiate the allocation of risks and responsibilities. As cyber risks continue to pose significant challenges in the M&A landscape, incorporating robust indemnification clauses is critical for securing the value and success of the deal.

About the authors

Anjali Das (L) is a partner and co-chair of **Wilson Elser**'s national cybersecurity and data privacy practice. She is a recognized authority on cyber-defense, including incident response, privacy compliance and risk management, regulatory investigations and enforcement actions, and the defense of nationwide data breach class actions. She can be reached at anjali.das@wilsonelser.com. **Gregory Parker** (R) is an associate at the firm in the cybersecurity practice. He serves as privacy and breach counsel to organizations that have experienced a cyber attack. He also counsels clients on cybersecurity risk and disclosures in connection with mergers and acquisitions. He can be reached at gregory.parker@wilsonelser.com. The authors are located in the Chicago office.

This article was first published on Reuters Legal News and Westlaw Today on February 5, 2025.