The vital role of cybersecurity representations and warranties in M&A

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

JANUARY 30, 2025

In today's digital landscape, cybersecurity has emerged as a critical concern in mergers and acquisitions (M&A). The risk associated with cyberattacks necessitates that security considerations permeate every stage of the M&A process. Just as financial, legal, operational, or reputational risks are meticulously assessed, a thorough evaluation of the target company's cybersecurity preparedness should be customary.

Despite rigorous due diligence, it's challenging to confirm with certainty that a target company is free from incidents compromising data security. Therefore, buyers increasingly seek protection through comprehensive cybersecurity representations and warranties in the purchase agreement. These contractual provisions are essential tools for risk allocation, enabling buyers to safeguard against potential cyber threats that could undermine the value of the transaction.

This is the second 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).

Why cybersecurity representations and warranties are essential

When acquiring a company — particularly through a stock purchase or merger — a buyer generally inherits not only the target's assets and opportunities but also its liabilities and risks. In asset acquisitions, by contrast, the buyer may have more flexibility in selecting which liabilities to assume, although certain obligations may still carry over depending on applicable law and contractual arrangements.

Cybersecurity breaches and data privacy issues can significantly impact the value of a deal, leading to financial losses, legal liabilities, reputational damage, and operational disruptions. While due diligence aims to uncover vulnerabilities, previous incidents, or outdated systems, it may not reveal all potential cyber risks.

Buyers rely on representations and warranties to determine an appropriate purchase price and to allocate risks effectively. These provisions serve as contractual assurances from the seller about the state of the target company's cybersecurity and data privacy practices. They supplement the due diligence process by:

- Allocating risk: Clearly defining which party bears the responsibility for specific cybersecurity risks.
- Providing legal recourse: Offering the buyer remedies if the actual situation differs materially from what was represented.
- Encouraging disclosure: Motivating the seller to disclose all relevant cybersecurity information during negotiations.
- Acting as a backstop: Protecting the buyer from cybersecurity issues that due diligence may not have uncovered.

Buyers increasingly seek protection through comprehensive cybersecurity representations and warranties in the purchase agreement.

Even when a buyer conducts robust due diligence, the seller has more intimate knowledge of the target entity. Therefore, the inclusion of carefully drafted representations and warranties can serve as a critical safety net.

Key cybersecurity and data privacy representations and warranties

A buyer should consider including the following representations and warranties to mitigate cyber risks effectively. Ideally, to ensure comprehensive protection these provisions should not have significant materiality or knowledge qualifiers.

Compliance with laws and regulations

Representation: The target entity has at all times conducted its business in compliance with applicable privacy and data security laws, which are expressly described in the purchase agreement.

Example: "The Company is and has been in full compliance with all applicable data protection, privacy, and cybersecurity laws, including but not limited to [list specific laws and regulations]."

Existence and adherence to privacy policies

Representation: The target company has established, implemented, and maintained comprehensive data security and

privacy policies in accordance with industry best practices and legal requirements.

Example: "The Company has adopted and adheres to written data security policies that comply with all applicable laws and accurately reflect its data handling practices."

No violations of policies or obligations

Representation: The consummation of the M&A transaction will not violate any existing policies, contractual obligations, or applicable privacy laws.

A cyberattack occurring between signing and closing could represent a material adverse change (MAC) in the target's business.

Example: "Neither the execution nor the performance of this Agreement will result in a violation of any data privacy or security policies, contracts, or legal obligations binding upon the Company."

Absence of data or security breaches

Representation: The target entity has not been the subject of a data or security breach, including any breach that required reporting to government entities, regulators, or affected individuals.

Example: "The Company has not experienced any data or security breaches, unauthorized access, or other compromises of its information systems or data that required notification under any applicable law."

Compliance with designated security standards

Representation: The target company's cybersecurity practices comply with certain designated security standards, frameworks, or practices, or exceed them where appropriate.

Example: "The Company maintains cybersecurity measures that comply with, or exceed, the requirements of [specific security standards/frameworks, e.g., ISO 27001, NIST Cybersecurity Framework]."

Compliance with contractual data privacy obligations

Representation: The target company complies with all data privacy and security provisions within its contracts with customers, vendors, and partners.

Example: "The Company is and has been in compliance with all data privacy and security obligations under its agreements with third parties, including customers, suppliers, and service providers."

Adequacy of security measures

Representation: The target company maintains appropriate and up-to-date security measures, technologies, and safeguards to protect its systems and data.

Example: "The Company has implemented and maintains commercially reasonable security procedures and practices appropriate to the nature of the information to protect personal data from unauthorized access, destruction, use, modification, or disclosure."

No legal actions or claims

Representation: There are no actions, claims, investigations, or proceedings threatened or pending against the target company concerning its data privacy or cybersecurity practices.

Example: "There are no current or past claims, investigations, or proceedings by any governmental authority or third party alleging violations of data privacy or cybersecurity laws or regulations."

Future compliance assurance

Representation: The target company commits to maintaining compliance with data privacy and cybersecurity laws from the date of the agreement until the closing of the transaction.

Even the most thorough due diligence may not reveal all potential cyber threats. Therefore, including detailed cybersecurity and data privacy representations and warranties in the purchase agreement is crucial.

Example: "Between the date of this Agreement and the Closing Date, the Company shall continue to comply with all applicable data privacy and cybersecurity laws and shall not undertake any actions that would cause a breach of the representations and warranties herein."

Negotiating representations and warranties

Since representations and warranties are ultimately about risk allocation, sellers may attempt to limit their exposure by:

- Introducing knowledge qualifiers: Limiting warranties to matters within the actual knowledge of certain individuals within the company.
- Adding materiality thresholds: Restricting warranties to issues that are materially significant to the value of the transaction.
- Setting look-back periods: Limiting the representations to a specific time frame in the past.

However, buyers should aim to minimize such limitations, especially for cybersecurity matters. Representations and warranties without significant materiality or knowledge qualifiers provide stronger protection, ensuring that the buyer can rely on the seller's assurances.

Impact of due diligence findings on representations and warranties

If due diligence uncovers vulnerabilities, previous incidents, or outdated systems, the buyer should anticipate additional costs to enhance the target's security infrastructure. This may prompt:

- Negotiation of purchase price adjustments: Seeking a lower price to account for the investment needed in cybersecurity improvements.
- Holdback or escrow mechanisms: Setting aside a portion of the purchase price to secure remedies for cyber risks post-closing.
- Specific covenants: Requiring the seller to undertake certain cybersecurity measures before closing.
- Extended survival periods: Implementing longer survival periods for cybersecurity representations and warranties, as deficiencies may not be detected until long after closing.

Moreover, a cyberattack occurring between signing and closing could represent a material adverse change (MAC) in the target's business. Properly drafted representations and warranties, along with MAC clauses, can enable the buyer to reassess the terms of the deal or potentially terminate the agreement.

Conclusion

Considering the significant risks associated with cyberattacks, cybersecurity should be an integral part of every stage in the M&A process. Even the most thorough due diligence may not reveal all potential cyber threats. Therefore, including detailed cybersecurity and data privacy representations and warranties in the purchase agreement is crucial.

These provisions not only allocate risk appropriately but also encourage full disclosure and compliance, ultimately protecting the buyer's investment. Buyers can mitigate the inherent cyber risks in M&A transactions by requesting representations and warranties that cover (1) the existence of and adherence to data security policies, (2) compliance with contractual obligations, (3) absence of unauthorized access and security incidents, and (4) the adequacy of security measures.

In an era where cyber threats are evolving, taking proactive steps through well-crafted representations and warranties is essential for securing the value and success of M&A deals.

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. They are located in the Chicago office.

This article was first published on Reuters Legal News and Westlaw Today on January 30, 2025.