Tannenbaum Helpern Syracuse & Hirschtritt LLP

Cybersecurity and Data Privacy in M&A Transactions

David R. Lallouz

Partner, Corporate and Cybersecurity & Data Privacy, Tannenbaum Helpern Syracuse & Hirschtritt LLP

Providing Solutions®

M&A IMPLICATIONS

- Key Risk Areas:
  - Employees
  - Systems
  - Trade Secrets/Company proprietary information
  - Information about the target's customers

MAJOR RISK FACTORS

- The proper identification of personal information (and sensitive personal information) that is collected, created or used
- Sources of data collected (i.e., employees, consumers, customers, vendors, etc.)
- Storage and protection of personal information
- Use of portable access points to process and store data (laptops, mobile devises, remote access systems, portable storage, etc.)
- Use or storage of data internationally requires a more complex scrutiny of international data security laws in a variety of jurisdictions, some of which are more restrictive than the United States
- Relationships with vendors can be a major source of risk to a business so vendor contracts must be scrutinized carefully

MAJOR RISK FACTORS

- Representations and covenants concerning privacy made when the data is collected can continue with the data unless consent is sought and obtained from the individual from whom data is collected
- This could affect merging buyer and target records post acquisition
- Potential successor liability issues could leave the buyer liable for pre-closing activities of the target

DUE DILIGENCE

- Identify what personal data the target company creates or collects
- Identify state and federal laws the target is subject to based on jurisdiction and industry
- Identify whether the target is protected by satisfactory cybersecurity insurance
- Review all contracts with any vendors who have access to confidential information of the target or any of its customers

DUE DILIGENCE

- Identify what safeguards and risk management the target employs
- Identify whether the target complies with industry standards and best practices

- Identify whether the data to be transferred is subject to consent obligations
- Review data retention and disposal policies and procedures
- Review incident management and response policies
- Evaluate implementation and enforcement of policies

DUE DILIGENCE

Like in all transactions, due diligence is a collaboration between legal and business teams and other advisors.

Make sure that the client has the right teams in place to review information and assess the risks

REPRESENTATIONS AND WARRANTIES

Examples of representations and warranties Buyers will want:

- Target has a privacy policy in place in connection with personal information stored, maintained, collected or generated by the target
- Target is in compliance with all applicable data security laws (including international)
- There have been no actions threatened or commenced by any third persons regarding target's treatment of personal information
- The consummation of the M&A transaction will not violate any policies or obligations or applicable privacy laws

REPRESENTATIONS AND WARRANTIES

- There have not been any security breaches of any personal information in the possession of the target
- The target is in compliance with all data privacy provisions with respect to all of its contracts
- There has been no unauthorized access or use of any of the personal information in the target's possession
- All of the target's systems are up to date with the most recent security patches and safeguards

REPRESENTATIONS AND WARRANTIES

- Example of language:
  - Privacy Policy: “The Seller has a privacy policy regarding the collection, use and disclosure of personal information in connection with the operation of the Business in the Seller’s possession, custody, or control, or otherwise held or processed on its behalf and is and in the past 6 years has been in compliance in all material respects with such privacy policy.”

REPRESENTATIONS AND WARRANTIES

- Compliance with Laws: “The target has complied at all times with all applicable laws regarding the collection, use, storage, transfer or disposal of personal information.”
- Contractual Obligations: “The target is in compliance with the terms of all contracts to which it is a party relating to data privacy, security or breach notification, including provisions that impose conditions or restrictions on the collection, use, storage, transfer or disposal of personal information.”

INDEMNIFICATION

Based on the buyer's assessment of the target's privacy and data security risk profile, indemnification can mitigate the risk.

Examples:

- Indemnification provisions require that the target indemnify the buyer for any costs incurred in connection with losses associated with privacy or data security
- Cybersecurity representations can be treated as fundamental representations so they won't be subject to the same expiration, baskets or caps of other representations
- Holdbacks and escrows can be tailored to deal with the cyber risks

INSURANCE

- The costs associated with data breaches are severe. They can include forensic and investigative activities, notification of third parties, and class action lawsuits
- The parties can procure a representation and warranty insurance policy or just a stand alone cybersecurity insurance policy. In some cases, R&W insurance will not cover cybersecurity
- Cybersecurity insurance can in some cases be the target's or the buyer's existing cyber policy. If a new policy needs to be ordered, this can be time-consuming and needs to be planned for early on
- Buyer and target should investigate whether tail insurance is possible for any existing cyber insurance policies of the target

Tannenbaum Helpern Syracuse & Hirschtritt LLP

David R. Lallouz
Partner, Corporate and Cybersecurity & Data Privacy

Tannenbaum Helpern Syracuse & Hirsctritt LLP
900 Third Avenue, 13th Floor
New York, New York 10022
Tel: (212) 702-3142
Email: lallouz@thsh.com

Providing Solutions®