Cybersecurity and Technology Considerations in M&A Transactions

David R. Lallouz
Tannenbaum Helpern Syracuse & Hirschtritt LLP

I. INTRODUCTION

There are privacy and data security risks in almost every M&A transaction, as virtually all enterprises rely on information technology and network systems to manage data. The dependence on technology has opened the door to numerous malicious attacks to enterprises in all areas of commerce, from banks to retail superstores to small business alike. According to Ponemon (2016), the average cost of breach is $221 per customer record and an average total cost to a company in excess of $7 million. All entities have some form of personal information and data.

Issues related to cybersecurity and privacy risks can be mitigated in a number of ways throughout the M&A process, such as during due diligence, as well as through representations and warranties, indemnification, and insurance provisions in the transaction documents.

II. M&A IMPLICATIONS

Understanding the nature and significance of the target company's cybersecurity and privacy landscape and vulnerabilities is essential for the buyer when assessing the risks of the transaction. There are four key risk areas associated with privacy and data breach concerns and vulnerabilities in the M&A context.

- The first issue concerns the employees of the target. Improper training or employee oversight increases the risk of a security breach, including, but not limited to, facilitating less sophisticated cyber-attacks, such as phishing schemes or spoofing scams.

- The second risk area is the target company's cybersecurity and data retention systems and whether these systems adequately minimize vulnerabilities.

- Third, the potential risk associated with the exposure of the target company's proprietary and/or trade secrets due to inadequate protection.

- Finally, inadequate protection of customer information. Breaches involving information about a company's customers generally result in major financial injury to the company.

The type of networks and virtual infrastructure the target company uses should be evaluated by a buyer for all four of these risks areas.

At a granular level, these risk factors are manifested in several organizational deficiencies, including, the improper identification of personal information, especially sensitive personal information, that is collected, created or used, and improper lack of attention to the sources of data collection, such as employees, consumers, customers, and vendors.

Improper security mechanisms for the personal data and proprietary data an entity collects leaves the entity at risk of exposure. More specifically, the way the entity stores and

protects personal information, in both the software and hardware context, are critically important in assessing an entity's vulnerability to cyberattacks. Similarly, risks must be assessed where the entity is engaged in the use of portable access points to process and store data, including, but not limited to, laptops, mobile devises, remote access systems, or portable storage. Some enterprises choose to store data internationally to take advantage of the favorable costs offered by overseas vendors. 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, such as the newly enacted EU General Data Protection Regulation ("GDPR").

Relationships with vendors can be a major source of risk to a business so vendor contracts must be scrutinized carefully. This is especially so if the business stores large quantities of data with a single vendor, such as a cloud service provider.

There are also risks that may arise post-acquisition. For example, representations concerning privacy made by the target pre-acquisition, when the data was collected can continue with respect to the data unless consent or waiver is sought and obtained from the data source. This could affect merging the buyer's and target's records post-acquisition. Further, potential successor liability issues could leave the buyer liable for pre-closing activities of the target.

III. DUE DILIGENCE

Like in all transactions, due diligence is a collaboration between legal and business teams and other advisors. As such, it is important to ensure that the client has the right teams in place to review information and assess the risks. Due diligence review of the target company's privacy and data security is multifaceted when done thoroughly.

With respect to data retention and collection, it is crucial to identify what personal data the target company creates or collects. Further, the due diligence team should identify how and where the target company collects and stores data, such as in locally hosted servers or third party cloud-based storage services.
Additionally, it is important to identify any state and federal laws the target is subject to based on jurisdiction and industry.

In reviewing the security practices of the target, the due diligence team should:

- Identify whether the target is protected by satisfactory cybersecurity insurance.
- Identify what safeguards and risk management the target employs.
- Identify whether the target complies with industry standards and best practices.

When reviewing customer, vendor, or even employment contracts, special attention should be paid to how the entity has agreed to treat personal information obtained by it. In particular, the due diligence team should identify whether the transfer of such data is subject to consent or notice obligations. Additionally, special attention should be paid to all contracts with any vendors who have access to confidential information of the target or any of its customers.

In-house procedures can give insight into how a company prioritizes cybersecurity and data privacy. As a matter of good practice, the due diligence team should:

- Review data retention and disposal policies and procedures.
- Review incident management and response policies.
- Evaluate implementation and enforcement of policies.

Thorough due diligence can provide the buyer with a framework understanding of the kinds of privacy and security risks present, which will be beneficial in mitigating those risks.

IV. REPRESENTATIONS AND WARRANTIES

There are certain representations and warranties that a buyer in an M&A deal should consider including in the purchase agreement. Adding privacy and security related representations and warranties is another approach that should be considered when addressing security and privacy risks in an M&A transaction. The inclusion of numerous cyber-related representations and warranties will supplement the due diligence conducted.

There are certain representations and warranties that relate to general compliance by the target with respect to data privacy and security. One such example is a representation and warranty that the target has a privacy policy in place in connection with personal information stored, maintained, collected or generated by the target.

Moreover, a buyer should require a representation that the target is in compliance with all applicable data security laws, including internationally, particularly where the target is subject to GDPR.

There should be a representation and warranty ensuring that the consummation of the M&A transaction will not violate any policies or obligations, such as any contractual obligations, or applicable privacy laws.

Similar to standard representations and warranties, there are representations and warranties specific to actions that have arisen or may arise in connection with privacy and security. Some examples of these types of representations and warranties include:

- There have been no actions threatened or commenced by any third persons regarding the target's treatment of personal information.
- 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.

There may be additional representations and warranties that become apparent from the information uncovered in due diligence.

V. INDEMNIFICATION

Indemnification can be a very useful tool when it comes to cyber security and privacy related risks. Based on the buyer's assessment of the target's privacy and data security risk, indemnification can be deployed as a mechanism to mitigate that risk. For instance, including indemnification provisions which require that the target indemnify the buyer for any costs incurred in connection with losses associated with privacy or data security.

To protect against unknown cybersecurity threats, the buyer may want to insist that the cybersecurity representations be treated as fundamental representations so they will not be subject to the same expiration, baskets or caps of other representations. And, for specific risks, such as those found during diligence, the buyer can ask for a specific indemnity, which would be subject to distinct limitations and recovery methods.

Additionally, holdbacks and escrows can be tailored to deal with the identified or unidentified cyber risks.

VI. INSURANCE

Insurance considerations are another important factor when approaching cyber security and privacy in an M&A transaction. The costs associated with data breaches are severe. They can include forensic and investigative activities, notification of third parties, and class action lawsuits. There are several different approaches to procuring the type of insurance needed to protect the buyer from the onerous costs associated with a data breach.

Representation and warranty insurance, which will cover the buyer for losses resulting from a target's breach of representations and warranties in the purchase agreement, is one type of insurance to be considered. The parties can procure a representation and warranty insurance policy or just a standalone cybersecurity insurance policy. In some cases, though, representation and warranty insurance may 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 procured, this can be time-consuming and needs to be planned for early on.

Additionally, the buyer and the target should investigate whether tail insurance is possible for any existing cyber insurance policies of the target.

Regardless of which type of insurance is chosen, the effectiveness of the policy will in part be determined by the breadth and accuracy of the due diligence conducted.

Special thanks to Alexa Zelmanowicz for her assistance with this article.