Published on *The National Law Review* https://natlawreview.com

Data Privacy & Security Considerations in Mergers & Acquisitions Due Diligence

Article By:

Linn F. Freedman

It has long been standard practice to include data privacy and security due diligence in mergers and acquisitions for technology companies. Over the last several years, there has been an increase in data breaches which are costly and damaging to a company's brand, and therefore, we have seen an uptick in companies including detailed requests from target companies about their data privacy and security posture, compliance and risk.

Any target company that has employees holds risky data, including its employees' names, addresses, dates of birth, social security numbers, financial information, drivers' license information, and more. Collectively, all of this data is protected by state laws and if there is an unauthorized access, use or disclosure of this data, notification to individuals and regulatory bodies may be required. In addition to employee data, target companies may have customer personal information and vendor or subcontractors' personal information. All of this data poses a risk and due diligence surrounding the risk is appropriate.

What happens if after closing the company finds out that the target company was the victim of a phishing scam and malware was introduced into the system, but it wasn't detected until after the closing? What happens if a forensic investigation has to be undertaken and the forensic investigation finds that there has been a reportable breach? Who is responsible for the costs associated with the incident?

Another scenario that has happened in our experience is a theft of company electronic data pre-closing by a rogue employee, but it wasn't detected until after closing. Another example is when a security incident that occurred pre-closing was detected post-closing, and ended up being the subject of an investigation by a regulatory body. Who is responsible for the costs of the regulatory investigation and/or fines and penalties imposed?

These are some of the questions that we get involved in with our partners who are leading mergers and acquisitions so due diligence questions can be presented and answered; security measures of the target company can be evaluated; questions about compliance with data privacy and security laws, security incidents or data breaches, and pending or threatened regulatory investigations can be posed; and appropriate language can be inserted into the closing documents, including representations and warranties, to address pre and post-closing incidents, including indemnification

and claw-backs.

Most target companies hold data that require compliance with state and federal laws, is valuable to the business and if compromised before the closing could be devastating to the business or the brand. Taking care to include data privacy and security in due diligence can assess and manage the risk during the transaction and afterward.

National Law Review, Volume IX, Number 31