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

Effective Management of Cybersecurity Risk in Transactional Due Diligence

Article By:

Alaap B. Shah

Eric W. Moran

According to a report by West Monroe Partners, Approximately 40% of companies engaged in corporate transactions reported finding a cybersecurity issue during post-acquisition integration of the target company. While companies routinely conduct robust transactional due diligence to manage legal risk, many fail to adequately conduct cybersecurity due diligence. As a consequence, many companies and investors are leaving themselves vulnerable to potentially severe latent cyber risks.

Cybersecurity is especially relevant in healthcare transactions as the industry continues to be riddled

with cyber-attacks. Protenus Breach Barometer reports that healthcare has been the most targeted industry over the last few years, with 1.13 million, 3.15 million, and 4.4 million patient records compromised in the first three quarters of 2018, respectively, and more than half of breaches occurring due to hacking. The cat is out of the bag. Healthcare entities usually amass very lucrative personal data – social security numbers, demographic information, health insurance records, and prescription information – making them attractive targets for hackers.

Despite the high frequency of cyber-attacks in the industry, many healthcare entities spend only half as much to improve security protections when compared to other industries. As a result, these companies remain vulnerable to cyber threats. In the case of a breach, companies could face penalties from government agencies as well as class action lawsuits. Cyber risks may intensify during acquisitions, as the likelihood of a breach increases with the expansion of the overall cyber footprint. Further, in a transaction, the target company's vulnerabilities ultimately become an issue for the acquiring company. Thus, if the target entity does not have adequate safeguards to protect patient records, then the acquiring company is at financial and reputational risk for those failings.

Given the potential risks, it is important that acquiring companies prioritize cybersecurity as an integral part of due diligence efforts. An effective due diligence process should at a minimum evaluate cybersecurity preparedness and risks related to the following: 1) current state of risk assessment; 2) technical security features of business-critical information systems and network architecture; 3) implementation of policies and procedures related to information security; 4) policies and procedures related to detecting, responding to, and recovering from cyber incidents; and 5) historical indicators of legal and regulatory compliance issues related to cybersecurity.

National Law Review, Volume IX, Number 11