ARTICLES

Think You're Safe from Cyber Risk? Think Again

By Joanne Censullo and Lauren Taylor

Jul 26, 2018

When a private equity firm acquires a company, whether it's a billion-dollar tech company or a mid-sized pizza franchise, the buyer may be taking on more than the seller's assets; they may also be taking on relevant exposure associated with those assets. One of the most malicious risks we've seen in recent years in M&A transactions is cyber liability, and, surprisingly, it's often overlooked.

Recent examples of cybersecurity breaches being uncovered during M&A cycles shine a light on the seriousness of the issue. Notably, in 2016 when Verizon agreed to acquire Yahoo! for approximately $4.8 billion, Yahoo! hadn't yet disclosed that it had been the target of a malicious cyber-attack. As the details and scope of the breach became clear -- hackers had stolen information from at least 500 million user accounts – it not only delayed the deal, it significantly changed the terms of the acquisition. The purchase price dropped significantly and because the breach was so large and had high long-term remediation costs, Yahoo! was forced to take legal responsibility for any subsequent lawsuits arising from the incident.

This and other high-stakes M&As involving cyber liability have demonstrated that cyber due diligence should be rigorous. Sometimes, cyber-attacks aren't disclosed during a deal, for various reasons, but more often, the seller isn't aware that its digital data has been compromised and the repercussions of an attack might not be felt until months or years later, long after the deal has been signed.

While it may be easier to grasp the dangers of cyber risk in transactions involving the high-tech, financial or healthcare industries, cyber is a looming threat for many enterprises. A small manufacturing company, for example, might not have an expectation of a cyber breach because of the nature of the business. Maybe it doesn't collect personal health records or credit card data from millions of users. Its machinery might operate independent of a sophisticated, automated computer network.

Yet they're not immune from breaches. Sensitive digital data in the form of employment records and invoices almost certainly exist in their computer systems. Their interactions with vendors and suppliers expose them to risks as well.

Cyber breaches are so ubiquitous that many experts classify companies into two categories: those who have been hacked, and those who don't yet know that they've been hacked.

When private data is exposed in a breach, remediation costs can run into the millions, and, in the case of the mega mergers, hundreds of millions of dollars. Once hacked, a company must comply with regulatory procedures, including all notification processes, and that can be costly.

Additionally, increased data privacy legislation such as Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018, are inflicting penalties for non-compliance, adding another layer of liability.

As the M&A space continues to explode, with no signs of slowing, private equity firms are under tremendous pressure to close deals quickly. As a broker, we understand the urgency of our clients to close deals as quickly as possible, but we advise them to fully analyze the risk.

Cyber due diligence that gives a full accounting of the target company's potential liability is crucial. Time is money, but so is risk. Risk not only has the potential to negatively impact the acquirer down the road, but it can affect the valuation of the company during the transaction. To learn more about private equity due diligence, contact us at jcensullo@risk-strategies.com.

TAGS:
Cyber Liability
Private Equity