5 Ways To Keep Cybersecurity Woes From Derailing A Deal
By Chelsea Naso

https://www.law360.com/articles/929630/5-ways-to-keep-cybersecurity-woes-from-derailing-a-deal

Law360, New York (July 19, 2017, 7:06 PM EDT) -- As corporate America becomes more reliant on technology in an increasingly digital world, data breaches and other cybersecurity concerns are threatening to derail a rising number of transactions.

Here, Law360 outlines five ways dealmakers can get ahead of potential cybersecurity deal-breakers.

Dive Deeper into Due Diligence

Due diligence is a regular part of the M&A process, but when it comes to cybersecurity, the normal course of due diligence will likely fall short, explained Ieuan Jolly, a Loeb & Loeb LLP partner and leader of the firm's privacy, security and data optimization practice.

"Typically the focus of the due diligence is on traditional risk areas like contracts, tax and intellectual property protections," he said. "But with data being the lifeblood of many companies and in many cases their most valuable asset, a standalone focus needs to be on the data handling and security practices of the target company."

Buyers need to evaluate a company's infrastructure and investigate whether there has been a data breach. That will include asking questions and requesting documents, but it may also require a deeper dive.

Depending on the company being acquired and whether it is believed they have experienced a breach or may be at risk of one, buyers should tap lawyers with privacy and data security experience. They may also want to bring in an outside cybersecurity company to conduct a risk assessment.

"The acquirer might even want to engage a technical service and want to do an audit. They might want to scan the network for the existence of malware, for example," said Jeewon Serrato, a Shearman & Sterling LLP counsel and co-head of the firm's global privacy and data protection group.

That might go further than due diligence normally does, but that extra mile can save a buyer from some expensive headaches down the line.

"These are novel levels of intrusion. Due diligence usually has not meant this level of scrutiny of the acquired company. Traditionally, sellers have said, 'If you want to buy the company, buy the company if you want representations and warranties with reasonable limits, but otherwise don't ask for too much,'" said Jed Davis, a Day Pitney LLP partner. "Part of the challenge of cybersecurity is you can't surmise what you don't know firsthand."

Ask for the Right Contractual Protections

While the terms of the merger agreement cannot take the place of in-depth due diligence, having the right contractual protections in place will help protect the buyer in case an issue arises or is discovered between signing and closing.

For starters, buyers should consider negotiating for representations and warranties to vouch for the target company's compliance with privacy and data-security laws, and where appropriate, with regulatory standards, to build indemnity, Jolly said.

"If the seller breaches those representations and warranties it made in the purchase agreement about privacy compliance and information security, and then the buyer suffers damages after the closing, the buyer will be indemnified by the seller for the breach of those representations that occurred pre-closing that led to the damages," he said.

Traditionally, material adverse effects govern changes that are outside of a target's control, like a change to tax law or an economic change. But a buyer may also want to try to explicitly include the scenario of material cyber attack in the material adverse effect portion of the merger agreement to help solidify its ability to terminate a transaction if a game-changing breach is revealed between signing and closing.

"By including cybersecurity events or privacy violations explicitly in that definition, the acquirer is able to trigger a right to walk away from a deal, or even use it as leverage to renegotiate better terms," Jolly said.

Get Creative with Deal Structure

If a cybersecurity issue is identified during the due diligence period, the buyer should consider going back to the drawing board to rethink the deal structure, according to Serrato.

The acquirer should consider buying specific assets rather than an entire company, she said, to help reduce any post-closing liabilities, particularly if the breach is tied to the piece of the business being left behind.

"If there are non-core assets, excluding them from the purchase would minimize or reduce the liability to the acquirer," Serrato said.

A carve-out can be more effective than contractual protections, as the target company still exists on its own.

"All the liabilities attached to the target company will attach to the acquirer if, let's say, a data breach is discovered post-M&A deal," Serrato said. "And so an M&A strategy taking privacy into consideration might be to acquire a specific set of assets and not do a stock acquisition."

Battle a Newly Identified Breach

Even the best due diligence can miss a breach, especially if the target company has yet to identify the issue itself.

When an issue is either identified or arises between signing and closing, the buyer needs to carefully consider its next move.

First, it's important to be sure the issue is contained. Then, as preparation for the public disclosure of the breach, the buyer needs to value how the seller discovered the issue, how it was handled and how extensive the damage is.

"We're going to want to prepare for the disclosure in advance, a little self-due diligence," said Karl Hochkammer, a Honigman Miller Schwartz & Cohn LLP partner and leader of the firm's information and technology transactions practice. "Because it's important to have the story straight and complete when you are talking to a potential buyer as part of the due diligence process."

It's also essential to outline a communications plan, because improperly disclosing the breach and its potential impact could spell trouble with regulators later on.

“All of those public communications may be used in a regulatory enforcement action if they have data that was regulated and a regulator is interested in taking action against a company,” Serrato said.

The buyer then needs to evaluate whether to move forward with the transaction. Even clear contractual protections can make it difficult to invoke a material adverse effect, which would effectively allow the buyer to walk away. Material adverse effects in general are a challenge to prove in court. In the case of a cybersecurity breach, it would be difficult to prove that the target company would face long-term consequences.

Turning to an adverse material effect, however, is often a good starting point for renegotiating the deal terms and moving forward, Hochkammer said.

“Most assertions of material adverse effect, an attempt to get out of the transaction, really are the first step in the renegotiation of the purchase price. Because it’s really hard to give a client a high degree of certainty that they are going to win a material adverse effect litigation — it almost never happens," he said.

Don’t Lose Perspective

Cybersecurity breaches do pose a significant risk to acquirers, and it is important to do the proper due diligence, get the proper contractual protections, and in some cases, think about structuring the deal differently. However, it’s important to also keep perspective, noted Seth Traxler, a Kirkland & Ellis LLP partner and co-leader of the firm’s technology and intellectual property transactions practice.

It’s difficult to identify every issue, and every issue is not necessarily worth risking a deal over, he explained.

“You’re never going to discover every vulnerability, because every company has a vulnerability somewhere. Perfect security is impossible. The challenge is to not get lost in ordinary course problems that every company has,” Traxler said.

And it’s also worth considering that given some of the recent high-profile deals that made headlines with cybersecurity issues, cybersecurity is the latest hot topic being tackled by law firms' client notices and the media, making it at times seem more pressing than it is, he said.

“The headlines don’t always reflect the reality. Cyberattacks in some situations rightly deserve headlines, but may not accurately reflect the true experiences of many corporations today who continue to be attacked, but perhaps not to the extent one might guess from reading headlines alone,” Traxler said.