Harvard Law School Forum on
Corporate Governance and Financial Regulation

SUPPORTED BY: pwc

The Emerging Need for Cybersecurity Diligence in M&A

Posted by Shilpi Gupta & Stuart D. Levi, Skadden, Arps, Slate, Meagher & Flom LLP, on Tuesday, May 2, 2017

Editor's note: Shilpi Gupta and Stuart D. Levi are partners, and William Ridgway is a counsel at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on a Skadden publication by Mr. Gupta, Mr. Levi, and Mr. Ridgway.

Cybercrime has emerged as one of the foremost threats a company faces. As a result of a few keystrokes, a company may find its customers' data sold on the dark web, its intellectual property in the hands of a competitor or its operations paralyzed by ransomware. It should come as little surprise, then, that cybersecurity has become a key risk factor in mergers and acquisitions.

A 2016 survey by West Monroe Partners and Mergermarket found that 77 percent of top-level corporate executives and private equity partners reported that the importance of cybersecurity at M&A targets had increased significantly in recent years. Given this trend, executives and directors contemplating acquisitions should consider the following cyber-related issues when conducting due diligence.

Key Considerations

Most companies depend on digital assets, whether in the form of customer data, trade secrets or business plans. Those assets are not only vulnerable to theft or destruction, they also may trigger complicated and evolving cybersecurity and privacy mandates from a variety of regulators in the United States and abroad. As a result, an acquiring company risks buying a company whose digital assets have already been compromised or assuming liabilities for past noncompliance with cybersecurity and data privacy laws. The latter could mean the acquiring company would take on potential fines, damages from private actions and lengthy consent decrees.

Cybersecurity due diligence cannot be one-size-fits-all. As with any diligence effort, the scope will depend on the transaction timeline as well as the target company's industry, the value of its digital assets, its regulatory environment and its cyberrisk profile.

Key areas to consider in cybersecurity due diligence are:

Industry Standards. One threshold question for the diligence team is whether the target company meets the relevant industry standards for cybersecurity practices and procedures. That assessment should involve interviews of key staff at the target company and a review of relevant documents, such as reports of vulnerability assessments, penetration testing, vendor audits and any resulting remedial measures, incident response plans and incident reports. Special attention should be paid to the maturity of the company's cybersecurity governance and vendor

management, the terms of any indemnification and cyber insurance policies, the existence of any past cybersecurity incidents and how they were handled, and whether the company has interacted with regulators, law enforcement or other third parties regarding potential cybersecurity and data privacy incidents.

Target Company's Network Security. The diligence team cannot simply rely on a target company's assurances without verification because organizations with serious security gaps seldom recognize the problem. According to a report by cybersecurity firm FireEye, companies more frequently find out about a data breach from an outside source (*e.g.*, law enforcement or a security vendor) than internally, and the median time to discover an incident is 146 days. If the target has never engaged a third-party forensic firm to conduct vulnerability assessments and penetration testing—a scenario that is becoming less common in many industries—the acquirer may want to retain a firm to undertake its own testing on the target company's network and perhaps even conduct searches on the dark web (the part of the internet that may only be reached with anonymization tools and where many hackers sell their spoils) to see whether the target's customer data or intellectual property is already compromised and available for sale. The acquirer should be aware, however, that the target will likely opt to conduct its own testing and provide a report rather than allow the acquirer to do so.

In an extreme scenario, the diligence investigation may uncover hackers lurking in the target company's network, but more likely the result will be a risk calculation based on the target company's governance and the administrative, technical and physical information security controls it uses to protect digital assets.

Deal Terms. The diligence results should inform deal terms, costs to remediate gaps in compliance or risk management, and any post-deal indemnity claims. One way to try to verify a target's representations about its cybersecurity and allocate potential liabilities is through well-crafted representations and warranties. Those provisions should be tailored to the target company's industry and regulatory environment, any risks identified in the diligence process and the acquirer's risk tolerance. At a minimum, representations and warranties should cover compliance by the target (and its affiliates and vendors) of applicable cybersecurity and data privacy laws, its own internal and external privacy policies, and the absence of unauthorized access to the target's network.

Acquirers should be prepared for the target company to request qualifications to these representations and warranties, limiting them to the knowledge of the target's management, imposing a materiality threshold or drafting exceptions in the disclosure schedule regarding the inability to know with certainty about cyber intrusions. An acquirer's willingness to acquiesce to such qualifications will depend in part on what the diligence investigation revealed. Indemnity may also be used to hold the target responsible for its representations and liable for hidden or undisclosed cybersecurity and data privacy liabilities that arise after closing. The parameters for these indemnity provisions should likewise flow from the diligence findings.

Cyber Insurance. The payoff for cybersecurity due diligence comes not only in deal negotiation but also in securing insurance, whether that be standalone cyber insurance or representation and warranty insurance, which has become commonplace in M&A transactions. In either case, in deciding whether to insure for cyberrisk, an underwriter likely will consider the quality and depth

of the acquirer's diligence review. Thus, a robust cybersecurity diligence investigation will likely pave the way for more favorable insurance policy terms.

Conclusion

Mergers and acquisitions due diligence has long been a critical tool for uncovering and protecting against key risks in a transaction. In our data-driven economy, cyberrisk must not be overlooked. Given the operational, financial and reputational costs at stake, cybersecurity should join the ranks of other traditional due diligence inquiries in deal practice.