315 W. 11TH AVE., DENVER, CO 80204 | 720–328–1418 | www.LAWWEEKCOLORADO.com VOL. 15 | NO. 22 | $6 | MAY 29, 2017

LAW WEEK COLORADO

Cybersecurity Due Diligence in M&A Transactions

BY **MATTHEW HOLOHAN** AND **RAYMOND AGHAIAN**
KILPATRICK TOWNSEND & STOCKTON

MATTHEW HOLOHAN

RAYMOND AGHAIAN

With more and more companies falling prey to cyberattacks, cybersecurity protections have become an important aspect of corporate governance. Unfortunately, in M&A transactions, cybersecurity issues are often an afterthought, if not ignored altogether. As no company is immune from cyberattacks, parties engaged in M&A transactions should treat cybersecurity as a critical stand-alone aspect of due diligence.

Software and networking companies have traditionally been viewed as prime targets for cyberattacks. But any company with significant intangible assets could fall victim to hackers. In our increasingly connected business environment in which nearly every company has a website and collects and maintains customer data in some form, data security is critical — and now a legally imposed obligation in various industries.

Thieves often target personal information regarding customers and employees, internal financial and other confidential information, and trade secrets. This is no longer an exclusive risk to high-tech companies. According to Forbes, the five industries most likely to have cyberattacks in 2015 were healthcare, manufacturing, financial services, government and transportation. All companies involved in M&A transactions, therefore, must pay attention to cybersecurity.

Cybersecurity issues can affect an M&A transaction in several ways. For example, an existing data breach can lower the value of a target company or lead the acquiring party to demand other concessions such as indemnification or shared liability. But an actual data breach is only one cyber security problem that could be discovered via due diligence. Lax cybersecurity standards and absent or insufficient response protocols should a data breach occur can also devalue a company or require future indemnification. An acquiring company may even withdraw from a deal if cybersecurity is too lacking, given the severe risks of data breaches and potential scrutiny by regulatory bodies.

A recent survey by the NYSE Governance Services asked 276 directors and officers of public companies about the impact of cybersecurity threats on their M&A due diligence process. In response, 85 percent of directors and officers stated that major security vulnerabilities were "somewhat likely" or "very likely" to affect a merger or acquisition. In fact, 22 percent said they would not consider acquiring a company that has recently suffered from a high-profile data breach, while 52 percent said they would consider such an acquisition "only at a significantly lower value."

An acquiring party should therefore conduct robust cybersecurity-related due diligence as part of any M&A transaction. This might begin with an identification of all intangible assets of the target company that may be vulnerable to attack. This includes anything from confidential personnel files and customer data to trade secrets maintained in the form of data. The acquiring party should provide a questionnaire asking for identification of any company assets that could be exploited or lost in a cyberattack, along with a detailed explanation of how such information is kept secure. Appropriate security measures vary among different industries and data types, but customary protections afforded to trade secrets might provide a helpful benchmark when measuring the sufficiency of data security protocols.

> *In our increasingly connected business environment in which nearly every company has a website and collects and maintains customer data in some form, data security is critical — and now a legally imposed obligation in various industries.*

The acquiring party should also inquire not only concerning any known data breaches and level of complexity of such attacks, but also of any known vulnerabilities within the target's security system. This includes the breadth of access to confidential information within the company and the level of enforcement for the company's security procedures. Further, as M&A deals are often followed by corporate restructuring and reorganization, the risk of data leaks or theft by employees may be enhanced following an M&A transaction. The acquiring party should assess these risks and determine what can be done by the target company to minimize them.

In addition to security protocols to prevent a data breach, all companies should have a response protocol in place in the event that a data breach nonetheless occurs. The acquiring company should know what this is so they can assess the sufficiency of the protocol and any improvements that need to be made prior to or following the acquisition, including an allocation of costs for any changes that need to be made. A deficient or nonexistent response protocol can significantly devalue a target company, as the acquiring company absorbs the risk of fallout from future data breaches or must invest resources in putting a proper protocol in place. Moreover, given the delay inherent in discovery of data breaches, the acquiring company should also asses any cyber insurance policy in place and what such a policy would cover in the event a breach is discovered after the acquisition.

The acquiring party might retain a third-party company, overseen by legal counsel, to conduct a review and audit of the target company's cybersecurity protocols. Such an audit might include an evaluation of compliance with industry security standards such as NIST and ISO, regulatory frameworks as recently enacted by the New York Department of Financial Services and various state guidelines established in California and Massachusetts. To enhance its own value, a target company anticipating acquisition might conduct its own formal review before negotiations take place, though doing so carries the risk that any acquiring company might be viewed as insufficient by the acquiring company.

Data breaches are a pervasive threat across all industries, and any companies involved in M&A transactions must take these threats seriously. To preserve the value of any M&A transaction, potential devaluations arising from cybersecurity concerns must be quickly identified and assessed. •

— Matt Holohan and Raymond Aghaian are both partners in the Denver office of Kilpatrick Townsend.