LEGAL ADVISOR

A PilieroMazza Update for Federal Contractors and Commercial Businesses

Managing Cyber Risks in M&A Transactions

By Kathryn Hickey and Dave Shafer

No company or industry is immune from cyber risks. With an increasingly digitized marketplace, proprietary company data, as well as the sensitive data of your customers and employees, is an attractive and often easy target for bad actors looking to profit from exploiting a company's vulnerabilities. While cybersecurity concerns are significant in the daily operations of a company, in the M&A deal context, they take on a particular importance because of the material impact cyber vulnerabilities can have on a buyer's risk and therefore deal pricing. A buyer in any acquisition will want to understand the full scope of a target's cyber infrastructure and risk for exposure to take steps in the definitive agreement and deal negotiations to address identified areas of exposure and develop a plan mitigate those risks post-closing. Conversely, the seller will want to get ahead of any cyber issues in order to avoid prolonged negotiations and potential decreases in company valuation due to the identification of exposure resulting from data breaches or failure to be in compliance with applicable law or industry standards. Getting ahead of potential issues early can save time and money for both parties in a transaction and avoid, as much as possible, any post-closing surprises.

One need not look any further for an example than the recent discovery that Marriott International inadvertently purchased a reservation database that had been previously compromised, with the unauthorized third-party still in the database undetected as of closing, during its merger with Starwood Hotels in 2016. The discovery occurred post-closing, shifting the exposure to Marriott, as opposed to a similar incident wherein Yahoo! discovered a similar breach prior to closing on a sale of its assets to Verizon Communications and thereby giving the parties the ability to leave the exposure with Yahoo! The comparison between these two situations is a perfect illustration of the value of thorough cyber diligence and its impact on a buyer's ability to mitigate post-closing exposure due to compromised seller systems. This article sets forth the framework for "best practices" in cyber M&A diligence and how parties can utilize these strategies in negotiating and closing deals.

Due Diligence — Assessing Cyber Risk

At the outset of any deal, a buyer should include in its diligence of the target company an effort to understand the target's cybersecurity systems, programs, policies, and standards to evaluate potential risk of breach. A key component of this evaluation is identifying the types of sensitive data that may be exposed due to any deficiencies in cyber protections. Sensitive information can include consumer credit card and financial information, personally identifiable information of employees and customers, biometrics, protected personal health information, internal company intellectual property, other proprietary information, customer lists, third party proprietary information, and government sensitive or secure data. Appreciating the types of information that could be vulnerable to a cyber-attack can inform the buyer's effort to determine the likely severity, legal exposure, and cost of a breach.

Related to the question of the type of sensitive information held by the target is the question of whether the target maintains compliant, secure systems at a level appropriate for the data it manages. A systems diligence team should evaluate protections at all systems levels in order to identify vulnerabilities or insufficiencies. This process can also evaluate the target's existing cyber

Continued on page 2

PILIERO MAZZA

 Continued from page 1

infrastructure, including systems and policies, to confirm compliance with industry cybersecurity standards. While industry recommended standards do not ensure protection from breach, they can be an important benchmark in determining the reasonableness of a seller's existing cyber practices. Diligence at this level should also include a review of the target's internal policies and procedures, breach response practices, and internal audits and controls.

The technical cyber diligence should also focus on identifying prior or existing breaches impacting the target and understanding the scope and potential damages associated with that breach. It is important to answer certain key questions in evaluating known breaches:

- When and for how long did the breach occur? Is there evidence or knowledge of any continuing breach?
- What information was compromised? Were copies made? Were changes made to the target's systems or files?
- Were measures taken to resolve vulnerabilities following the breach? Are they sufficient?
- Was there compliance with all required notifications/reporting requirements upon discovery of the breach?
- Are there potential claims by third parties resulting from the breach? Is there a likelihood of any shareholder derivative suit or class action?
- Did the breach create grounds for a "for cause" termination under any material contracts of the seller?

In answering these types of questions, a buyer can attempt to put boundaries around known breaches and any continuing liabilities for an acquirer of the seller.

The complementary component to diligence of a target's cyber systems and programs is diligence of the target's existing contracts from a cyber risk allocation perspective. In reviewing a target's vendor contracts or subcontracts, a buyer and their legal team should focus on determining who bears the contractual responsibility for ensuring the security of electronic data that vendors access, control, or manage. If security is the vendor's responsibility, a buyer should ask what, if any, safeguards the seller has in place to ensure that the vendor complies with its contractual obligations. Is there a vendor management plan or audit process in place? Do vendors self-certify? Are vendors required to provide evidence of minimum cybersecurity insurance coverage, and does that coverage extend to the seller? Are there clearly defined indemnification obligations governing which party will bear the economic risk in the event of a data breach and, if so, is the party that bears the indemnification obligation financially capable of satisfying those obligations? A review of the seller's insurance policies should include a focus on cybersecurity coverage, coverage limits, exclusions, and notification requirements that may impact the seller's ability to recover under an insurance policy if it does not strictly adhere to such requirements.

Addressing and Mitigating Cyber Risk

Once thorough cyber diligence is conducted, the parties to an M&A transaction can take measures to mitigate, as much as possible, the risk and potential exposure for any issues that have been identified.

The seller and buyer should work together to correct flaws in cybersecurity in advance of closing, if possible, including IT systems updates, as well as updates to company policies and programs. To the extent full corrective measures are not possible pre-closing, the parties should implement a post-closing plan to further strengthen security and ensure effective systems integration, with milestone targets at 30, 60, and 90 days post-closing.

With respect to any known cyber risks that were identified in the diligence process, the parties should negotiate specific protections within the definitive agreement for the transaction. At a minimum, from the buyer's perspective, this should include fulsome representations and warranties from the seller around cybersecurity issues, including:

- ☑ Representations as to the seller's compliance with cybersecurity industry standards and disclosure of all applicable regulatory or contract requirements relating to cybersecurity and data protection;
- ☑ Representations as to the seller's compliance with any applicable reporting requirements; and
- ☑ Disclosure schedules detailing all known prior or existing breaches.

The buyer may wish to negotiate for longer survival periods for cybersecurity representations in the definitive agreement given the long potential latency of claims related to a breach. In addition, for any known

Continued on page 3

 Continued from page 2

breaches or known cyber vulnerabilities, the buyer may desire special indemnification rights, including carving out claims arising from those matters from any applicable indemnification cap or other indemnification limitations. The buyer may also wish to require an increased or lengthier escrow of purchase price funds to cover any such claims. Ultimately, depending on the severity of any issues identified in diligence, the buyer may need to seek a downward adjustment to the purchase price due to an overall decrease in the target's enterprise value.

It is never possible to know the full scope of risk in any M&A deal, and cybersecurity risks can be particularly difficult to identify and quantify, but failure to address cybersecurity risks can lead to potentially catastrophic losses on both sides of the table. It is in both parties' best interest to work from the outset of the diligence process to understand these issues in order to provide the time and opportunity to mitigate them as much as possible in advance of closing and avoid messy and prolonged post-closing disputes.

About the Authors: Kathryn Hickey is a partner and chairs the Business and Corporate Group. She may be reached at khickey@pilieromazza.com. Dave Shafer is an associate in the Business and Corporate Group. He may be reached at dshafer@pilieromazza.com.