PLANNING FOR CYBERSECURITY RISKS IN M&A TRANSACTIONS

Date: 15 November 2017

Cybersecurity and Mergers & Acquisitions Alert

By: Jennifer H. Thiem, James E. Scheuermann

A glance at any media outlet shows that cyber risk is pervasive and increasing, and that virtually no company is immune to a cyber incident. Almost all companies and associations collect and store some type of data, whether it is customer or employee data (such as personally identifiable information, personal health information, or cardholder data), intellectual property, confidential corporate information (such as historical financial data and projections, customer lists, or corporate strategies), or other confidential information (who is accessing which websites, consumer buying habits, and the like). Similarly, virtually all companies communicate with their customers and vendors through emails, social media, or websites. And companies are increasingly purveyors of or reliant on devices connected through the internet of things or the industrial internet of things (industrial control systems), many of which lack adequate security. With a plethora of valuable targets and points of entry, cyber criminals, hacktivists, and nation-states do not lack for motives or opportunities to engage in cyber attacks.

The costs associated with cyber incidents often are severe. For example, the costs associated with a data breach may include forensic and investigative activities, assessment and audit services, crisis management, notification of affected third parties, consumer class action or other litigation with customers, vendors, or business partners, regulatory investigations and fines, business interruption or contingent business interruption losses, and loss of reputation and goodwill.

As the threat of cyber attacks increases, dealmakers would be prudent to familiarize themselves with a target's cyber risks and implement strategies, such as cyber representations and warranties in the definitive acquisition agreement and insurance for cyber risks, for minimizing that risk in order to protect buyers in the M&A setting.

Understanding and addressing cyber risks in connection with an acquisition is important for both buyers and sellers. That, however, can be a difficult task. Cyber issues may be latent and the extent of potential damage often is difficult to quantify. Many data breaches, for example, are not discovered for many months or years after their inception. Parties run the risk of closing a deal well before an attack is discovered.

From a seller's perspective, an internal review of a company's vulnerabilities prior to going on the market is a beneficial initial step for several reasons. A would-be target company will strengthen its posture by having already identified and addressed weaknesses in its cybersecurity policies and procedures. Reduced risk of a post-closing cyber attack will be an attractive feature in the eyes of a buyer and likely will be reflected positively in the overall purchase price and in the terms of reps, warranties, and indemnification clauses.

Buyers can conduct due diligence to analyze the potential cyber risks associated with an acquisition target. Such due diligence may include a fulsome set of diligence requests regarding cybersecurity and require complete and satisfactory responses from the seller. In addition to an examination of any known past breaches or other cyber incidents, diligence requests may include a detailed inquiry into (i) the identification of sensitive data and data

assets; (ii) the location of sensitive data and data assets; (iii) the seller's cybersecurity infrastructure; (iv) the adequacy of the target's cybersecurity policies and procedures, including penetration testing, vulnerability assessments, and corrective follow-up; and (v) the cyber-relevant terms of vendor and customer contracts, especially including indemnification provisions for cyber incidents.

Buyers can also incorporate a robust set of reps and warranties regarding cybersecurity within the definitive acquisition agreement to supplement the diligence conducted. While reps are typically tailored to the specifics of the transaction, generally reps relating to cybersecurity will cover at least known incidents as well as the policies and procedures in place at the target company. Additionally, the buyer, through its own research and diligence, will likely have a strong understanding of: (i) whether a cybersecurity industry standard exists for the target; (ii) any applicable privacy laws, such as the Digital Privacy Act or the Health Insurance Portability and Accountability Act (HIPAA); and (iii) the target's contractual obligations and protections relating to cybersecurity. Buyers can specifically track these considerations in the corresponding reps.

If the acquisition agreement contains an indemnity, buyers may consider, based on their diligence, how the cybersecurity reps should be treated related to other reps. For example, for unknown cybersecurity problems, buyers can push for the cybersecurity reps to be treated as "fundamental reps" so they are not subject to the same survival, caps and baskets limitations as non-fundamental reps. And for either known or unknown cyber risks, buyers could negotiate for a "specific indemnity" which is subject to a separate set of limitations and methods of recovery.

An alternative risk-shifting mechanism that has recently become prevalent in M&A deals, especially in the middle-market, is representation and warranty insurance ("R&W insurance"). The rising use of R&W insurance is due, in part, to its increased scope of coverage as well as decrease in cost. An R&W insurance policy typically covers the buyer for losses resulting from a seller's breach of reps and warranties in an acquisition agreement. Good diligence by the buyer may prove helpful as the underwriter will typically rely on the depth of the buyer's diligence, typically through review of the diligence memorandum, when crafting the policy.

R&W insurance is most commonly used in acquisitions of private companies and in "carveouts" (acquisitions of divisions or product lines of public or private companies). Nonetheless, R&W insurance can also be useful for acquisitions of public companies where there is usually no other means of recovery for a buyer for breaches of reps and warranties (because there is typically no survival of reps and no indemnity, due in part to the impracticability of trying to recover from a large group of shareholders).
R&W insurance policies, like all insurance policies, have their limitations. For example, they only insure against unknown claims. Further, like indemnification provisions, recovery will be limited to the extent of the policy limits. Moreover, many insurers are unwilling to insure against various types of risks (e.g., certain environmental or tax risks), which may be expressly excluded from coverage. Fortunately, policies can be negotiated extensively. Dealmakers will want to carve out an appropriate amount of time and resources to devote to negotiating the R&W insurance policy to ensure that the buyer has sufficient coverage for cyber as well as other risks.

If R&W insurance is not an option, or cybersecurity claims are excluded from the R&W insurance policy, another way to protect against the risks of cyber threats is through a stand-alone cyber insurance policy. That policy may be the seller's or the buyer's existing cyber policy, depending on how the acquisition and change of control clauses in those policies are worded and the size of the deal, or it may need to be an entirely new cyber policy. If

a new cyber policy is required, placing a cyber policy sometimes is an extended process, and so early planning and focus on this issue may be essential to a timely closing of the transaction.

The risk of a cyber incident occurring continues to increase, and the magnitude of the costs associated with a cyber incident is likewise on the rise. In the context of M&A, the basis for adequately accounting for cyber risk for buyers and sellers is conducting a thorough investigation into the target company's cyber history, and its cybersecurity infrastructure and policies. Parties armed with this knowledge may then consider appropriate cyber reps, warranties, and indemnities in the definitive agreement as well as cyber risk management through R&W insurance and/or cyber insurance to reflect the risks discovered in diligence.

A special thank you to Richard Doelling, former K&L Gates lawyer and current General Counsel at MDK Hospitality, who contributed greatly to this article.

KEY CONTACTS

JENNIFER H. THIEM
PARTNER

CHARLESTON
+1.843.579.5638
JENNIFER.THIEM@KLGATES.COM

