ANALYSIS

CYBERSECURITY: M&A DUE DILIGENCE AND PROTECTING PRIVILEGE

By Gary D. Gerstman, Geeta Malhotra and Alan C. Raul[1]

The potential liability from a material cyber-attack is wide-ranging. Accordingly, companies that experience network intrusions, system disruptions or unauthorized access to information databases must be prepared for a variety of potential consequences, each attended by its own costs:

- ***Investigation and Remediation Costs.*** Cyber-attacks often take time to detect, investigate, and contain, resulting in significant investigation costs. For example, Sony Corporation reported approximately $41 million in costs related to the highly publicized cyber-attack on Sony Pictures in 2014, primarily for investigation and remediation activities.
- ***Lost Business, Loss of IP, Disruption of Business Operations or Reputational Harm.*** Cyber-attacks may also result in a loss of intellectual property, cause significant disruption of business operations, erode investor confidence, drive away customers or disrupt relationships with partner businesses. In its 2016 study, Ponemon identified lost business as the biggest financial consequence of a data breach, at a cost of $3.97 million per breach.[2] The annual cost of cybercrime and theft of intellectual property in the U.S. is estimated to be nearly $100 billion, with global costs ranging between $450 billion and $600 billion.[3]
- ***Notice Costs.*** If notice of the breach must be provided to consumers, the company will incur additional costs of mailing notification letters, providing credit monitoring services and operating a call center.
- ***Legal Defense Costs.*** Companies must be prepared for potential legal liability as well. Breaches involving sensitive and confidential information often result in class action lawsuits by consumers or employees, or counter-party suits brought by business partners. Shareholder derivative or securities litigation may also follow a cyber-attack that causes a significant loss or negatively affects the company's performance or stock price. Investigating and preparing to defend against these claims can be expensive even if no legal liability is ever imposed.
- ***Regulatory Action.*** Cyber-attacks frequently draw the attention of regulators, including the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), the Securities and Exchange Commission (SEC) and state attorneys general. Industry-specific regulators, such as banking agencies, healthcare or other financial or insurance regulators, and international regulators and data protection authorities may also get involved. The resulting investigations may result in penalties and orders requiring the company to take remedial action.

Noteworthy Aspects of Cybersecurity Due Diligence in M&A

In light of the magnitude of potential liability, cybersecurity due diligence in M&A transactions needs to be a core area of review. Like other diligence processes, there is no "one size fits all" approach. Instead, the extent of diligence will depend on a number of factors, including, for instance, the nature of the acquisition, the availability of resources, the nature of the target company's business, the type(s) of information held and/or used by the target company, industry standards and the overall risk profile. The manner in which the diligence is performed will likewise vary. Diligence efforts will often include some

1 Gary D. Gerstman is a partner in Sidley's Chicago office and a global co-leader of the firm's Technology Industry Group. Geeta Malhotra is a litigation partner in Sidley's Chicago office. Alan C. Raul, a partner in Sidley's Washington, D.C. office, is the founder and leader of the firm's Privacy, Data Security and Information Law practice. The views expressed in this article are those of the authors and do not necessarily reflect the views of the firm.

2 IBM and Ponemon Institute, "2016 Cost of Data Breach Study: United States" (June 2016), http://www-03.ibm.com/security/data-breach/.

3 CSIS Cyber Policy Task Force, "From Awareness to Action: A Cybersecurity Agenda for the 45th President," at 5 (January 2017), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

combination of document and information requests as well as discussions with key information security and privacy representatives. In addition, it can also include an in-depth review or testing of actual processes, procedures and systems. Privacy and data protection issues should often also be included in the diligence process to address personal information issues as well as data collection, use, transfer and analytic practices.

The following provides a sample list of areas of inquiry to help inform an acquirer's cybersecurity, privacy and data protection diligence:

- ***Nature and use of information.*** The types and volume of information collected, used, maintained, shared and/or sold by the target, with a particular focus on information that could be deemed sensitive (e.g., financial data, IP or trade secrets, personally identifiable information, personal health information, etc.).
- ***Representations regarding security and data.*** The representations made to, for instance, its customers, business partners and/or the public regarding security as well as its collection and treatment of sensitive data.
- ***Policies and training.*** The policies, written procedures and trainings in place to help guide security and privacy issues, and how they are applied or administered in practice.
- ***Organization and responsibility.*** The extent to which the target has employed individuals with defined cybersecurity and privacy roles and responsibilities, and dedicated resources to those roles.
- ***Involvement at the top.*** The extent to which upper management and/or the Board of Directors are briefed regarding, and are otherwise involved with, decisions relating to cybersecurity and privacy issues.
- ***Incident history.*** The history of incidents experienced by the target, if any, and the actions taken by the target in response.
- ***HR practices.*** The practices employed by human resources to, for instance, conduct background checks regarding employees (to identify potential red flags), educate employees (e.g., through trainings and the provision of policies) and work with IT to terminate access rights and prevent unauthorized system access as well as the taking or destruction of information upon departure.
- ***Audits and assessments.*** The extent to which the target conducts audits, assessments or other cybersecurity or privacy-related reviews, and the feedback generated.
- ***Technical controls and security measures.*** The technical controls and other protections that are in place.
- ***Encryption practices.*** To the extent not covered by the controls-related inquiries, the encryption practices and controls employed by the target.
- ***Legal and compliance history.*** The target's legal and compliance obligations and history, including, for instance, the extent to which it complies with filing and disclosure obligations, or has been the subject of litigation, government inquiries or government enforcement proceedings.
- ***International issues.*** Other significant international data transfer or cross-border issues, incidents, practices and/or policies.
- ***Cybersecurity insurance.*** Whether the target has cyber insurance and, if so, the scope and coverage.
- ***Third-party controls***. The nature of its third-party relationships as well as the safeguards in place with respect to those third parties, including, for instance, whether the target tracks its third-party relationships, conducts diligence, incorporates cyber- or privacy-related contractual provisions, provides or requires training, limits system access and/or implements other controls.

Through its diligence efforts, the acquirer should focus on asking the right questions so it can understand potential risks and accurately assess value. Based on the results, it can then evaluate whether additional steps can or should be taken to help mitigate risk and/or address valuation issues (e.g., by implementing additional controls, considering cybersecurity insurance, incorporating specific representations and warranties or, in a private company transaction, requiring indemnification), or if no amount of remediation would be sufficient to address the identified issues (which may be a deal breaker, depending on the circumstances).

In any transaction where the consideration being paid includes stock of the acquirer, the target company will need to assess carefully the extent of "reverse" due diligence that should be done on the acquirer. Similar to other areas, the level of "reverse" due diligence will depend upon the relative size of the parties and the amount of stock being delivered. In addition to possibly causing a material decline in the acquirer's stock price, cybersecurity issues have the potential to undermine the benefits of the combination. For instance, if an acquirer does not have sufficient protections to satisfy representations made by the target company regarding the handling of information, there could be challenges integrating the target's operations with the acquirer or leveraging the target's information and systems as part of the combined organization. For these reasons, in many cases, a target company should consider performing "reverse" due diligence regarding the acquirer's (i) use of information and representations to its customers and business partners regarding this use, (ii) policies and training, (iii) incident history and (iv) legal and compliance history. Depending on the outcome of these inquiries and the nature of the businesses being combined, a more in-depth review may be advisable.

Protecting Privilege

Companies experiencing a breach may become the target of lawsuits by government enforcement agencies, consumers, employees, shareholders or business partners. In a public company M&A transaction, the acquirer will inherit these liabilities without recourse to the seller. As a result, if there has been a material breach of the target's systems or if cybersecurity risks are otherwise significant, an acquirer may benefit from a review by a cybersecurity technology consultant. Materials generated by the consultant may be subject to discovery unless the acquirer takes specific steps to conduct the work under privilege. Certain steps should be considered to enhance the likelihood that assertions of privilege and attorney work product will be sustained:

- Consider appropriate non-disclosure and common interest agreements with the target.
- The consultant should generally be retained by outside counsel, not by the acquirer.
- The agreement and statement of work should be signed by outside counsel and should specify that the consultant has been engaged for the purpose of assisting the attorney in providing legal advice, and that the work is being performed at the direction of legal counsel and in anticipation of potential litigation and/or legal or regulatory proceedings.[4]
- As much as possible, the point of contact for the consultant should be outside counsel or (if necessary) the acquirer's general counsel.
- Counsel should participate in communications and briefings between the consultant and the acquirer's internal security personnel.
- The consultant's work flow should be directed by counsel, and the consultant's reports should not be forwarded to the acquirer directly without reflecting or incorporating legal advice.

4 See *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168 (M.D. Tenn. Mar. 10, 2014) (sustaining a claim of privilege over the work of a consultant hired by general counsel to assist with rendering legal advice in anticipation of litigation resulting from a data breach).

As with any other matter where it is important to maintain privilege, it is important to follow standard protocols: mark documents confidential, limit direct communication between the consultant and the acquirer and do not share the results of the consultant's work with third parties. Although no privilege claims are certain to be absolute, taking these steps will decrease the potential of waiver and increase the likelihood that investigation materials are protected from discovery in any future litigation.

A