SAUL EWING ARNSTEIN & LEHR LLP

Alert

CYBERSECURITY AND PRIVACY PRACTICE



JANUARY 2019

AUTHOR

MICHAEL A. GOLD
APRIL F. DOSS
ALEX P. FERRARO
JOURDAN A. SIMKO

Marriott Breach Highlights Importance of Cybersecurity Due Diligence in M&A Deals

SUMMARY

In 2016, Marriott International announced its acquisition of Starwood Hotels & Resorts Worldwide. Coined by Marriott as a "smooth transaction," the announcement of the acquisition received an overwhelmingly positive response. Two short years later, on November 30, 2018, Marriott made an announcement to consumers that received a very different response: hackers had breached Starwood's reservation system beginning in 2014 and continuing through September 2018. As a result, Marriott announced that it had acquired Starwood while Starwood was under cyberattack, failed to identify such a cyberattack during its due diligence investigation, and allowed cyberattackers to continue to compromise the personal data of up to 500 million of its customers, undetected. This announcement caused Marriott embarrassment and left Marriott, not Starwood, to bear the full financial and reputational hit from the breach.

Marriott's current dilemma is not an isolated incident, as both acquiring companies and acquisition targets have seen previously undisclosed data breaches impact deals. Other companies have experienced similar situations with detrimental results, leading to concerns for other transactions large and small. Approximately 63 percent of U.S. CEOs say they are extremely concerned about cyber threats, and only 25 percent of consumers believe that companies handle their sensitive personal data responsibly.

In addition to data breaches of the type experience by Starwood, companies engaged in M&A due diligence should be alert to cyber risks that could compromise the security of a company's critical intellectual property or other proprietary information, and also to whether a target company's data privacy practices are in full compliance with the increasingly complex framework of national and international data privacy laws. Any failings in these areas can significantly decrease a company's true valuation, and expose the acquirer to significant legal risks and costs, including the costs of remediation, litigation and fines. To mitigate negative effects stemming from an undetected cybersecurity or data privacy issue, any potential acquirer must engage in a comprehensive cybersecurity and data privacy due diligence investigation of the target. Appropriate evaluation of cybersecurity networks, systems, and personnel policies and procedures on critical areas such as data protection and cybersecurity awareness, could have a major impact on the value of the target company and the deal as a whole.

Many acquirers still underappreciate the need for cybersecurity due diligence as a distinct risk category. Purchasers frequently combine cybersecurity due diligence with information technology due diligence, when in fact this type of due diligence does not necessarily examine the appropriate risks. Information technology due diligence often focuses narrowly on hardware and technology documentation rather than taking a deep dive into systems, servers, networks, data processing and the ways that targets conduct those processes. Information technology diligence often fails to assess whether a company has a data governance process in place; whether it has a thorough understanding of the data privacy and information protection requirements which apply to its business model and scope of operations and whether it has policies and procedures to prevent, detect and respond to human error or malfeasance.

COPYRIGHT © 2019 SAUL EWING ARNSTEIN & LEHR LLP, A DELAWARE LIMITED LIABILITY PARTNERSHIP. ALL RIGHTS RESERVED.



It's axiomatic in cybersecurity that the very best technology cannot compensate for human failings, and that both technical and organizational measures are necessary in order to have an effective cybersecurity and data privacy program. Traditional approaches to information technology diligence frequently fail to assess the risks created by targets taking or failing to take certain actions. As a result, limited due diligence into information technology will be insufficient to identify dangerous cybersecurity risks. Cybersecurity is a risk category in its own right, one that companies are statistically less likely to report, if they are even aware of potential or actual cybersecurity breaches at all.

The combination of a thorough due diligence process, an experienced team, and a cybersecurity due diligence component should, now more than ever, be an essential part of every M&A transaction. The American Bar Association's publication "The Importance of Cybersecurity Due Diligence in M&A Transactions" identified several key areas of cybersecurity due diligence review:

- A review and risk assessment evaluation of the target's current cybersecurity policies;
- A study of network security assessments conducted by a third-party forensic firm;
- Identification of prior breaches and incident-response capabilities of the target, such as what data was compromised, how the target responded, and comparisons of the currently active network files with a backup that the attacker did not alter; and
- Identifying internal and external threats to past and future cybersecurity safety.

In order to be able to assess these risks, purchasers should update their due diligence procedures as follows:

- Diligence document requests lists should request disclosure of all the target's cybersecurity policies and procedures, risk assessments and network security assessments, both internal and by external consultants or agents;
- Diligence document requests lists should ask targets to identify any prior breaches of their systems and describe incident responses, including seeing incident response reports;
- Diligence document requests should request disclosure of all the target's policies and procedures relating to data privacy compliance, to include the organizational mechanisms for compliance with any national or international regulatory frameworks, including cross-sector regulations such as the European Union's General Data Protection Regulation (GDPR) and sector-specific requirements for data privacy and compliance (such as in the healthcare and financial services industry), as well as the existence of best practices such as data inventory and data governance programs and board-level oversight of privacy and cybersecurity programs;
- Purchaser diligence teams should include cybersecurity experts who should request access to the personnel at the target who are responsible for ensuring cybersecurity as well as responding to breaches;
- Purchasers should consider and consult with their attorneys about the need to hire forensic experts to assess network security and/or compare network files with backup files; and
- The diligence team members with the appropriate data privacy and cybersecurity expertise should interview the target's cybersecurity team about internal and external threats and the level of cybersecurity risks created by the target's business model.

COPYRIGHT © 2019 SAUL EWING ARNSTEIN & LEHR LLP, A DELAWARE LIMITED LIABILITY PARTNERSHIP. ALL RIGHTS RESERVED.

If due diligence is conducted with a focus on cybersecurity and data privacy risks, purchasers will be well situated to request and negotiate the inclusion of certain representations and warranties in the operative deal documents. Such representations and warranties would include:

- Representations about known incidents (and the target's responses);
- Representations that the target is compliant with applicable privacy and data security laws and regulations (which may or may not be focused on the target's particular industry); and
- Representations about the absence of consumer complaints, litigation or investigations regarding privacy and data security.

Representations and warranties are never a substitute for comprehensive due diligence, but they can help to mitigate the purchaser's post-closing cybersecurity risk to some degree, particularly for past or ongoing cyberattacks.

Saul Ewing Arnstein & Lehr's cybersecurity and mergers & acquisitions law practitioners regularly assist acquiring companies and targets entering into transactions in performing due diligence and responding appropriately to due diligence requests. For more information, contact the authors or the attorney at the Firm with whom you are regularly in contact.

This Alert was written by Michael A. Gold, co-chair of the Firm's Private Equity and Venture Capital Practice, April F. Doss, chair of the Firm's Cybersecurity and Privacy Practice, and Alex P. Ferraro and Jourdan A. Simko, associates in the Firm's Business and Finance Practice. Michael can be reached at 202-295-6651 or michael.gold@saul.com. April can be reached at 410-332-8798 or april.doss@saul.com. Alex can be reached at 412-209-2517 or alex.ferraro@saul.com. Jourdan can be reached at 215-972-8675 or jourdan.simko@saul.com. This publication has been prepared for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute "Attorney Advertising."

COPYRIGHT © 2019 SAUL EWING ARNSTEIN & LEHR LLP, A DELAWARE LIMITED LIABILITY PARTNERSHIP. ALL RIGHTS RESERVED.