Bloomberg Law®

bloombergbna.com

Mayer Brown LLP partner Joe Castelluccio continues his four-part series on cybersecurity and data privacy risks in mergers and integrations by describing the importance of data privacy policies in realizing the value of a transaction. The final part will address how cyberattacks can impact a merger or integration.

INSIGHT: Missiles, Malware and Merger Management: Why Cybersecurity and Data Privacy Matter to M&A Practitioners—Part III

BY JOE CASTELLUCCIO

One of the key drivers for a buyer in any merger or integration is to realize the value that was the basis for the transaction. The value of data collected and used by businesses has become a growing part of transaction value. As a result, understanding the ways in which data can be used—and ways it can't be used—is critical to realizing this value.

A company's right to use the data it collects is governed by the company's privacy policies in effect at the time the data was collected. (Separately, certain applicable U.S. and non-U.S. laws may (and often do) have stricter rules that apply despite the terms of the relevant privacy policies. Some of those laws are discussed in the second installment of this series.) But a company's data policies are not static and can be changed over time. As a result, data collected by a company under different privacy policies at different times may have different rights and restrictions associated with them.

As a result, a key part of due diligence in a merger or acquisition is determining what policies—and restrictions—apply to certain data. These restrictions may thwart an efficient integration, limit the ways in which an acquirer may use data in its future business plans, and ultimately prevent an acquirer from maximizing transaction value.

In this context, regulatory authorities can also play a role in ensuring that privacy policies are respected. For example, the U.S. Federal Trade Commission (FTC) has issued public guidance on privacy policies to all companies that may be involved in mergers or acquisitions. In particular, the FTC has noted that a merger or similar transaction does not nullify the privacy promises made by a company when the data was first collected.

Following the closing of a merger or acquisition, the acquirer can take one of two approaches to the target company's data and policies: It can keep the promises that were previously made by the target company to its customers—and maintain the privacy policies that apply to this data—or it must obtain permission from these consumers to make material changes in how it collects, uses, or shares these consumers' data.

Changing policies or privacy promises that relate to data collected prior to the merger require the affirmative consent of the consumer to opt in to the new practices. Changes to practices or usage of data to be collected in the future from those customers requires notice of the change and the opportunity to accept them. (Merely revising the existing privacy policy or user agreement is not sufficient.) In either case, companies that choose to change privacy policies in the wake of a

Joe Castelluccio is a partner in Mayer Brown LLP's Corporate & Securities practice in New York. He helps clients balance risks and opportunities in global mergers and acquisitions with a combination of legal acumen and business experience. He focuses his practice on complex, cross-border M&A, joint ventures, equity transactions and other corporate matters.

merger or acquisition may find that these changes are closely scrutinized by regulators and the public alike.

Despite these hurdles, there are a few ways that an acquirer can seek to limit the surprises—and resulting damage—from restrictive or overlapping privacy policies that apply to key parts of a target company's business.

First, an acquirer should not assume it can monetize the data it is purchasing in a merger or acquisition without a thorough review of the policies under which the data was collected and stored. This diligence may take place at different stages throughout the course of the transaction, but all members of the deal team and integration team should understand the potential impact of data collection, storage, and usage that is inconsistent with the applicable privacy policies. Any restrictions or limitations that are discovered should be shared across workstreams and with the entire team.

In addition, an acquirer should not simply assume that a target company has been following its own privacy policies. As part of its diligence, an acquirer must also review the target's compliance with its policies, not just the existence of the policies. As noted in the last installment, understanding the target company's culture—in other words, how it functions day-to-day, not merely how it looks on paper—will be critical to assessing this type of risk.

In the last installment of this series, I will describe some of the ways that companies involved in transactions and integrations can be vulnerable to cyberattacks and data breaches, as well as some ways to mitigate these vulnerabilities.