Bloomberg Law®

bloombergbna.com

Mayer Brown LLP partner Joe Castelluccio continues his four-part series on cybersecurity and data security risks in mergers and integrations by introducing the broad potential impact of these risks on a transaction. The next two parts will address how data privacy policies and cyberattacks can impact a merger or integration.

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

BY JOE CASTELLUCCIO

In the first installment of this series, I described some reasons why cybersecurity and data privacy issues should be front of mind for M&A practitioners. In this installment, I will talk about the ways that an acquirer's—and a target company's—compliance programs can play a significant role in the success of a merger or integration.

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.

The regulations that apply to cybersecurity and data privacy issues are numerous, overlapping, constantly evolving, and in some cases, even contradictory. One of the most recent and wide-ranging regulations to come into effect is the General Data Privacy Regulation, or GDPR, Europe's new data privacy regulation. Like many other laws in these areas, the GDPR has forced companies around the world to evaluate and, in many cases, make meaningful changes to their compliance programs.

Built into the GDPR is a powerful incentive to comply with it—violations of the GDPR can result in fines of up to 4 percent of a company's global revenue or €20 million per violation, whichever amount is greater. In crafting these regulations and the related penalties for noncompliance, the European Union's motivations were clear: It wanted to make companies outside the EU—particularly in the U.S.—pay attention and comply.

Fulfilling the requirements of the GDPR and similar laws around the world requires strong, efficient compliance programs. This obligation is especially relevant for acquirers in M&A transactions, because compliance programs are critical to successful integrations and strong post-closing performance. In addition to costly fines and penalties, violations of the GDPR (and other similar laws) can also result in slowed growth, missed financial targets, and overall loss of synergies and value that was the basis for the transaction.

While there may be different approaches to addressing compliance programs in the context of a merger or integration, in most cases a successful integration calls for more than just overlaying an acquirer's compliance programs onto the target company's business. If a com-

pany has been on top of its compliance programs—and been proactive about planning for the GDPR and other regulatory developments—it might be tempted to approach this issue by simply leveraging its existing compliance programs onto the target company and the newly combined business. However, there are a number of reasons why an acquirer's compliance program might not work out of the box when applied to the target company or the combined business, for example:

- The target company's systems may not be designed, or able, to function under the acquirer's compliance programs.
- The target company may be operating in countries or jurisdictions where the acquirer does not currently do business. These different countries or jurisdictions may have different (and more onerous) requirements than the acquirers is currently subject to.
- The acquirer's compliance programs may need to be right-sized or adjusted to account for the new parts of the business that come with the target company. While updates and maintenance of these programs happen periodically anyway—or they should—the programs should also be looked at as part of the transaction and integration planning.
- The target company may have aspects of its compliance programs that the acquirer wants to adopt or incorporate into its own programs.

To address these and other mismatches between the compliance programs of an acquirer and a target company, the deal team—and especially the integration team—should look to identify and address several potential risks.

- Out-of-date or non-compliant practices or elements of programs in all relevant jurisdictions (not just an acquirer's or target company's base of operations).
- Incompatible/contradictory practices (within a target company's own programs or between target company's and an acquirer's programs).
- Poor implementation or failure to follow one's own programs. On this point, assessing and understanding culture is particularly important. Even the best-prepared compliance programs can fall short in preventing costly violations and reputational harm if they are not followed.

Any of these risks—or a combination of them—can be costly, result in delays, and jeopardize key milestones in the overall integration timeline. As a result, the deal team should focus on these areas to identify potential trouble spots as soon as possible. Early in the integration planning, integration teams should leverage the diligence performed by other parts of the deal team on these issues to prevent late surprises.

In the next installment of this series, I will describe some of the ways that data privacy policies can hinder an acquirer's ability to realize value in a transaction.