Bloomberg Law®

bloombergbna.com

Mayer Brown LLP partner Joe Castelluccio starts off a four-part series on cybersecurity and data security risks by introducing the issues and scope of potential hazards to the transaction. The following three parts will address compliance programs, data privacy policies, and cyberattacks.

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

BY JOE CASTELLUCCIO

What does a nuclear missile accident have in common with a cybersecurity or data privacy issue in a merger or integration? While it is easy to see that most people would prefer not to encounter either of them, in both situations, small missteps can lead to wide-ranging and potentially catastrophic consequences. As an M&A practitioner, however, you are much more likely to be dealing with the GDPR than an ICBM.

In fact, M&A practitioners are almost assured of encountering these issues in the course of a deal and integration. That's because there is no area in M&A and integration practice that is as complex, rapidly changing, and risky as cybersecurity and data privacy. There are several reasons for this.

- There are few areas in a company's business that have as many different, overlapping, potentially contradictory, and rapidly evolving regulations.
- There's no other area of a company's business that has as many potential weak spots and points of entry. Companies are under constant threat of attack by a diverse group of attackers—crime syndicates, anarchists, profiteers, state actors and hacktivists, to name a few. Every email, mobile device and connected device is a potential entry point and weak link in a company's cybersecurity and data privacy defense system.
- Due to this constant threat, cybersecurity and data privacy issues are at the forefront of discussions in business, government and media. There's no other issue as likely to land on the front page of newspapers, headline cable new shows, trend on Twitter and go viral across the Internet as the latest confidence shaking breach of data security and privacy.

If you are an M&A practitioner and you not sufficiently concerned about these risks so far, there are many reasons you should be. One reason is that hackers do not only target tech companies or other high-profile targets. In fact, attackers frequently do not pick the most obvious targets. For example, attackers may not actually be targeting your information, but they will take advantage of your systems and infrastructure if they are accessible and vulnerable. Attackers can then coordinate attacks on several unrelated networks at the same time, leveraging different pieces of them to achieve their ultimate goals—disruption, theft, ransom, blackmail, and more.

Another reason that this should be front of mind in M&A is that attackers are rarely concerned with unintended victims and are not troubled by collateral damage. For example, one of the largest malware attacks

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.

ever—the NotPetya attack—exploited a flaw in a Ukrainian tax preparation software program and had a wide-ranging impact because most companies that did business in Ukraine at the time were required to use this software. As a result, the breadth of networks exposed ranged from energy companies to banks to the power grid. Even if a company network was not an intended target, it may still have been a victim.

In addition, since the data collected and used by businesses is a growing part of M&A transaction value, it is increasing important to understand the data privacy laws and policies that apply to this data. Different types of data being collected, stored, used, or processed—as well as different countries where data is collected, used or stored—make this a complex and challenging issue to navigate.

As a result, cybersecurity and data privacy issues are not just the purview of a company's IT or security team. That's because these issues don't merely impact an IT network, they impact a company's entire business. As a result, boards of directors are focused on these issues, and so are heads of strategy and business units and all members of a merger or integration team. Anyone that's conducting due diligence, handling sensitive information, or planning for the post-closing operations of the business needs to understand how these issues impact their workstreams, the integration as a whole, and the entire business.

In this series of articles for National Cybersecurity Awareness Month, I will examine three cybersecurity and data privacy issues that can jeopardize a successful merger or integration and put at risk the value being sought in a transaction: compliance programs, data privacy policies, and cyberattacks. While it is nearly impossible to prevent all of these issues, I will also discuss some best practices to mitigate these risks. Stay tuned.