Bloomberg Law®

bloombergbna.com

Mayer Brown LLP partner Joe Castelluccio concludes his four-part series on cybersecurity and data privacy risks in mergers and integrations by discussing some ways that cyberattacks can impact a merger or integration and presenting some best practices for risk awareness.

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

BY JOE CASTELLUCCIO

Cyberattacks and security breaches have become a daily threat to businesses everywhere. A merger or acquisition can increase a company's chances of a breach or attack by opening weak points in a company's defenses and providing opportunities for attackers to access its networks.

There are a number of deal-related activities that can increase a company's vulnerability to an attack. For example, press releases are an obvious source of attention—attackers will know that the companies involved in a transaction will be transmitting sensitive data and information via email and other electronic means. As a result, they can focus their efforts (for example, through spear-phishing) on a handful of senior executives or third-party advisors.

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.

Another example of a deal-related cybersecurity risk is the additional people that come with a transaction or an integration process. In other words, increased numbers of people with access to sensitive information means increased weak points and likelihood of breaches. While these additional individuals may be critical parts of the transaction or integration team, any of them that are not trained to handle sensitive information via email and other electronic means or follow best practices for security can be the weak link that is exploited by an attacker.

Not surprisingly, there are a host of negative effects that this kind of attack or breach can have. To name just a few:

- Loss of data, trade secrets and/or trust; theft of IP: For example, as the result of an IP theft, a company may no longer have a monopoly on its proprietary IP; the stolen IP may now be in the hands of a competing firm or a foreign actor. This can result in a number of different costs and damages, including decreases in future revenues and reputational damage. It may be difficult, or impossible, to quantify or recover these types of damages—or ''un-ring the bell''—from disclosed trade secrets.

■ Loss of deal value: Verizon's purchase of Yahoo is a well-known example. The post-signing, pre-closing announcement of two of the largest cyber breaches in history resulted in Yahoo shareholders receiving $350 million less in consideration in the deal.

■ Loss of cash: Attackers that are able to access bank account and related information for a company may be able to reroute transmissions of money (to offshore or untraceable accounts) or access the bank accounts themselves.

■ Declines in stock prices: Not surprisingly, numerous studies have shown that there is significant negative impact on the stock prices of companies following news of an adverse cyber event.

Despite the broad range of risks and potential damages, there are some best practices that can be used as part of a tailored cybersecurity risk management program to minimize the risks of cyberattacks and breaches in the context of a merger or integration.

One of these best practices is for companies to be up to date on the most current risks and methods of attackers. For example, anyone can sign up to receive free email alerts from the Department of Homeland Security with information about current security issues and vulnerabilities. Moreover, membership in sector-specific Information Sharing and Analysis Centers allows companies to stay current on threats against their industry.

In addition, all members of the deal and integration teams should be trained and aware of these risks and ways to mitigate them. These include ways to handle and share sensitive information (including the status of the deal itself) and ways that attackers may seek to compromise a network, including by targeting individuals on the deal team.

Along the same lines, parties can encrypt sensitive communications, even internally or with outside advisors. In the event a company's system is compromised, this provides an additional layer of security to reduce the impact of a breach before the breach is discovered.

Lastly, the acquirer must have a thorough understanding of the data, software and hardware that will move onto its network prior to joining together its and the target's IT infrastructures. If the target's systems are vulnerable, those vulnerabilities may transfer to the acquirer's systems when they are integrated. If the acquirer cannot get a sufficient level of comfort regarding the target's systems, it may be necessary to run the systems separately until the systems can be appropriately remedied, even if this results in lost operational efficiency and synergies.