The Legal Intelligencer

Cybersecurity and Due Diligence: Avoiding Liability for Someone Else's Mistakes

Corporate acquisitions are like poker games—players have only limited opportunities to improve their hands before the betting ends. When one company acquires another, whether in a friendly deal, the sale of stock or assets in a Chapter 11 bankruptcy, or a hostile takeover, the result is the same: the acquirer bets on the privacy and security practices of the acquired entity.

By **David Shonka and Matthew Rotert** | July 17, 2020

David Shonka, left, and Matthew Rotert, right, of Redgrave LLP.

Corporate acquisitions are like poker games—players have only limited opportunities to improve their hands before the betting ends. When one company acquires another, whether in a friendly deal, the sale of stock or assets in a Chapter 11 bankruptcy, or a hostile takeover, the result is the same: the acquirer bets on the privacy and security practices of the acquired entity. It not only assumes responsibility for protecting acquired personal information but also liability for any pre-acquisition security breaches. Assessing risks is difficult because often the acquiring company has little opportunity to evaluate the cards it does not see. It lacks visibility into the target's cybersecurity protocols and practices. In a friendly transaction, the target will be reluctant to allow any "outsider" to examine its sensitive security secrets; in Chapter 11, time pressures may limit any opportunity for scrutiny; and in a hostile takeover, the acquirer will not have any chance to examine these matters. The result: acquisitions are often consummated with the acquiring company having little knowledge of the target's privacy and security protocols, the

type of data subject to protection, the risks associated with that data, how the target uses the data, or the tools it uses to protect the data. An acquiring company may be forced to gamble with the cards it has been dealt, and the resulting losses can be significant.

The Gamble—the Potential Cost of Not Being Prepared

Enforcement actions related to information security represent more than 70% (€332,967,397) of the fines issued by EU Data Protection Authorities under GDPR as of June 2020. Similarly, the FTC has entered consent orders—including a $5 billion settlement with Facebook related to cybersecurity deficiencies—and has entered strong remedial orders against numerous other companies. Although the CCPA does not generally support a private right of action for all potential damages, California law gives consumers a right to seek statutory damages for breaches caused by poor security practices. Additionally, there is the ever-present threat of class-action litigation based on federal and state statutes. In short, the stakes for an acquiring company are high.

U.K. Information Commissioner, Elizabeth Denham, summed it up this way:

The GDPR makes it clear that organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected.

The Information Commissioner's Office (ICO) has acted consistently with this view. In 2019, it fined the Marriott International approximately $123 million for data security breaches rooted in its Starwood acquisition. Marriott was held accountable for security breaches that likely began within the Starwood group two years before the acquisition. It then took Marriott two more years to detect the breach—a fact the ICO viewed negatively, finding "that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems."

In the United States, acquiring companies are also facing the consequences of their data breaches. In 2016, Verizon agreed to purchase Yahoo for $4.83 billion. After the initial agreement, the parties learned that Yahoo was the subject of cybersecurity breaches that exposed three billion Yahoo user accounts between 2013 and 2016. Because of the breach, the acquisition price was cut more than $300 million to $4.48 billion before Verizon completed the acquisition in mid-2017. Verizon subsequently had to defend a class action lawsuit, which it ultimately settled by paying the plaintiffs $117.5 million and committing to spend $306 million on information security between 2019 and 2022.

These two examples vividly show that the failure to exercise due diligence and take other measures before finalizing any acquisition increases the odds of playing with some very bad cards.

Observing the Players and the Cards to Uncover Information

Just as a successful poker player will observe the other players, be mindful of the observable facts, and understand the odds, so too must an acquiring company learn what it can about its target's privacy and security practices. The goal for a poker player is to know the cards held by other players and the order of the cards that have not yet been dealt—in other words, to have complete knowledge. Unfortunately, that is not possible in poker or in acquisitions where the determination of "reasonable" cybersecurity practices requires a fact-intensive examination and solid legal analysis.

Despite these limitations, the acquirer needs to gather as much intel as possible, and the below is necessary to obtain:

- The identity of all the target's key privacy and security players, including the CIO, the CPO, the IT Directors, Data Privacy Officers, and any other personnel identified in the Privacy and Cybersecurity Breach Response Protocol(s)
- The target's privacy and security protocols, response plans, and actual practices
- The results of a complete forensic analysis of the target's computer and network systems
- Any previous privacy and security findings and recommendations, regardless of the source

- The terms of all third-party agreements involving the transfer, storage, and data security of personal information or other sensitive or confidential information such as trade secrets and financial information
- All publicly available information, including information on the dark web that indicates prior cybersecurity breaches
- A detailed analysis of legacy systems that may be acquired in the transaction and whether there is a need or ability for continued access
- A comprehensive legal analysis of relevant privacy and security issues

Although perfect knowledge is not obtainable, knowing what constitutes complete knowledge can help an acquiring company evaluate the value of the information that it can gather and guide its post-acquisition practices. In other words, it can help it play the hand it is dealt. Moreover, efforts to identify prior cybersecurity breaches *and* potential vulnerabilities must continue post-acquisition. Therefore, the acquirer must develop a post-acquisition integration plan that focuses on privacy and security issues that, at a minimum, includes:

- Engaging a forensic audit team to identify, collect, and review system log files from the target company and to complete data mapping efforts
- Continued retention, if practical, of key individuals responsible for cybersecurity from the target company
- A systematic—and deliberate—approach to systems integration that considers not only how but why systems should be integrated
- The continued engagement of counsel to advise on integration and privacy and security risks and obligations

Card Counting and Hedging Bets

Perhaps the best way to enhance the odds for a lower-risk acquisition is to retain an independent monitor and counsel to conduct a complete assessment and forensic analysis of the target's computer systems and networks as well as its privacy and security programs, and prepare a report of findings and recommendations (if any). This approach offers many advantages. It obviates any risk that the target may later be accused of misrepresentations or concealment. It assures the acquiring party that it is not being dealt low value cards when there is a lot of money on the table. Having such an independent assessment even before any negotiations occur will also facilitate the sale of a company that plans to put either itself or a division on the market. Indeed, a good report may enhance the ultimate sales price.

Similarly, pre-planning can be helpful in Chapter 11 proceedings. Companies are well-positioned to anticipate their own Chapter 11 filings. Given the short time frames that govern restructuring proceedings, having an independent monitor's report already in hand can expedite the process and prevent the risk of last-minute glitches. Absent such preparation, the bankruptcy court may need to appoint a consumer privacy ombudsman to evaluate the privacy and security practices of the debtor, which may cause substantial delays in the proceedings and loss of company value.

Of course, independent assessments and reports are not always available; and the acquiring company must do what it can to protect itself. Perhaps the best way is to hire its own independent assessor and legal counsel to gather as much information as possible and then analyze factual and legal risks based on the available evidence. Here, the independence of the assessor and counsel may be especially important to protect the acquiring party from any starry-eyed analysis of the true state of affairs. Moreover, the related legal advice will be protected by the attorney-client privilege, if suitable precautions and arrangements are made.

When the circumstances do not permit the use of an independent monitor, the acquiring company should insist on an indemnification clause or reserve fund. These protections should specifically and unambiguously cover privacy or security losses that predates the acquisition's consummation. Even when problems are uncovered before consummation, besides (re)negotiating the final acquisition price, the acquiring party should insist on indemnification for privacy and cyber-related liabilities that remain uncovered. While such arrangements are not feasible with stock acquisitions of publicly traded entities, they are likely feasible when an acquisition involves the sale of assets or business units.

Finally, although several years ago cyber-insurance policies were a rarity, today, they have evolved into a robust business line. Assuming a business has such coverage, its acquisition of a new entity or line of business should necessitate a review of the existing policies, and an update to sufficiently cover potential losses resulting from the transaction. Similarly, if a business has not yet invested in such protection, acquiring a new entity or line of business with potentially substantial (by definition) and unknown risks is the perfect time to consider such a policy in conjunction with the acquisition.

Conclusion

Corporate acquisitions inevitably raise challenges and present new opportunities. They do not need to present unavoidable privacy and security risks for the acquirer. Acquisitions should be investments, not blind gambles.

David Shonka *is a partner with the law firm of Redgrave LLP in its Washington, D.C. office. Shonka focuses his practice on issues related to privacy, security, e-discovery, cross-border data transfers, government civil law enforcement investigations, and information governance. Prior to joining the firm, he served three terms as the Acting General Counsel at the Federal Trade Commission and 10 years as the agency's Principal Deputy General Counsel. He can be reached at dshonka@redgravellp.com.*

Matthew Rotert *is counsel with the law firm in its Chicago office. He has over a decade of e-discovery experience and technical skill in a broad range of data privacy and protection issues, including the GDPR, CCPA, and cross-border data transfers across the globe. Rotert is also a Certified Information Privacy Professional/Europe. He can be reached at mrotert@redgravellp.com.*
