Artificial Intelligence and Cybersecurity in M&A

Gregory E. Ostling
Marshall L. Miller
Wachtell, Lipton, Rosen & Katz

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY IN M&A

All companies today rely on networked computer technology in conducting their day-to-day business. Most of a company's transactions and records are created, used, and stored in digital form. The finances, internal and external communications, and even the physical machinery of a business are handled electronically through operational software. Technology has provided companies with significant economic benefits, including reduced costs and increased productivity. However, this reliance on technology has also resulted in a substantial increase in the volume of data to manage and the number of cybersecurity vulnerabilities that can result in major harm to the business and its stockholders in the event of a security breach.

A. Artificial Intelligence

M&A transactions are time-intensive, requiring the parties and their advisors to sift through and organize documents, prepare data rooms and conduct due diligence just in the preliminary stage of contract negotiations. As deals become larger in value and scope and as technology allows businesses to preserve more documents and records for longer periods of time, the due diligence process has become a considerable burden on all parties involved. To increase efficiency, minimize errors and lower costs, companies and their financial and legal advisors are increasingly looking to incorporate technology into the transaction process, such as the use of artificial intelligence platforms in due diligence.

Through coded software, artificial intelligence platforms aim to assist users in conducting due diligence by improving the speed and accuracy of review so that users can focus their time and energy on more sophisticated tasks. Artificial intelligence platforms first filter agreements from non-agreements and categorize them by language and by type of contract (*e.g.*, leases, employment agreements, banking documents). Users can then have artificial intelligence analyze the contents of the agreements for selected standard provisions and extract the information into a separate chart, which can be used in contract summary and due diligence reports. Examples of commonly searched provisions include term and termination, change-of-control, assignability, confidentiality, non-disclosure, and indemnification. Artificial intelligence platforms save this information for as long as the user needs, allowing the user to quickly search for information again if necessary.

Artificial intelligence platforms have offered case studies to support their claims that artificial intelligence increases efficiencies in law firms and legal departments. According to the artificial intelligence platform Kira Systems, Deloitte used the platform in its IFRS 16 compliance review process of approximately 2,500 equipment and real property leases to accelerate the process by up to 30% over manual review.[1] In another example, the law firm Freshfields Bruckhaus Deringer LLP used Kira in its task of reviewing a set of over 11,500 documents with healthcare professionals and medical facilities for a German client in the healthcare sector following a change in German anti-bribery and corruption law to assess its level of exposure. Kira stated that Freshfields experienced efficiency gains of 20–40% on the project with the help of Kira.[2] Another law firm, Fenwick & West, found Kira enabled Fenwick's M&A licensing team to cut document review time by half on average.[3] Other artificial intelligence platforms, such as Luminance Technologies and Seal Software, have made similar claims about the potential value of artificial intelligence to legal practitioners.[4]

Despite the promising developments in artificial intelligence, the uptake of this technology by the legal industry seems to be slower than expected. Although artificial intelligence platforms for due diligence have been around for nearly a decade, only in recent years has there been any significant media coverage of the potential time- and cost-cutting benefits of artificial intelligence in M&A transactions. One reason may be that M&A transactions are costly and risky, so law firms and their clients may wish to adhere to the tried-and-true method of manual review, even if manual review may cost more and take more time than use of artificial intelligence platforms. Some law firms use artificial intelligence platforms to verify their work rather than as the initial first step of the due diligence process. Although the time-saving benefits of artificial intelligence platforms are not realized in such cases, legal practitioners can still use artificial intelligence platforms as a tool to improve accuracy and reduce human error.

Data privacy is another issue to consider in connection with artificial intelligence platforms. As businesses are becoming more wary of cybersecurity issues, they are increasingly restricting access to virtual data rooms and limiting what a user can do with a document. For example, privacy settings can be set so that documents are non-downloadable, non-printable, and/or non-readable by software. At this time, an artificial intelligence platform cannot identify or analyze the contents of such documents, assuming they can be uploaded to the artificial intelligence platform in the first place.

Notwithstanding these hurdles, artificial intelligence platforms have great potential for growth in the legal industry. The greatest strength of artificial intelligence is its ability to continuously learn and adapt through machine learning. Artificial intelligence platforms are generally designed to retain knowledge of key contract clauses and previously encountered due diligence issues and apply this information in subsequent operations. The more an artificial intelligence platform is used, the better it becomes in identifying and analyzing contracts. With enough time, artificial intelligence will develop enough to provide significant assistance to legal practitioners in due diligence.

B. Cybersecurity

Our growing dependence on electronic records, networked computer infrastructure, and computing devices embedded in industrial and operational systems greatly increases the risk of unauthorized access, theft, misuse, and disclosure of a company's data. The U.S. Securities and Exchange Commission recently expressed its concern with the increasing frequency, magnitude, and cost of cybersecurity incidents, stating: "As companies' exposure to and reliance on networked systems and the internet have increased, the attendant risks and frequency of cybersecurity incidents have also increased. Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century."[5]

The costs of failing to keep data secure are increasing rapidly as well. According to an IBM-sponsored study, the average cost of a data breach in 2018 rose 6.4% over the previous year, with costs of high-volume data breaches skyrocketing into the hundreds of millions of dollars.[6] Target Corporation, for example, experienced a data breach in 2013 in which an intruder stole credit card and other customer information from Target's network, ultimately costing the company

"$292 million of cumulative expenses, partially offset by insurance recoveries of $90 million, for net cumulative expenses of $202 million."[7]

In light of rising cybersecurity costs and increasing market expectations that well-run companies will operate effective cybersecurity programs, the acquirer in an M&A transaction often must now consider an assessment of the cybersecurity risk exposure that acquisition of the target may carry. Indeed, in many cases, an effective cybersecurity risk and liability assessment may be critical to properly valuing the transaction.

But while cybersecurity may be an emerging area for attention in M&A due diligence, potential acquirers should approach cybersecurity issues in a manner similar to more traditional diligence areas involving liability and operational risks, through a combination of pre-transaction due diligence, contractual protections, and post-transaction assessment and integration.

1. Due Diligence

The acquirer in an M&A transaction should consider performing tailored cybersecurity due diligence to identify and evaluate the steps taken by the target to protect its electronic information and systems, its intellectual property, and the data with which it has been entrusted by third parties. An acquirer's approach to cybersecurity due diligence should address three primary areas of review.

a. Company profile

Because the cybersecurity risk profile of a target will differ based on the nature of its business and the value of its electronic "crown jewels," the acquirer should first review the target's company profile to judge the level of importance of cybersecurity to the target and tailor its level of due diligence accordingly. The acquirer should begin with an evaluation of the company's reputation, governance, and leadership. A company with strong leadership and a robust governance system is more likely to have addressed the growing issue of cybersecurity and will be able to respond more quickly and effectively to cybersecurity incidents than a less mature company, lacking experienced leadership.

The industry and business model of the target company will significantly affect the cybersecurity risks presented. For example, the core business of a target tech company is likely to be its intellectual property and the consumer data it collects and protects, generally triggering a need for more extensive cybersecurity due diligence. Similarly, more robust cybersecurity due diligence would be in order where the acquisition target is a retail company that manages a consumer-facing website, maintaining personal identifying information of customers and utilizing stored consumer data. By contrast, an acquirer would likely need to perform a more moderate degree of cybersecurity diligence where the target is a B2B company that does not collect or store personal identifying information or other customer data.

The regulatory environment in which the target company operates will also impact the level and type of cybersecurity diligence involved. While companies in industries that are the subject of cybersecurity regulation or geographic locations with stricter data privacy regimes are more likely to have mature cybersecurity programs, they also face enhanced risks of regulatory enforcement if those programs are found lacking.

Notably, in this day and age, where companies of every shape and size and in every industry face cybersecurity risks, from ransomware to phishing campaigns, some level of cybersecurity due diligence is increasingly likely to be a part of M&A transaction diligence.

b. Cybersecurity architecture

Critical to the cybersecurity due diligence process is an assessment of the target's cybersecurity architecture, including its existing Information Technology and Information Security personnel, systems, and controls, to identify vulnerabilities. An acquirer should not only assess the adequacy of the target's technical security systems – from network setup and firewalls to data encryption and backup systems – but also its core procedures, such as cyber governance, data security, access control, and training policies and incident response, disaster recovery, and business continuity plans. And an acquirer should evaluate the target's cybersecurity oversight systems, including internal controls, internal and external audit and testing programs, and the role and level of engagement of executive management and the board of directors.

The acquirer should also evaluate whether the target utilizes third party providers to store its sensitive information or manage security services. Use of third parties can provide additional storage and security firepower, but also presents coordination and communication risks.

While comprehensive cybersecurity systems, policies, and procedures can be indicative of a strong foundation for cyber-defense, how well the target company has operationalized those policies and procedures is equally important. Due diligence should aim to test the effectiveness of the target company's implementation of its cybersecurity systems.

Where the cybersecurity risk is elevated, an acquirer may wish to consider bringing in a third party specialist to perform a deeper analysis of a company's cybersecurity architecture.

c. Incident history

Analysis of the target's cyber incident history completes the three-part due diligence framework. In addition to designing diligence questions aimed at unearthing prior incidents and reviewing cyber incident response logs, the acquirer should pay close attention to any audits of the target's cybersecurity profile and history, including both internal and external audit reports, such as payment card industry (PCI) audits, NIST or ISO 27001 assessments, or other cybersecurity compliance reviews. Prior cyber-related interactions with government entities, particularly regulatory inquiries or law enforcement reports, may shed light on a company's cybersecurity risks and potential liabilities. Disclosures to the market and breach notifications to any third party should also be examined for descriptions of past, open, or potential cybersecurity incidents. The acquirer should also carefully review the target's board minutes and materials, as any cybersecurity incident reported to the board of directors significant.

2. Contractual Protections

In some cases, an acquirer can mitigate cybersecurity risks through the strategic use of contractual protections, similar to those employed to mitigate other liability risks in a merger or acquisition. Contractual protections can be especially useful to apportion risk of an undetected data

breach that may have occurred prior to the completion of a transaction, but which has yet to come to light and whose impact has yet to be experienced.

a. Representations & Warranties, Indemnity, and Escrow

In appropriate cases, an acquirer may wish to negotiate for specific representations and warranties from the target regarding the company's compliance with its own internal cybersecurity policies and procedures, as well as any governmental or industry-specific cybersecurity requirements applicable to the company. In addition, in particular cases, because the adverse effects of a data breach or other cyber incident may remain latent and undetected for months or even years, an acquirer could also consider requesting post-closing remedies that apply for a longer period than is customary.

In a private transaction, representations and warranties can form the basis for post-closing indemnification of damages arising out of breaches that occur prior to the closing of the transaction. As with any indemnification provision, the parties should negotiate in advance key specifics, such as how long the representations and warranties survive and whether a cap or basket will apply to the indemnity.

b. Purchase Price Adjustment

If the target is a public company, post-closing adjustments of the purchase price may be difficult to attain. However, if the target is a private company, the acquirer may consider negotiating for a holdback on the purchase price to cover the costs of cybersecurity incidents the target should have discovered and disclosed. The details of any adjustments, including the procedures for making claims on the holdback, the limit on such claims, and the calculation of damages, would be the subject of negotiation by the parties, with weight given to the size of the transaction and any identified liabilities.

c. Representations & Warranties Insurance

Another risk-shifting mechanism gaining in prevalence in M&A transactions is representations and warranties (R&W) insurance. An R&W insurance policy typically covers an acquirer for losses resulting from a target's breach of representations and warranties in an agreement. The underwriter will typically rely on the acquirer's due diligence when crafting the policy, highlighting the importance of tailored and effective cybersecurity diligence. R&W insurance can provide an acquirer of a public company some measure of recovery, even where there is no survival of representations and warranties and no indemnity.

In a 2016 West Monroe Partners' and Mergermarket's survey of senior executives at entities that frequently conduct M&A transactions, 63% of respondents reported that R&W insurance is among the most important protections in mitigating data security risk.[8] Among the benefits of R&W insurance identified by respondents was the ability to customize coverage for the specific transaction.[9]

3. Post-Transaction Assessment and Integration

Finally, the acquirer in an M&A transaction should plan carefully and proactively for post-transaction cybersecurity assessment and integration, beginning well in advance of the closing of the transaction. Risks and vulnerabilities identified during due diligence should be targeted for swift remediation, and appropriate steps should be deployed to fill in any diligence gaps and identify any undetected vulnerabilities. The identification of potential or existing liabilities by such an audit will enable the acquirer to capitalize on any contractual protections for which it negotiated. Post-transaction integration will then need to be executed strategically across multiple axes, at the personnel, systems, policy, compliance, and governance levels. Great care should be taken to ensure that any vulnerabilities in the target company's cybersecurity systems, policies, and procedures are identified and remediated before they render the acquirer more vulnerable through system integration.

Endnotes

1 *Deloitte Harnesses the Power of Kira for Lease Accounting Contract Review*, KIRA SYSTEMS, https://info.kirasystems.com/resources (last visited September 1, 2018).

2 *Freshfields Wins New Business and Improves Efficiency by 20-40%*, KIRA SYSTEMS, https://info.kirasystems.com/resources (last visited September 1, 2018).

3 *AI Helps Fenwick Work Smarter and Faster*, FENWICK & WEST LLP (July 11, 2018), https://www.fenwick.com/Media/Pages/AI-Helps-Fenwick-Work-Smarter-and-Faster.aspx.

4 Aebra Coe, *Vendors Say AI Will Allow Attorneys To Do Better Legal Work*, LAW 360 (August 20, 2018, 7:18 PM), https://www.law360.com/articles/1075119/vendors-say-ai-will-allow-attorneys-to-do-better-legal-work.

5 SEC Statement and Guidance on Public Company Cybersecurity Disclosures, 17 Fed. Reg. 229, 249 (February 26, 2018).

6 Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview, IBM (July 2018), https://www.ibm.com/security/data-breach.

7 Target Corporation, Annual Report (10-K) (March 8, 2017).

8 Mergermarket, Testing the Defenses: Cybersecurity Due Diligence in M&A, WEST MONROE PARTNERS (July 12, 2016), https://www.westmonroepartners.com/Insights/Newsletters/Best-of-the-West-July-2016/MA-Security-Survey.

9 *Id.*