WATSON FARLEY
&
WILLIAMS

M&A and the Technology Revolution

New digital technology, especially digitalization, has brought massive changes across all industries in the last decade. Indeed, the spread of the technological revolution does not make any exception for those involved in M&A business. It affects the market as well as the process itself in many ways. This paper focuses on two heavily discussed topics of the technology revolution at the moment: artificial intelligence and cyber security.

I. Artificial Inteligence in M&A Transactions

Artificial intelligence (AI) is a broadly defined concept relating to systems which are able to or appear to be able to perform some form of decision making. This ranges from systems that make decisions in a pre-specified, rule-based way to more modern machine learning algorithms, which are able to learn how to make optimal decisions in a given context from examples in a given 'training' data set. The quality of the output usually improves the more data the machines receive.

1. M&A legal practice

There are several parts of M&A deals which are affected by artificial intelligence (AI).

(i) There is the M&A market which seems to be shifting. Deals are increasingly characterized by the acquisition of AI and other information-technology related companies, typically start-ups. Besides the venture capitalists which have traditionally advised in this area, we have noticed an increase in larger corporations starting their own venture capital business by acquiring start-ups to acquire their skills and work. Additionally, the types of collaboration also seem to be more varied: for example, besides the takeover of IT businesses, we have seen an increase in know-how-joint ventures.

This has implications on the way these acquiring corporations are now having to conduct their due diligence. The focus of the due diligence usually needs to move away from the history of the target company to its future development. Aspects such as the capability for innovation and the assumed future market position have to be assessed as being more relevant. This also affects the work of the lawyers who need to provide their views on the legal framework and feasibility of the young target business.

(ii) The transaction process itself can be affected by AI and legal tech in general which we will discuss further below.

2. AI in the transaction process

Although the use of AI tools in an M&A transaction, especially in the due diligence process, is widely discussed most law firms are not yet using AI in their day to day business. To understand why, it is useful to know what kind of tools are on the market and what they are able to do.

(1) AI tools on the market

Digital technology is in use in almost every M&A transaction. Today it is standard to provide the information required for the due diligence via online or virtual data rooms. In recent years, new technology tools have appeared on the market which particularly use AI technology.

In addition to smart contracts and negotiations via BlockChain (which is not yet widely used mainly because the legal conditions are not fully developed), AI is generally used via tools which can identify, classify, organize, prioritize and highlight documents and contracts within the due diligence process and provide a "smart" data room. Such a process is particularly effective for standard, clear terms.

Other tools relevant to due diligence / data include algorithms to search for documents, to translate them and to shift and organize them into helpful order. This can be particularly useful during time-pressured transactions where potentially relevant documents can be more easily identified; moreover, when relevant information may be found in unexpected places such as emails rather than formal written agreements. Furthermore, they are also helpful for the acquirer analyzing the documents for other purposes, for example, automatically detecting certain clauses like rent increase clauses or period of cancellation clauses in lease agreements to detecting potential deal breakers and RedFlags.

Using AI tools in a due diligence process is intended to save time during the legal review of the target company. It obviously takes a lot of time to check all the documents and certain programs promise a 70% time safety not only by checking the documents but also by making it easier for lawyers to quickly identify where relevant documents are located and what content they contain. Being able to check hundreds of documents in a minimal amount of time, with accuracy and detail could lead to improved knowledge about the target which may become beneficial also during the negotiation process.

(2) Limitations of the tools

Programs using a rule-based approach are transparent and predictable. They are already trained and do not need an abundant amount of data to function. The downside is that they can only be used in a few specific cases and need complex and manual development and maintenance. The program needs to be adapted to every single decision or change manually and they will not work for finding terms involving specific information.

To achieve more flexibility 'machine learning' tools seem to be the favored option. They are more flexible, but of course they require supervision and need to be programmed. It is also important that they have enough and high quality data, which can limit their use. However, providers are forced to offer programs in this way because the data required has to be provided by the user. Therefore, their use is limited in transactions which have limited data or are time-sensitive because of the time required to 'train' the system.

Besides these specific limitations AI programs are generally constrained by not being able to undertake consistent semantic assessment. They cannot understand a language in the way humans do. As a consequence the most important part in a due diligence process will remain at the law firms and their lawyers. The main real benefits which firms can deliver for their clients is therefore a time benefit and potentially lower costs in the due diligence process.

These factors are part of the reason why many law firms are not currently using AI programs hence market penetration of AI tools is not currently very strong Other factors for the limited use of AI in law firms at the moment are financial and liability risks. There is a financial risk in purchasing an expensive software license right now without being sure if and how beneficial it will be and

whether clients actually have sufficient trust in the tools. Another problem is the liability. If the output of the tool is incorrect, the liability of the lawyers does not differentiate from the liability for due diligence reports without the help of AI. Therefore, deliverables of the AI will probably have to be checked manually to reduce the liability risk, which falls to the law firm.

Ways to avoid this extra amount of work might be a liability limitation agreement, a suitable insurance or an adjustment of the main contractual obligation, but whether these options are available can be dependent on local law and the strength of the client/lawyer relationship.

3. M&A practice in five years

There is another field of AI, which is called Natural Language Processing (NLP). Researchers in this field try to make it possible for AI programs to be fully understanding, including the legal semantics aspect. It is not currently possible to predict if this will ever be the case or when. So, provided there is no immediate breakthrough in NLP, lawyers will still be necessary during the entire transaction process. The main impact seems to be that their work tasks will change and certain tasks will be fully automated.

Additionally, it is possible that either lawyers need to learn more IT/AI skills or law firms will need to hire experts to use and develop AI systems

Developers of programs which require large amounts of data to ensure they can provide useful outputs, may in future try to solve this problem by ”training” their systems by merging data banks to effectively create a ’crowd-training’ type of solution before providing it to the market so that it is more useful to users. The problem of the lack of data is likely to be solved either way. This is likely to also lead to a higher appreciation of data. The quality and quantity of the owned data might becomea competitive advantage.

Whether full integration of AI will be five, ten or twenty years from now depends on its technical development and how quickly the data problems can be solved. It will be important for law firms not to be left behind and to try to integrate the tools into their daily work. Law firms which have already begun using AI systems and those which begin now can create a decisive competitive edge in certain areas or aspects of M&A transctions, in particular in due diligences where a huge quantity of similar or standardized information is part of the due diligence review.

II. Cybersecurity

1. Cybersecurity issues in M&A transactions

(1) Overview of different cyber risks

Cyber risks in general can be separated into different groups.

(i) Cyber risks that can be traced back to human failure. This can be simple things like using open Wi-Fi, faulty operations of IT-systems but also the non-observance of rules and laws. Regarding the latter, the acquiring company should assess the target’s compliance with privacy and data protection laws in its home country as well as in any international jurisdiction where it

operates. It is important to be aware that certain countries may impose privacy and data security laws that are more far-reaching than others. In the U.S, compliance with federal laws, which are relevant to the target's industry, should be assessed.

(ii) Being the victim of a hacker attack. This could range from data sets being stolen or malware installed via USB-sticks. In these circumstances, it is conceivable that the company network will be overloaded with requests, so that it cannot be used anymore.

(iii) Blackmail Trojans, which are distributed via security lacks in web browsers, email attachments or file hosting services.

(iv) In addition to the above, there are also "non-human" risks like blackouts or force majeure.

The above mentioned issues have general application in addition to being relevant to M&A transactions. From the perspective of a law firm it is important to make sure that the own security and data infrastructure is robust and that employees are trained and understand the risks. In the context of an M&A transaction, it is important to ensure that the same approach is being implemented by the target company both for due diligence and also generally by it and the acquiring company so that a cyberattack during the M&A negotiation does not hold up or terminate the deal or implies a major risk for the business itself not only due diligence but also going forward after closing.

(2) Businesses with particular cyber risks

Depending on the business of the target company, a transaction may be heavily influenced by cyber risks. Special attention needs to be paid to the following types of businesses:

(i) If a target is particularly interesting because of a special idea or know-how, a cyber-attack during the process can be a potential deal breaker.

(ii) If a target uses critical infrastructure, a cyber-attack may paralyze the entire business. Because these risks are so incalculable, Germany passed the IT-Security-Law (IT-Sicherheitsgesetz) which imposes special requirements for these companies regarding cyber security. Generally, these companies are obliged to maintain the highest IT security standard for the critical parts of their business.

(iii) Companies whose businesses are data driven or which have a huge amount of data have to be watched more carefully as well. Buying a company means buying the company's data, which can also mean buying its data security problems. Across all industries the costs for each data breach amount 3,2 Million Euro.[1] These costs have to be considered when setting the target price. It is therefore important to make sure the data was gained legally and can be used in the intended manner (including the transaction). Having to pay fines is one risk. In Europe it is possible to impose fines up to 20 million dollar or 4% of the annual turnover due to the new European Union's General Data Protection Regulation

[1] *Zahn/Kuegler*, Erwerb digitaler Targets – Implikationen für den M&A Prozess, M&A Review 9/2018 p. 286, 288.

(GDPR), which came into effect on 25 May 2018. Additionally, it can involve a disproportionate effort to restructure a company to operate in conformity with data protection requirements.

(iv) The proper way to handle data is even more important if the business model itself is data driven. There is a risk that the acquirer may be forced to delete data and not be able to use it after the merger. This can depress the value of the target enormously.

Potential pitfalls can not only derive from the target gaining the data illegally but also from the acquirer. Existing data sets from the acquirer cannot always be consolidated legally with the new data sets because acquired data is often tied to a special purpose.

In addition, attention should be paid to checking whether the target's existing IT infrastructure is fully licensed and compatible with the IT infrastructure of the acquirer. Usually these problems are addressed in IP and IT due diligences, which will, no doubt, continue to evolve into a standard procedure.

2. Cyber due diligence on the buyer side - cyber-speficic reps and warranties

To more fully estimate the potential risks, it is essential to undertake cyber due diligence. The scope of this will vary from case to case, but there are some issues which should be considered in almost every case.

(1) Content of a cyber due diligence

In relation to the target company, cyber due diligence should be considered both from the inside-out perspective as well as the outside-in perspective.

The Inside-Out perspective examines the information standards and the IT-security standards (security controls). This includes governance aspects such as policies, respective guidelines or segregation of duties as well as technical aspects such as encryption of data carriers, virus protection for servers and end devices and network security. Results of former IT-security audits or technical security reviews (penetration tests) should be examined. If no recent audit reports or reviews are available, statements regarding possible data breaches or other IT-security incidents in the recent past will not be possible within the M&A contracts or due diligence.

If the inside-out perspective cannot be performed due to a lack of information[2], the outside-in perspective should be undertaken. This is essentially a backwards-looking security examination which does not rely on any information about the target company's cyber performance in the recent past. It investigates whether compromised records can be found via file sharing (optionally also in the dark net), whether stolen access data of employees are accessible and it also checks technical standards such as patching the server or secure certificates of the externally accessible systems.

From all of this, the potential buyer should be able to obtain the required information which includes: not yet revealed cybersecurity problems, estimated costs to remediate the issues, information about the risk of existing problems, indication of compliance problems, understanding of

[2] *Zahn/Kuegler*, Erwerb digitaler Targets – Implikationen für den M&A Prozess, M&A Review 9/2018 p. 286, 289.

security framework and architecture and awareness of breaches and how they have been responded to.

(2) Consequences of the due diligence

There are different ways to deal with revealed cybersecurity risks and issues. It is possible to agree on representations and warranties, which will typically include what has been disclosed during the due diligence and what has not been disclosed or cannot be accessed. Buyers could ask for representations and warranties that cover the absence of current and past security incidents, implementation of appropriate internal rules and regulations, compliance with applicable law and the absence of disputes and investigations.

In the case of existing, but not yet quantifiable risks, indemnification letters are the better option. These apply mainly for general cyber risks as they are comparable to pending litigation or environmental letters.

Another way of dealing with the revealed risks are MAC clauses (material-adverse-change), which protect the buyer from negative developments of the target between signing and closing. This is especially relevant if there is a long time between signing and closing and because not every cyberattack will result in or be sufficiently covered by a breach of warranties. Besides warranty claims further consequences might be a reduction of the deal value.[3]

3. Cyber insurances

One option to insure cyber risks in an M&A transaction is to obtain representation and warranty insurance. Both parties are able to obtain it. This type of insurance has been on the market for 30 years but for a long time, it was too expensive for many companies to obtain. While this type of insurance is now more affordable, it is typically confined to the middle market transactions because the maximum insurance sum is often not high enough for higher value matters. In addition, the insurance only covers direct financial losses or damages resulting from the breach of the reps and warranties. In most cases predictable, highly probable damages are excluded.

A cyber risk insurance, which is not related to M&A transactions, could be a useful addition to the representation and warranty insurance. It offers comprehensive coverage for cyber risks (which includes a coverage for indirect damages and consequential damages) while a rep and warranty insurance covers individual guarantee statements only. Therefore the cyber risk insurance is advantageous for the target company if it is a victim of a cyberattack during the M&A transaction or before, with consequences such as a failure of the transaction or a decrease in the value of the target company. It is also an advantage for the buying company to take it over in case third party claims arise due to an earlier cyberattack (for example because of the loss of sensible data). Risks like the failure of infrastructure or costs in connection with finance market transactions are usually excluded, but can often be underwritten on a case-by-case basis whereas it is not possible to underwrite deliberate or knowing derelictions of duty. It might also help if the cyber security issues only arise after closing and after the expiry of any time limitations for claims of the buyer against the seller under the M&A contract

[3] Freshfields Bruckhaus Deringer, Cyber Security in M&A, p. 11.

4. Awareness of the cyber security issues

General awareness of cyber risk issues– and in M&A transactions - has certainly increased. This is reflected in the amount of legislation and regulations[4]; in particular, in relation to individual data protection such as GDPR and also arising out of a series of high-profile strikes on businesses including eBay, Target and Yahoo!

Nevertheless, we have not noted any meaningful changes in the M&A transaction practice as yet. The explained – and strongly needed – cyber due diligence is not undertaken in most transactions. In a study conducted by Freshfields Bruckhaus Deringer 2016 78% of the surveyed[5] believed that cyber security is not analysed in great depth or specifically quantified as part of M&A due diligence.[6] Despite that, the same survey shows that 90% of those surveyed believe that cyber security breaches can reduce the value of a deal.[7] What has changed, however, is the increasing use of security technology on phones, laptops and in virtual data rooms.

Although more firms are now offering training for deal teams, there is lot of room for improvement, especially regarding the use of cyber due diligence. The most likely reason for the general lack of practical implementation of cyber security due diligence is that this topic is still a relatively new area for advisors as well as for their clients. This applies even more for Europe than North America, which may be due to the difference in the amount of follow-on litigation (class actions).[8]

Torsten Rosenboom
Partner
Watson Farley & Williams

[4] E.g. Statement on cyber security published by the U.S. Security and Exchange Commission, Cybersecurity Requirements for financial service companies published by the New York Department of Financial Services (specifically addresses to risks in M&A transactions).
[5] 214 global deal makers from corporates, financial institutions, investors and legal service providers.
[6] Freshfields Bruckhaus Deringer, Cyber Security in M&A, p. 6.
[7] Freshfields Bruckhaus Deringer, Cyber Security in M&A, p. 6.
[8] Only 39% of the Europeans have seen cyber security due diligence become a key part whereas 51% of the North Americans have; Freshfields Bruckhaus Deringer, Cyber Security in M&A, p. 9.