Data Due Diligence in Investment and Acquisition

Are we buying a company…or a big fine and a trashed reputation?

An already much quoted case study, the Starwood Hotel Business acquisition by the Marriot Hotel Group has attracted comment from Data Privacy Professionals, not only because it involves an American company, but due to the apparent lack of attention the M&A due diligence process gave to key new, high profile, data privacy, security and protection regulations – in Europe and globally.

Marriot have been criticised and have received a notice of intention to fine from the ICO, the UK data protection regulator, for not investigating more deeply the data breach suffered by its acquisition of Starwood Hotels, albeit back in 2015. The ICO said that, "With all the resources they have, they (Marriott) should have been able to isolate hackers back in 2015."

The Key Lessons:

- Accepting on trust that there are good security practices, good data hygiene and that no breaches have occurred is not enough.
- Investors and acquiring organizations should see proof of security practices and controls, policies and actual processes from the target organisations.
- All investors and acquirers should perform extensive technical due diligence to ensure their investment is wise.
- Target organizations should be prepared or risk a reduction in valuation or cancellation of investment.

The regulatory and commercial importance of data privacy and security has been increasing rapidly in parallel with the growth in the information economy. In general, data are the most critical assets of a company. In an M&A context, it is now more important than ever to understand what personal data is held within the organisation, where that data is held, who can access the data and how the data is processed and used.

- The stick: large fines being imposed by regulatory authorities for data privacy breaches and data misuse.
- The carrot: competitive advantage through increased and stakeholder trust. We are also likely to see increased interest from investors and acquirers in companies that have class leading data asset management.

When considering acquiring, investing or partnering with another organisation, it is common to undertake a due diligence process. This often concentrates on financial metrics and financial risks. Technical and Intellectual Property due diligence is often undertaken, to a greater or lesser extent. Often this is a box ticking exercise that tries to identify obvious risks.

Dr Graham Dodgson of The Trust Bridge states that "Now must be added a data protection audit. Every acquiring company or investor must undertake this process with the utmost thoroughness. An inadequate due diligence process opens the acquiring company up to immense financial and reputational risks."

The Data Due Diligence process should ensure that the organisation to be acquired conforms to data regulations, and if not, has demonstrable plans in place to become fully compliant. This will typically be achieved by means of a detailed due diligence questionnaire and the review of existing policies and procedures.

Equally importantly, the acquirer must carry out a technical audit to establish whether the target company is aware of:

- what its data assets are and where they are;
- the level of accuracy and importance of any data asset;
- access permissions to that data;
- what physical and cyber security protocols are in place;
- whether the data are "portable".

This must include continuing processes to cope with the inevitable data security problems that will arise, such that any disruption caused will be ameliorated, especially where user data is involved.

This is not a one-off fix for the organisation.

Excellent data asset management is key to business performance and it is not an exaggeration to say it will be key to survival.

Although many of the current regulations of concern deal with personal data, the data assets of a company cover much more information and knowledge. In general, it behoves a company to understand data at a strategic level and not assume just because the company is compliant with regulations at a given time, all is well with the organisations data policies and procedures.

The "How" of Data Due Diligence

An outside expert advisor is key. An organisation that understands the regulations, what new regulations are emerging and has the legal and technical expertise and resources to assess risk and fix what is non-compliant or should be improved.

When hiring a specialist firm to investigate the data management of an organisation during the due diligence process, it is important to assess the **financial and business risks** involved in any subsequent deal, whether acquisition, merger, investment, or partnership.

Key to this risk assessment is understanding, not just the current situation, but also developing a remedial plan to achieve current regulatory compliance. Assuming there are deficiencies, an action plan is then vital to move the organisation towards best of breed data asset management.

For example, we work with clients to implement any necessary changes to operations and procedures to comply with regulations. Over and above this necessary level of compliance, there is an opportunity for companies to evolve their data security and privacy systems and processes into best practice. And to embed a data-aware culture across their organisation and third-party suppliers and partners.

"No acquirer or investor can afford to take on trust that an acquisition target has full control of their data and that they are compliant with existing and emerging regulations." Alex Brown, Partner, Simmons & Simmons.

It is important to note that an acquisition target organisation may not be compliant with regulations but may well be attractive once an understanding is gained of the financial, operational and technical implications of bringing the company to good practice.

Our services help guide the acquirer to make an informed decision to proceed with the takeover or merger, and whether to modify the takeover conditions or price or seek other forms of protection in the deal documentation.

It may also arise that an acquisition target will be considered even more valuable if its data privacy and security systems and processes follow best practice and are more developed than those of the acquiring company. In this case, the acquirer can learn from the target company and reverse engineer their processes and procedures into the acquirer.

In this sense the acquirer is leveraging the intellectual property of the target company since excellent data systems and processes can be considered valuable proprietary knowledge in much the same way as a better production method for a product or a patent on a technical product or process.

Following an acquisition, there will be a period of alignment, both with regulation and between the policies, processes and systems of the two companies. The priorities for regulatory alignment will have been identified during the due diligence/ audit process. This may well require staff training and education, amalgamation of records of processing activities, reviews of the risks including undertaking or updating Data Protection Impact Assessments across the combined organisation, management of data subject rights and consents, and standardisation of all legally required documents. Again, this post acquisition activity should not be under estimated.

Conclusion:

Data privacy and protection regulations, starting with the EU General Data Protection Regulation, have forced organizations to revise their data practices, and demand that better processes are implemented. Good data hygiene, high levels of security, and transparency of data use across the entire data ecosystem, including 3rd parties, together engender greater trust in customers and suppliers. This extends to any investor or acquirer of a business.