Cyber due diligence in transactions

Preserving value

November 2022

PERSPECTIVES

www.accuracy.com

Analysing.

Questioning.

Deciphering.

Discover our Perspectives on trends, industries, technologies and so much more.

Protecting data, preserving value

Due diligence ahead of a transaction generally focuses on analysing the finances of the entity in question, as well as its market and strategy, in order to prepare financial forecasts and determine its value.

In addition to these essential criteria, other elements, including tangible and intangible assets, infrastructure, intellectual property and the company's customer portfolio, must also be taken into account and evaluated, depending on the business sector.

THE DATA AT THE HEART OF THE COMPANY

In an ever more digitalised economy, information systems take on an ever more central role, particularly when it comes to infrastructure. Intellectual property and customer portfolios are systematically digitalised, insofar as the intellectual property is often software and the portfolios are often databases. This group of assets, though heterogeneous in appearance but linked through their digital nature, is therefore often designated by the generic term 'data'.

Such data, which remains important no matter the case at hand, has now become essential, particularly in industry and software, where processes are at the heart of value. Indeed, this applies to such an extent that a transaction is now perhaps less the sale or acquisition of a company in its classic sense and more the sale or acquisition of intellectual property and/or a customer/user database.

In short, acquiring a company comes down to buying data.

THE DATA AT THE HEART OF VALUE

With these developments in mind, significant changes in terms of valuation have come to light, especially considering that the generic term 'data' may well include a mix of technical data (codes or processes) and personal data with particular characteristics.

This data diversity has consequences: the wealth it covers whets the appetites of a wide range of parties, including those with few scruples between them. Moreover, public authorities, judging (with reason) that it is their duty to protect the personal aspect of this data, have created legal and regulatory frameworks for holding and using data, non-compliance with which may lead to considerable financial penalties.

INTEGRITY AND SECURITY OF DATA, ESSENTIAL CRITERIA FOR VALUATION

If valuing data lies at the heart of valuing a company in the context of a transaction, it is essential to scrutinise the data's security and integrity. This applies not only for obvious security reasons but also for financial reasons linked to the objective valuation of the company and the regulatory environment in which it develops.

1 The cyber stakes in a transaction

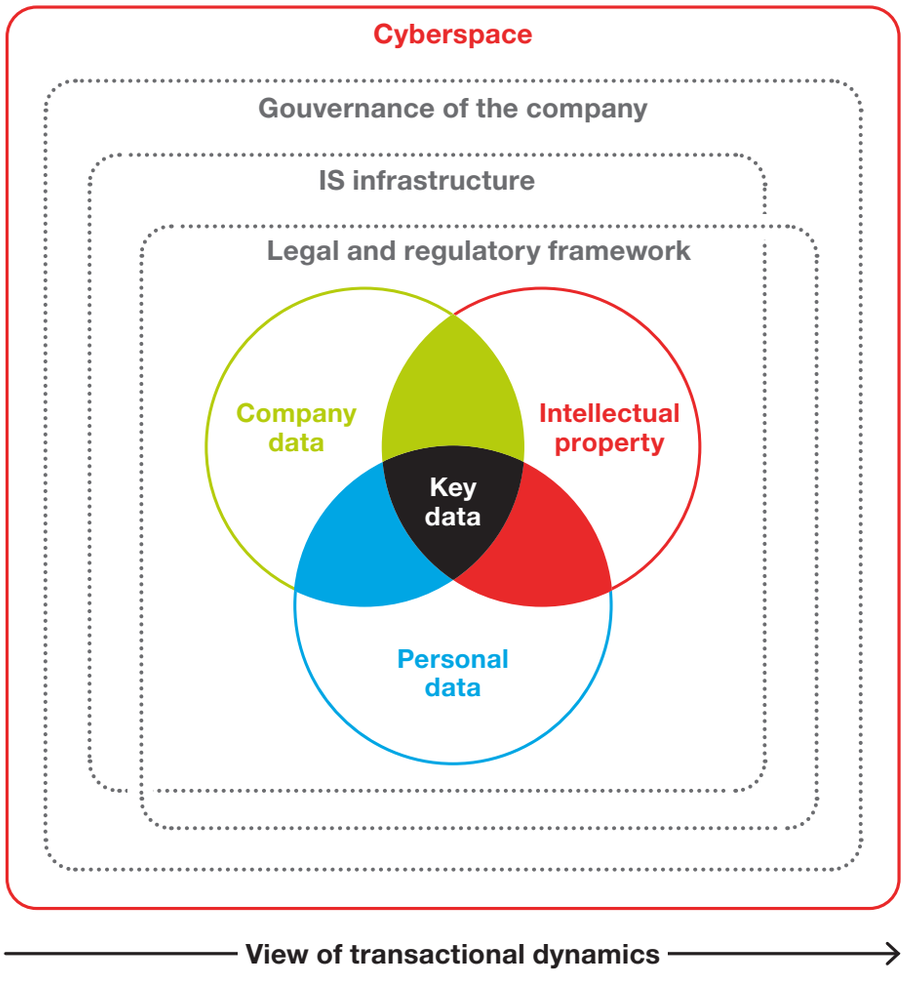
The cyber stakes in a transaction are multidimensional, touching on highly technical aspects, corporate management and even legal and insurance elements.

The approach to these different topics must focus on two critical elements: (i) the precise identification and conservation of key company data and (ii) the constant consideration of dynamics specific to a transactional context.

It is therefore not merely a question of judging the 'thickness of the ramparts' of the company (i.e. the robustness of its information systems), but rather of tackling the topic in its entirety as part of its past, present and future development.

The issue is therefore vast. Key data, infrastructure, the legal framework, governance and cyberspace are all points to consider in the strategic and mobile context of a transaction.

Cyberstakes in transaction



Source: Accuracy

Incorporating cyber in a transaction

2

ON THE BUY-SIDE (BSDD)

A transaction from a buyer's perspective is particular in that certain constraints set by the target must be accepted and the due diligence process may have to be conducted in a very short time frame. This set of circumstances is not particularly conducive to in-depth analyses before signing.

Nevertheless, the risk of acquiring an empty or compromised shell must remain at the forefront of the buyer's mind throughout an acquisition process. The difficulty in obtaining a precise idea of the target before signing should lead to a phase of in-depth analysis between signing and integration, the aim of which would be to avoid any incidents and to be able to foresee any price revaluations and remediation, if necessary.

The following three-phase approach is critical to ensuring a productive and safe transaction.

Phase 1 – Prepare

The actions able to be taken during this phase depend on the willingness of the target. For this purpose, the degree of consideration given to cyber elements in the sell-side due diligence is an indicator of the level of maturity of the target on this topic. A cyber clause can be included in the price negotiation.

Phase 2 – Perform

The actions to be taken during this phase must be performed with care and control to ensure that the buyer's initial business is not corrupted by the integration of a compromised target. Capacity for cyber crisis management must be adapted and maintained during this phase.

These analyses can lead to a price revaluation.

Phase 3 – Prolong

Processes and systems should be harmonised quickly – unless facing exceptional circumstances – so that incomprehensible and possibly divergent organisations do not survive for long.

ON THE SELL-SIDE (SSDD)

The transaction from a seller's perspective offers greater possibility for a longer and more complete process, especially in the context of a complex carve-out from a group. During the due diligence process, adaptations or even improvements to the cyber policy can be made if necessary.

In any event, the approach should have two objectives:

- To secure the division of systems and data that will result from the transaction, in order to maintain the security and integrity of the remaining value during the process and afterwards
- To be financially assessable as part of the transaction as a guarantee of the value and integrity of the asset sold.

Again, the three-phase approach is critical.

Phase 1 – Prepare

Cyber due diligence should be considered as an investment that makes it possible to obtain a price supplement on the sale and contributes to avoiding legal and financial risks that a subsequent cyber incident could generate.

Moreover, the due diligence should facilitate the precise and secure carve-out of data in order to control the cyber risk on the remaining part of the business.

Phase 2 – Perform

The seller should be able to answer all the legitimate questions of the buyer. However, it will be necessary to monitor the security and confidentiality of the data when facing buyers with unknown motives. As a result, VDD reports created by trusted third parties during the preparation phase should answer the quasi entirety of requests.

This transparency and seriousness should be valued financially.

Phase 3 – Prolong

Preserving the value of the data in the remaining entity should be a priority during the transition phase and the subsequent phase. This change can lead to changes in governance but also to reflections on investments and renegotiations of cyber insurance.

3 For a strategic vision of threat analysis

Cyber threats must be factored into a transaction. Indeed, the parties involved in a transaction need an accurate picture of the asset at stake, and it is perfectly legitimate and necessary for them to take cyber threats into account in this process. In addition, because of the organisational changes it induces and its intrinsically strategic nature, a transaction gives rise to threats that can take several forms:

- An opportunist taking advantage of the vagaries of changes in governance and control
- An activist seeking to prevent an undesirable business combination
- A brutish competitor looking to compromise a transaction that may be unfavourable to its interests
- A state actor spying on or blocking a transaction that it considers a threat.

These threats, which can even be cumulative (e.g. a state actor manipulating a militant to compromise a transaction for the benefit of one of its national champions, a competitor of the target) are not just the fruit of the imagination. Preventing them naturally raises the question of their attribution, or more simply of their origin.

This attribution is made possible by the analysis of technical data on cyber incidents within the company, the search for similarities with known elements (technical design and modus operandi). Done well, this attribution is very instructive. In particular, it can help to shed light on the competitive and geopolitical context of the company and to decipher the way in which its adversaries react to its strategy.

Such a detailed understanding, once acquired, naturally has a feedback impact on the company's strategy, its design and its geo-economic implementation. It can lead to reinforcement, adaptation or reorientation with more informed arguments.

Far from being an area reserved for IT technicians and engineers and unrelated to the business challenges of a company, cybersecurity can therefore be an integral part of the company's strategy.

About Accuracy

Accuracy is a wholly independent international consulting firm providing advice to company management and shareholders for their strategic or critical decisions, notably in transactions, disputes and crises.

Accuracy's strength is to connect strategy, facts and figures. Accuracy's teams are international and multicultural, combining various skills to provide bespoke services to our clients. We recruit consultants from the best.

Accuracy is present in 13 countries in Europe, North America, Asia, Middle East and Africa and leads engagements all over the world.

We serve our clients all around the world

Nicolas Bourdon
Partner
nicolas.bourdon@accuracy.com

Arthur Couvreur
Director
arthur.couvreur@accuracy.com

Accuracy

www.accuracy.com