PERSPECTIVES

The new Cyber challenges in a transaction context

in collaboration with SYNACKTIV

March 2023

Values and data in a transaction context

Vendors and investors usually define a period of time during which different analyses of the assets covered by the potential transaction are concentrated. Enshrined within the term due diligence, the reflections carried out may be of various natures. While financial, tax, and legal are the classics of the genre, a new discipline is beginning to emerge: analysing the enterprise's exposure and compromise to future or past cyber attacks. While the principle seems simple, cyber due diligence actually hides a variety of very different and complementary aspects, far beyond solely the technical issue. The digital revolution means redefining the scope of the risk for the enterprise.

The angle selected here is that of the buyer analysing a target. However, any areas discussed in this context could enrich an analysis conducted by a seller prior to a transaction.

Understanding the target environment

Just as the financial analysis of an enterprise or an asset is informed by its confrontation with market comparables, cyber analysis is greatly enriched by contextualisation of the threat facing the entity. Also, before undertaking a cyber resistance analysis, it is relevant to understand the ecosystem in which the enterprise operates and its potential particular features. Using these benchmarks, analysis of existing cybersecurity investments and mechanisms helps to better estimate cyber risk awareness and the level of maturity of the enterprise. The challenge is then to assess whether this perceived level of risk is appropriate in relation to the threat and the investments made.

The threat is not the same for everyone. Although any structure with systems connected to the internet faces systematic threats, with phishing attempts being the most known, some assets have to be concerned with more targeted attacks: particularly lucrative sector, strategic or politically controversial activities or entities and sectors known for their low technical investment, etc. Depending on the complexity of the case, this first step in a comprehensive cyber analysis requires linking various competencies. These include knowledge of the sector-specific threat history, an enterprise's reputation and incidents, and even geopolitical decoding of its market and the country it is based in. The level of threat related to the conflict between Russia and Ukraine could more broadly impact allied companies on an economic or a logistics supply level (energy, military, humanitarian, etc.). On another level, we note that the hospital sector is largely targeted by ransomware in view of their exposure, but also by the amalgam that exists without a doubt with attackers between the French public hospitals' model and that of American private hospitals. In the context of a sensitive activity (the concept of a significant or essential entity has been re-specified again recently by the European NIS2 directive – energy, transport, finance, health players, etc.) the assessment even benefits from relying on a comprehensive analysis of the risks faced by the enterprise, among which cyber risk is only one element. This must therefore be understood as both a risk in its own right as well as a supporting risk for the scope of other risks. Thus, a vulnerability on a server exposed to the internet can lead to a risk of major media exposure following a disclosure of the data. Internally, failure to manage permissions on an accounting application can alter the truthfulness of the enterprise's financial statements.

A valuable component for financiers, this first step can lead to a comparative study of losses in the sector caused by cyber attacks, thus providing a first quantified conclusion.

While it is currently rarely practiced, particularly due to the wide skill set required, this preliminary step of threat analysis as a whole provides highly innovative enlightenment for most economic players. In all cases, it allows us to address the analysis of the enterprise's internal mechanisms, this being the subject of the next step, with a much more detailed understanding of its issues, in its market and its geography.

Defending the castle...

This is the most obvious point of attention and is the best known: are the target's information systems normally robust, i.e., can they withstand reasonable attacks? The buyer, beyond the security issue of its asset, is wanting to know whether the target will require additional investments to improve its shielding or to align it to a level of security equivalent to its other assets. Price is therefore at stake and this new element tailors it according to its conclusions, opening up a new field of negotiation.

Unsurprisingly, the issues raised by cyber due diligence bring up issues of normativity and market practices. In fact, absolute protection against cybercrime is almost impossible to guarantee, everything being a question of the time and resources deployed by attackers. So, it's about judging the reasonable resistance and detection capabilities of a system against professional attackers, but also looking for efficiency to turn to easier targets. When it comes to cyber, like elsewhere, you need to know how to calibrate your response to have a level of security within a mean that is highly proportionate to the risk and threat level assessed in the previous step.

In the due diligence phase, it is therefore a question of usefully informing the buyer about the level of embedded risks without unnecessarily causing alarm. The knowledge of the market and the average level of protection deployed, acquired in the preliminary phase, will therefore be a key aspect of the quality of the analysis proposed to maintain a reasonable recommendation, which informs the negotiations around the price in a balanced manner.

To do this, what practices are accepted in the due diligence phase to conduct an internal analysis? Two main types of work will be differentiated:

- It may first be an analysis on a documentary or reporting basis: understanding of systems, regularity of maintenance work and backups, tests, conclusions of tests carried out and corrections made, level of obsolescence of the installed base and technical debt, structuring of IT teams, etc. This work shows an overview of the attention paid and the resources deployed by the target to cyber risk management. This operating procedure is frequently accepted by sellers. It requires approximately two to four weeks of work, which is perfectly compatible with the time allotted for other due diligence. This work often involves good coordination with the target's teams in order to initiate an effective dialogue.
- Less common, the Penetration Test Exercise (Pentest) seeks to obtain an independent measure of the stability of the device by looking for vulnerabilities, i.e., attempting to break into the target's systems, either from outside or with access to the corporate network. This work stops when access is gained and never reaches the point where information is copied. However, these tests are obviously more intrusive and involve having a formal agreement from the seller. They are limited in time and scope: implementation is ultimately simple and quick, as it does not require the use of the target's teams, and the target can also continue its routine business. These situations are common, or even regulatory, when cybersecurity is at the core of the enterprise's business or in particularly exposed sectors. It is obviously more difficult for the competitive processes of M&A to lend themselves to this mode of due diligence, unless they switch to exclusivity, usually giving a few additional weeks to carry out these investigations.

...but for what treasure?

This is the last aspect of cyber analytics. After the resistance of the perimeter wall, it should be ensured that assets on sale have retained their value and are not in the process of losing it or even worse destroying it. We will also differentiate two types of work, both radically different:

- On the one hand, the search for leaks of sensitive data that may already be circulating on the internet, or even for sale on criminal forums,
- On the other hand, the search for compromises, i.e., past or existing intrusions within the systems to place active or prepositioned malware there pending its activation (espionage, encryption & ransomware). Again, high-exposure or high-tech sectors incorporating R&D and intangible assets are particularly exposed. It is virtually no holds barred: for example, the widespread adoption of managed services has promoted the emergence of so-called *"supply chain"* attacks for a few years. They consist of introducing themselves to a subcontractor or, in this case, to an enterprise in the process of being acquired, with a view to subsequently moving up to the final target. This attack also has a multiplier effect for the cybercriminal, as it makes it possible to target all of the customers of this subcontractor.

Conclusion

The reality of the cyber threat and the awareness of investors and officers are greatly accelerating the development of this work. *Cyber threat intelligence* (CTI) analysis shows that investment funds are targeted like other sectors. Who knows whether attackers could imagine that these companies are more willing to pay ransom demands?

Today, the customers of this due diligence are frequently former victims who have painfully become aware of the issue of these analyses. The level of maturity of officers on this subject is still variable and the understanding of cyber issues too often confined to ransoms alone. The behaviours are therefore still imbued with the “alarm syndrome” where the installation occurs most of the time... after the theft.

However, the digital revolution delivers a succession of new challenges: large-scale industrial espionage, private or state-owned, business paralysis, data commoditisation and privacy protection are issues that far exceed mere hacking and require data management to be integrated into all stages of business development. This applies to the protection of the business model, its employees and more generally the societal role of the enterprise.

The transaction phases are therefore by their nature times of tension that invite economic players to expand their usual field of analysis.

Contacts

Arnaud Pilon
Head of incident response activities
Synacktiv
arnaud.pilon@synacktiv.com
+33 6 70 88 19 26

Arthur Couvreur
Director
Accuracy
arthur.couvreur@accuracy.com
+33 6 66 69 65 15

Nicolas Bourdon
Partner
Accuracy
nicolas.bourdon@accuracy.com
+33 6 23 82 23 15

Accuracy is a French independent consulting firm, with two main areas of expertise: strategy and finance.
Synacktiv, the French reference in offensive security, helps companies to evaluate and improve the security level of their information systems.