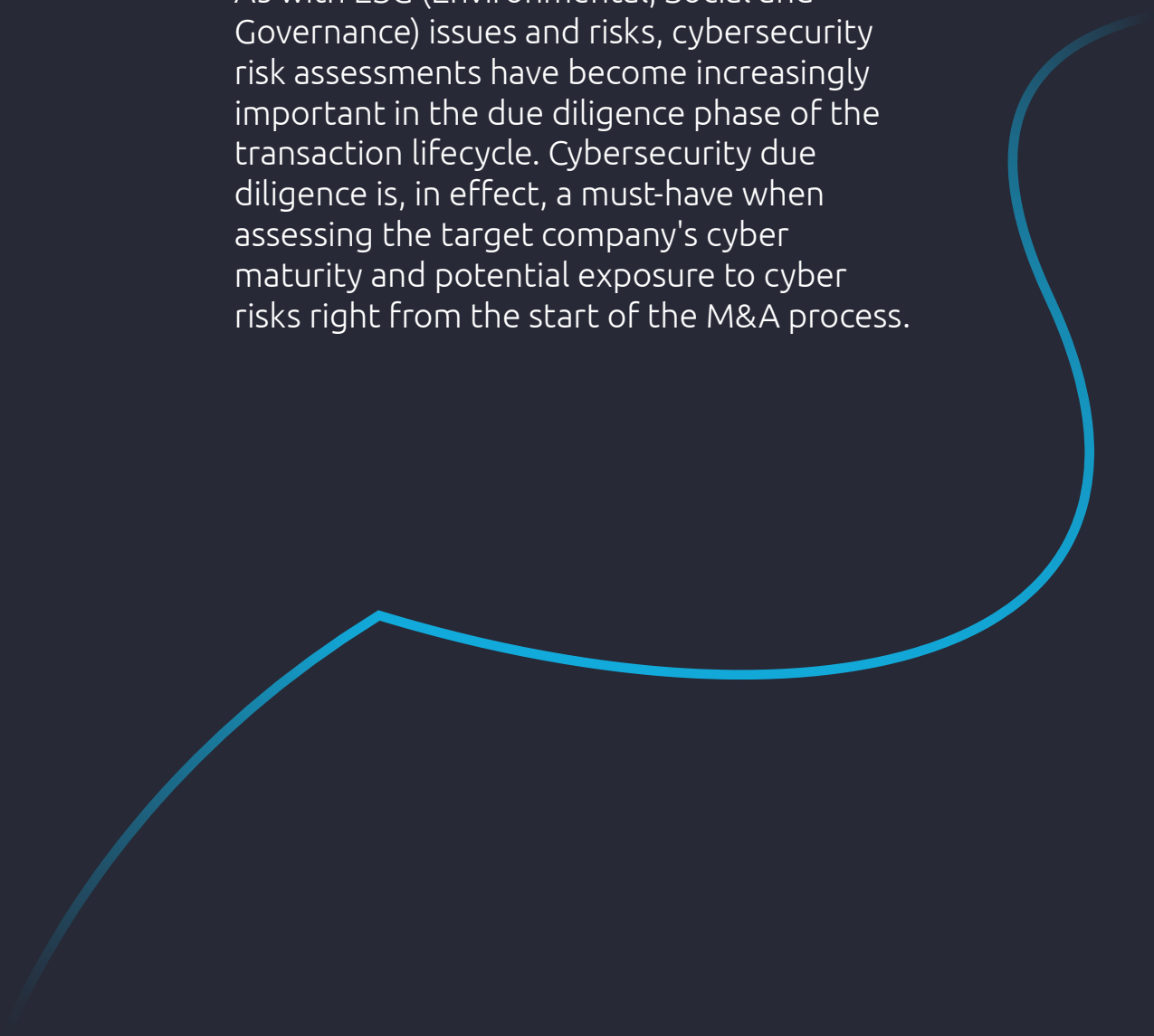
MERGERS & ACQUISITIONS

Cybersecurity at the heart of M&A transactions

Capgemini

As with ESG (Environmental, Social and Governance) issues and risks, cybersecurity risk assessments have become increasingly important in the due diligence phase of the transaction lifecycle. Cybersecurity due diligence is, in effect, a must-have when assessing the target company's cyber maturity and potential exposure to cyber risks right from the start of the M&A process.



Cybersecurity due diligence, a “deal-changer” rather than a dealbreaker

Cybersecurity due diligence is not commonly a dealbreaker. It rather aims to **adjust the assessment of the target company's value** by considering cybersecurity **risks** (business interruptions, disturbances, data leaks...), and analyzing their potential **impacts** on revenue, market share and reputation. This most often also extends to analyzing the potential **remediation** costs and regulatory **sanctions** involved.

In addition to estimating the target company’s fair value, cybersecurity due diligence also allows:

To **protect the buyer** and **avoid cross-contamination** of both companies' information systems after Day One, by identifying and anticipating the measures to be implemented. When separate systems of a transaction are interconnected, the new system resulting from this combination is often exposed to the “weaknesses” of the system with the weakest level of cybersecurity. Companies are particularly exposed to cybersecurity risks during M&A transactions, deriving from sources such as: media exposure, increased attack surface, opportunities for social engineering, etc.

To **identify any Cyber investment costs** (one-off costs) needed to support the buyer's ambitions and business plan (change of scale, API processes and exposure to other players, interoperability, etc.).

To **cover an eventual "cyber debt"**, for incidents that occurred before the transaction, but for which the impacts appear afterwards. These elements are partly covered in the "Reps and Warranties" chapter of the SPA (Share Purchase Agreement), as well as by an alignment of the buyer's Cyber-insurance.

To **prepare the target company’s integration strategy** for the so-called “strategic” acquirers (as opposed to “financial” acquirers) who intend to integrate the acquired company. In particular, this preparation can involve facilitating the negotiation of TSAs (Transition Service Agreements) for cybersecurity services, and further defining the actions needed to converge cyber tools and processes.

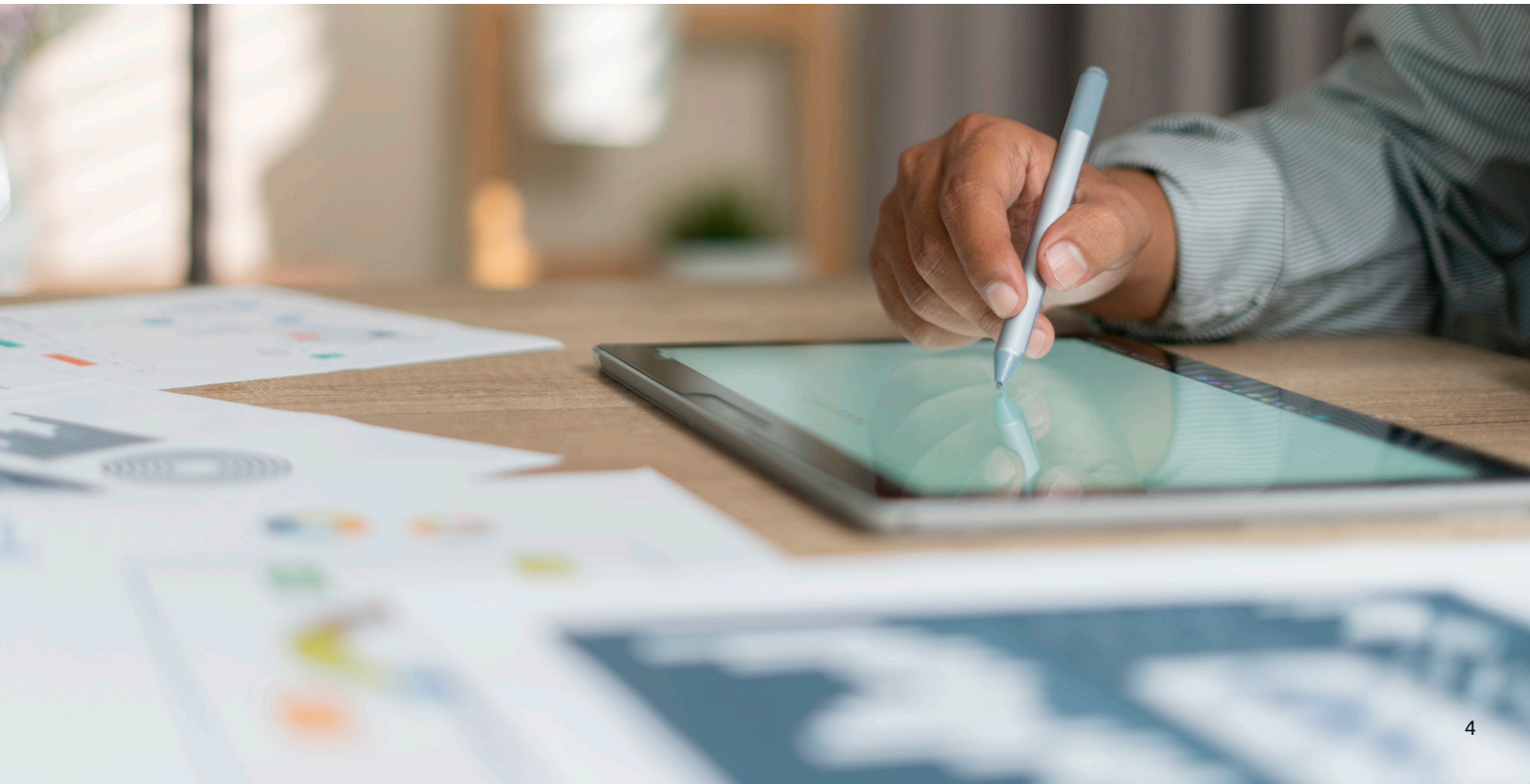
Cybersecurity due diligence: a panel of tools available to buyers

There is a whole array of methods and tools, both internal and external, to gain an insight of a target company's level of cybersecurity maturity.

External, non-intrusive approaches allow the acquirer a certain degree of autonomy:

- Analyzing the target company's **risk profile** by assessing, among other elements : the sector in which it operates, the nature of its operations, its geographical footprint and regulations. This allows to establish a macro view of the type and level of cybersecurity risk it might face.
- Using **external rating platforms** allows to quickly and cost-effectively obtain a view of the target company's exposed assets and cyber maturity with its evolution over time.
- Searching for **data leaks** on the hidden subset of the web allows to detect any past incidents, in particular leaks of personal or strategic data (patents, etc.).

However, internal and/or intrusive approaches such as audits, code analysis, penetration test, and evaluation through interviews, questionnaires, or document collection, allow to provide a more detailed view of the target company's cyber maturity. This detailed view permits to assess compliance with a standard or perform a gap analysis with the acquirer's cyber maturity.



Cybersecurity due diligence in practice

In theory all the methodologies previously mentioned should provide a clear view of the target company's maturity. The practical application of these methodologies, however, is more complex and often hindered by limited implementation or results that lack credibility.

The results of purely external approaches are often incomplete, with no visibility of the company's internal information system, and with non-transparent rating methodologies. This is particularly true when it comes to analyzing third parties or subcontractors with whom the target company interacts in its value chain, and who may themselves contribute to the company's cyber risk.

As for internal approaches, they require a strong cooperation will from the target company, which is not always possible. Cooperation from the target company will largely depend on:

> **The type of acquisition:**
>
> The company will be more reluctant to share its cyber elements with a strategic buyer (potentially a competitor) than with a financial buyer.

> **The acquisition phase:**
>
> During the due diligence process, the number of questions, shared documents, and point of contacts is often limited. The further along the deal is, the greater the level of trust, and therefore more information can be gathered.

There is no standard methodology for cybersecurity due diligence. The acquirer must therefore combine the tools at their disposal to carry out a cybersecurity due diligence. The results of the latter will always depend on the stakes, the context, and the acquisition phase of the transaction. When it comes to cybersecurity due diligence and its level of uncertainty, exhaustive results may not always be guaranteed for the acquirer.

The secret: learning to manage uncertainty while preparing for an integration

It is difficult to provide a perfect overview of all the security risks a company might be faced with through cybersecurity due diligence alone. While we will need to combine assessment methodologies so that we may obtain the best "big picture" view, we must also accept a certain degree of uncertainty, so long as the degree of risk remains minimal.

Fortunately, this uncertainty can be contained by:

- Establishing pre-closing agreements that detail the conditions required for further investigations, or by establishing closing conditions that require the implementation of additional security measures prior to Day One.
- Negotiating guarantees and indemnities to protect both parties.
- Defining metrics, Service-Level Agreements and penalties for cybersecurity services as part of the Transition Service Agreements.
- Subscribing to a cyber insurance policy.

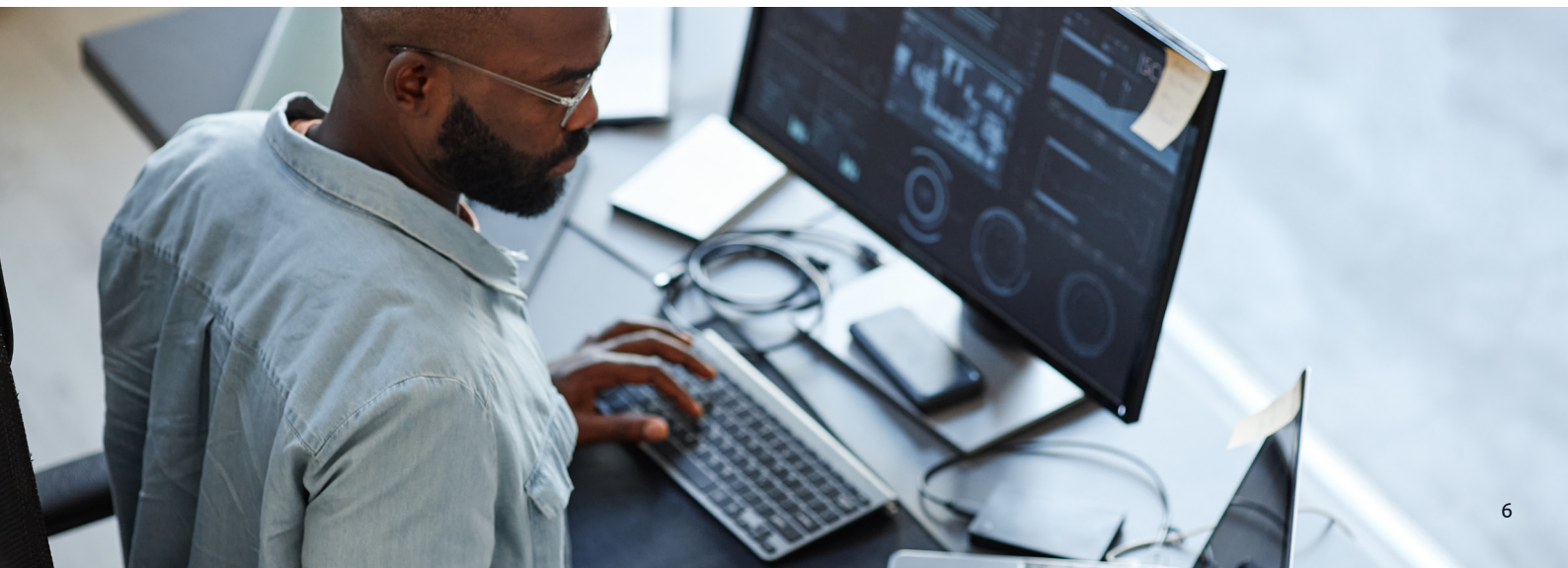
In all, the cyber due diligence exercise should be seen as the first step of a long yet beneficial process, with cybersecurity risk management being integrated end-to-end within the M&A deal lifecycle:

- **With the preparation of Day One:**

  By preparing security measures for Day One (reduction of SOC detection levels, crisis preparation, increasing awareness, etc.), and by contracting the launch of in-depth security audits for Day One.

- **With the integration preparation:**

  By integrating cyber risk into the IT & Business integration strategy (e.g. interconnections management between multiple information systems).



Cybersecurity due diligence on the seller's side

The secret to a successful cybersecurity due diligence also lies with the sellers, who benefit from the analysis and results just as much as the buyers, in order:

- To **maximize the value of the transaction:** vendor audits enable identification and remediation of vulnerabilities that could have led to a reduction in the value of the sold assets, therefore sending a positive message to buyers regarding the seller's cyber risk management.
- To **protect the company's assets post carve-out:** vendor audits help identify potential vulnerabilities impacting the entirety of assets.

The cybersecurity due diligence exercise must therefore be approached as both a negotiating lever and as a preparatory stage for Day One and integration, for both seller and buyer.

Take-away key ideas

Cybersecurity has become an essential part of M&A transactions, right from the due diligence stage. Cyber due diligence is both a negotiation lever and a risk management tool.

There is no standard methodology for implementing a cyber due diligence. A range of tools is available to the acquirer to carry out this exercise, granted that they be sorted and combined depending on the context, the stakes, the timing, and the target company's level of transparency. At Capgemini, we work with companies to define a customized methodology that matches their context, challenges, and acquisition strategy.

The key to successfully executing a cybersecurity due diligence is by accepting uncertainty from the start, and thus insisting on integrating cybersecurity risk management into the negotiation process. Cyber due diligence should therefore be considered a key pillar of the M&A transaction, with it being integrated along every step of the deal to manage cybersecurity risks in their entirety.

Have you ever experienced cases where a wrongly managed cyber due diligence has negatively impacted your integration project? If so, partner with Capgemini Invent to navigate the complexities of Cyber IT M&A and drive seamless integration. Contact us today to embark on your journey towards transformative growth!

Authors

Chloé Molinari

Director Digital Trust & Security
Capgemini Invent

Youssef Sbai

Vice President Mergers & Acquisitions
Capgemini Invent

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get The Future You Want | www.capgemini.com