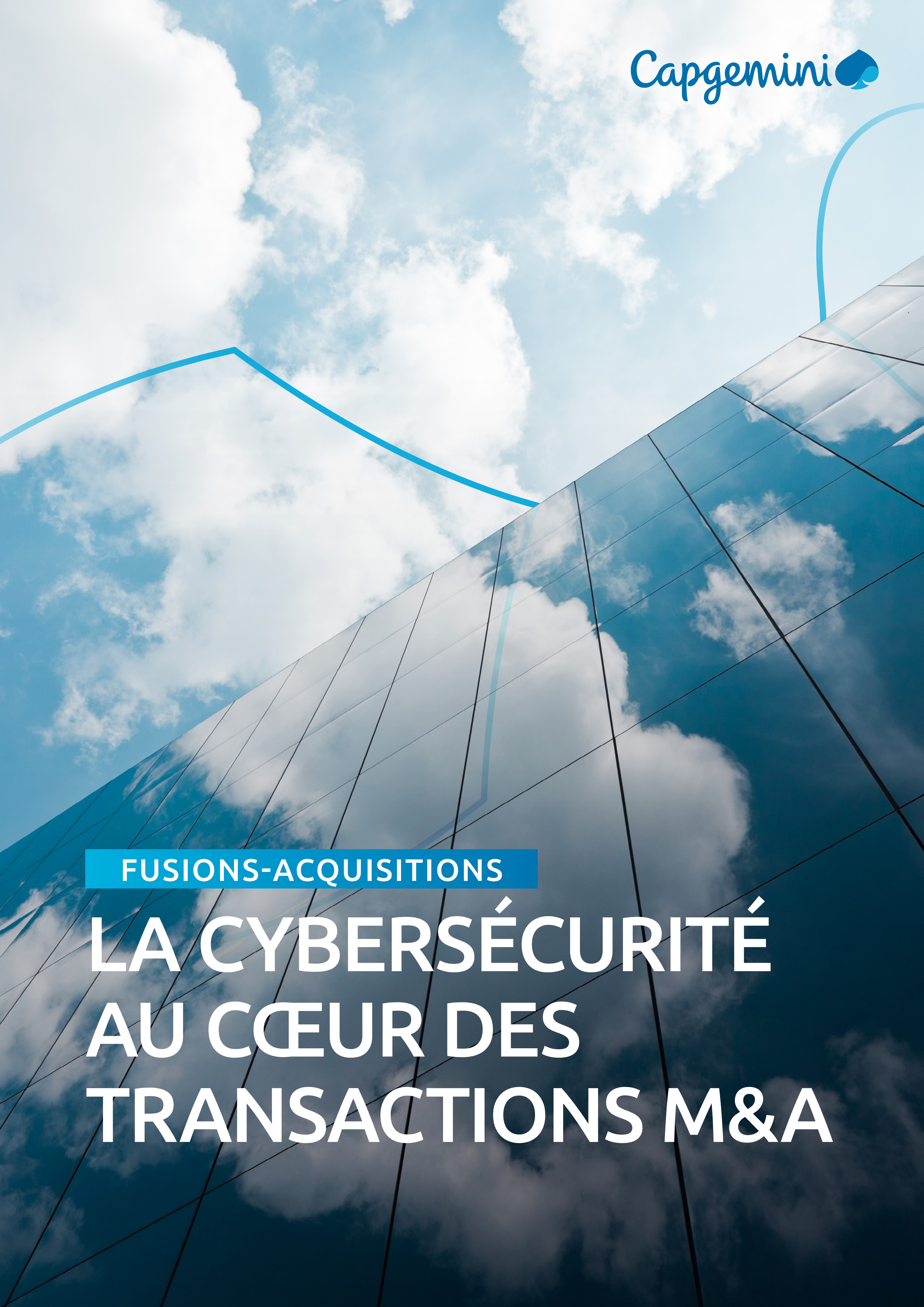


Capgemini

FUSIONS-ACQUISITIONS

LA CYBERSÉCURITÉ AU CŒUR DES TRANSACTIONS M&A

Tout comme les enjeux et risques ESG (Environnementaux, Sociaux et de Gouvernance), l’évaluation des risques de cybersécurité a pris une importance croissante dans la phase de due diligence.

Cette due diligence cybersécurité est devenue un incontournable, permettant d’évaluer la maturité et les risques cyber de l’entreprise ciblée, dès les prémices de l’exercice de fusion-acquisition.

LA DUE DILIGENCE CYBERSÉCURITÉ, un dealchanger plutôt qu'un dealbreaker

Cette due diligence cybersécurité est rarement un dealbreaker ; elle vise plutôt à **ajuster l'évaluation de la valeur de l'entreprise cible**, en prenant en compte les **risques** cybersécurité (interruption ou perturbation de l'activité, fuite de données…), et en analysant leurs éventuels **impacts** sur les revenus, la part de marché et la réputation, ou encore les coûts de **remédiation** et les **sanctions** règlementaires.

Au-delà de l'estimation de la valeur, la due diligence cybersécurité permet aussi :

de **protéger l'acquéreur et d'éviter une contamination croisée** des systèmes d'information des deux entreprises après Day One, en identifiant et anticipant les mesures à implémenter.
En effet, dans deux systèmes interconnectés, l'ensemble hérite souvent du niveau de cybersécurité le plus faible et les entreprises sont particulièrement vulnérables en période de M&A (exposition médiatique, augmentation de la surface d'attaque, opportunités de social engineering etc.)

d'**identifier les éventuels coûts d'investissements** Cyber (one-off costs) nécessaires pour porter les ambitions et le Business Plan de l'acheteur (changement d'échelle, API-sation et exposition à d'autres acteurs, interopérabilité, etc.).

de **couvrir une éventuelle «dette cyber»**, pour des incidents ayant eu lieu avant la transaction, mais dont les impacts n'apparaissent qu'après.
Ces éléments sont couverts en partie dans le chapitre «Reps and Warranties» du SPA (Share Purchase Agreement), ainsi que par un alignement de la Cyber-assurance de l'acheteur.

de **préparer**, pour les acquéreurs dits «stratégiques» ayant vocation à intégrer l'entreprise acquise, **la stratégie d'intégration** de l'entreprise cible, notamment en facilitant la négociation des TSA (Transition Service Agreement) sur les services de cybersécurité et la préparation des actions de convergence des outils et processus cyber.

LA DUE DILIGENCE CYBERSÉCURITÉ, un panel d'outils à disposition des acquéreurs

Il existe tout un panel de méthodes et d'outils, qu'ils soient internes ou externes, pour obtenir une vue du niveau de maturité cybersécurité d'une entreprise cible.

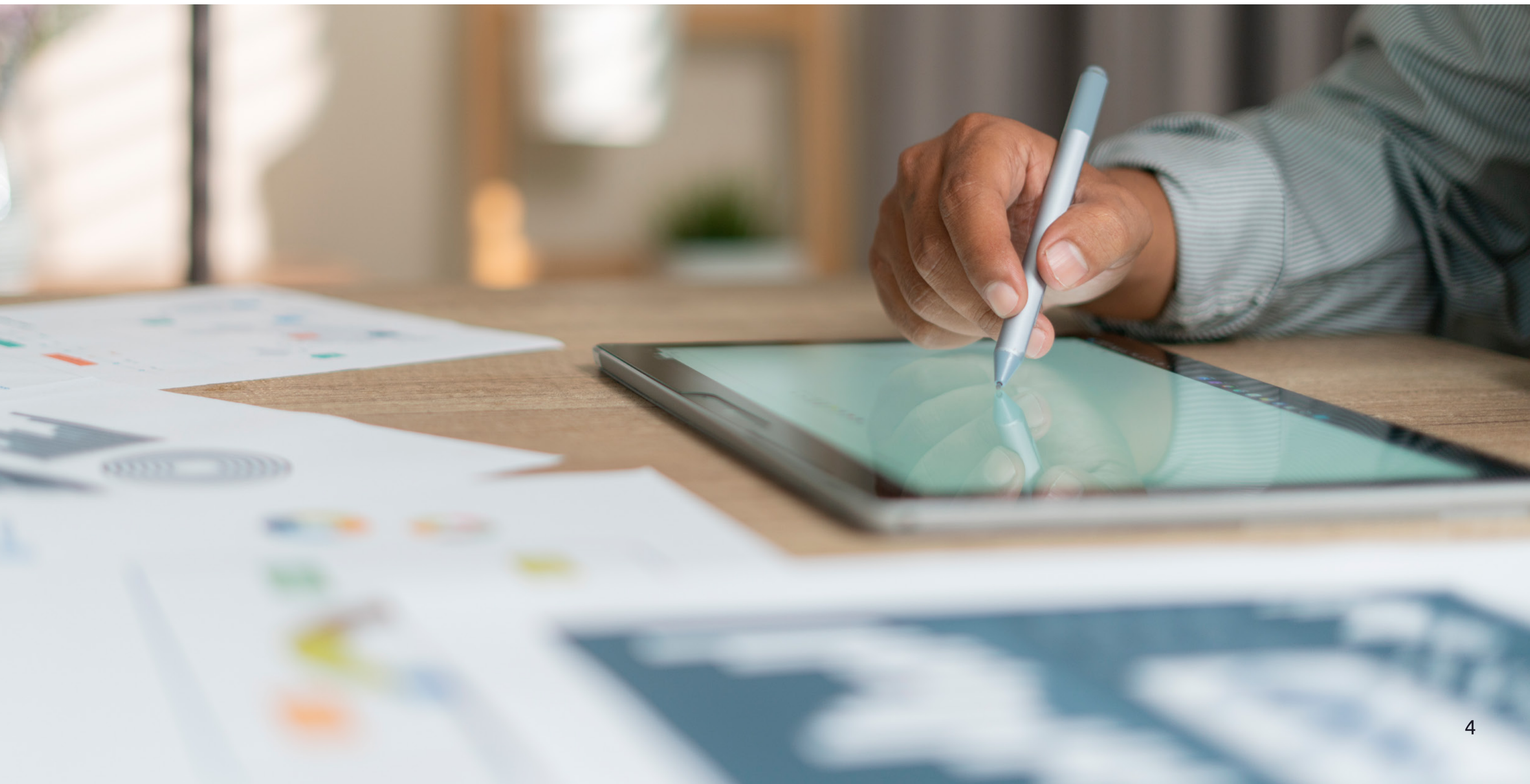
Les approches externes, non intrusives, permettent une certaine autonomie à l'acquéreur :

> l'analyse du **profil de risque** permet d'établir une vue macro du type et du niveau de risque cybersécurité via l'analyse du secteur dans lequel l'entreprise cible opère et de la nature des opérations, de l'empreinte géographique, des règlementations…

> l'utilisation de **plateformes de rating externes** permet, de façon rapide et peu couteuse, d'obtenir une vue de la maturité cyber des assets exposés de l'entreprise cible et de son évolution au cours du temps.

> la recherche de **fuites de données** sur le dark et deep web permet de déceler d'éventuels incidents passés, en particulier les fuites de données personnelles ou des données stratégiques (brevets…).

Les approches internes et/ou intrusives, quant à elles, comme les audits, analyses de code, pentest et évaluation via entretiens, questionnaires, ou collecte documentaire, permettent d'obtenir une vue plus détaillée, d'évaluer la conformité à un standard ou de faire une analyse d'écart avec la maturité cyber de l'acquéreur.



LA DUE DILIGENCE CYBERSÉCURITÉ,
en pratique

En théorie, l'ensemble de ces méthodes doit permettre d'obtenir une vue claire de la maturité de l'entreprise cible, mais l'application pratique est plus complexe, et se heurte à une mise en œuvre limitée ou des résultats manquant de crédibilité.

Les résultats des approches purement externes sont souvent partiels, sans visibilité sur le SI interne, ou avec des méthodologies de rating opaques. Ceci est d'autant plus vrai quand il s'agit d'analyser les tiers ou sous-traitants avec qui l'entreprise cible interagit dans sa chaine de valeur et qui peuvent eux même contribuer au risque cyber de cette entreprise.

Quant aux approches internes, elles nécessitent une forte coopération de l'entreprise cible qui n'est pas toujours possible. La coopération de l'entreprise cible va dépendre :

Du type d'acquisition :

l'entreprise sera plus reluctante à partager ces éléments à un acquéreur stratégique (potentiellement un concurrent) comparé à un acquéreur financier.

De la phase d'acquisition :

durant la phase de due diligence, le nombre de questions, de documents et d'interlocuteurs accessibles est souvent limité.
Plus le deal sera avancé, plus la confiance sera forte et permettra de collecter des éléments.

Il n'y a pas de méthodologie standard pour la due diligence cybersécurité ; l'acquéreur doit donc combiner les outils à sa disposition pour l'effectuer, en fonction de l'enjeu, du contexte et de la phase d'acquisition, sans toutefois pouvoir espérer des résultats exhaustifs.

LE SECRET,
apprendre à gérer l'incertitude pour préparer l'intégration

La due diligence cybersécurité ne permet pas d'avoir une vision parfaite de tous les risques de sécurité d'une entreprise. Il faut donc, tout en combinant les méthodes d'évaluation pour avoir une vision la plus complète possible, accepter un certain degré d'incertitude.

Cette incertitude peut cependant être mise sous contrôle via :

- L'établissement de conventions pré-closing pour obtenir les conditions requises pour des investigations plus poussées, ou de conditions de closing pour la mise en place de mesures de sécurité additionnelles en amont du Day One
- La négociation des garanties et indemnités protégeant les deux parties
- La définition de métriques, Service-Level Agreements et pénalités des services de cybersécurité dans le cadre du Transition Service Agreement
- La souscription à une cyber-assurance

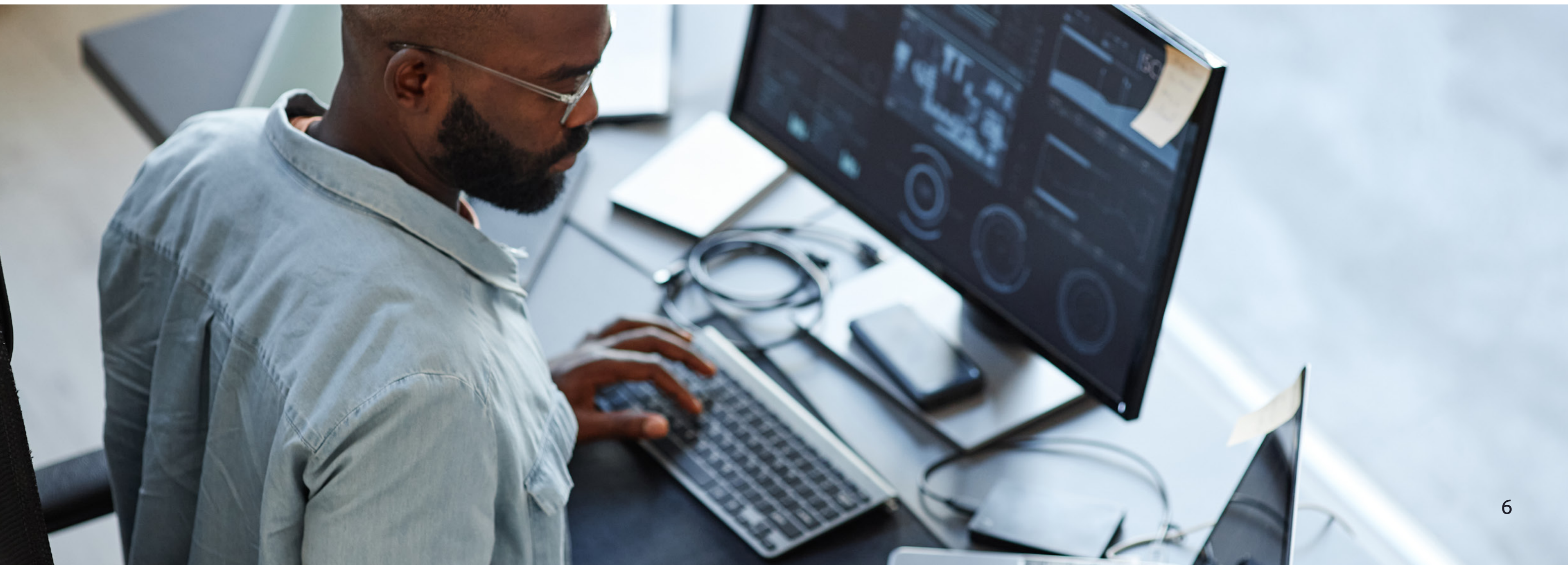
Enfin, il faut surtout considérer l'exercice de due diligence Cyber comme une première étape d'un long processus, la gestion des risques cybersécurité devant être intégrée de bout en bout dans l'exercice de fusion-acquisition :

Avec la préparation de Day One :

en préparant les mesures de sécurité à Day One (diminution des paliers de détection SOC, préparation à la crise, sensibilisation…), et en préparant et contractualisant le lancement des audits de sécurité approfondis à Day One

Avec la préparation de l'intégration :

en intégrant le risque cyber dans la stratégie d'intégration IT & Business (ex : gestion des interconnections entre les deux systèmes d'information)



LA DUE DILIGENCE CYBERSÉCURITÉ, côté vendeur

La clé d'une due diligence cybersécurité réussie repose également sur les vendeurs : la due diligence cyber est un exercice qui se prépare et qui bénéficie tant côté acquéreur que côté vendeur :

- Afin de **maximiser la valeur de la transaction** : les audits vendeurs permettent à la fois d'identifier et de remédier les vulnérabilités pouvant mener à une diminution de la valeur du périmètre cédé, et de renvoyer un message positif aux acquéreurs sur la gestion des risques cyber

- Afin de **protéger le périmètre de l'entreprise post carve-out** : les audits vendeurs permettent d'identifier de potentielles vulnérabilités impactant l'ensemble du périmètre

Ainsi, l'exercice de due diligence cybersécurité doit être abordé comme un levier de négociation et comme une étape de préparation du Day One et de l'intégration, pour le vendeur comme pour l'acquéreur.

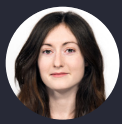
TROIS POINTS À RETENIR

La cybersécurité est devenue incontournable en M&A, dès l'exercice de due diligence ; la due diligence Cyber est à la fois un levier de négociation et un outil de gestion des risques

Il n'existe pas de méthodologie standard pour la mettre en œuvre : un panel d'outils est à disposition de l'acquéreur pour exécuter cette due diligence Cybersécurité, à combiner en fonction du contexte, des enjeux, du timing et du niveau de transparence de l'entreprise cible. Chez Capgemini, nous accompagnons les entreprises pour définir la méthodologie sur-mesure qui correspond à leur contexte, leurs enjeux et leur stratégie d'acquisitions.

La clé pour aborder cette due diligence cybersécurité : accepter l'incertitude en l'intégrant dans la négociation, et considérer la due diligence cyber comme une étape qui s'inscrit dans un processus d'intégration permettant de gérer les risques cybersécurité

À propos des auteurs



Chloé Molinari

Directrice Digital Trust & Security
Capgemini Invent France

Experte en cybersécurité et directrice de l'offre Digital Trust & Security chez Capgemini Invent, Chloé accompagne les CxO dans la définition et la mise en oeuvre de leur stratégie cybersécurité, en particulier sur les aspects de gestion de risques, M&A cyber, et direction de programme de transformation complexes.

Youssef Sbai

Senior Director Mergers & Acquisitions
Capgemini Invent

Youssef SBAI a plus de 15 ans d'expérience internationale dans le domaine des fusions/acquisitions et du conseil aux DSI, notamment en matière de Due Diligence et de SI, de gestion de programmes de transformation et de mise en place de services partagés. Il a soutenu de nombreuses fusions/acquisitions en pré et post transaction, pour des fonds d'investissements ainsi que de grandes entreprises.

À propos de Capgemini

Capgemini Invent fait partie du groupe Capgemini, un leader mondial, responsable et multiculturel, regroupant 360 000 personnes dans plus de 50 pays. Partenaire stratégique des entreprises pour la transformation de leurs activités en tirant profit de toute la puissance de la technologie, le Groupe est guidé au quotidien par sa raison d'être : libérer les énergies humaines par la technologie pour un avenir inclusif et durable. Fort de 55 ans d'expérience et d'une grande expertise des différents secteurs d'activité, Capgemini est reconnu par ses clients pour répondre à l'ensemble de leurs besoins, de la stratégie et du design jusqu'au management des opérations, en tirant parti des innovations dans les domaines en perpétuelle évolution du cloud, de la data, de l'Intelligence Artificielle, de la connectivité, des logiciels, de l'ingénierie digitale et des plateformes. Le Groupe a réalisé un chiffre d'affaires de 22 milliards d'euros en 2022.

Get The Future You Want*
Plus d'informations sur www.capgemini.com

*Capgemini, le futur que vous voulez