Les audits cyber : le nouveau deal-changer des opérations M&A

Par Stéphanie Lapeyre-Castellane, Caroline Basdevant-Soulié, associées, et Ouisse Weiss Akhonzada, cabinet Oyat

La cybersécurité est devenue un élément clé dans les opérations M&A. Une faille non détectée, des systèmes insuffisamment protégés ou une chaine de sous-traitance non encadrée peuvent faire basculer une transaction, effondrer une valorisation ou exposer à des sanctions non anticipées. Pourtant, les audits cyber restent encore trop souvent négligés ou traités comme un exercice théorique, déconnectés des enjeux juridiques et financiers de la négociation.

Au-delà des risques opérationnels et financiers immédiats — par exemple en cas d'attaque interrompant l'activité — la cible peut être porteuse d'un passif réglementaire cyber significatif, à apprécier à l'aune de plusieurs textes.

Le RGPD demeure le socle : une non-conformité — comme l'absence de registre des traitements, des mesures de sécurité insuffisantes, des sous-traitants non encadrés contractuellement — expose à des sanctions pouvant atteindre 20 M€ ou 4 % du chiffre d'affaires annuel mondial. Au-delà du risque de sanction, c'est surtout une dette de mise en conformité que l'acquéreur devra financer post-closing.


S. Lapeyre-Castellane

La directive NIS 2, dont la transposition en droit français se fait attendre, élargit substantiellement le périmètre des entités tenues à des obligations de gouvernance, de gestion des risques et de notification d'incident. Sanctionnées là encore par des amendes élevées — 10 M€ ou 2 % du chiffre d'affaires mondial pour les entités essentielles, 7 M€ ou 1,4 % pour les entités importantes — et assorties d'un régime de responsabilité personnelle des dirigeants, ces obligations nécessitent une analyse dédiée, y compris pour les sociétés qui, sans être elles-mêmes assujetties, se voient répercuter des exigences contractuelles strictes par leurs clients régulés.

Pour les cibles du secteur financier, le règlement DORA, applicable depuis le 17 janvier 2025, ajoute un cadre unifié de résilience opérationnelle numérique qui mérite un examen tout aussi attentif. L'articulation contractuelle avec les fournisseurs de services TIC y appelle une vigilance particulière, les contrats en place n'intégrant pas toujours le contenu minimal exigé par le texte, pouvant alors contraindre à de lourdes renégociations post-closing.

Ces trois textes ne sont pas les seuls en jeu : selon l'activité de la cible, le Cyber Resilience Act, le régime des opérateurs d'importance vitale ou des exigences sectorielles peuvent également s'appliquer. Cartographier les régimes pertinents est le premier travail de la due diligence.

Réaliser des audits adaptés

Connaître les textes ne dit encore rien du niveau réel de conformité de la cible, ni du coût de sa remise à niveau — remédiation technique, formation, gouvernance, reprise des contrats. C'est l'objet de l'audit, dont la portée dépend du degré de coopération obtenu.

Les audits externes peuvent être conduits par l'acquéreur de manière autonome, sans intervention de la cible. Ils reposent sur l'observation périmétrique des systèmes et, parfois, des méthodologies de rating qui restent néanmoins peu transparentes. Faute d'accès au SI interne et aux pratiques opérationnelles, ils n'offrent cependant qu'une vision partielle du niveau de sécurité, notamment pour l'évaluation des tiers et sous-traitants critiques, dont les vulnérabilités alimentent directement le risque de la cible.

Les audits conduits en coopération avec la cible, à privilégier, se déploient sur deux plans. Le premier est documentaire : politiques de sécurité, gouvernance, certifications, rapports d'audit, historique des incidents, contrats fournisseurs et couverture assurantielle. Il vérifie ce que la cible a formalisé. Le second est technique : infrastructure et configurations, gestion des vulnérabilités et des correctifs, protection des données, traitement des incidents. Il vérifie ce que la cible pratique. C'est l'écart entre les deux qui est instructif : lui seul permet d'apprécier la maturité réelle de la cible et de peser sur la décision d'acquérir.

Encadrer contractuellement le risque

Les constats de l'audit n'ont de portée que s'ils se traduisent dans la documentation contractuelle. Dès la lettre d'intention, des conditions suspensives cyber peuvent être prévues, telles que l'absence d'incident matériel sur une période déterminée ou la mise en conformité préalable des systèmes critiques.

Le contrat de cession pourra quant à lui intégrer des déclarations et garanties spécifiques, portant notamment sur l'exactitude des informations relatives aux incidents de sécurité, aux vulnérabilités connues, au niveau de conformité réglementaire et aux principaux référentiels de sécurité.

Le régime d'indemnisation sera par ailleurs ajusté par des indemnités spécifiques, des plafonds propres aux risques cyber, une franchise adaptée au profil de risque de la cible et une durée de garantie allongée.

Le contrat organisera enfin la période intercalaire, entre le signing et le closing, par des obligations de notification d'incident et de maintien des mesures de sécurité.

L'encadrement ne s'arrête pas au closing. Postacquisition, des mécanismes de complément ou d'ajustement de prix, indexés sur des indicateurs de sécurité et de conformité, alignent la valorisation sur la trajectoire de remédiation. L'assurance suppose des stipulations dédiées, organisant notamment le maintien des polices cyber. Les Transitional Service Agreements (TSA) règlent quant à eux le calendrier d'intégration des outils et processus de cybersécurité — enjeu d'autant plus sensible qu'une fois les systèmes interconnectés, l'ensemble hérite du niveau de sécurité le plus faible.■

LA LETTRE DES JURISTES D'AFFAIRES • Éditeur : **Lamy Liaisons** • Siège social : 7 rue Emmy Noether Immeuble Euroatrium 93400 Saint-Ouen • Associé unique : Karnov Holdco France. RCS Bobigny B 480 081 306 • Directrice de la publication : **Rokhaya Pondi** • Directrice de clientèle : **Laure Doligé** • Rédactrice en chef : **Ondine Delaunay** • Rédactrice en chef adjointe : **Anne Portmann** • Journaliste : **Marine Landau** • Maquette et rédaction graphique : **Nord Compo** • Commission paritaire : 0629T87011 • Dépôt légal : à parution • **Abonnements annuels (47 lettres hebdos et 6 magazines LJA) • Entreprise et cabinet d'avocats < 10 :** 1605 € HT - 1638,70 € TTC • **Cabinet d'avocats entre 10 à 49 :** 1835 € HT - 1873,53 € TTC • **Cabinet d'avocats 50 et plus :** 2182 € HT - 2 227,82 € TTC • **Tarif étranger :** nous consulter • Toute reproduction ou représentation intégrale ou partielle, par quelque procédé que ce soit, du contenu de cette publication, effectuée sans autorisation de l'éditeur, est illicite et constitue une contrefaçon, y compris toute utilisation par des systèmes ou modèles d'intelligence artificielle ou toute reproduction ou extraction à des fins de fouille de textes et de données (TDM), notamment en application de l'article 4 de la Directive (UE) 2019/790. L'éditeur se réserve expressément ces utilisations.

Pour contacter le service client : N°Cristal 09 69 39 58 58 APPEL NON SURTAXÉ
Courriel : contact@lamyliaisons.fr
Internet : www.liaisons-sociales.fr
www.lamyline.fr
www.lamy-liaisons.fr
LAMY KARNOV GROUP LIAISONS

IMPRESSION Dupliprint
2 rue Descartes, 95330 Domont.
Origine du papier : Slovaquie
Taux de fibres recyclées : 0%
Certification : PEFC
Eutrophisation : Ptot 0,0016 kg/tonne

BAC DE TRI

PEFC Certifié PEFC Ce produit est issu de forêts gérées durablement, de sources recyclées et contrôlées 10-31-3706 www.pefc-france.org