Maîtriser le risque cyber

pour sécuriser les opérations de fusions-acquisitions, protéger ses investissements, et créer de la valeur

Omniprésente dans la vie des entreprises, la menace cyber est particulièrement prégnante lors des opérations de fusions-acquisitions. C'est pourquoi l'évaluation du risque cyber constitue aujourd'hui une étape nécessaire d'une due diligence efficace. Mais, plus qu'une contrainte supplémentaire, la maîtrise du risque numérique représente aussi une véritable opportunité de valorisation.

Les cyberattaques se multiplient à une vitesse fulgurante. Entre 2020 et 2021, l'Agence nationale de la sécurité des systèmes d'information (Anssi) a observé une augmentation de 37%[1] du nombre d'intrusions avérées dans les systèmes d'information en France. En 2021, 54%[2] des grandes entreprises membres du CESIN (le « Club des Experts de la Sécurité de l'Information et du Numérique ») déclaraient en avoir été victime au moins une fois. À l'échelle mondiale, la valeur annuelle de la cybercriminalité devrait atteindre 10,5 billions de dollars d'ici 2025.[3] Ces effractions concernent l'ensemble des secteurs et des acteurs, sans distinction de taille ou de secteurs. Pour preuve, les petites et moyennes entreprises en concentrent 62%[4] à l'échelle mondiale. Difficile donc, voire impossible, de dresser le portrait-robot de la victime type. Cependant, certains moments de la vie de l'entreprise semblent particulièrement propices aux actes de cyber malveillance. Et c'est notamment le cas des fusions-acquisitions.

Fusions-acquisitions, un grand moment de vulnérabilité cyber

En effet, ces projets font l'objet d'une forte exposition. Ils donnent lieu à l'échange d'un important volume de données, dont certaines très sensibles, et font intervenir de nombreux acteurs tiers, cabinet d'avocats ou de conseil... Cette visibilité a pour conséquence d'attirer l'attention des cybercriminels et d'offrir un terrain fertile à des scénarios d'attaque. La sensibilité et la vulnérabilité particulières occasionnées par la fusion-acquisition appellent donc à une extrême vigilance de l'ensemble des parties concernées tout au long de la conduite de l'opération.

D'autant que la découverte d'une faille préexistante au projet d'acquisition peut s'avérer lourde de conséquences, tant pour l'entité acquéreuse que pour la société vendeuse. Les exemples sont nombreux. En 2016 aux Etats-Unis, la révélation de piratages massifs des comptes clients de Yahoo a, par exemple, contraint

l'entreprise à accepter une révision à la baisse de 350 millions de dollars de son prix de rachat par Verizon.[5] En 2020, le groupe hôtelier Marriott a été jugé légalement responsable des conséquences du vol des données clients subi par Starwood avant son rachat et condamné par le gouvernement britannique à verser une amende de quelque 20 millions d'euros.[6] La même année, l'américain Spirit AeroSystems a, quant à lui, dû abandonner son projet de fusion-acquisition avec Asco Industries, l'entreprise aéronautique belge n'ayant pu respecter les échéances fixées par les autorités européennes pour approuver l'opération du fait d'une attaque par ransomware à grande échelle.[7]

Ces quelques cas en témoignent, l'objectif de création de valeur visé par une opération de fusion-acquisition peut être fortement compromis par une attaque cyber, que ce soit du fait de l'arrêt forcé de l'activité, du vol de la propriété intellectuelle, de l'atteinte portée à la réputation de l'entreprise ou des pénalités encourues pour non-respect de la réglementation. Les enjeux sont donc extrêmement importants. Pourtant, la cybersécurité reste souvent le maillon faible des opérations de due diligence. En 2022, ces due diligences poussées, destinées à vérifier la sincérité du business plan de la société cible, se limitaient encore trop souvent aux seuls aspects financiers, juridiques, stratégiques, commerciaux et opérationnels.

Le risque cyber, un élément-clé des due diligences

La complexité des enjeux, la multiplicité des menaces, des réglementations (sectorielles et géographiques) et des acteurs en présence rendent difficile l'évaluation du risque cyber par des non spécialistes. Elle est pourtant impérative pour éviter les mauvaises surprises. La due diligence cyber a pour objet d'identifier les principaux risques en matière de cybersécurité (« Red Flag »), les vulnérabilités, et d'évaluer les coûts nécessaires à leurs remédiations. Elle est articulée autour de revues documentaires, d'analyses, de tests techniques et de recherches sur le Dark Web. Elle permet également de s'assurer de la conformité des dispositifs et processus de sécurité avec la législation en cours et de mesurer le niveau de résilience de l'entreprise face aux attaques. L'évaluation du risque cyber est donc clairement un élément-clé de l'évaluation d'un actif et a un impact sur sa valorisation financière. Mais cette prise en compte de la cybersécurité est aussi fondamentale pour la réussite de l'intégration.

Intégrer la cybersécurité à chaque étape du cycle de vie de la fusion-acquisition

Des mesures peuvent être prises à l'issue de la phase de due diligence pour remédier à certaines vulnérabilités. Il est donc nécessaire d'anticiper cette phase de risque accru en mettant en place des mesures correctives dès la signature du contrat de vente et d'achat.

Une seconde étape consistera à établir un plan de gestion des risques cyber et d'amélioration des performances. Outre les aspects techniques, ce plan de transformation devra porter à la fois sur la gouvernance de la cybersécurité, la mise en conformité réglementaire, l'adaptation des organisations et des modèles opérationnels, le renforcement de la protection des données, de la détection des attaques et de la résilience sans oublier, bien sûr, la sensibilisation et la formation du personnel.

L'élaboration et la mise en œuvre d'un tel plan requiert de nombreuses expertises, techniques, juridiques ou encore opérationnelles, et une veille permanente pour faire face à l'évolution de la cybermenace et des législations s'y référant. L'accompagnement par des experts prend donc ici tout son sens.

Cybersécurité, une contrainte créatrice de valeur

Au-delà de la maîtrise des risques, ces plans d'amélioration de la cybersécurité présentent bien d'autres avantages, à commencer par la diminution du coût des primes d'assurance et de la mise en conformité efficiente avec les cadres réglementaires.

La sécurisation des données constitue aussi un réel atout concurrentiel auprès des clients en leur garantissant une parfaite confidentialité des échanges et la protection de leurs informations.

Une politique de cybersécurité efficace peut enfin favoriser le développement de nouveaux produits et services cyber-résilients, générateurs de chiffre d'affaires additionnel. Autant d'éléments qui, au moment de la cession des actifs, se traduiront par une véritable création de valeur.

On l'aura compris : la cybersécurité n'est pas seulement un rempart contre la destruction de valeurs. C'est aussi un puissant levier de valorisation.

QUELQUES CHIFFRES

4 000, c'est le nombre d'attaques par ransomware survenant chaque jour dans le monde.[8]

602 millions de dollars en bitcoins ont été versés à titre de rançon en 2021.[9]

Une PME sur deux fait faillite dans les 18 mois suivant une cyberattaque.[10]

[1] https://www.ssi.gouv.fr/actualite/une-annee-2021-marquee-par-la-professionnalisation-des-acteurs-malveillants/

[2] Baromètre annuel Club des Experts de la Sécurité de l'Information et du Numérique (Cesin)

[3] https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html#:~:text=Every%20U.S.%20business%20is%20under%20cyberattack&text=18%2C%202020%20(GLOBE%20NEWSWIRE),%243%20trillion%20USD%20in%202015.

[4] IBM

[5] https://bourse.lefigaro.fr/indices-actions/actu-conseils/rachat-de-yahoo-verizon-obtient-un-rabais-de-350-millions-de-dollars-6040390

[6] https://www.usine-digitale.fr/article/marriott-ecope-d-une-amende-de-20-millions-d-euros-pour-avoir-mal-protege-les-donnees-de-ses-clients.N1023739

[7] https://www.lecho.be/entreprises/defense-aeronautique/le-groupe-belge-asco-ne-sera-pas-repris-par-l-americain-spirit/10253174.html

[8] The FBI Cyber Division

[9] https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/

[10] Ministre délégué chargé de la Transition Numérique et des Télécommunications

THOMAS HUTIN
Senior Managing Director, Head of Cybersecurity, France
+33 (0)6 34 40 98 96
thomas.hutin@fticonsulting.com

THIERRY MIREMONT
Senior Managing Director, Head of Business Transformation & Restructuring, France
+33 (0)6 23 49 22 11
thierry.miremont@fticonsulting.com