masuda funai

コーポレート／ファイナンス／**M&A** スナップショット
2026 年 **6** 月
カール・ヴォンドレイセン

米国 M&A 取引におけるサイバーセキュリティ DD の重要性
Cybersecurity Due Diligence Remains a Critical Focus in U.S. M&A Transactions

M&A 取引の買い手企業において、サイバーセキュリティに関する事故が発生した場合に生じうる財務リスク、業務運営リスクおよびレピュテーションリスクが認知されるようになってきました。そのため、M&A を検討する際に行われるデュー・デリジェンス（以下、「DD」といいます。）においてサイバーセキュリティも極めて重要な確認項目の一つとなってきています。背景には、最近のサイバーセキュリティに関する規制動向や開示要件の拡大、またランサムウェアによる攻撃や情報漏洩事件の増加があり、買い手企業としては対象会社のサイバーセキュリティ対策に対してより厳格に DD を行うことが増えています。このような傾向の中で、買い手企業は DD の過程で対象会社のサイバーセキュリティ対策、インシデント対応能力およびプライバシーデータ保護法への準拠・遵守状況の評価に対して、より高い関心を持つようになっています。

買い手企業は、対象会社が過去にサイバーセキュリティインシデントを経験したかどうかの評価に加え、対象会社のサイバーセキュリティプログラム全体がどれだけ体系的・継続的・効果的に機能しているかといったサイバーセキュリティプログラムの成熟度（Maturity）を確認する場面が増えています。特に重点的に確認されている項目としては、対象会社のガバナンス体制、サードパーティベンダーの管理、従業員への研修、情報へのアクセス制限、サイバーセキュリティ保険の補償範囲およびサイバーセキュリティの脅威の特定・対応手順などが挙げられます。また、大量の個人情報、財務情報または機密データを扱う企業の買収を検討する場合、買い手企業は適用のある連邦法および州法上のプライバシー要件への準拠・遵守状況についても確認し、規制当局による調査や民事訴訟から生じる潜在的なリスクを評価しています。

サイバー関連リスクの重要性が高まっていることを踏まえ、各取引当事者は、取引プロセスの早い段階でサイバーセキュリティに関する検討を行うことが望ましいと考えられます。サイバーセキュリティに関する検討を早期に行っておくことで、買い手企業としては、クロージング条件として、サイバーセキュリティに関する十分な内容を規定した表明保証条項や具体的な補償条項、あるいは救済措置条項を契約交渉の中で求めることができるようになります。他方で、売り手企業の立場では、事前にサイバーセキュリティに関する検討を行っておくことで、売り手として M&A 市場に参入する前に、売却対象となる事業における潜在的な脆弱性を特定し、事前に対処することができるため、M&A 取引における利益を確保することができる可能性が高まります。今後も企業価値の評価、取引のタイミングおよびクロージング後の統合作業においてサイバーセキュリティという要素を無視できない状況が続くことが見込まれるため、サイバーセキュリティに関する DD を徹底的に行うことは、単にコンプライアンスの観点で行うのではなく、売却対象となる事業の取引価値を評価する際の、あるいは取引価値を損なわないための重要な要素であることを買い手・売り手双方の立場から十分に理解しておく必要性が高まってくるでしょう。このように買い手企業としてサイバーセキュリティに関するリスクを積極的に評価し、そのリスクをマネジメントすることができれば、M&A 取引の効率的

な実行、クロージング後の予期せぬ事態の回避、買収した事業のより円滑な統合といったメリットを享受できるものと考えます。

masudafunai

Corporate, Finance & Acquisitions Snapshot

June 2026

Karl W. Von Drathen

Cybersecurity Due Diligence Remains a Critical Focus in U.S. M&A Transactions

Cybersecurity has become a central component of M&A due diligence as buyers increasingly recognize the potential financial, operational and reputational risks associated with cyber incidents. Recent regulatory developments, expanded disclosure requirements and a growing number of ransomware and data breach events have heightened scrutiny of target companies' cybersecurity practices. As a result, acquirers are devoting greater attention to evaluating cybersecurity controls, incident response capabilities and compliance with applicable privacy and data protection laws during the diligence process.

In addition to assessing whether a target has experienced prior cybersecurity incidents, buyers are increasingly examining the maturity of the target's overall cybersecurity program. Areas of focus often include governance structures, third-party vendor management, employee training, access controls, cybersecurity insurance coverage and procedures for identifying and responding to security threats. For businesses that handle significant volumes of personal, financial or sensitive data, buyers are also reviewing compliance with applicable federal and state privacy requirements and evaluating potential exposure arising from regulatory investigations or private litigation.

Given the growing significance of cyber-related risks, transaction parties should address cybersecurity considerations early in the deal process. Buyers may seek enhanced representations and warranties, specific indemnification protections or remediation measures as conditions to closing, while sellers can benefit from identifying and addressing potential vulnerabilities before entering the market. As cybersecurity continues to influence valuation, transaction timing and post-closing integration efforts, robust cyber diligence is increasingly viewed not merely as a compliance exercise, but as a critical component of assessing and preserving deal value. Companies that proactively evaluate and manage these risks will be better positioned to execute transactions efficiently, avoid post-closing surprises and facilitate a smoother integration of acquired operations.