CYBER DEFENSE
MAGAZINE

2025 SPECIAL EDITION

RSAC™ | 2025 Conference

Cybersecurity Due Diligence in Mergers and Acquisitions: Essential Focus Areas

By Tom Cockriel, co-leader of Trenam Law's Business Transactions practice group, Trenam Law

Introduction

Many companies view mergers and acquisitions (M&A) as opportunities for growth, market expansion, talent acquisition and enhanced operational efficiencies. However, they also include potential cybersecurity risks that, if not properly assessed and addressed, could result in financial losses, reputational damage and legal liabilities for the acquirer.

Cybersecurity due diligence should be a core part of any M&A strategy so that acquirers are fully aware of potential risks before finalizing the acquisition. Diligence should include members of the acquirer along with third-party advisers such as technical IT and cybersecurity advisers and legal counsel. This article explores essential areas, largely from a legal perspective, that acquirers must examine when conducting cybersecurity due diligence during M&A transactions. It should be noted that data protection and privacy regimes and industry practices are fast-evolving, and cybersecurity diligence does and will continue to evolve as well. Acquirers should work with knowledgeable internal and third-party advisers and take into account any industry-specific and geographic-specific concerns related to the target company.

1. Assessments of Security Framework

The first step in cybersecurity due diligence is evaluating the target company's security framework to determine its overall cybersecurity practices. This assessment should cover:

- **Compliance Standards:** Assess whether the company adheres to specific regulatory requirements such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI DSS) and National Institute of Standards and Technology (NIST) frameworks. The applicable requirements will vary based on the company's industry, products, services, and data collection and usage practices, among other factors.
- **Incident Response Plans:** Review the company's incident response capabilities, including documented processes, and response teams, as well as how those capabilities were implemented during (and updated since) past breach history.
- **Security Infrastructure:** Evaluate existing security controls, including firewalls, intrusion detection systems (IDS), encryption protocols and endpoint protection mechanisms. The infrastructure will likely include functionality controlled by the company and products and services provided by third parties.
- **Vulnerability Management:** Analyze the company's approach to patch management, software updates and vulnerability assessments to determine whether it follows best practices.
- **Third-Party Risk Management:** Determine how the company manages cybersecurity risks posed by vendors, suppliers and partners with access to its systems.
- **Penetration Testing and Audits:** Review the company's history of penetration testing and security audits to gauge the robustness of its defenses. These tests and audits will include recommendations from the auditors; however, companies frequently do not implement all recommendations. Additionally, tests that were conducted several years prior to the acquisition may not adequately address the current state of cybersecurity needs and concerns and may not offer much valuable to the acquirer's review.
- **Cyber Insurance Coverage:** Determine whether the company has cyber insurance and assess the terms, limitations and coverage of potential cyber-related incidents. The acquirer likely will not be able to assume the coverage after closing of the acquisition; however, the target company might be able to extend its preclosing coverage by utilizing a tail policy.

2. Reviews of Data Management Policies

Data is a very valuable asset in many organizations, regardless of industry, and the acquirer should include it as a focus in M&A due diligence. A thorough review of data management policies should focus on:

- **Data Collection, Use and Transfer:** Examine how data is collected, stored, used and transmitted within the company.

- **Data Classification and Handling:** Examine how sensitive data is categorized, stored and transmitted within the organization.
- **Access Controls:** Assess whether data access is based on the principle of least privilege (PoLP), ensuring that employees can only access information necessary for their roles.
- **Data Retention and Deletion Policies:** Determine how long data is retained and whether the company follows best practices for securely deleting obsolete information. The company may have legal and contractual obligations related to its retention and deletion practices.
- **Encryption Standards:** Review whether sensitive data is encrypted at rest and in transit.
- **Data Breach History:** Investigate whether the company has suffered data breaches, how they were handled, and whether vulnerabilities were adequately remediated and proper notice procedures were followed.
- **Data Backup and Recovery Plans:** Review the robustness of data backup policies and disaster recovery plans to understand the company's business continuity in case of security incidents.
- **Cloud Security:** Examine security controls in place for cloud-based infrastructure, including vendor management, access controls and encryption protocols.

3. The Role of Emerging Technology Within the Company

As emerging technologies such as artificial intelligence (AI) and machine learning (ML) become more prevalent in business operations, cybersecurity due diligence must evaluate the security implications related to those technologies. Key considerations include:

- **AI/ML-Driven Security Measures:** Determine whether AI and ML are being used for threat detection, anomaly detection and automated incident response.
- **Potential AI-Related Risks:** Assess whether AI systems are susceptible to adversarial attacks, model or data poisoning, or data manipulation.
- **Third-Party AI Vendors:** Evaluate the security posture of AI service providers and the potential risks associated with outsourcing AI-driven tasks.
- **Automated Decision-Making Risks:** Review the company's AI governance policies to ensure that automated decisions do not introduce security blind spots or biases.
- **Regulatory Compliance:** Confirm that AI-driven data processing aligns with relevant data protection regulations and ethical AI standards.
- **Integration with Legacy Systems:** Examine how AI solutions integrate with existing infrastructure and assess potential security gaps in interoperability.
- **AI Model Transparency and Accountability:** Ensure that AI models used in the organization maintain transparency and auditability to prevent biased or erroneous decisions that could compromise security.

4. Assessments of Employee Access to Secure Information

Human factors remain one of the most significant cybersecurity risks. Evaluating employee access to and handling of sensitive information is critical to preventing insider threats and unauthorized disclosures. Key areas of assessment include:

- **Identity and Access Management (IAM):** Determine whether the company implements multifactor authentication (MFA), role-based access controls (RBAC) and single sign-on (SSO) mechanisms.
- **User Privilege Audits:** Conduct audits of accounts to identify excessive permissions and ensure proper access governance.
- **Security Training and Policies:** Evaluate the company's cybersecurity training programs, phishing simulations and employee adherence to security policies.
- **Employee Exits:** Analyze processes to ensure that departing employees no longer have access to sensitive systems and data.
- **Third-Party Contractor Access:** Assess security policies for contractors and vendors who may have temporary access to the company's infrastructure and ensure that third parties are subject to written contracts that include proper acknowledgements and indemnities.
- **Remote Work Security Measures:** Assess how the company secures remote access, including VPN usage, endpoint security controls and mobile device management.

Conclusion

Cybersecurity due diligence in M&A transactions is no longer optional or limited to target companies engaged in specific industries. It is now a critical part of the deal process across deal sizes, industries and geographic locations. By conducting assessments of security frameworks, data management policies, emerging technologies and employee access controls, organizations can mitigate cybersecurity risks before finalizing an acquisition. A proactive approach to cybersecurity due diligence minimizes exposure to known and unknown cyber threats and data practices noncompliance.

Furthermore, organizations should consider post-merger integration strategies to maintain cybersecurity continuity. Establishing a unified security framework, harmonizing policies and continuously monitoring for new threats will help ensure long-term protection and operational stability. By prioritizing cybersecurity due diligence, M&A stakeholders can transform cybersecurity risks into strategic advantages, better positioning themselves for a more secure target company and successful acquisition while minimizing potential post-closing issues.

About the Author

Tom Cockriel is the co-leader of the Business Transactions practice group of Trenam Law. He focuses on corporate and business transactions, including mergers, acquisitions and sale transactions; capital raising transactions; intellectual property and technology agreements; trademark and copyright protection; commercial contracts; and other general business matters. Tom may be reached online at tcockriel@trenam.com and at our company website https://www.trenam.com/people-list/thomas-j-cockriel/