Invisible threats: Why cybersecurity due diligence is nonnegotiable in M&A

By Anjali Das, Esq., and Gregory Parker, Esq., Wilson Elser

JANUARY 24, 2025

As the business community anticipates a surge in mergers and acquisitions (M&A) due to a more business-friendly administration and post-pandemic recovery, companies are preparing to seize new opportunities. Organizations aim to expand their market positions, master new capabilities, and drive growth through strategic acquisitions. However, this optimistic horizon is met with an increasingly hostile cybersecurity environment. Cyber threats are escalating in frequency and sophistication, making it imperative for both acquiring and target entities to prioritize cybersecurity due diligence in their M&A activities.

High-profile cyberattacks have exposed vulnerabilities in even well-established organizations, leading to significant financial losses, reputational damage, legal liabilities, and, in some cases, deal failures. The average cost of a data breach has surged, with studies indicating costs exceeding millions of dollars per incident. This reality underscores the necessity for rigorous cybersecurity due diligence in the M&A process. This is the first in a series of articles focusing on cybersecurity in M&A and navigating the hidden risks.

Cybersecurity due diligence is nonnegotiable

When acquiring a company through a stock purchase or merger, the buyer generally steps into the target's existing cybersecurity posture, including its vulnerabilities, past breaches, and latent threats. Meanwhile, a target organization that prepares thoroughly — by documenting past incidents, closing known security gaps, and clarifying compliance measures — can help avoid last-minute complications and maintain deal value.

Undiscovered cyber risks can significantly diminish the value of the deal or, worse, lead to post-acquisition crises that more thorough due diligence might have prevented. Failing to adequately identify and address cybersecurity risks can result in substantial financial losses, legal repercussions, and irreparable reputational damage for both sides.

Data protection regulations such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) impose strict obligations regarding data privacy and breach notifications. Noncompliance can lead to hefty fines and legal actions, adding layers of complexity to M&A transactions.

Moreover, M&A activities inherently expand an organization's attack surface. Integrating disparate IT systems, networks, and applications can create new vulnerabilities. Cybercriminals often target companies during transitional periods, exploiting weaknesses that arise during the integration process.

Key considerations for effective cybersecurity due diligence

Buyers should verify the target's cybersecurity posture, and confirm data privacy compliance and sound risk management. Sellers can help by keeping updated security documentation, showing clear governance, and disclosing any incidents or regulatory actions.

Cyber threats are escalating in frequency and sophistication, making it imperative for both acquiring and target entities to prioritize cybersecurity due diligence in their M&A activities.

The points below guide both sides in reducing cyber threats and protecting the deal's value.

1. Assess policies, compliance frameworks, and leadership

- **Buyer perspective**: Verifying alignment with NIST (National Institute of Standards and Technology) or ISO 27001 and compliance with GDPR, CCPA, HIPAA (Health Insurance Portability and Accountability Act), or PCI DSS (Payment Card Industry Data Security Standard) reveals the target's risk profile. Reviewing policies, procedures, and governance structures shows how deeply these practices shape daily operations. Leadership commitment — evident through a Chief Information Security Officer (CISO) and board reporting — signals robust oversight. Consistent policy enforcement, breach notifications, consent protocols, and data rights management reflect cybersecurity maturity.
- **Target perspective**: Well-documented policies and regular audits give buyers confidence in the target's defenses.

Demonstrating leadership oversight, such as board reports or a CISO, highlights strong governance. Employee training materials reveal the effort to spread cybersecurity awareness across the organization. Sharing these elements shows the target's commitment to governance and compliance.

2. Examine governance of incident response and data management

- **Buyer perspective**: Confirm that the target's incident response, business continuity, and disaster recovery plans exist and undergo regular testing. Examine how leaders and teams coordinate during incidents, aiming for quick containment and clear communication. Strong data classification protocols protect sensitive information. Data Loss Prevention (DLP) tools or similar solutions reduce risks from unauthorized transfers. Also check data retention policies for unnecessary storage practices.
- **Target perspective**: Buyers want proof of incident response and data governance practices that are well-documented and updated. Training materials, test results, and clear leadership roles during incidents highlight readiness. Strong data classification procedures and the use of DLP tools show proactive risk management. Regular updates and drills confirm the target's focus on operational continuity.

3. Evaluate technical infrastructure and security measures

- **Buyer perspective**: A detailed inventory of hardware, software, and networks reveals possible gaps. Checking for outdated systems, unpatched vulnerabilities, or missing controls is critical. Firewalls, intrusion detection, antivirus software, and patch processes should be examined. For cloud services, confirm encryption, identity access management, and formal Service Level Agreements (SLAs). Remote access security, including Multi-Factor Authentication (MFA), Virtual Private Networks (VPNs), and Mobile Device Management (MDM) tools, must also be verified.
- **Target perspective**: Documentation of IT assets and security controls helps buyers gauge technical infrastructure. An inventory of hardware, software, and patch records shows dedication to secure operations. SLAs with cloud providers, plus remote work protocols such as MFA, VPNs, and MDM, further reduce risks. Reports on vulnerability assessments, patch cycles, and threat responses communicate a proactive approach.

4. Consider emerging technologies (IoT, AI, and machine learning)

- **Buyer perspective**: Identify how IoT (Internet of Things), AI, and machine learning systems may introduce new threats. Check if these technologies are securely configured, isolated from sensitive segments, and tested for performance or adversarial risks. Review privacy and security policies governing data handling and confirm regular security assessments.
- **Target perspective**: Show evidence of secure IoT, AI, and machine learning deployments, including integration with existing systems. Penetration tests, vulnerability assessments, and documented update processes indicate risk management. Explain how data is protected, anonymized, or encrypted, meeting privacy regulations. This balanced approach signals readiness for modern challenges.

5. Investigate past cybersecurity incidents and risk management

- **Buyer perspective**: Study how past breaches or incidents were handled and resolved. Confirm that remediation plans addressed vulnerabilities and that risk management processes are thorough. Periodic vulnerability assessments or penetration tests, with records of improvements, show an ability to adapt and strengthen defenses.
- **Target perspective**: Full disclosure of past incidents and a clear risk management history build trust. Provide evidence of consistent processes for detecting, assessing, and fixing weaknesses. Demonstrate regular testing and timelines for remediation. Document updates to protocols, new tools, or training that followed major incidents.

6. Review third-party and supply chain risks

- **Buyer perspective**: Examine how the target manages vendors or partners that access critical systems or data. Check contracts for cybersecurity clauses and breach notification obligations. Evaluate vendor security audits, certifications, and oversight. Confirm plans for managing cross-border risks and varying data laws.
- **Target perspective**: A strong vendor management framework shows commitment to securing external partners. Provide evidence of onboarding, monitoring, and offboarding procedures. List vendor certifications (ISO 27001, SOC 2) or audit results. Outline efforts to manage supply chain vulnerabilities, such as closer reviews for high-risk vendors.

7. Understand Legal and Contractual Obligations

- **Buyer perspective**: Check how the target defines "data breach" or "cyber incident" in contracts. Look for data privacy and security clauses that survive the deal. Investigate ongoing or past litigation, regulatory probes, or enforcement actions. Confirm any cross-border compliance measures, such as GDPR clauses, that could affect operations.
- **Target perspective**: Consistent contract terms help buyers see the target's legal strategy for cybersecurity. Confirm that definitions of "data breach" and "cyber incident" match applicable regulations. Show how privacy and security obligations appear in vendor and customer agreements. Disclose any legal or regulatory actions, including cross-border compliance steps.

8. Analyze intellectual property protection

- **Buyer perspective**: Check how the target safeguards proprietary software, trade secrets, and sensitive data. Confirm

access controls, encryption, and confidentiality agreements. Validate the status of patents, trademarks, or other registrations. Note any ongoing disputes or lapses that might affect operations.

- **Target perspective**: Strong IP protection practices reassure buyers about critical assets. Provide evidence of secure access controls, encryption, and confidentiality agreements with employees and contractors. Include proof of valid patents, trademarks, or other filings, as this documentation signals robust measures for guarding important IP.

9. Determine insurance coverage and financial preparedness

- **Buyer perspective**: Review the target's cyber insurance policies, including limits and exclusions. Check if these policies match risks seen during due diligence. Investigate the target's claim history and interactions with insurers. Also examine the organization's security budget and staffing to spot any resource gaps.
- **Target perspective**: Detailing cyber insurance policies and financial commitment to security shows readiness to handle threats. Share policy information, including any tail coverage and renewal schedules. Provide examples of efficient claims processes. Show how budgets and staffing protect against cyber risks, reinforcing the target's diligence.

Conclusion

In an era where cyber threats are escalating and M&A activities are set to increase, cybersecurity due diligence is an indispensable component of the transaction process. By proactively integrating cybersecurity assessments, both buyers and target organizations can protect their investments and minimize exposure to unexpected risks.

By proactively integrating cybersecurity assessments, both buyers and target organizations can protect their investments and minimize exposure to unexpected risks.

Ensuring regulatory compliance, demonstrating a strong culture of security, and establishing a stable foundation for post-acquisition integration remain critical steps for success. As the cyber landscape continues to evolve, staying vigilant and adaptable is key to managing the complexities of M&A transactions in the digital age.

About the authors

Anjali Das (L) is a partner and co-chair of **Wilson Elser**'s national cybersecurity and data privacy practice. She is a recognized authority on cyber-defense, including incident response, privacy compliance and risk management, regulatory investigations and enforcement actions, and the defense of nationwide data breach class actions. She can be reached at anjali.das@wilsonelser.com. **Gregory Parker** (R) is an associate at the firm in the cybersecurity practice. He serves as privacy and breach counsel to organizations that have experienced a cyber attack. He also counsels clients on cybersecurity risk and disclosures in connection with mergers and acquisitions. He can be reached at gregory.parker@wilsonelser.com. The authors mare located in the Chicago office.

This article was first published on Reuters Legal News and Westlaw Today on January 24, 2025.