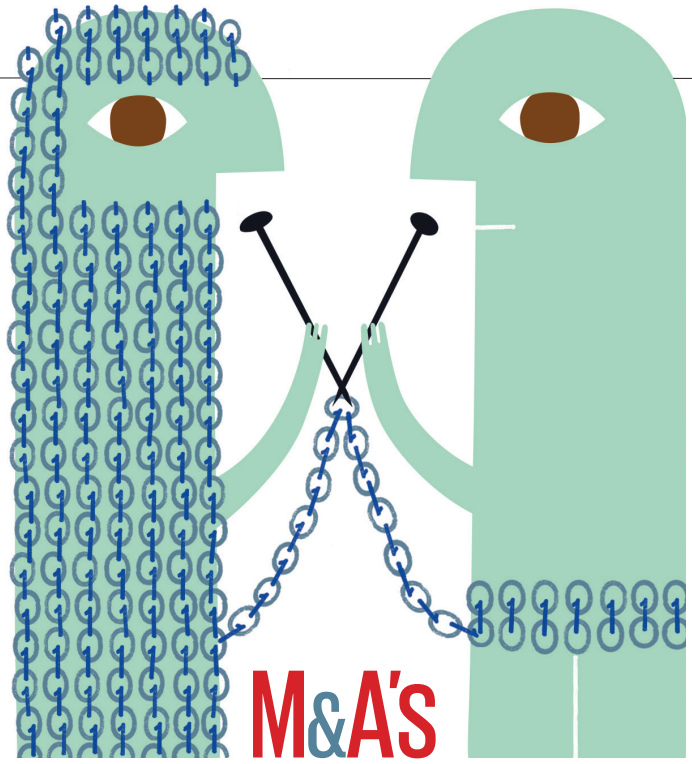

M&A's Privacy Imperative

Undetected data privacy risks can sink the best-laid plans. By ARMIN TADAYON.

Widgets International spends months preparing for the acquisition of rising star Glue, a move to strengthen Widgets' market position, diversify its offering and accelerate growth. The deal is a huge success, a feather in the cap of Widgets' leadership.

Until a fly lands in the ointment: Post-merger, a data security issue rooted in previously unknown vulnerabilities within Glue's systems emerges during the integration of the infrastructure of two companies, unleashing a torrent of liabilities for Widget.

A public relations dream suddenly becomes a nightmare as privacy risks are exposed, creating challenges across the organization, reputation not the least.

Such a hypothetical underscores a harsh reality: Fragmented privacy regimes and differing standards can create substantial risk. Assessing such risk needs more than ticking compliance boxes—it demands thoughtful, jurisdiction-specific evaluation of how data is handled.

Any acquisition opens windows of vulnerability—employees, customers and partners grow anxious over how the deal will affect their relationships and interests. Meanwhile, detractors probe for weaknesses. All of this unfolds amid geopolitical instabilities and a regulatory climate beyond either company's control. Activist investors can pounce on missteps.

With such pressures, data privacy may seem a relatively small thread. But if treated as an afterthought, it can unravel all the rest.

PRIVACY IN THE M&A LIFE CYCLE

The M&A process typically follows six stages: target identification; due diligence; negotiations; announcement to closing; integration; and post-deal monitoring and compliance. Of these, three are critical for privacy concerns: due diligence, negotiations and integration.

Due Diligence: The purpose of due diligence is to uncover potential risks that could threaten a transaction's value or viability. In today's information-driven economy, one of the most valuable assets is data—information about employees, customers, partners and vendors.

Incompatible databases and IT systems, conflicting privacy standards and regulatory obligations, legacy data that may no longer fit the buyer's compliance framework or risk appetite—all of these pose potential problems for the combined company. Data-sharing with third party outlets is common and can expose the buyer to new international partners and regulatory regimes.

Despite all this, in common due diligence practice, the focus often remains on financial practices and hard assets, while data is given short shrift or overlooked altogether. Incorporating data as a core part of enterprise risk management protects this asset. Failure to do so can create a potential drag on post-deal value.

Negotiations: Here, any uncovered privacy risks must be put on the table. Such risks alone shouldn't sink a deal, assuming they can be properly addressed. Specific indemnities and warranties can be negotiated to cover potential liability from risks both known and unknown tied to privacy compliance. Looking ahead to integration, both companies must be prepared to take the necessary steps to verify and meld their data privacy practices.

Once public, scrutiny intensifies. To guarantee clarity in stakeholder communications—especially regarding data stewardship—you must prepare beforehand. This planning is essential to maintain narrative control when attention is at its peak.

Integration: Post-acquisition, the deal's challenges are compounded by intense time pressures and the need to prove out the strategy behind the deal. Simply merging personnel introduces privacy challenges. Uncertainty and possible layoffs can increase the chance of both accidents and insider threats. With more employees and systems, outside attackers have a naturally expanded target.

An acquired company may have looser interpretations of privacy compliance, reflecting the culture of the organization. Without unified expectations, employees may unintentionally engage in risky behaviors.

Focusing on these three phases, let's rewind our hypothetical acquisition to its start. With everything else about the deal staying the same, Widgets identifies discrepancies between the two companies' data privacy systems during due diligence. The problems are not ignored—they're examined, built into strategy and addressed with intent. The road is still bumpy, but Widgets moves forward with eyes wide open and avoids calamity.

THE COMBINED COMPANY

Successfully navigating privacy risks in M&A isn't just about avoiding pitfalls—it's about embedding privacy considerations as a core element of value creation and all that that entails. That means elevating privacy due diligence to the level of financial, legal and operational assessments—scrutinizing data governance, regulatory compliance and reputational alignment. Following an acquisition, leaders must establish priorities:

Establish a clear narrative around data stewardship: Frame privacy not merely as a compliance requirement, but as a core principle and market differentiator. The values of the company are reflected in how it handles privacy.

Communicate transparently: Tailor messaging for clear privacy policies. Educate employees on safeguarding data and informing partners of any changes in data handling expectations.

Engage high-risk stakeholders: For organizations with a global footprint, compliance demands navigating diverse privacy regimes, some much stricter than others. Engagement is critical.

Communicate post-integration privacy enhancements: Where data privacy improvements strengthen governance or branding, share these with stakeholders. This reinforces trust by demonstrating a commitment to responsible data stewardship.

Privacy is central to M&A because it is central to protecting value generally. Embedding these practices can help turn privacy into a lasting source of stakeholder confidence and strategic value. ◆

Armin Tadayon is a Director with Brunswick in Washington, DC.

ILLUSTRATION: MELINDA BECK