Five Cyber Traps That Kill M&A Value (And How to Spot Them Early)

In M&A transactions, over 60% of post-acquisition cyber incidents stem from issues that could have been identified before closing. Yet most deals proceed with minimal cybersecurity scrutiny, leaving acquirers holding liabilities they never bargained for.

As I highlighted in my previous article Cybersecurity Due Diligence: Playing Your Cards Right in M&A Deals, thorough security assessment isn't optional—it's critical for deal valuation. According to Gartner, acquirers who implement robust cybersecurity due diligence reduce post-merger integration costs by 28% and accelerate time-to-value by nearly four months.

Let's examine the five most dangerous cyber traps that routinely sink deal value.

Trap 1: Shadow IT and Ghost Systems

Shadow IT refers to technology used without IT department approval. Ghost systems are worse—forgotten infrastructure that may contain sensitive data or provide unauthorized access.

Organizations now average 187 undocumented systems for every 1,000 employees according to IBM. During an acquisition, these invisible assets transfer alongside everything else—but they won't appear on any inventory list.

These invisible systems create significant risks through unknown attack surfaces, unpatched vulnerabilities (often years old), potential compliance violations, and data stored outside approved repositories.

Detecting shadow IT requires comprehensive discovery scanning across networks, anonymous employee surveys about unofficial tools, traffic analysis to identify unapproved services, and cloud account audits including personal accounts used for business.

Trap 2: AI Misuse and LLM Leakage

As organizations adopt AI, there's growing risk of IP exposure through prompt engineering, model abuse, or uncontrolled data sharing with public AI systems.

A 2024 GitClear study found 39% of developers routinely upload proprietary code to generative AI tools without permission. Meanwhile, KPMG found only 17% of organizations have implemented formal controls around AI usage.

For acquirers, this creates serious risks including intellectual property leakage to third-party AI providers, competitive intelligence exposure, and contamination of training data with regulated information.

One private equity firm I advised discovered their acquisition target had inadvertently exposed their entire product roadmap through employees sharing confidential information with ChatGPT. That's like accidentally broadcasting your poker hand to the entire table.

To detect AI risks, conduct an AI usage audit across all departments, review policies around AI governance, analyze data flow between systems and third-party AI services, and examine employee interactions with AI tools through prompt library review.

Trap 3: Dormant Access and Inherited Credentials

Dormant access paths represent former employees, contractors, and partners who retain system access. Inherited credentials are privileged accounts with excessive permissions transferred during acquisitions without proper review.

According to Beyond Identity, 83% of organizations fail to revoke access within 24 hours of employee departure, while 37% admit having active credentials for employees who left more than a year ago.

These access issues create significant hazards through unauthorized access by former employees, excessive privileges enabling lateral movement, and inability to attribute actions to specific individuals.

Deloitte highlighted how one manufacturing firm discovered over 300 active administrator accounts without assigned owners during post-merger integration, including several used to access financial data after closing.

Detecting access issues requires identity and access mapping across all systems, activity analysis to identify suspicious usage patterns, privilege audit for administrative accounts, and user attestation process to verify account ownership.

Trap 4: Data Classification Chaos

Data classification chaos occurs when organizations lack consistent methods for identifying, labeling, and protecting sensitive information.

Ponemon Institute found organizations typically have visibility into less than 50% of their sensitive data, with that figure dropping to just 30% for companies that underwent mergers in the past 24 months.

For acquirers, this creates several problems including unknown compliance obligations related to sensitive data, inability to identify and protect intellectual property, and excessive access to sensitive information.

One SaaS company acquisition I advised revealed sensitive customer data stored in development environments with no access controls—data that wasn't included in any pre-deal disclosure. It's like discovering you've been playing with marked cards after the game ends.

To detect data classification issues, conduct data discovery sampling across systems, review existing classification schemes, audit storage locations to identify sensitive data, and map regulated data in unexpected places.

Trap 5: Vendor Risk Sprawl

Vendor risk sprawl occurs when organizations accumulate numerous third-party providers without adequate oversight or security assessment.

Venminder found the average mid-market company uses over 180 third-party services, yet only conducts security and governance assessments on about 10%. Meanwhile, BlueVoyant reported 82% of organizations experienced a supply chain breach in the past year.

Vendor sprawl creates multiple challenges through inherited third-party breach risks, unknown data sharing with vendors, and excessive third-party system access.

A recent PE acquisition I consulted on discovered the target had granted admin-level database access to 14 different vendors—including several with no current business relationship—resulting in a six-month remediation project.

To detect vendor risks, create vendor inventory across all departments, review access levels to identify vendor privileges, analyze contracts for security requirements, and assess security posture of critical vendors.

The Risk Landscape at a Glance

Cyber Trap	Prevalence	Detection Approach	Impact
Shadow IT	187 systems per 1,000 employees	Discovery scanning, employee surveys	Hidden vulnerabilities, compliance risk
AI Misuse	39% of developers upload proprietary code	AI usage audit, prompt library review	IP exposure, competitive intelligence loss
Dormant Access	37% have credentials for employees gone >1 year	Identity mapping, privilege audit	Unauthorized access, lateral movement
Data Classification	<50% visibility into sensitive data	Data discovery sampling, regulatory mapping	Compliance violations, privacy breaches
Vendor Sprawl	Only 10% of vendors security-assessed	Vendor inventory, access review	Supply chain compromise, data exfiltration

Strategic Recommendations

1. **Standardize AI data usage policies before diligence begins.** Implement clear guidelines for AI system usage, including approved tools, permitted data sharing, and IP protection protocols.
2. **Use red-flag scans as a routine step in early diligence.** Deploy automated discovery tools to quickly identify potential cyber traps before committing significant resources.
3. **Make IAM hygiene a non-negotiable pre-close requirement.** Require target companies to clean up access issues before closing, including removing orphaned accounts and documenting administrative access.
4. **Integrate data classification review into Day 1 planning.** Develop a standardized approach to data classification that can be implemented immediately post-acquisition.
5. **Build security questions directly into investment committee briefs.** Ensure cybersecurity findings are included in all deal review materials, with clear articulation of risks and remediation timelines.

The Path Forward: From Detection to Protection

Most cyber issues in M&A don't emerge suddenly—they're inherited through inadequate due diligence. Identifying these five common traps early not only protects deal value but can enhance it by providing a clearer picture of true acquisition costs.

Organizations that master cyber due diligence don't just avoid pitfalls—they transform security into a value driver that accelerates integration and enhances ROI.

After all, in both poker and M&A, reading the table correctly isn't just about avoiding bad hands—it's about maximizing value when the cards are in your favor.

Struggling with cybersecurity visibility in your upcoming transactions? Connect with me directly to discuss how these five traps might be affecting your deals. Let's pressure-test your diligence playbook together and explore our secure deal-readiness framework that identifies these risks before they impact your acquisition value.

#CyberDueDiligence #MAVC #DealSecurity #LV #DataRisk #Mergers