



TOM COCKRIEL
CO-LEADER OF THE BUSINESS
TRANSACTIONS PRACTICE GROUP
TRENAM LAW

Cyber and AI Diligence in M&A

Businesses across Tampa Bay are bought, sold and merged every week, and buyers routinely spend weeks reviewing financial statements, customer contracts and employment matters. Cybersecurity diligence, once an IT formality reserved for technology targets, now shows up in deals from manufacturing to professional services and family businesses. The question is no longer whether buyers examine cyber risk, but what they look for and when.

BEFORE THE LETTER OF INTENT

A handful of questions asked early will tell a buyer more than a full technical assessment asked later. Has the company had a reportable security incident, and what did it disclose to whom? What categories of sensitive data does the company hold, and does holding that data — health information, payment card data, or information about European or California individuals — pull the company into a regulatory regime that the buyer is not currently set up to handle? Does the company carry cyber insurance, and at what limits?

Insurance in particular deserves an early look, because the seller's policy rarely follows the acquired business. A runoff or tail endorsement can sometimes keep pre-closing claims covered, but that is a negotiation to open while there is still leverage, not something to raise during the closing checklist.

DURING CONFIRMATORY DILIGENCE

Three aspects of confirmatory diligence will help a buyer test whether the company's stated practices are actual practices.

The first is evidence of testing. Most companies can produce a penetration test report, but the more important information is which recommendations were implemented, by whom and when.

The second is data practices — how data is collected, where data is stored, how it is classified, who can access it, how long it is kept, and whether encryption covers both stored data and data moving across networks. Retention practices are not always aligned with commitments the company made to its own customers and vendors, making this a legal problem as much as a technical one.

The third is people. A buyer will examine the company's policies and training practices. Multifactor authentication, permissions tied to job function, and disciplined removal of access when employees depart are important controls, and their absence may signal other weaknesses in the company's practices. Contractors and vendors with system access should be under signed agreements addressing confidentiality, security obligations and indemnification.

THE AI LAYER

AI diligence should be included in every deal, with a focus on exposure at three levels.

What the company knows it is using. Ask for an AI inventory of systems, vendors, data flows, and personnel who approve them. Many software vendors have switched on AI features by default, routing customer data to model providers the company never vetted and creating disclosure obligations it may not know it has.

What the company does not know it is using. The company's employees may be using AI products without the company's knowledge or approval. Identifying such use may require management interviews, review of software spend and network activity, and direct questions about use.

What the company has built. If the company develops or modifies its own models, IP ownership and training data provenance become important. The company should be able to document that the data was licensed, purchased and/or properly consented to.

CLOSING AND BEYOND

Turn findings into terms. A red-flag finding that is not addressed in the transaction documents is wasted effort, and the AI questions above are the ones most likely to require new language, because standard forms do not yet cover them. Consider representations that the AI inventory is complete, that training data was licensed or properly consented to, and that no customer data has been used to train a third-party model. Where the company cannot stand behind those statements, the gap belongs in an indemnity, an escrow holdback, and/or a closing condition requiring remediation before the deal closes.

Integration efforts. Risk identified during diligence should be remediated in the weeks after closing, when two sets of credentials, policies, vendors and security practices merge. Settle before closing who is responsible for security on the first day, which accounts are revoked immediately, and which of the company's AI tools remain in use. Then confirm that the resulting policies are actually implemented and followed.

Each of these questions costs far less to ask before closing than to answer afterward. A buyer who finds an unlicensed dataset or an unpatched system during diligence still has a negotiating point. A buyer who finds it two years later simply owns it and the costs associated with it.

Tom Cockriel co-leads the Business Transactions practice group at Trenam Law, where he focuses on mergers and acquisitions, capital raising, intellectual property and technology agreements, and commercial contracts. He can be reached at tcockriel@trenam.com. ♦