Cyber Risk Is a Line Item on Every Deal

Even If You Don't Know It Yet

By Jason Rorie, CISSP-ISSMP | Founder & CEO, Triad InfoSec

Every deal has a number nobody wants to find after close.

In M&A, that number usually shows up as a purchase price adjustment, an indemnification claim, or an operational crisis during integration. In cybersecurity, it shows up as an undisclosed risk that was never quantified before the ink dried.

This is not a technology problem. It is a valuation problem. It is showing up in more transactions than most deal teams want to admit.

The Gap Between What Diligence Covers and What It Misses

Standard due diligence has gotten better at asking cybersecurity questions. The checklist usually includes items related to firewalls, data breaches, and compliance certifications.

What it often does not include is an honest answer to the question that matters most: what would it cost to operate, recover, or remediate this environment post-close?

I sat across the table from a deal team last year, reviewing a target company in the professional services space. The target had a clean compliance record, no reported incidents, and an IT provider that had been with them for eight years. From the outside, it looked fine.

When we dug into operational dependencies, the picture changed. A single line-of-business application was running on an unsupported server with no redundancy. A ransomware event, which statistically is not an if but a when, would have halted billing operations across the entire company for an estimated four to six days. For a company billing $2M per month, that single exposure represented $300,000 to $400,000 in operational disruption before factoring in recovery, remediation, or reputational cost. That exposure had never been modeled. It had never been priced into the deal. Based on how these conversations typically go, it had likely never been thought about at all.

The issue was not a lack of tools or controls. It was a lack of financial context. The seller did not know the number. The buyer did not ask the right question to find it.

Cyber Risk as a Valuation Input

Most acquirers treat cybersecurity as a compliance verification exercise. The question being answered is: has this company had a breach, and does it meet baseline requirements?

The better question is: what financial exposure is embedded in this environment, and how does it affect our return?

That reframe matters because cyber risk is not binary. It is a spectrum of exposure with direct financial consequences. EBITDA stability is at risk any time a disruption interrupts operations during a critical revenue period. Remediation costs in a distressed or neglected environment can run into the six- or seven-figure range, often surfacing as a post-close surprise that was entirely avoidable. Reps and warranties coverage is increasingly complicated by insurers excluding cyber-related claims that were foreseeable at closing. Integration timelines stretch when two environments with mismatched security postures are connected, creating a compounding risk that multiplies the longer it goes unaddressed. Employee and customer trust, while harder to quantify, is immediately felt when something goes wrong.

When cyber risk is not quantified going into a deal, the acquirer is effectively pricing it at zero. That assumption rarely holds.

What Underprepared Looks Like in Practice

The warning signs are usually visible if you know where to look.

A target company that treats cybersecurity as an IT function tends to exhibit a predictable pattern. Security decisions are driven by whatever the IT provider most recently recommended. Budgets are set by precedent, not exposure. Leadership assumes that because nothing has visibly gone wrong, the organization is protected.

What that company often cannot tell you reveals the depth of the problem. It cannot tell you how long operations would continue if a key system went offline, or what a ransomware recovery would realistically cost. It cannot identify which vendors or third parties have access to its environment and under what conditions. It often cannot confirm whether its cyber insurance policy would pay out in the scenarios most likely to occur.

These are not exotic questions. They are the operational and financial basics that should be answerable by any company carrying meaningful risk on its books. When a target cannot answer them, that uncertainty belongs in the model.

The Acquirer's Blind Spot: Post-Close Integration Risk

Even when pre-close diligence is thorough, the integration window creates its own exposure.

Connecting two environments is not a technical event. It is a risk event. Every new connection point is a potential entry path. Every period of transition, where ownership is unclear and attention is split, is a period of elevated vulnerability.

The companies that absorb this well are the ones that treat integration security as a defined workstream with clear ownership, not an afterthought handled by whichever IT team member has available bandwidth.

IBM's Cost of a Data Breach report consistently shows that breaches identified during or after system migrations cost significantly more to contain than those caught in stable environments. The integration window is not just a technical transition. It is the period of highest exposure in the entire deal lifecycle. Organizations that do not treat it accordingly tend to learn that lesson within the first 18 months after close.

What Rigorous Cyber Diligence Looks Like

For deal teams serious about quantifying this exposure, the standard checklist is not enough. A rigorous approach answers four questions:

1. What would disruption cost this business?

This means identifying critical systems, modeling downtime scenarios, and translating them into daily or weekly revenue impact. A company that bills $2M per month and loses billing capability for five days has a quantifiable number. That number belongs in the diligence report, not in a post-close conversation.

2. What is the remediation gap?

Not whether the company is compliant, but what it would cost to bring the environment to a defensible posture under new ownership. This is often the most expensive post-close surprise, and it is almost always avoidable with the right assessment pre-LOI.

3. How does cyber exposure affect insurance and reps and warranties coverage?

Insurers are paying close attention to this. A target with known vulnerabilities, an expiring or inadequate policy, or a history of incidents can complicate coverage and affect deal structure. This conversation needs to happen before close, not after.

4. Who owns this risk post-close, and for how long?

Defining accountability for cyber risk during the integration period is not a legal formality. It is an operational necessity. Without a clear owner, the risk is managed by no one, which is the worst possible outcome in any transition.

The Seller's Perspective: Cyber Posture as a Value Driver

This conversation runs in both directions.

For companies preparing for a liquidity event, cybersecurity posture is increasingly a factor in how buyers perceive risk and, by extension, how they price it. A seller that can demonstrate a clean environment, quantified controls, and documented recovery capability removes a variable from the buyer's model.

That removed variable matters. Diligence findings that surface unquantified cyber risk routinely result in purchase price adjustments, escrow holdbacks, or deal restructuring. Sellers who have invested in documenting their security posture before going to market are not doing so because they love compliance. They understand that every unknown in a buyer's diligence process becomes a negotiating lever on price. A defensible, well-documented security posture removes that lever before the conversation starts.

Where Deal Teams Can Start

For M&A professionals looking to close this gap, the practical steps are straightforward and do not require creating a new practice.

Start by adding operational disruption modeling to your diligence framework alongside compliance verification. For targets where technology is core to the business model or revenue operations, commission a pre-LOI cyber risk assessment. It is a fraction of the cost of a post-close remediation project and removes the guesswork from your model.

On the seller side, require a remediation cost estimate as part of the disclosure package. Engage a third-party cybersecurity advisor during integration planning, not after issues surface. Explicitly define post-close cyber risk ownership in deal documents to avoid ambiguity about accountability during the transition window.

None of this is complicated. It is simply applying the same financial discipline to cyber risk that deal teams already apply to every other material exposure in a transaction.

The Bottom Line

Cyber risk does not disappear at close. It transfers, and it multiplies through integration.

The question every deal team should be asking is not whether a target has had an incident. It is what the financial exposure looks like today, what it would cost to absorb a disruption, and whether that exposure is priced into the deal.

The organizations on both sides of the table that understand this are making better decisions, protecting value, and moving through integration with fewer surprises.

The ones that don't are finding out after the fact. My hope is that it is not a threat that entered through integration, leading to that expensive discovery.

About the Author

Jason Rorie is the Founder and CEO of Triad InfoSec, a cybersecurity advisory firm focused on helping organizations understand and manage cyber risk as a financial and operational business risk. A U.S. Navy veteran and former operator who built and exited a leading managed services firm, he works with executives, investors, and deal teams to quantify cyber exposure and support risk-informed decision-making across transactions and operations. He holds the AIGP, CISSP-ISSMP, CCSP, CISM, CISA, and C|CISO, among other credentials, and is a doctoral candidate in Computer Science (Cybersecurity).