CAGI

INSIGHTS

PRACTICAL CYBER DUE DILIGENCE FOR INVESTORS

Executive Thought Leadership Series

PAPER 2 OF 12

Why Good Cyber Reports Still Miss Material Deal Risk

Why the quality of the report is often the wrong question

Written for private equity deal partners, investment directors, boards and corporate development teams

Author
Michael J. Loginov

AUGUST 2026 | VERSION 1.0 | APPROX. 10 MINUTE READ

> A professionally written report can be completely accurate and still fail commercially because it examined the wrong business boundary.

Executive Summary

Investment committees increasingly ask whether cyber diligence has been completed before approving an acquisition. That is not enough. The better question is whether the diligence was designed to identify the risks capable of changing enterprise value.

Across more than 140 executive cyber maturity and risk assessments spanning some 40 transactions, I have reviewed diligence reports ranging from fewer than twenty pages to well over one hundred. Some were technically excellent. Some were not. Report quality was rarely the determining factor. The reports that concerned me most were often professionally written, logically structured and technically accurate. They simply answered a different commercial question from the one investors needed answered.

Every observation in the report could be factually correct while material risk remained undiscovered. Once an executive summary concludes that cyber maturity is appropriate, consistent with industry practice, or that no material concerns were identified, few readers challenge whether the assessment asked the right questions.

My judgement is that cyber diligence should be evaluated in the same way as financial or legal diligence. A technically accurate report is only valuable if it examines the issues capable of changing the investment decision. The quality of the report matters, but scope accuracy determines whether that quality has commercial value.

A professionally written report can be completely accurate and still fail commercially because it examined the wrong business boundary.

Figure 1. The Cyber Diligence Value Chain

The assessment outcome is shaped before testing begins. A weak scope cannot be repaired by excellent analysis or polished reporting.

The illusion of completeness

Unsuccessful diligence often shares a common feature: the report appears complete. Maturity scores, heat maps, risk matrices, benchmark comparisons, executive summaries, recommendations and appendices are all present. The format looks professional, and that professionalism creates confidence.

But confidence is not evidence. A report can document what was tested in impressive detail while saying very little about what was never considered.

A simple test is to set the findings aside and ask: what evidence shows that every material business system was considered? The answer is often unclear. Most reports explain what entered scope; far fewer

explain what was excluded, why it was excluded, and whether those exclusions could affect the investment decision.

Reports answer the questions they were asked

This is not primarily a criticism of diligence providers. Professional firms deliver against the agreed scope. If a client requests an enterprise IT assessment, that is what should be delivered. The commercial problem begins when readers assume the report represents the organisation rather than the agreed scope.

I say that as someone who has worked on both sides of it. I have delivered this work under the methodology of a major professional services firm at Grant Thornton, and as a retained specialist inside one of the leading specialist risk consultancies, where I led the recovery of an industrial business after a breach had halted production. Working to a firm's own method and quality process is not a constraint on this argument. It is where the argument came from.

Imagine commissioning structural engineers to inspect the upper floors of a building while excluding the foundations. Their report might be accurate in every respect. Nobody would conclude that the building had therefore been fully assessed. Cyber diligence often creates exactly that misunderstanding.

Material risk frequently sits outside traditional ownership

Modern organisations are collections of technology accumulated over decades. Corporate IT owns some of it. Operations, engineering, facilities, suppliers, acquired businesses and joint ventures own the rest. Cloud providers operate another layer. None of this is unusual.

The difficulty is that organisational ownership rarely aligns with operational dependency. An industrial robot may depend upon engineering software running on a workstation purchased fifteen years earlier. A warehouse may rely upon vendor-maintained equipment connected through unmanaged remote access. A production line may depend upon a building management controller that has never appeared in the vulnerability programme. Each system contributes to enterprise value. Few appear within conventional cyber inventories.

The difference between technical risk and commercial risk

One lesson became increasingly clear during my work across industrial and critical environments. Technical severity and commercial severity are rarely the same thing.

Security professionals naturally prioritise vulnerabilities using technical characteristics such as exploitability, patch availability, authentication requirements and exposure. Those measures are useful for engineering. Investment committees care about revenue, cash flow, customer delivery, regulatory interruption, operational resilience and reputation.

A medium-severity weakness affecting production scheduling during peak manufacturing may represent a larger commercial exposure than several critical vulnerabilities affecting isolated office systems. Traditional reporting does not always make that distinction visible.

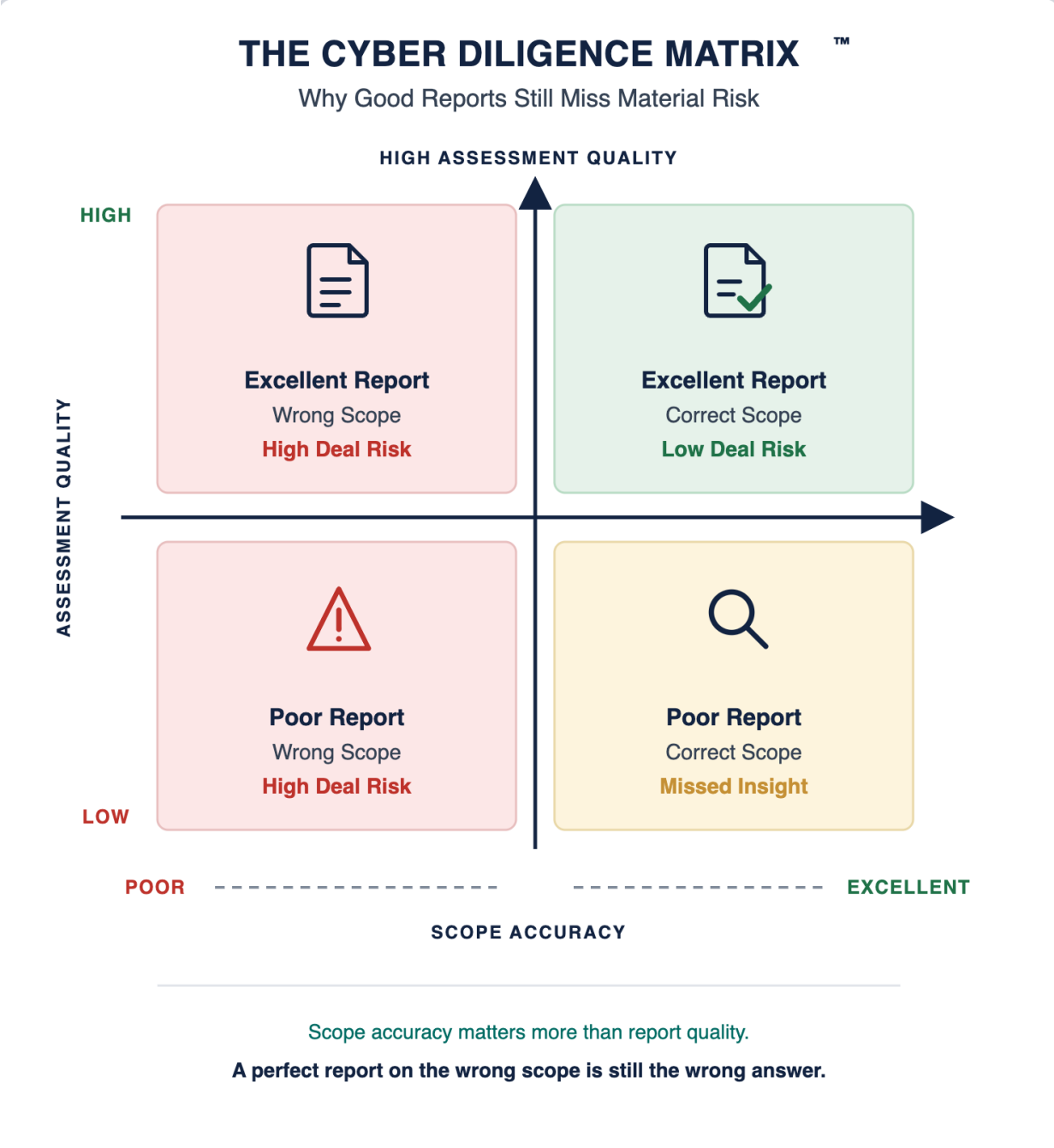
The reverse is equally true, and worth stating because it cuts against my own interest.

Working through Grant Thornton and applying their methodology, I assessed a breach at a high-profile online gambling operator. The loss was real and it was quantified at roughly two million pounds. The finding was valid, the control weakness was genuine, and on a conventional severity scale it would have been reported prominently.

The chief executive was untroubled. The business was generating several times that figure every day, the incident had not interrupted trading, and he regarded the loss as a cost of doing business in that sector. He was right. Measured against enterprise value, it was not material, and it did not belong in a price argument.

That engagement shaped how I have worked since. A finding is not made material by being true, by being expensive to fix, or by being uncomfortable to read. It is made material by what it does to the value of the business. Reporting everything is not diligence, it is transcription, and it costs the reader the ability to tell which findings matter.

Figure 2. The Cyber Diligence Matrix



The highest-risk outcome is an excellent assessment applied to the wrong scope. Its professionalism can create misplaced confidence and suppress further challenge.

Project Forge

Project Forge involved an industrial business operating multiple production facilities acquired over many years. The original diligence reached a reassuring conclusion. Enterprise controls compared favourably with industry peers. Identity governance was improving. Endpoint protection appeared mature. Cloud adoption was well managed. The executive summary concluded that no material cyber issues had been identified.

That conclusion changed when operational dependency mapping began. Several critical production processes depended upon supplier-managed equipment supported through remote access arrangements that were not visible to corporate security. Maintenance contracts varied across sites. Authentication controls differed between suppliers. Operational ownership remained fragmented.

Nothing identified represented evidence of immediate compromise. Everything represented operational dependency. The report had accurately described enterprise IT. It had not described the whole business.

Maturity does not equal resilience

Cyber maturity frameworks remain valuable. I have implemented and relied upon them throughout my career. They provide consistency, support governance and assist benchmarking. They do not automatically measure resilience.

Two organisations with identical maturity scores may have completely different operational exposure. One may manufacture pharmaceuticals. The other may develop software. An interruption at the first may affect patient treatment and regulated supply. An interruption at the second may delay a software release. The maturity score can remain identical while the commercial consequence changes completely.

Investment committees should therefore avoid confusing governance maturity with enterprise resilience.

The first one hundred days

Many hidden cyber costs emerge after completion: identity rationalisation, network redesign, supplier contract reviews, legacy technology replacement, operational segmentation, asset discovery, engineering documentation and backup modernisation.

These costs rarely appear because somebody performed poor diligence. They appear because nobody commissioned diligence to identify them. The first one hundred days after acquisition then become an expensive discovery exercise. By that point the purchase price has already been agreed, and the negotiating leverage has gone.

Six questions every Investment Director should ask

Final observations

Cyber diligence is becoming more sophisticated. Investment committees now expect more than vulnerability summaries and governance observations. They expect commercial insight.

Across the engagements where scope was widened beyond the original brief, the additional findings supported a price adjustment or a specific indemnity in roughly sixty per cent of cases, with a median enterprise value effect between one and three per cent. The remaining cases were equally useful: they established that the wider estate was sound, which is worth knowing before signing rather than after.

None of this depends on a single individual. The scoping method is documented, it is taught, and it is applied by engineering and assessment specialists working to a defined evidence standard. What does not delegate is the judgement about materiality, which is why the person who did the fieldwork should be the person who defends it at the investment committee.

That requires a change in thinking. The objective is not to produce a technically impressive report. It is to reduce uncertainty before capital is committed. Sometimes that means confirming strong governance. Sometimes it means identifying hidden operational exposure. Occasionally it means changing the transaction, the price, the protections or the integration plan. All of those outcomes can represent successful diligence.

Ultimately, cyber diligence should answer one commercial question: what could materially reduce the value of this business after we own it? Everything else is supporting evidence.

CAGI Insights: Practical Cyber Due Diligence for Investors

This paper is the second in a twelve-part executive series examining how cyber risk affects transaction value, operational resilience and post-acquisition performance.

1. What Cyber Diligence Misses in Industrial and OT Heavy Targets
2. **Why Good Cyber Reports Still Miss Material Deal Risk**
3. Cyber Risk That Never Appears in the Data Room
4. The Hidden Cost of Third Party and Supply Chain Trust
5. AI Due Diligence, Beyond the Hype
6. When Cyber Becomes an EBITDA Problem
7. The First 100 Days After Acquisition
8. Operational Resilience as Enterprise Value
9. Ransomware, Recovery and Deal Economics
10. Cyber Warranties That Actually Matter
11. Separating Security Theatre from Material Risk
12. The Future of Cyber Due Diligence in Private Equity
13.
14.