CAGI
INSIGHTS

PRACTICAL CYBER DUE DILIGENCE FOR INVESTORS

Executive Thought Leadership Series

PAPER 1 OF 12

What Cyber Diligence Misses in Industrial and OT Heavy Targets

Why the Scope Matters More Than the Findings

Author:
Michael J. Loginov

ABOUT THIS SERIES

A collection of twelve executive papers written for investment directors, deal partners, boards and corporate development teams. Each paper focuses on one material issue that influences enterprise value, transaction risk and post-acquisition resilience.

PAPERS IN THE SERIES

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

.....

12. The Future of Cyber Due Diligence in Private Equity

Each paper is designed to be read independently in under fifteen minutes while forming part of a coherent reference series for executives responsible for investment decisions.

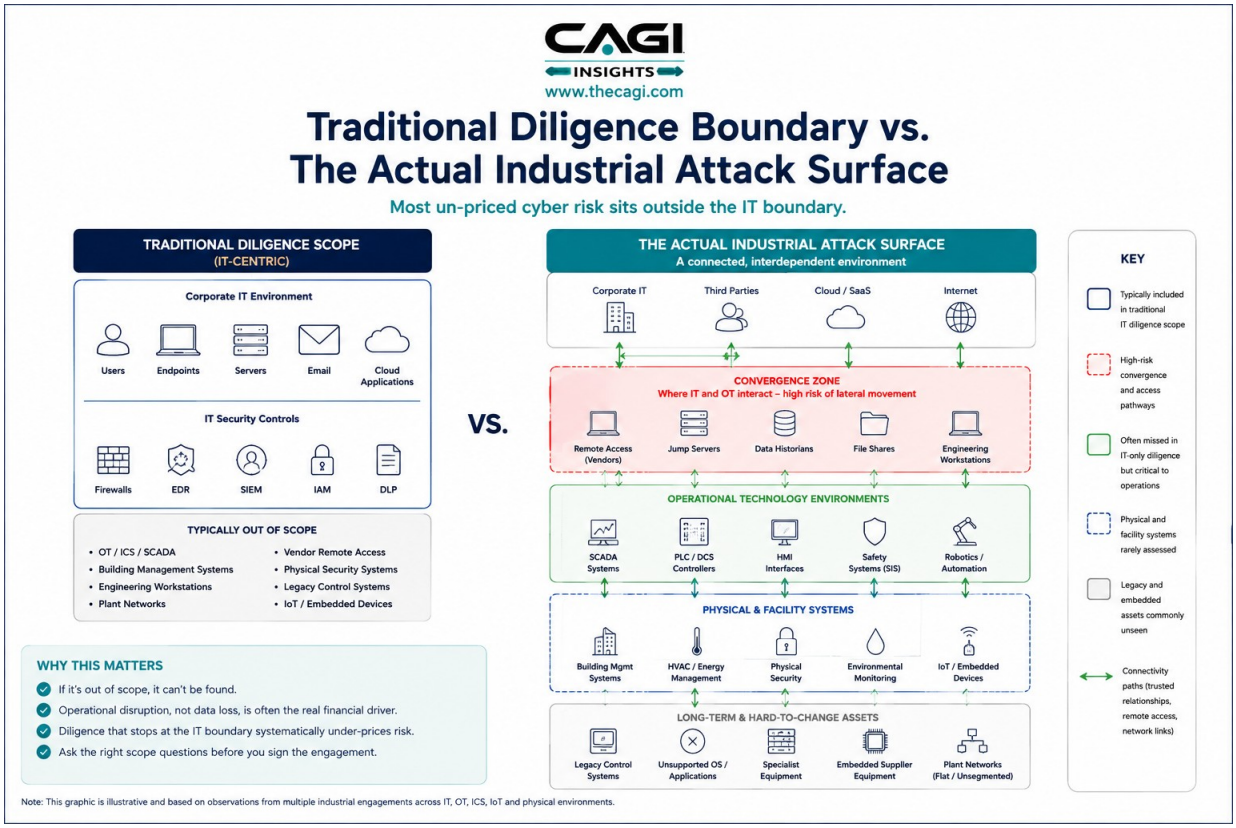
Executive Summary

Standard IT-led cyber diligence often stops at the enterprise IT boundary. In industrial organisations the highest-value operational risks frequently reside outside that boundary. This paper argues that the scope of diligence determines the value of its findings. If operational technology, industrial control systems, engineering workstations, building management systems and vendor remote access are excluded from scope, they cannot be assessed, priced or reflected in transaction negotiations.

"The most expensive cyber risk is often the one that was never included within the diligence scope."

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

Figure 1. Traditional Diligence Boundary vs. The Actual Industrial Attack Surface



Traditional cyber diligence generally follows the corporate IT boundary because that is where enterprise security teams maintain visibility. Industrial organisations rarely operate within that boundary. Operational technology, ICS, engineering workstations, vendor remote access, embedded supplier

equipment, building management systems and legacy operational assets frequently sit outside standard discovery processes.

Industrial environments operate under different engineering principles

Operational technology has traditionally been managed using the philosophy, 'if it works, do not touch it'. Many OT assets remain operational for decades. Unlike enterprise IT, changes are introduced cautiously because availability and safety take precedence over feature upgrades. Assessment methods therefore differ significantly. Traditional IT penetration testing techniques can disrupt production or affect safety systems. OT assessments require specialist methodologies including passive discovery, engineering validation and tightly controlled testing windows.

Project Anvil (Anonymised Example)

Across six production sites the assessment identified three unmanaged remote access paths supporting two critical production processes, engineering workstations retaining privileged access beyond operational requirements and limited segmentation between IT and OT environments. None of these findings appeared in the original IT-only diligence.

Risk Observation

When executive leadership remains fully engaged, budgets are approved promptly and procurement actively supports remediation, stable operational recovery can typically be achieved within approximately six months. This reflects professional experience from delivery engagements rather than an industry benchmark.

Why Capable Providers Miss It

It is worth being clear that this is rarely a failure of competence. The providers conducting cyber diligence are generally skilled at what they were asked to do. The difficulty lies earlier, in the scope they were given.

This is not a comment on the quality of the work. The firms operating in this market are technically strong, and a report delivered against a well-drawn scope is a genuinely valuable document. The constraint is almost never capability. It is that the scope is fixed before the provider is appointed, and a provider cannot report on what it was never asked to examine. The remedy therefore sits with the commissioning party, and it sits before the engagement letter is signed.

The pattern is consistent enough to be worth stating plainly. In eleven of the last fourteen industrial diligences I have conducted or reviewed, material risk sat outside the commissioned scope. In every one of those cases the report itself was accurate.

Most diligence scopes are inherited. They are adapted from a template built for software, services and other asset-light businesses, where the enterprise IT estate genuinely is the estate. Applied to an industrial target, that template produces a thorough examination of the part of the business that does not make the product. The report is accurate. It is simply answering a question that was too narrow.

This matters because scope is agreed early, quickly and often by people whose attention is elsewhere. It is treated as an administrative step ahead of the real work, when in practice it is the point at which the value of the entire exercise is decided.

The Commercial Consequence

A finding that falls outside scope has three separate effects, and each one costs money.

It cannot be priced. Remediation that was never identified does not appear in the cost to remediate, so the number presented to the investment committee is understated by an amount nobody can quantify.

It cannot be negotiated. Price adjustments and specific indemnities require evidence. A risk that has not been examined cannot support either, and general warranty language rarely provides meaningful protection for operational technology exposure.

It does not disappear. It surfaces during the hold period, usually as unplanned downtime or a production interruption, at which point it is recorded as an operational loss rather than a cyber loss. The connection back to the diligence that missed it is seldom made.

The distinction that matters commercially is between one-off and recurring cost. Capital items such as segmentation, monitoring and controlled remote access are argued as a cash adjustment to price. Permanent additions to the cost base, including specialist staffing and ongoing monitoring, are argued against the multiple and are materially more expensive over a hold period. Conflating the two is the most common error in cyber diligence, and it consistently favours the seller.

A worked example: one finding taken to a deal term

Consider the most common finding in industrial diligence. There is no segmentation between the corporate IT network and the plant control networks. Engineering workstations, historians and human-machine interfaces sit on the same flat domain as the finance estate, and vendor remote access terminates inside it. A single set of domain credentials reaches from an office laptop to a programmable logic controller.

Recorded as a technical observation, it changes nothing. Taken through to a deal term, it looks like this.

One-off capital cost	€1.35m	Discovery, segmentation design, industrial firewalls, implementation and programme management. Argued as a cash item.
Permanent run-rate cost	€475k per year	Monitoring, licensing, maintenance and two OT security engineers. This does not go away.
Applied to the entry multiple	9.0x	The recurring cost reduces normalised EBITDA at the multiple being paid.
Enterprise value effect	€4.28m	The valuation argument, and the number the seller will contest.
Total opening position	€5.63m	Roughly 2.4 per cent of a €234m enterprise value, from a single finding.

Time to defensible is fourteen months, and the binding constraint is neither budget nor skills. Segmentation cannot be cut over while a production line is running, and this business has four scheduled

maintenance windows a year across six sites. That single fact sets the shape of the plan and therefore the shape of the negotiation.

The figures above are illustrative and drawn from a fictionalised target. The method is not. Every material finding is costed this way and rolled up into the total carried in the investment committee paper.

Six Questions to Ask Before Accepting the Scope

These can be put to any provider before work begins. The answers take a few minutes and reveal a great deal.

1. **What business systems were excluded from the assessment?** Ask for the exclusions in writing, not the inclusions.
2. **What evidence validates the completeness of the asset inventory?** Do not assume the inventory is complete. In industrial targets it rarely is.
3. **Who owns operational technology, and how does that function interface with corporate IT?** Ownership determines both risk and visibility.
4. **Which findings could interrupt revenue generation or production?** This reframes the report around commercial impact rather than technical severity.
5. **What work would need to occur in the first hundred days after close?** A provider who cannot answer this has not thought about the asset as an investment.
6. **Would the conclusions change if operational technology entered scope?** If the answer is uncertain, the scope is not yet adequate.

What Adequate Scope Looks Like

Adequate scope is defined by the business rather than by the network. It begins with the question of how the organisation generates revenue, then works outward to every system that revenue depends on, irrespective of which function manages it or whether it appears on an IT asset register.

In practice that means operational technology and industrial control systems, engineering workstations, building management and safety systems, embedded supplier equipment, vendor remote access paths, and legacy operational assets that remain in service precisely because they still work.

Scope defined this way costs more and takes longer. It is also the only version capable of producing a number that survives the hold period.

The schedule below is what that looks like in practice. It can be lifted directly into an engagement letter.

Domain	Evidence required	Exclusion to state explicitly
Corporate IT	Asset register reconciled to network discovery	Nothing. This is always in scope
Operational technology and ICS	Passive discovery, engineering validation, site walkdown	Any site not physically visited
Engineering workstations	Privileged access review against current role	Contractor-owned devices, if excluded
Building management and safety systems	Ownership confirmed, network path traced	Landlord-managed systems, if excluded
Vendor and OEM remote access	Enumerated connections with named owner	Any vendor declining to participate
Embedded supplier equipment	Contractual position on patching and support	Equipment beyond vendor support life
AI and analytics in production use	Inventory, provenance, data rights position	Systems in development only, if excluded

The incremental cost of extending scope this way is typically well under 0.1 per cent of the enterprise value it is protecting. Set against a single finding capable of moving the number by two per cent or more, the arithmetic is not close.

A perfect report on the wrong scope is still the wrong answer.

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