INSIGHT PAPER · TRANSACTION ADVISORY

Pricing remediation

Turning cyber findings into deal terms

Written for deal teams and investment committees. Michael J. Loginov, August 2026.

IN SHORT

- A cyber finding that arrives as a risk rating cannot be negotiated. A finding that arrives as a one-off cost, a permanent run-rate cost and a date is a deal term.
- The run-rate cost is almost always the larger number, because it is multiplied by the entry multiple. It is also the number most often missed.
- The binding constraint on remediation in industrial and asset-heavy targets is rarely money. It is operational downtime, and it determines whether the fix lands inside the hold period.

The problem with the risk rating

Most cyber due diligence arrives at the investment committee in the wrong currency. It says that identity management is weak, that the backup regime is immature, that the target has no security leadership. All of this may be true. None of it can be used.

The committee is being asked to make one decision: whether to pay this price for this asset. A report that describes the condition of the estate without pricing it hands that translation back to the deal team, who are not equipped to do it and who are, at that point in the process, out of time. In practice the report gets summarised into a single line in the paper, the risk is noted, and the price does not move.

The waste in that is considerable. Kroll's 2026 study of more than three hundred private equity executives found firms carrying an average financial impact of around US$2.1m per cyber incident, with roughly a quarter reporting a reduced valuation or exit price as a direct consequence. The exposure is real and it is being priced by the market. It is often simply not being priced by the buyer at the point where the buyer still has leverage.

> **A finding that cannot be expressed as a cost, a timeline and a decision has not been finished.**

Three numbers, not one

A finding is complete when it carries three figures. Each answers a different question and each is used differently in the negotiation.

Number	What it is and how it is used
Value at risk	The modelled loss if the exposure is realised, expressed as a range against the target's own revenue concentration, contract penalties and recovery profile. This is the number that justifies attention. It is not the number that moves the price.
Cost to remediate	What it costs to reach a defensible position, split between one-off capital and permanent annual run-rate. This is the number that moves the price, and the split is where most of the value sits.
Time to defensible	How long until the exposure stops being material, constrained by the asset's real operating calendar rather than by an ideal project plan. This determines whether the fix lands inside the hold period.

The common failure is to produce the first number well and the other two badly. Value at risk is the easiest to model and the most persuasive to write about, which is exactly why it is over-represented in diligence reports. But a sponsor cannot take a loss model to a seller. A sponsor can take a costed remediation plan to a seller, because the seller's own advisers can check the arithmetic and will find it holds.

The distinction that decides the number

One-off cost and run-rate cost are argued in different currencies, and conflating them is the single most expensive error in cyber diligence.

One-off cost is a cash item. Hardware, implementation, a design, a programme manager for the duration. It is argued as a cash adjustment or, more often, absorbed into the value creation plan. Sellers expect this conversation and arrive prepared for it.

Run-rate cost is permanent. Monitoring that has to be watched by someone, licences that renew, engineers who do not leave when the project closes. It reduces normalised EBITDA, and it does so at the multiple being paid. On a 9.0x entry, a permanent cost of €475k per year is an enterprise value argument worth €4.28m. The same finding, described only as a €1.35m capital project, is worth a third of that.

Sellers rarely challenge the existence of the run-rate cost. They challenge its permanence, and they challenge whether it is genuinely necessary or merely the buyer's preference. Both challenges are answerable when the estimate has been built from operational experience rather than from a benchmark table, because the answer is specific: this estate cannot be operated safely without this capability, and here is what happens on the days it is absent.

> **Lead with the run-rate, not the capital. It is the larger number and it is harder to dismiss, because it is arithmetic on the seller's own multiple.**

Building an estimate that survives challenge

A costing is credible when it can be walked line by line and when each line has a stated basis. Four disciplines make the difference.

- Cost to defensible, not to ideal. There is always a version of the fix that is three times the price and does not change the risk position inside a hold period. Pricing that version discredits the whole estimate and hands the seller an easy argument.
- Separate what the asset needs from what the sponsor's policy requires. Portfolio-wide standards are legitimate, but they are the sponsor's cost, not the seller's. Mixing them into the ask is how a well-built estimate loses credibility in one meeting.
- Price the people separately from the technology. Headcount is the line a seller will attack hardest. It needs its own justification, ideally one that already exists in the target's own documents, such as an insurance renewal that assumes a capability the business does not have.
- State the range and give the point estimate anyway. A range without a central figure reads as evasion. A point figure without a range reads as false precision. Give both, and say what would move it.

Time to defensible is an operational question

In asset-heavy and industrial targets the constraint on remediation is almost never budget and almost never skills. It is downtime. Network segmentation cannot be cut over on a running production line. A business with four scheduled maintenance windows a year across six sites has a fixed number of opportunities to do the work, and that fact sets the shape of the plan regardless of how much money is available.

This is where diligence conducted by people who have only reviewed estates diverges sharply from diligence conducted by people who have run them. A plan that assumes work can be scheduled on demand will be presented to the committee, approved, and then quietly slip by two quarters once the operations director sees it. The sponsor discovers in year two that the risk they thought they had priced is still open.

The more useful output is not the completion date but the risk reduction curve. A sponsor should know the month at which the exposure stops being existential, which is usually well before the programme closes. In a typical multi-site segmentation programme, sixty percent of the risk is gone by month nine of a fourteen month plan. That is the number that belongs in the investment committee paper.

Turning the numbers into deal terms

Priced findings convert into four distinct instruments, and choosing the right one matters as much as the quantum.

Instrument	When it is the right one
Price adjustment	For permanent run-rate cost and for capital that is unavoidable and quantifiable. This is where the bulk of the value is recovered, and it is the hardest for a seller to argue away because it rests on their own multiple.
Specific indemnity	For known incidents, contestable insurance positions and regulatory exposure with an uncertain quantum. A general cyber warranty does not cover a breach the seller has already told you about.
Condition precedent	For anything that must be true before signing, such as confirmation of the insurance disclosure position or delivery of an asset inventory for sites not visited.
Value creation plan	For remediation that is genuinely investment rather than repair, and which the sponsor intends to convert into an exit credential. This is a different conversation and should not be mixed into the price ask.

A practical note on negotiation. Open with the full build shown rather than a rounded total, and expect to land between fifty-five and seventy percent of the ask, with the balance handled through indemnity rather than price. A costing that can be walked survives challenge. A round number invites a round counter-offer.

Five ways the estimate goes wrong

- The IT boundary is treated as the estate boundary. Operational technology, industrial control systems, building management and embedded supplier equipment sit outside most diligence scopes and hold most of the un-priced risk in industrial targets.
- Benchmark costs are used in place of delivery costs. Published figures assume conditions that rarely hold: available internal resource, standard architecture, no production constraints. They are usually low by a wide margin in multi-site environments.
- The run-rate is folded into the capital figure. This understates the ask by roughly the entry multiple, which is to say by most of it.
- Findings are counted rather than weighted. Twenty findings look thorough. If three of them carry ninety percent of the exposure, the other seventeen are noise that dilutes the argument in the room.
- AI systems are omitted because nobody owns them. Model provenance, training data rights and third party AI embedded in purchased software carry real contractual exposure, and in EU-scoped targets a compliance timetable that has already started.

A short checklist for the deal team

Six questions to put to whoever is running your cyber diligence, before the report is written rather than after.

- Which three findings carry most of the exposure, and what is each one worth in enterprise value terms?
- For each priced finding, what is the split between one-off and permanent run-rate cost?
- What is the operational constraint on the remediation timeline, and who confirmed it?
- At what month does the exposure stop being material, as distinct from when the programme completes?
- What did you not see, and how would the estimate move if it turns out to be worse than assumed?
- Which of these belongs in the price, which in an indemnity, and which in the hundred day plan?

If those six questions cannot be answered from the report, the diligence has described the target rather than priced it, and the committee is being asked to decide without the one thing it needs.

ABOUT THE AUTHOR

Michael J. Loginov advises private equity sponsors, investment committees and risk advisory firms on cybersecurity due diligence, technology risk and AI governance across the transaction lifecycle. He has held sixteen security leadership mandates spanning global, group, executive director and advisory remits, including inaugural Group CISO at NEOM and executive cybersecurity leadership inside an Inflexion Private Equity-backed platform. In several of those roles the CISO reported to him. He has led five major cyber recovery programmes, including an industrial breach that halted production and threatened insolvency.

UK CISO of the Year 2020 · UK Cyber Security Hall of Fame · Author of CISO: Defenders of the Cyber Realm, with a foreword by Vint Cerf

Market data referenced is drawn from Kroll's 2026 research into cybersecurity risk in private equity. Figures used to illustrate method relate to a fictionalised target and are not derived from any client engagement. This paper is general commentary and is not advice on any specific transaction.