COLLATED PACK · AUGUST 2026

Cyber due diligence

engagements and sample deliverables

Five documents. What can be commissioned, what the output looks like, and the method underneath it.

Contents

A note on the samples

Documents 01 to 03 relate to Project Anvil, a fictionalised mid-market industrial target. They are constructed to illustrate method and are not derived from any client engagement. No client information appears in this pack.

They are deliberately connected. Finding F1 appears on the heat map in document 02, is costed line by line in document 03, and arrives at the investment committee as a priced position in document 01. Read together they show a single finding travelling from observation to deal term.

Individual mandates, findings and client information remain subject to confidentiality and non-disclosure obligations.

Michael J. Loginov

Independent cyber due diligence and transaction advisory

mike@loginov.me · +66 933 299 000 · michaelloginov.com · linkedin.com/in/mikeloginov

ILLUSTRATIVE SAMPLE DELIVERABLE · FICTIONALISED TARGET · NO CLIENT INFORMATION

PROJECT ANVIL

Cybersecurity Due Diligence · Investment Committee Summary

Target	Meridian Actuation Group B.V.	**Sponsor**	Buy-side, mid-market industrials fund
Sector	Industrial actuation and motion control	**Enterprise value**	€234m (9.0x FY25 EBITDA €26m)
Footprint	6 plants: DE, NL, PL, MX. 1,400 FTE	**Scope**	Confirmatory diligence, IT / OT / AI
Fieldwork	18 days, 3 sites visited	**Prepared for**	Investment Committee, 14 March

RECOMMENDATION

Proceed, with price adjustment and two conditions

No deal-breaker identified. The estate is under-invested rather than compromised. The exposure is priceable and the remediation is deliverable inside the hold period, but the run-rate cost is permanent and should be reflected in the entry multiple.

VALUE AT RISK
€14m – €31m
Modelled single-event loss, 8 to 15 day production halt

COST TO REMEDIATE
€4.3m
€2.9m one-off, €0.9m recurring annual run-rate

TIME TO DEFENSIBLE
14 months
To a control posture that survives buyer scrutiny at exit

FINDINGS THAT MOVE THE NUMBER

- No segmentation between corporate IT and plant control networks at any of the six sites. A commodity ransomware event on the corporate domain reaches production. This is the dominant driver of the value at risk range.
- Backups are neither tested nor isolated for OT. Recovery from the 2024 attempt was achieved by rebuilding from vendor media over eleven days.
- No accountable security leadership. The function is carried informally by an IT infrastructure manager at roughly 0.4 FTE alongside a full operational workload.
- NIS2 scope confirmed for the German and Dutch entities, with no registration, reporting process or management-body accountability in place.
- Cyber insurance renewal warranties on MFA and privileged access are not met as described. A claim under the current policy would be contestable.

DOMAIN ASSESSMENT

Governance & organisation	**Red**	**OT & plant systems**	**Red**
Resilience & recovery	**Red**	**Identity & access**	**Amber**
Third party & supply chain	**Amber**	**Data protection & regulatory**	**Amber**
AI governance	**Amber**	**Incident history**	**Green**

DEAL IMPLICATIONS

Price	Recurring cost of €0.9m against a 9.0x multiple supports an €8.1m enterprise value argument, plus €2.9m one-off. Open at €11.0m.
SPA	Specific indemnity for the 2024 incident and for the insurance warranty position. General cyber warranty is not sufficient here.
Conditions	Seller to confirm current insurance disclosure position pre-signing. Vendor to provide OT asset inventory for the two unvisited sites.
First 100 days	Appoint accountable security leadership in month one. Segment the two highest-revenue plants by month four. Full plan in the accompanying report.

Basis and limitations. Prepared from management interviews, documentation review, external attack surface analysis and site inspection at three of six locations. No intrusive testing was performed. Figures are ranges based on comparable programmes and are indicative for negotiation, not a warranty of outcome. Full findings, evidence and remediation plan are set out in the accompanying diligence report.

ILLUSTRATIVE SAMPLE DELIVERABLE · FICTIONALISED TARGET · NO CLIENT INFORMATION

PROJECT ANVIL

Cyber Risk Heat Map · Pre-remediation position at confirmatory diligence

Ten findings plotted by operational impact and assessed likelihood over a three year hold. Position reflects the estate as found, before any remediation. Cost to remediate for each finding is set out overleaf and rolls up to the €4.3m total in the investment committee summary.

IMPACT

IMPACT \ LIKELIHOOD	Rare	Unlikely	Possible	Likely	Almost certain
Severe Multi-site production halt, >€10m loss			F5	F1	
Major Single-site halt, €2–10m loss		F10	F4	F3	F2
Moderate Degraded output, €0.5–2m loss			F8	F7	F6
Minor Contained disruption, <€0.5m			F9		
Negligible No operational effect					

Critical
Priced into the deal. Remediation begins pre-close or day one

High
Addressed in the first 100 days. Cost carried in the value creation plan

Moderate
Scheduled within 12 months. Monitored at board level

Low
Accepted or managed through routine operations

Finding register

Ranked by combined score. Target rating is the position achievable within the first 100 days and the following year.

Ref	Finding	Impact	Likelihood	Cost to remediate	Now / target
F1	No segmentation between corporate IT and plant control networks at any of the six sites	5	4	€1.35m	Red → Amber
F2	End-of-life operating systems on plant control workstations and HMIs	4	5	€0.62m	Red → Amber
F3	No detection or monitoring coverage outside business hours	4	4	€0.48m	Amber → Green
F4	Privileged access uncontrolled. Shared domain administrator credentials	4	3	€0.31m	Amber → Green
F5	Backups untested and not isolated. No recovery capability proven for OT	5	3	€0.44m	Amber → Green
F6	OEM remote access into plant networks unmanaged and unmonitored	3	5	€0.18m	Amber → Green
F7	No accountable security leadership. Function carried at approximately 0.4 FTE	3	4	€0.52m	Amber → Green
F8	NIS2 obligations unaddressed in the German and Dutch operating entities	3	3	€0.21m	Amber → Green
F9	AI vision inspection running in production with no assurance or ownership	2	3	€0.09m	Amber → Green
F10	Cyber insurance warranties not met as described. Claim position contestable	4	2	€0.10m	Amber → Green

Impact and likelihood are assessed against the target's own operating model, not a generic benchmark. Likelihood reflects a three year hold. Costs are indicative ranges for negotiation, not quotations. F1 is developed in full in the accompanying remediation costing example.

ILLUSTRATIVE SAMPLE DELIVERABLE · FICTIONALISED TARGET · NO CLIENT INFORMATION

PROJECT ANVIL

Worked remediation costing · Finding F1 · From finding to deal term

This is a single finding taken end to end. It shows how one observation becomes a cost, a timeline and a position at the negotiating table. The same method is applied to each finding and rolled up into the total remediation figure carried in the investment committee summary.

1. The finding

There is no segmentation between the corporate IT network and the plant control networks at any of the six manufacturing sites. Engineering workstations, historians and human-machine interfaces sit on the same flat domain as office file servers and the finance estate. Vendor remote access terminates inside the same network. A single set of domain credentials reaches from an office laptop to a programmable logic controller.

Nothing here is exotic. This is the most common finding in industrial diligence and it is the one most often recorded as a technical observation and then dropped from the commercial narrative.

2. Why it matters commercially

- A commodity ransomware event on the corporate estate, the kind this business already experienced in 2024, propagates to production. The company is not being targeted. It does not need to be.
- Recovery of OT systems from vendor media, which is what happened in 2024, took eleven days at one site. Across two sites in peak season the modelled loss is €14m to €31m in lost contribution, expedited freight and contractual penalties.
- The four largest customers now require evidence of network segmentation at supplier audit. Two contracts, representing €38m of revenue, carry a right to audit that has not yet been exercised.
- At exit, a sophisticated buyer will run the same diligence. An unsegmented estate is a visible discount. Fixing it in year one converts a discount at exit into a credential.

3. Cost to remediate

Costed to a defensible position, not to a best-practice ideal. The scope is zone separation with controlled conduits, monitored vendor access and proven recovery. It is not a full Purdue model rebuild, which would cost roughly three times this and would not change the risk position materially inside a hold period.

Workstream	One-off	Annual run-rate	Basis of estimate
OT asset discovery and network mapping, six sites	€160k	–	Passive discovery tooling plus 4 weeks of specialist effort per cluster
Segmentation design and reference architecture	€85k	–	One design, applied six times. Not six designs
Industrial firewalls, switching and data diodes	€560k	€78k	Six sites, 3 zones per site. Vendor list price less typical discount
Implementation and commissioning	€290k	–	Two plants per wave, executed in scheduled maintenance windows
Managed remote access platform for OEM vendors	€85k	€42k	Replaces 14 uncontrolled vendor connections
Monitoring extension into the OT estate	€55k	€165k	Sensor deployment plus 24/7 coverage through a managed provider
Two OT security engineers	–	€190k	Loaded cost, Poland and Germany. Permanent capability, not project
Programme management and assurance, 14 months	€110k	–	0.5 FTE programme lead plus independent design review
Total, finding F1	**€1.35m**	**€475k**	Range €1.15m to €1.60m including contingency

Estimates are built from comparable programmes delivered in multi-site industrial environments. They assume the target's own engineering resource is available for plant coordination. They exclude any equipment replacement driven by obsolescence rather than security, which is a separate capital question for the operational team.

4. Time to defensible

Fourteen months for this finding. The constraint is not money and it is not skills. It is production downtime. Segmentation cannot be cut over while a line is running, and this business has four scheduled maintenance windows per year across six sites. That single fact sets the shape of the plan.

Months	Activity	Binding constraint	Risk reduced
0 – 2	Discovery, asset inventory, design	Specialist availability	**None yet**
2 – 4	Procurement and staging	Industrial switching lead times, 10 to 14 weeks	**None yet**
3 – 9	Plant implementation, two per wave	Scheduled maintenance shutdowns only	**60%**
9 – 11	Vendor remote access and OT monitoring	OEM contract renegotiation	**85%**
11 – 14	Validation, tabletop exercise, evidence pack	Nothing external	**100%**

Sixty percent of the risk is removed by month nine. That matters more than the completion date. A sponsor with a hold period should know when the exposure stops being existential, not just when the programme closes.

5. Effect on price

Two costs, argued two different ways. Conflating them is the most common error in cyber diligence and it usually costs the buyer money.

Permanent run-rate cost	**€475k per year**	Monitoring, licensing, maintenance and two engineers. This does not go away.
Applied to entry multiple	**9.0x**	The recurring cost reduces normalised EBITDA at the multiple being paid.
Enterprise value effect	**€4.28m**	The valuation argument. This is the number the seller will contest.
One-off capital cost	**€1.35m**	Argued separately as a cash item, not an EBITDA adjustment.
Total opening position, F1	**€5.63m**	Against a €234m enterprise value. Roughly 2.4% of EV from one finding.

How this is argued

- Lead with the run-rate, not the capital. Sellers expect a capex conversation and are prepared for it. The permanent EBITDA effect is the larger number and is harder to dismiss because it is arithmetic on their own multiple.
- Separate the two engineers from the hardware. Headcount is the line a seller will attack as buyer preference rather than necessity. It is defensible here because the estate cannot be operated safely without it, and because the target's own insurance renewal already assumes the capability exists.
- Do not ask for the full number and do not open with a range. Open at €5.63m for this finding, with the build shown. A costing that can be walked line by line survives challenge. A round number does not.
- Expect to land between 55 and 70 percent of the ask, with the balance addressed through a specific indemnity for the 2024 incident rather than through price.

What would change this number

- Two of the six sites were not visited. If their OT estate matches the visited sites, the estimate holds. If either runs a materially different control platform, the hardware line moves by up to €200k.
- Industrial switching lead times have moved between eight and twenty weeks over the past two years. A longer lead time does not change cost, but it extends time to defensible by up to a quarter.
- If the sponsor intends to bolt on further sites during the hold, designing for that now adds roughly €90k and avoids a repeat programme later.
- If the seller has already committed capital to this work, which management indicated but did not evidence, the one-off cost reduces and the argument shifts to timing and completion risk rather than quantum.

This document is an illustration of method. Figures relate to a fictionalised target and are not derived from any client engagement. Ranges are indicative for negotiation and are not quotations or a warranty of outcome.

ENGAGEMENT PACK

Cybersecurity due diligence for private equity

Six engagements, mapped to the points in a deal and the hold period where cyber decides value. Scope and deliverables are set out in full. Commercial terms are agreed against the mandate.

Michael J. Loginov

Independent cyber due diligence and transaction advisory

mike@loginov.me · +66 933 299 000 · michaelloginov.com · linkedin.com/in/mikeloginov

How I work

Every engagement is delivered by me. There is no team behind the proposal that you do not meet, and no junior analyst writing the report. That constrains how much work I take on, which is the point.

The output is written for the person making the investment decision, not for the security function. A finding that cannot be expressed as a cost, a timeline and a decision has not been finished.

I have run these estates rather than only reviewed them. Sixteen security leadership mandates across global, group, executive director and advisory remits, from greenfield builds at sovereign scale to industrial crisis recovery. In several of them the CISO reported to me. Remediation estimates come from having delivered the work, not from a benchmark table.

I have no product to sell, no managed service to upsell and no downstream remediation contract to protect. The recommendation is the deliverable.

THE SIX ENGAGEMENTS

ENGAGEMENT	DURATION	DEAL STAGE	PRIMARY OUTPUT
01 Red Flag Screen	7 to 14 working days	Pre-LOI	One-page screen. Proceed, price or walk
02 Confirmatory Diligence	3 to 4 weeks	Exclusivity	Investment committee paper with priced findings
03 First 100 Days	3 to 12 months	Post-close	Executed remediation plan and interim leadership
04 AI Governance Review	3 weeks	Any stage	Gap assessment against EU AI Act and ISO/IEC 42001
05 Fractional or Interim CISO	6 to 24 months	Hold period	An accountable security leader and a functioning team
06 Non-Executive Board Advisor	12 months, rolling	Any stage	Independent challenge on cyber and AI in the board pack

Engagements are sized to the mandate and the pace of the transaction. They can be run individually or in sequence across the deal lifecycle and the hold period. Delivered on site or remotely across Asia, Europe and the Middle East.

01 Red Flag Screen

A fast, outside-in read on a target before terms are set

DURATION	DEAL STAGE	ACCESS REQUIRED
7 to 14 working days	**Pre-LOI**	**Minimal**

WHAT I DO

- External attack surface and exposure analysis, conducted without contact with the target where confidentiality requires it.
- Breach and incident history research, including leaked credential exposure and dark web presence.
- Assessment of the target's regulatory position, including NIS2, DORA and sector obligations where they apply.
- Where management access is available, a single structured session with the senior technology or operations lead.
- Identification of anything that should stop the deal or change the terms before you commit to exclusivity.

WHAT YOU RECEIVE

- A one-page screen with a clear recommendation: proceed, proceed with conditions, or walk.
- Traffic light rating across eight domains, with the basis for each rating stated.
- An indicative remediation cost range, given as a band rather than a point estimate at this stage.
- A short list of the questions to press in confirmatory diligence, and where management is most likely to be optimistic.
- A verbal debrief with the deal team, usually within 24 hours of the written output.

WHAT THIS IS NOT

This is not confirmatory diligence and should not be relied on as such. A screen of this length buys you a view on whether the risk is worth investigating properly, and on whether the terms should reflect it. It does not buy you a defensible position for the investment committee.

02 Confirmatory Diligence

Findings quantified in terms an investment committee can price

DURATION	DEAL STAGE	ACCESS REQUIRED
3 to 4 weeks	**Exclusivity**	**Full**

WHAT I DO

- Management interviews across technology, operations, finance and, where relevant, plant engineering.
- Documentation and evidence review against the target's own operating model rather than a generic framework.
- Site inspection where operational technology, industrial control systems or physical estate are material.
- Assessment of the full estate: IT, OT, IoT, ICS and AI. Most under-priced risk sits outside the IT boundary.
- Costing of each material finding into a one-off figure, a permanent run-rate figure and a delivery timeline.
- Modelling of value at risk against the target's own revenue concentration and operational dependencies.

WHAT YOU RECEIVE

- An investment committee paper, written to be read by people who are not security specialists.
- A risk heat map plotting each finding by operational impact and assessed likelihood over the hold period.
- Cost to remediate and time to defensible, built line by line so that every figure can be walked and defended.
- A price adjustment argument where the evidence supports one, separating capital cost from permanent EBITDA effect.
- Recommended SPA positions, including where a specific indemnity is needed rather than a general warranty.
- Attendance at the investment committee to present and defend the findings, at no additional cost.

WHAT THIS IS NOT

This is not a penetration test, a compliance audit or a certification exercise. Where intrusive technical testing is warranted I will say so and can specify it, but it sits outside this engagement.

03 First 100 Days

Turning diligence findings into a de-risked asset

DURATION	DEAL STAGE	BASIS
3 to 12 months	**Post-close**	**Fractional or interim**

WHAT I DO

- Convert the diligence findings into a sequenced remediation plan built around the asset's operational constraints.
- Establish accountable security leadership, whether by recruiting it, standing in as interim CISO, or both.
- Post-merger integration of security and technology governance where the asset is a platform or bolt-on.
- Build the board and sponsor reporting line so that cyber risk is visible in the same cadence as financial performance.
- Where required, act as interim CISO or CAIO through the transition rather than advising from the outside.

WHAT YOU RECEIVE

- A prioritised remediation roadmap with owners, sequencing and the operational windows the work must fit into.
- A governance structure that survives the sponsor's reporting requirements and the eventual exit process.
- Quarterly progress reporting written for the sponsor, showing risk reduced rather than tasks completed.
- A capability that continues after I leave, including the specification and recruitment of the permanent hire.
- Evidence packaged as it is generated, so that exit diligence is a retrieval exercise rather than a reconstruction.

WHAT THIS IS NOT

This is not a staff augmentation arrangement and it is not an outsourced security function. The objective is a management team that no longer needs me.

04 AI Governance Review

AI risk assessed with the discipline investors expect of financial and legal diligence

DURATION	DEAL STAGE	FRAMEWORKS
3 weeks	**Any**	**EU AI Act, ISO 42001**

WHAT I DO

- Inventory of AI systems in use, in development and embedded in third party products, which is usually where the surprises are.
- Classification against EU AI Act risk tiers, with a clear position on which obligations apply and by when.
- Gap assessment against ISO/IEC 42001 and the NIST AI Risk Management Framework.
- Assessment of model provenance, data rights and the contractual position on training data, which carries real deal risk.
- A board or investment committee workshop to establish where accountability for AI risk actually sits.

WHAT YOU RECEIVE

- A gap assessment with obligations mapped to deadlines and to named owners.
- An implementation roadmap costed to the same standard as the cyber remediation plan.
- A written position on AI-related deal risk suitable for inclusion in the investment committee paper.
- Executive workshop materials and a governance framework the business can operate without external support.

WHAT THIS IS NOT

This is not a legal opinion on the EU AI Act and does not replace counsel. It establishes the factual and operational position that legal advice is then given against.

05 Fractional or Interim CISO

Accountable security leadership without a permanent hire

DURATION	COMMITMENT	BASIS
6 to 24 months	**2 to 4 days a month, or full time**	**Fractional or interim**

WHAT I DO

- Hold the CISO accountability formally, reporting to the board, the audit committee or the sponsor.
- Own the security strategy, budget and roadmap, and the decisions about what is not being done and why.
- Lead the existing function, or build one, including structure, hiring specification and supplier consolidation.
- Represent security externally: to clients in their own diligence, to insurers at renewal, and to regulators where DORA, NIS2 or sector rules apply.
- Lead the response if a material incident occurs on watch, including board and sponsor communications.
- Specify and recruit the permanent successor, then hand over against a documented plan.

WHAT YOU RECEIVE

- A named, accountable security leader at a fraction of the cost of a permanent executive hire.
- Board and audit committee reporting in the cadence the sponsor expects, written in business terms.
- A costed roadmap that survives challenge, and a team capable of delivering it.
- Client-facing and insurer-facing assurance, which frequently unblocks revenue that a security gap was holding up.
- Continuity of judgement across the hold period rather than a sequence of short consulting engagements.
- A documented handover to the permanent CISO, with the capability left standing.

WHAT THIS IS NOT

This is not a part-time consultant without authority. The role carries accountability and the decisions that go with it. Nor is it intended to be permanent: the measure of success is a business that no longer needs the arrangement.

06 Non-Executive Board Advisor

Independent challenge on cyber and AI risk at the top table

DURATION	COMMITMENT	BASIS
12 months, rolling	**Board cycle, plus call-off**	**Advisory or non-executive**

WHAT I DO

- Sit on the board or advisory board, or attend the audit and risk committee as the cyber and AI specialist.
- Challenge the executive's reporting: whether the risk position presented is the real one, and whether the assurance behind it holds.
- Advise the chair or the sponsor privately on where the reported position and the operational reality diverge.
- Support the sitting CISO rather than displace them, including acting as a sounding board between meetings.
- Provide an independent read on cyber and AI readiness ahead of a fundraise, refinancing or exit.
- Review incident and near-miss reporting for what it says about the control environment rather than the incident.

WHAT YOU RECEIVE

- Independent challenge on the cyber and AI content of the board pack, before it reaches the buyer or the regulator.
- A cyber voice at the top table that is not reporting to the executive it is assessing.
- Early warning where a control gap is likely to surface in exit diligence, while there is still time to fix it.
- Access between meetings for the chair, the sponsor or the CISO when a decision cannot wait for the next cycle.
- An annual written opinion on the maturity trend, suitable for the sponsor's own reporting.

WHAT THIS IS NOT

This is not executive management and it is not the CISO role. Independence is the value, so I will not hold both positions in the same business at the same time.

Confidentiality and how information is handled

Cyber diligence involves being told, in writing, exactly where a business is weakest. That information is commercially sensitive to the sponsor and existentially sensitive to the target. How it is handled is part of the engagement, not an afterthought.

BEFORE ANYTHING IS DISCUSSED

Mutual NDA	A mutual non-disclosure agreement (MNDA) is put in place before a target is named. Mutual rather than one-way, because the method, pricing approach and working papers are mine, and the target and deal thesis are yours. I will work to your paper or provide a short form MNDA if that is faster.
Conflicts check	Run before any target is discussed in detail. If I hold a current mandate that conflicts, I will say so and decline rather than manage around it. Where I have prior knowledge of a target from an earlier engagement, that is disclosed before we proceed.
Clean team	Where a transaction requires clean team arrangements, I can work inside them and will sign the associated protocols. Competitively sensitive material is handled accordingly.

DURING THE ENGAGEMENT

- Target material is held only for as long as the engagement requires it, in an encrypted store under my sole control.
- No target information is placed in third party AI tools, cloud analysis services or shared drives.
- Where the target is not aware of the transaction, the work is scoped so that nothing I do signals it. Outside-in analysis is used in place of contact.
- Findings are reported to the commissioning party only. I do not brief the target, its management or any other bidder unless you instruct it in writing.

AFTER THE ENGAGEMENT

- Working papers and target material are destroyed or returned on request at engagement close, subject to any retention the MNDA or your own policy requires.
- The deliverable is yours. It can be shared with your investment committee, lenders and advisers without further permission.
- Engagements are not referenced publicly. Nothing in my own materials names a target, a sponsor or a transaction without written consent.

A NOTE ON ABORTED DEALS

Deals fall over, sometimes because of what the diligence finds. Where an engagement is stopped mid-flight, you are billed for work delivered to that point and the findings are handed over in whatever state they have reached, rather than withheld pending completion.

Commercial basis

Terms are agreed against the mandate rather than published, because the same engagement carries different value on a €30m carve-out and a €900m platform. What follows is how the work is structured.

Basis	Fixed-scope assignment · Retained · Day rate · Fractional or interim · Advisory or non-executive
Engaged	Directly by the sponsor, or through advisory, risk and consulting firms as a named specialist under their contract and brand
Mobilisation	Typically within five working days for a screen, ten for confirmatory diligence. Fractional and non-executive arrangements start at the next board or reporting cycle
Coverage	Asia, Europe and the Middle East. On site as the mandate requires, remote where it does not
Confidentiality	Mutual NDA before a target is named. Standard sponsor NDAs accepted. Conflicts checked before any target is discussed
Capacity	Engagements are taken in limited number so that each is delivered personally. Confirmatory diligence in particular is capacity constrained during exclusivity periods
Combining engagements	A screen credits against confirmatory diligence on the same target. Diligence findings carry directly into First 100 Days without a re-scoping exercise

WHERE I AM NOT THE RIGHT FIT

I am probably not the right choice if you need a twenty-person team, an audit sign-off, or a commodity compliance assessment. Those are legitimate requirements and there are firms built to meet them. My work is concentrated on complex transactions where experienced judgement informs the investment decision, and where the person who did the fieldwork is the person who defends it in the room.

NEXT STEP

A 30 minute conversation about the deal, under MNDA if preferred, is usually enough to establish whether the risk is worth investigating and which engagement fits.

Michael J. Loginov

UK CISO of the Year 2020 · UK Cyber Security Hall of Fame · Author, *CISO: Defenders of the Cyber Realm*

mike@loginov.me · +66 933 299 000 · michaelloginov.com

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.