Appendix: Illustrative Cost Model

Companion to: *From Telemetry Inflation to Decisive Observability* (main strategic paper)

This appendix is a **sensitivity exercise, not a forecast**. It expands the condensed economics note in the main paper with editable placeholders, tables, and meeting prompts. **All monetary amounts are USD.**

Terminology: In the main paper, *high-fidelity proof*, *decisive evidence*, and *richer evidence* refer to the same outcome: trusted explanatory proof delivered on operational time. This appendix uses **proof** and **evidence** in that same sense.

Illustrative Cost Model (Sensitivity Exercise, Not a Forecast)

Leadership conversations stall when observability remains only qualitative. The figures below are a **deliberately simple calculator**: they exist to show **which levers move the budget**—bridge duration, headcount on a bridge, and incremental "insurance-shaped" infrastructure—not to assert audited savings.

Replace every input with your own (region, labor mix, incident taxonomy, and risk appetite).

Shared assumptions (editable)

Input	Example value	What it stands for
Blended fully loaded cost per incident hour	**$200 / hr**	Mixed L2/L3, duty managers, vendor time (order-of-magnitude)
Average concurrency on a major bridge	**8 people**	Parallel streams (NOC, app, network, storage, security, leadership)
Major "ambiguous transient" incidents per year	**12**	Severity-1/2 events where causality is disputed for hours

These inputs are not recommendations. They are **placeholders** so finance can run a one-page sanity check.

OPEX: bridge time dominates

Bridge labor cost per incident is roughly:

> **concurrency × blended hourly cost × hours to trusted explanatory story**

Using the placeholders:

Scenario	Hours to trusted story (example)	Labor-only bridge cost (example)
A — Late proof (re-capture, widen windows, debate artifacts)	6 hr	8 × $200 × 6 = **$9,600**
B — Earlier decisive proof (same staffing, shorter ambiguity window)	2 hr	8 × $200 × 2 = **$3,200**

Illustrative **delta per incident**: **$6,400** in bridge labor alone—before customer credits, SLA penalties, opportunity cost, or vendor charges.

At **12** such incidents per year, that single line item is on the order of **~$77k/year** of *bridge-time difference* in this toy model. Change concurrency to **12** people or hourly cost to **$350**, and the same math scales linearly.

> **The point is not the exact dollars. The point is that the function is multiplicative: people × time × incident rate.**

All figures in this appendix are **USD**. The same formula scales linearly with whatever burdened hourly rate finance accepts (for example **$250/hr** or **$350/hr** instead of $200/hr).

CAPEX: "insurance-shaped" observability stacks compound

A separate line—often buried in refresh cycles—is incremental capital spent to reduce uncertainty: more capture, hotter retention, wider analytics clusters. A three-year program might add **single-digit to low tens of millions** of USD in large environments, depending on scope; amortization and refresh rules determine how it hits the P&L.

Illustrative 3-year TCO shell (always-on capture / wide observability path)

The table below is an **order-of-magnitude TCO skeleton** for a "widen the net" program—not a quote. Ranges intentionally wide; finance should substitute vendor pricing and internal run costs.

Line item	Illustrative 3-year TCO band (USD, large enterprise)	What typically drives the spread
Tap / SPAN / packet broker fabric + optics	**$3M–$8M**	Port count, speeds (100G–800G), redundancy
Capture appliances / probes	**$1M–$4M**	Sustained throughput, buffering, form factor

Line item	Illustrative 3-year TCO band (USD, large enterprise)	What typically drives the spread
Storage + hot retention for flow / metadata / PCAP-adjacent data	**$2M–$6M**	TB/day ingest, retention policy, replication
Analytics / SIEM / datastore ingest uplift	**$1M–$4M**	EPS, licensing, compute cluster
Implementation + 3-year run (FTE + contractors + training)	**$1M–$3M**	Often under-modeled

Rough combined band: about **$8M–$25M** over three years for a heavy "insurance-shaped" posture in a large footprint—**before** you can show a modeled reduction in **hours of ambiguity** per incident.

> **TCO is not the enemy.** The question is whether the next dollar reduces **forensic time** enough to justify itself, or mainly expands **capacity to store uncertainty**.

An evidence-activation posture does not magically eliminate that baseline. It targets a different failure mode: **spending for universal high fidelity and still paying long bridges** because proof arrives on forensic time.

A useful internal question is therefore:

> **If we spend the next tranche of CAPEX on wider always-on capture, what is our modeled reduction in *hours of ambiguity*—and who owns that assumption?**

SLA credits and contractual exposure (illustrative add-on)

Bridge labor is only one line. Many organizations also carry **contractual** exposure: service credits, rebates, or penalties tied to **minutes** of outage or sustained degradation. This is **not legal advice**; it is a reminder to put **revenue-at-risk** next to **hours on bridge**.

Input	Example (placeholder)
Monthly recurring revenue (MRR) under an affected contract	**$500,000**
SLA: cumulative **30 minutes** of violation triggers a **10%** monthly service credit (cap varies)	Policy-dependent
One incident drives **45 minutes** of billable violation time	Simplified

If the credit applies as **10% of MRR** for that month, **one** qualifying month exposes on the order of **$50,000** in credits—**before** vendor overtime, customer churn risk, or regulatory reporting costs.

> **A single material SLA month can swamp the bridge-OPEX line.** That is why "faster proof" is not only efficiency—it can be **revenue and relationship protection**.

How to use this appendix in a meeting

- Treat the tables as a **spreadsheet shell**, not a claim.
- Force alignment across networking, operations, and finance on **hours to trusted story** for one historical incident; the argument becomes empirical quickly.
- If the organization cannot estimate **hours to trusted story**, that is already a signal: **the cost model is missing the variable that actually invoices.**

← Back to main paper

License Notice