

The breach already happened.

INCIDENT 001 MMG

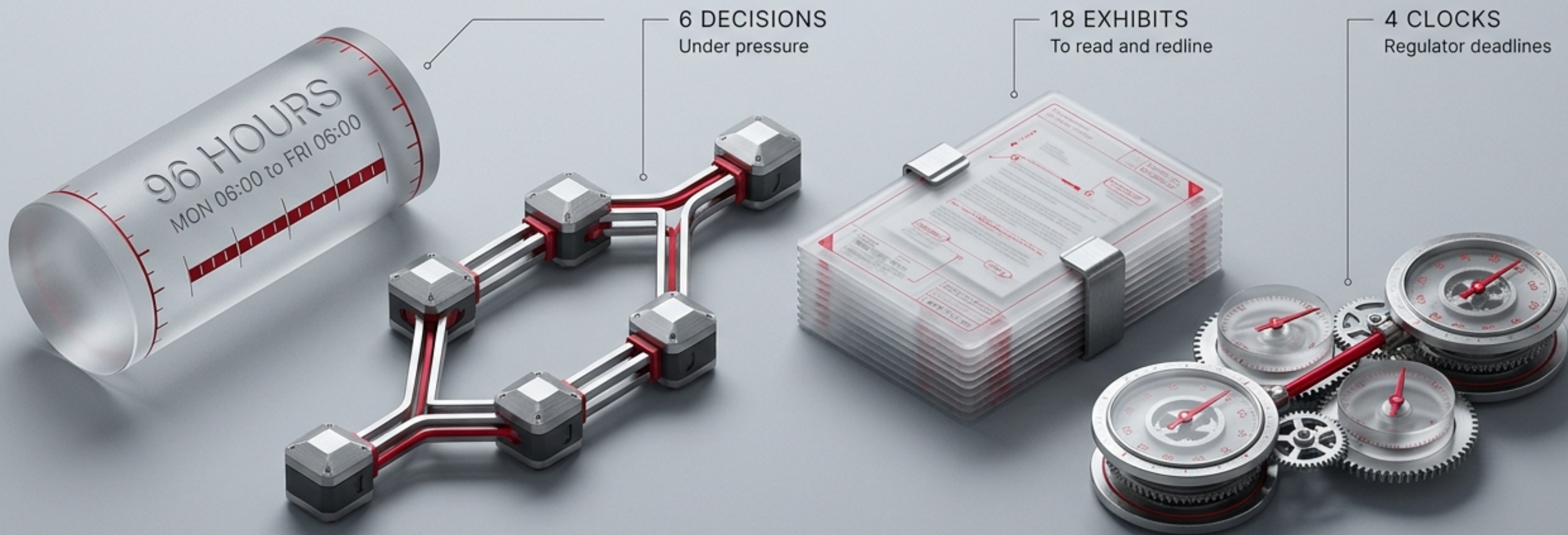
Third-party breach. First-party consequences.

Counterparty: Lattice Transfer Institution
Meridian Mutual Command window: 96 hours
Exercise: Synthetic

T+00:00 · MON 06:00 ET

GENERAL QUARTERS IS A NINETY-SIX-HOUR CRUCIBLE FOR INCIDENT COMMANDERS.

What gets examined afterwards is what you decided, and when. Two scenarios: Banking (file-transfer breach) and Healthcare (ransomware attack).



T+04:00 · MON 10:00 ET

The same breach yields entirely different consequences based on when you act.

We watch two commanders replay the exact same threat matrix starting at T+00:00.



T+08:00 · MON 14:00 ET

The regulatory clocks run from when examiners say you knew, not when you declare it.

Holding the word back for two days does not move the deadline. The simulator dates your "determination" strictly from the internal bridge notes.



Four relentless clocks run on the board while you work.

Nobody reminds you. You file each one yourself, at the hour you choose.



36h from determining a notification incident

72h from determining a cybersecurity incident (including third-party)

4bd (business days) from determining material impact. Must come without unreasonable delay.

24h countdown. Opens only if payment is made, written justification due in 30 days.

T+24:00 · TUE 06:00 ET

Survival requires finding the blocking answers hidden in the document tray.

Every inject lands new intelligence on your desk. The vendor is evasive. Counsel is cautious. An analyst closed the SOC ticket that mattered: "Consistent with month-end backlog. No action."



T+32:00 · TUE 14:00 ET

One sentence is only safe to keep if your own prior actions made it true.

You must mark up the draft SEC Form 8-K (Item 1.05) and the customer notice sentence by sentence.

KEEP

The affected data includes names, addresses and account numbers for approximately 2.1 million customers.

STRIKE

~~The Company has found no evidence that any customer information has been misused.~~

(Fails because exfiltration was confirmed)

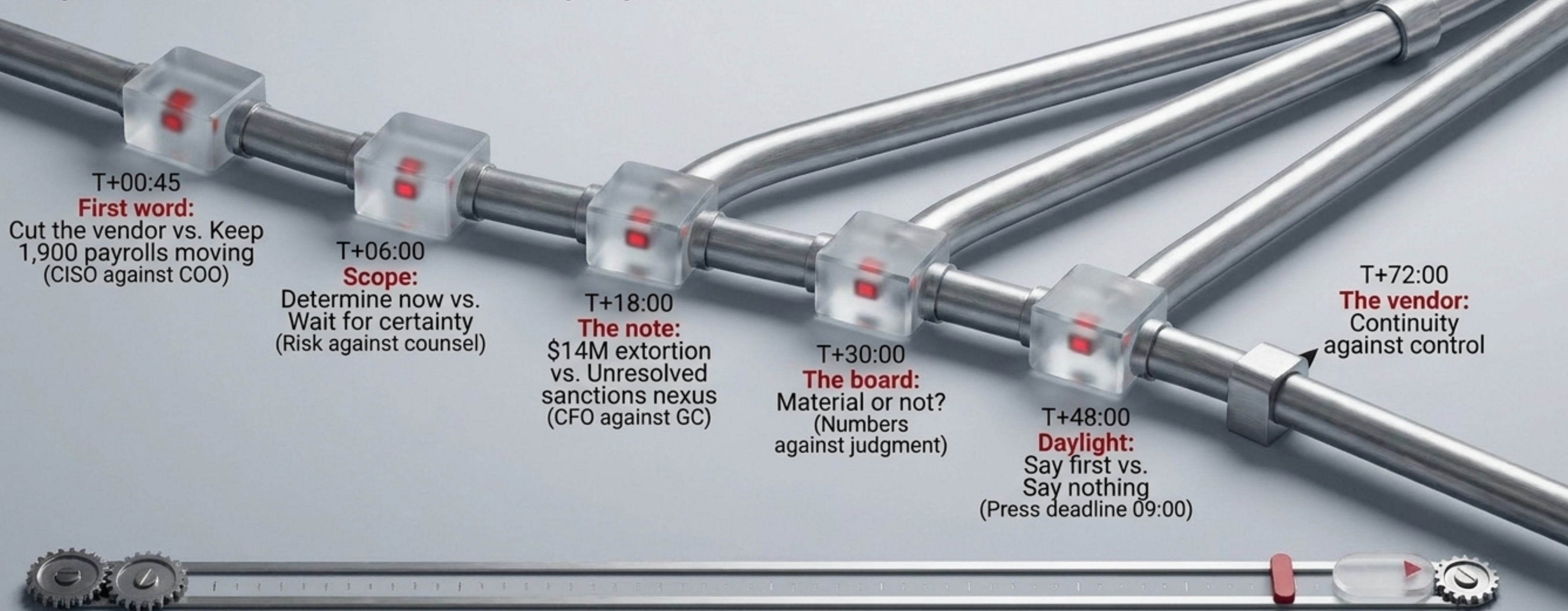
STRIKE

~~The incident resulted from a sophisticated zero-day that could not reasonably have been prevented.~~

(Fails because a SOC ticket was ignored)

Six sequential calls force competing priorities into direct conflict.

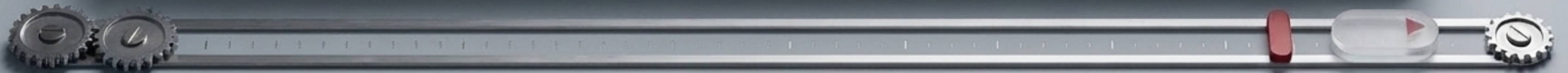
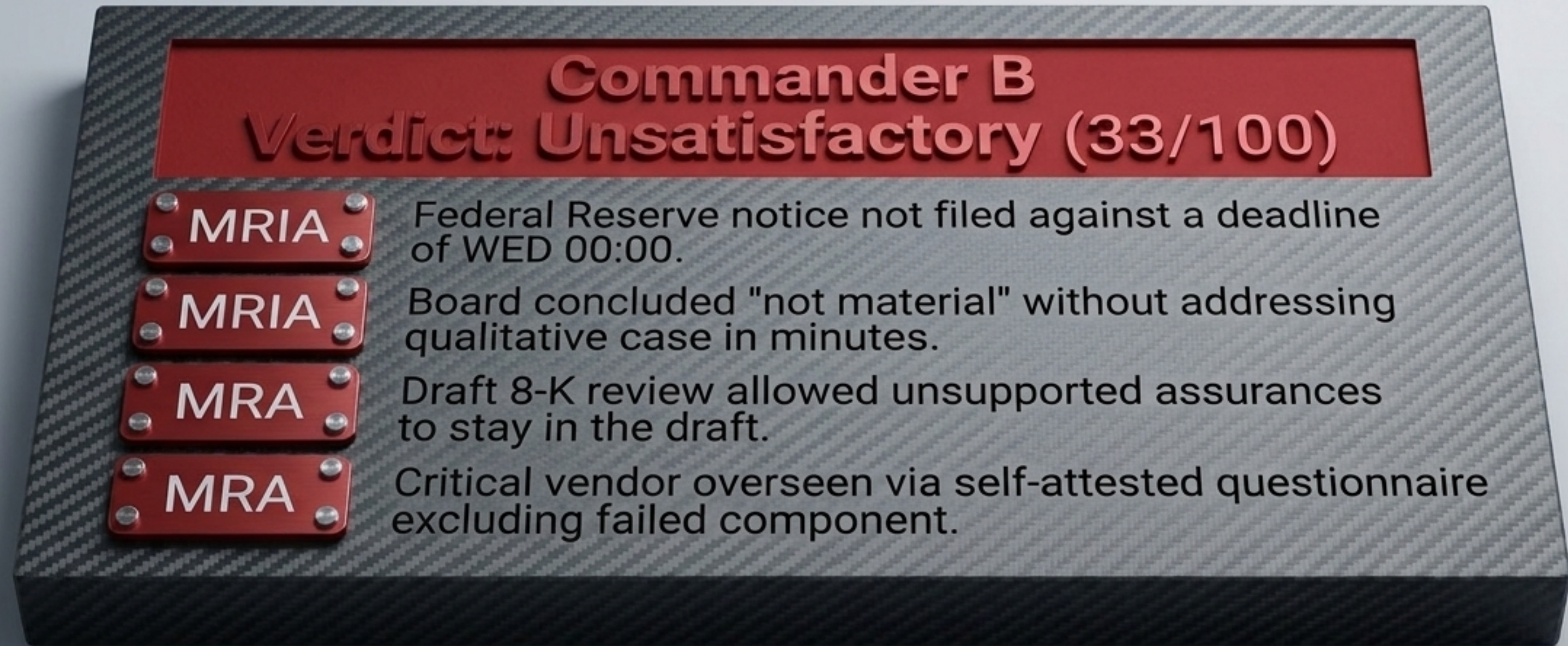
Earlier choices change what lands later. Hold the vendor open, the stolen dataset grows. Pay the ransom, the data surfaces anyway.



T+72:00 · THU 06:00 ET

The after-action stands as an immutable record of your oversight.

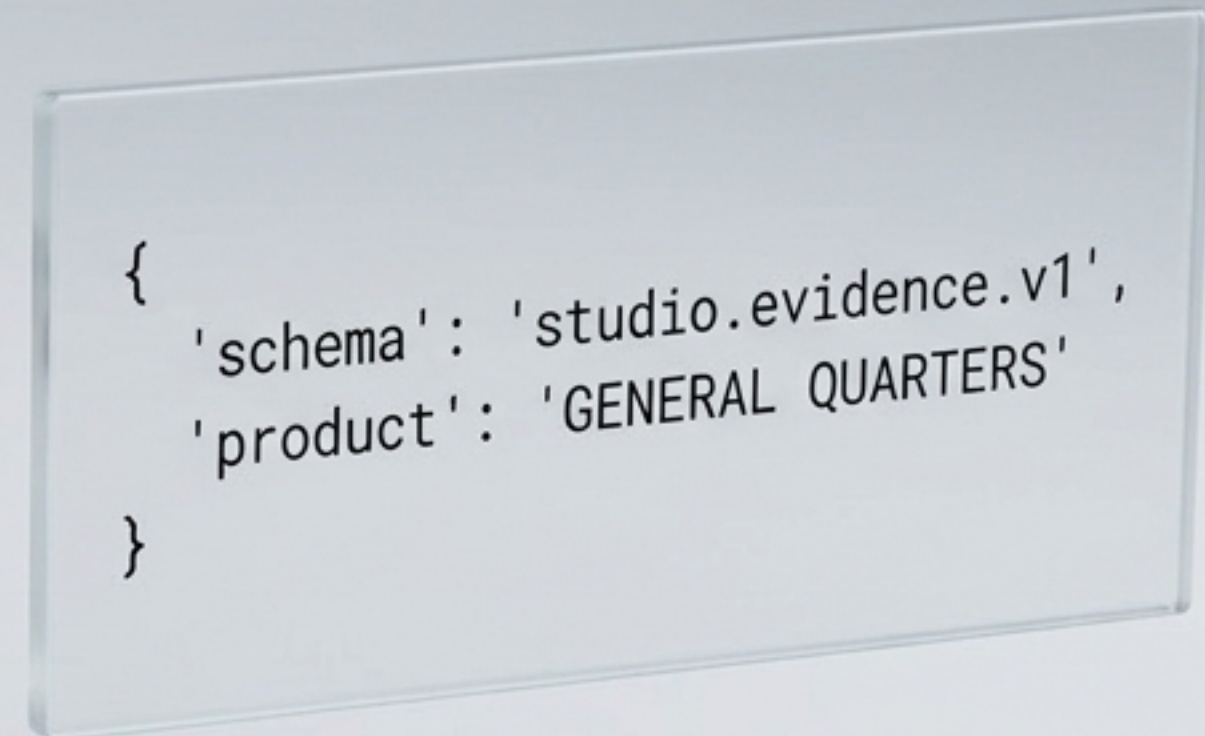
At stand-down, findings are graded exactly as supervisory examiners grade them.



T+84:00 · THU 18:00 ET

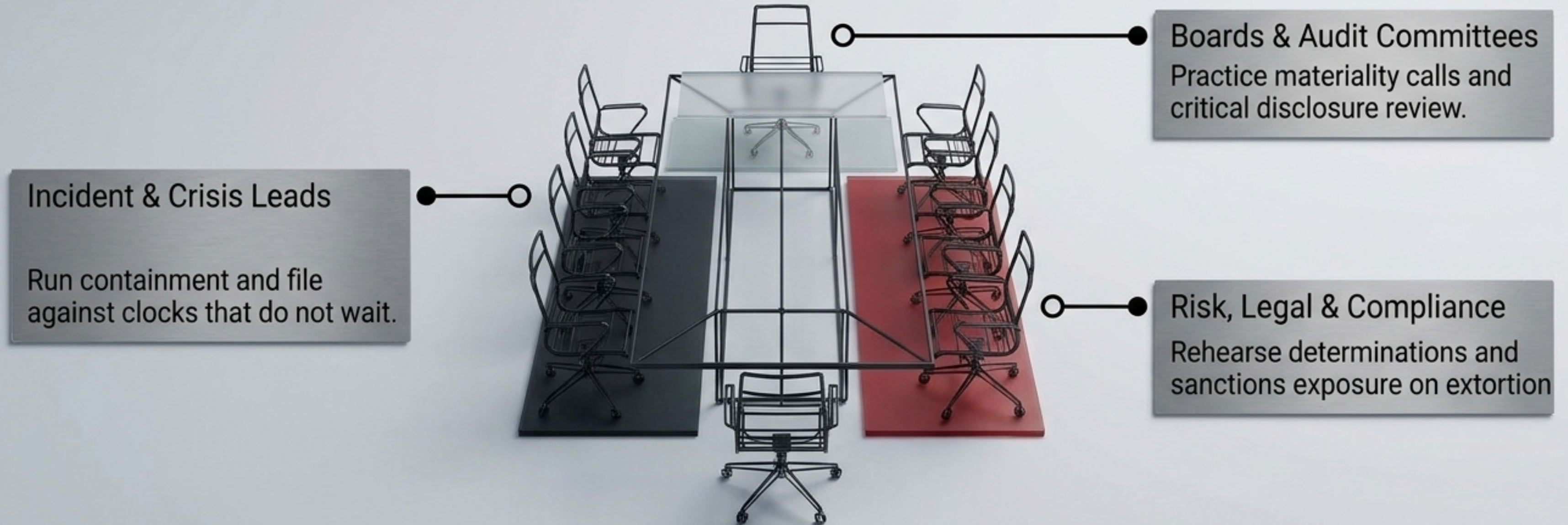
A sealed, cryptographic ledger of every choice made under pressure.

Each entry is SHA-256 chained to the one before it. The final export is a permanent evidence file: `studio.evidence.v1`.



Built strictly for the people whose names go on the filings.

There is no attack to stop and no keyboard to grab. The skills exercised are the ones examined afterwards: timing, judgment, disclosure, and oversight.



T+94:00 · FRI 04:00 ET

Monday, 05:58 ET. A vendor email arrives.
Ninety-six hours. Eighteen exhibits. Four clocks.

The breach is already done. The record of how you handled it is not.

TAKE COMMAND

[About 40 minutes]
- One run, start to
stand-down

[Browser only]
- Nothing installed.
Nothing leaves the page.

[Watch timer]
- Optional 180
seconds per inject

[Evidence pack]
- studio evidence.v1,
hash-chained.

T+96:00 · FRI 06:00 ET