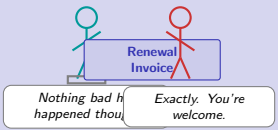
Operational Resilience Business Models

How do vendors get paid to prevent something that, if you're honest, hasn't happened to you yet?

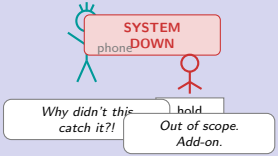
Digital Finance

vs.

The Calm Office



The Crisis Room



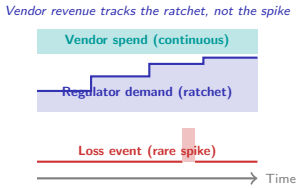
"You sell peace of mind — and the bill comes due whether or not the calamity does."

Why Do Banks Pay a Subscription for an Outage That Has Not Yet Happened?

The Insurance-Adjacent Friction
Operational-resilience vendors solve a friction that the buyer cannot verify until it is too late. The bank wants assurance that, when a core system, a critical third party, or a control plane fails, the recovery is faster than the regulator's tolerance window.

The friction is not the failure itself — it is the absence of provable preparedness. Boards demand evidence. Supervisors demand attestations. Auditors demand traceable runbooks.

- The buyer pays for assurance, not an event.
- The vendor accumulates evidence the buyer cannot generate alone.
- The longer nothing breaks, the harder the renewal conversation.



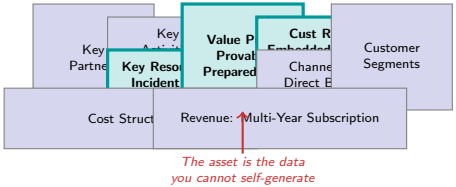
The Value Proposition block of the BMC for resilience vendors is provable assurance. The customer pays the renewal even when nothing has gone wrong.

What Does the Business Model Canvas Look Like for a Resilience-as-a-Service Vendor?

The Resilience-Vendor BMC Pattern
Operational-resilience vendors share a strikingly consistent canvas: their core asset is not technology but *accumulated incident intelligence*. The Key Resources block dominates everything else.

- **Value Proposition:** provable preparedness — evidence the regulator and board will accept.
- **Key Resources:** a catalogue of incident playbooks, threat-actor profiles, and recovery patterns harvested from the combined customer base.
- **Revenue Streams:** multi-year subscription, scoped by number of critical functions covered.
- **Customer Relationships:** embedded technical-account managers; the relationship survives even when no incidents occur.

The pattern: the vendor monetises the *absence* of catastrophe. Renewal logic depends on continued regulator pressure, not on operational failures actually striking the customer.



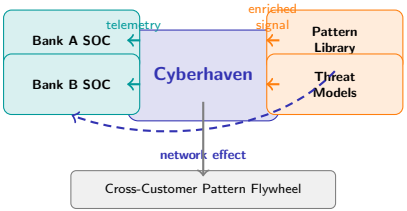
Osterwalder's BMC reveals that resilience vendors monetise an accumulated incident dataset that no individual customer can recreate alone.

How Does Cyberhaven Turn Data Lineage Into a Cross-Customer Platform?

The Cyberhaven Platform Case

Cyberhaven (US-headquartered data-security startup based in Palo Alto, California) tracks every piece of sensitive data as it moves through endpoints, cloud apps, and external sharing channels. The product generates a graph of where information flows — and the more enterprises that participate, the more accurate the cross-customer threat-actor and exfiltration-pattern signal becomes.

- **Multi-sided platform:** customer security teams on one side, anonymised cross-customer pattern feeds on the other.
- **Network effects:** each new tenant adds telemetry that improves detection accuracy for every other tenant.
- **Chicken-and-egg:** early customers received free analyst hours so the data flywheel could spin up before the product had paying scale.
- Result: a platform whose detection quality is itself a competitive moat that grows faster than any single bank's internal team can match.



Two-sided platform economics: customer telemetry on one side, enriched detection on the other. The flywheel makes detection impossible for a single bank to replicate alone.

How Did Resolver Start as a Logbook and End as an Enterprise Risk Suite?

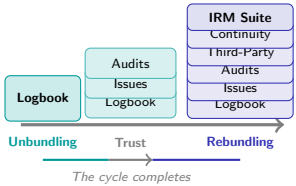
(In business-model language, a *moat* = a competitive advantage that rivals cannot easily copy.)
Unbundling = pulling one service out of a historical bundle and offering it alone; *rebundling* = stacking adjacent services back on once trust is established.
Clayton Christensen (Harvard Business School) argued disruptors start narrow and cheap, earn trust, then expand upward — the *unbundling* phase followed by the *rebundling* phase.
Christensen's Disruption Cycle Applied

Phase One — Unbundling: Resolver (Canadian-headquartered integrated-risk-management vendor based in Toronto) entered as a single proposition: a clean, searchable logbook for risk-event capture that replaced spreadsheets and email threads.

Phase Two — Trust Earned: Compliance teams adopted the logbook for incidents, then asked for issue tracking, audit findings, and policy attestations to live in the same workspace.

Phase Three — Rebundling: Internal audit, third-party risk, business continuity, and integrated risk management modules were stitched onto the original logbook. The single-purpose tool became an integrated risk-and-resilience platform.

The point solution rebundles itself into the same shape as the legacy *GRC* (governance, risk, and compliance) suites it originally disrupted.



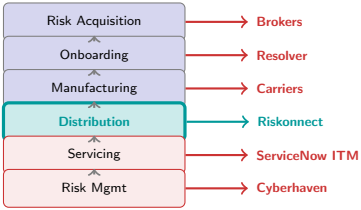
Christensen predicts the rebundling endpoint: the focused entrant ends up looking like the legacy GRC suite it originally disrupted.

Where Exactly in the Insurance-and-Risk Value Chain Does Riskonnect Insert Itself?

The Insurance-Adjacent Resilience Chain
Evans and Wurster argued that information-rich value chains will deconstruct into specialist links. Insurance broking and corporate risk operate that way: every link is contestable.

- **Risk Acquisition** — corporate-broker introductions
- **Onboarding** — exposure-data intake and validation
- **Manufacturing** — claims-and-loss aggregation
- **Distribution** — broker-of-record portals
- **Servicing** — live claims-portal integrations
- **Risk Management** — aggregate-exposure analytics

The critical insight: Riskonnect (US-headquartered integrated-risk platform based in Atlanta, Georgia) attacks the **distribution** link. By owning the *broker-of-record* portal (the software through which a corporate insurance buyer nominates a single broker as the authorised intermediary for all policies and claims) that connects corporate risk teams to insurers and claims handlers, it controls the relationship even though it neither underwrites the policy nor handles the claim. The portal becomes the data choke point through which every incident notification, every renewal quote, and every loss-run report has to pass.



Evans-Wurster value-chain deconstruction: the broker-of-record portal owns the distribution link, which controls the relationship without owning the underwriting risk.

Is the DORA Mandate Behind ServiceNow ITM a Lasting Moat or a Closing Window?

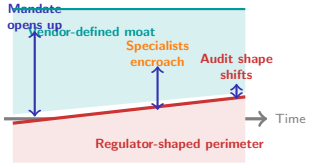
Regulatory arbitrage = a firm earns profit specifically because it faces a lighter rulebook than competitors, not because it is better at the underlying business. The advantage lasts only as long as the rulebook gap does.

The Mandate Arbitrage

DORA (Digital Operational Resilience Act — EU regulation forcing regulated financial firms to prove in writing that their technology estate can absorb and recover from failures) is the canonical *ICT-risk* (information-and-communications-technology risk: outages, cyber intrusions, third-party-provider failures) regime. Every firm in scope becomes a forced buyer of the assurance the rule demands.

- **ServiceNow ITM** (Integrated Threat Management — US-listed workflow platform in Santa Clara, California) pre-existed the mandate; once supervisors specified the evidence shape, it was the path of least audit-resistance.
- **Mandate-driven moats** look unassailable the day they arrive — but the regulator can reshape them with a single consultation.
- Specialists — *chaos engineering* (deliberately breaking parts of a live system to prove that the recovery machinery actually works), runbook-as-code, third-party scoring — chip away at the suite's outer perimeter.

The arbitrage turns negative when the rule shifts to demand evidence the suite was not built to emit.

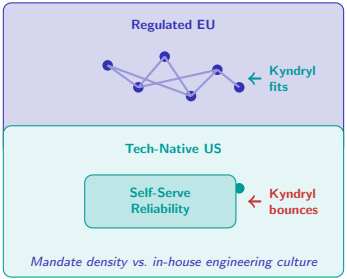


Mandate-driven arbitrage works only as long as the vendor's evidence shape is the one the supervisor still wants tomorrow.

Why Does Kyndryl's Managed-Resilience Model Win in the Regulated EU but Stall in the Tech-Native US?

The Kyndryl Carve-Out Lesson
Kyndryl (US-listed managed-infrastructure operator headquartered in New York, spun out of IBM) inherited a portfolio of regulated EU customers whose mainframes, custody platforms, and cross-border settlement engines could not credibly be moved to a hyperscale public cloud. Managed resilience for those estates — sold on contractual *MTTR* (mean time to recover — the average minutes or hours between the moment a failure begins and the moment service is restored) targets — became a concentrated commercial opportunity.

- In jurisdictions with prescriptive ICT-risk supervision, the managed-services BM has a tailwind: regulator scrutiny rewards a named accountable operator more than a self-serve cloud SLA.
- In tech-native ecosystems where engineering teams expect to own their reliability stack, the same managed model looks like an expensive abdication of control.
- Fundamentally different from a SaaS resilience tool: Kyndryl sells operational accountability, not a software seat.
- Lesson: the BM's value depends on the regulator-and-talent topology of the buyer's market, not on the technology.



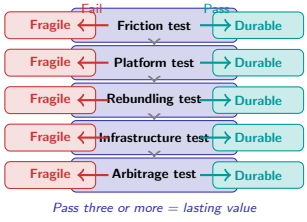
Context-dependency: the managed-resilience BM tracks the regulator-and-talent topology of the buyer's market, not the technology underneath.

Which Five Tests Predict Whether a Resilience Vendor Creates Lasting Value?

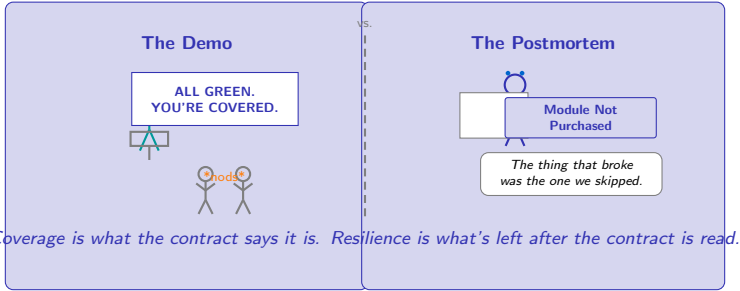
The Five-Test Synthesis (Resilience Lens)

1. **Friction test:** does the buyer renew when nothing has gone wrong? Cyberhaven passes this test when the telemetry graph earns its keep on quiet days.
2. **Platform test:** does cross-customer telemetry compound into detection or recovery quality the buyer cannot reach alone? Cyberhaven again — its data-lineage signal is only as good as the combined tenant base.
3. **Rebundling test:** can the vendor add adjacent modules — audit, third-party risk, continuity — without losing its original wedge? Resolver is the canonical rebundler on this slate.
4. **Infrastructure test:** is the buyer cloud-native and self-serve, or estate-bound and supervised? Kyndryl wins estate-bound EU mandates, stalls in tech-native US clouds.
5. **Arbitrage test:** when the supervisor publishes the next consultation, will the evidence shape the platform emits still match the rule? ServiceNow ITM rides this question; the moat holds only as long as the mandate shape does.

Lasting value here requires passing at least three of the five. The preparedness BM can survive on the friction and infrastructure tests alone in the right jurisdiction — but cannot scale internationally without the platform and arbitrage tests.



The five-test synthesis applied to resilience vendors: friction-and-infrastructure passes survive locally; platform-and-arbitrage passes scale globally.



"Coverage is what the contract says it is. Resilience is what's left after the contract is read."