Post-Class Summary: Operational Resilience Business Models

Key Frameworks

Business Model Canvas Applied to Resilience Vendors

The Business Model Canvas reveals that operational-resilience vendors share a strikingly consistent shape: the Key Resources block dominates everything else. The accumulated incident-and-pattern dataset is the asset no individual buyer can self-generate, and the rest of the canvas — channels, customer relationships, revenue streams — is largely undifferentiated across the category. The Value Proposition block is provable preparedness: the vendor sells assurance the buyer can hand to the regulator and the board. Renewal logic depends on continued supervisory pressure, not on operational failures actually striking the customer.

Platform Economics Applied to Resilience Vendors

Cyberhaven illustrates the canonical multi-sided platform pattern in this space. Customer security teams supply telemetry on one side; an enriched cross-customer pattern feed flows back on the other. Each new tenant improves the signal that every other tenant consumes, and the resulting flywheel makes detection quality structurally impossible for a single bank's internal team to match. The chicken-and-egg problem is resolved by attracting the telemetry side first — typically through design-partner programmes that subsidise the cold-start cost in exchange for outsize roadmap influence.

Unbundling-Rebundling Applied to Resilience Vendors

Resolver is the textbook Christensen arc in this category. Phase one: a single-purpose, focused logbook that replaced spreadsheets and email threads. Phase two: trust accumulated through workflow integration. Phase three: rebundling into an integrated risk-management suite covering issues, audits, third-party risk, and continuity. The endpoint resembles the legacy GRC suite the entrant originally disrupted — the canonical disruption irony. The pattern repeats across the category: Cyberhaven stretches into adjacent insider-risk modules, ServiceNow ITM extends from IT-service workflow into integrated threat management, and Riskonnect layers analytics atop the broker-portal core.

Value Chain Deconstruction Applied to Resilience Vendors

The corporate risk-and-insurance value chain decomposes into Risk Acquisition, Onboarding, Manufacturing, Distribution, Servicing, and Risk Management. Riskonnect attacks the Distribution link by owning the broker-of-record portal that connects corporate risk teams to insurers and claims handlers. The portal is the data choke point through which every incident notification, every renewal quote, and every loss-run report has to pass — which lets Riskonnect control the relationship even though it neither underwrites the policy nor handles the claim. The pattern matches Evans and Wurster's prediction: information-rich value chains deconstruct, and the link that controls the customer interface captures the most value.

Regulatory Arbitrage Applied to Resilience Vendors

ServiceNow Integrated Threat Management illustrates the mandate-driven moat: when supervisors specify an evidence shape the platform can already emit, every regulated firm in scope becomes a forced buyer. The arbitrage is positive when the vendor invests early in regulator-shaped attestations and converts the regulatory gap into a compliance moat before competitors are forced to comply. It turns negative when the next supervisory consultation reshapes the audit surface faster than the platform can adapt. Mandate-driven moats look unassailable on the day they arrive but the regulator can reshape them with a single consultation cycle.

Company Cases Summary

Company	Value Creation Mechanism	Key Framework	What Makes It Different
Cyberhaven	Cross-customer data-lineage telemetry that compounds into superior insider-risk detection	Platform economics, network effects	Detection quality grows faster than any internal team can match
ServiceNow ITM	Integrated threat-and-control catalogue mapped to supervisor-shaped evidence requirements	Regulatory arbitrage as a moat	Pre-existing platform shape matched a mandate timing window
Resolver	Single-purpose risk-event logbook rebundled into integrated risk management	Christensen unbundling-to-rebundling cycle	Wedge product earned the trust that adjacent modules required
Riskonnect	Broker-of-record portal that owns the orchestration layer between buyers, insurers, and claims handlers	Evans-Wurster value-chain deconstruction	Captures the relationship without owning underwriting risk
Kyndryl	Named accountable operator for supervised legacy estates that buyers cannot or will not run in-house	Context-dependent value creation	Premium proposition under prescriptive supervision; redundant elsewhere

The Five-Test Framework (Resilience Lens)

Test 1: Friction test — does the buyer renew when nothing has gone wrong? Cyberhaven passes: forensic lineage evidence remains valuable even in a quiet quarter because the regulator and the board want it on demand.

Test 2: Platform test — does cross-customer telemetry compound into detection or recovery quality the buyer cannot reach alone? Cyberhaven passes; ServiceNow ITM passes through its broader operational data graph; pure managed-services operators struggle.

Test 3: Rebundling test — can the vendor add adjacent modules without losing its original wedge? Resolver passes by stitching IRM modules onto its logbook core without diluting the focused entry point.

Test 4: Infrastructure test — is the buyer estate-bound and supervised, or cloud-native and self-serve? Kyndryl passes the test in jurisdictions with prescriptive ICT-risk supervision; the same product fails the test in tech-native ecosystems.

Test 5: Arbitrage test — when the next supervisory consultation drops, will the evidence shape the platform emits still match what the rule asks for? ServiceNow ITM is on the right side of the test today; that position has to be re-earned every consultation cycle.

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

Connections to Other Topics

The resilience-vendor BM connects directly to three other course topics. First, it shares the cross-customer telemetry flywheel with the cybersecurity vendor BM (CrowdStrike, Coalition, Recorded

Future): both monetise pattern libraries that no individual buyer can self-build. Second, the mandate-driven moat overlaps with the RegTech vendor BM (ComplyAdvantage, Onfido, Quantexa): in both, the supervisor's evidence shape becomes the product specification, and the vendor's commercial position depends on whether the rule still asks for the same shape next year. Third, the broker-of-record orchestration pattern at Riskonnect echoes the embedded-finance BaaS pattern from L02 (Solaris, Marqeta, Synctera): in both, the vendor wins by owning the integration choke point in a value chain even though it neither manufactures nor distributes the underlying product. The structural lesson across all four: in regulated B2B categories, value accrues to whoever owns the data and integration layer through which evidence and entitlements have to pass.

