Pre-Class Discovery Handout: Operational Resilience Business Models

Activity 1: Business Model Canvas Detective — Cyberhaven

Scenario: Look up Cyberhaven — a data-lineage and insider-risk vendor used by enterprise security teams. Investigate how the company actually creates value. Then fill in the Business Model Canvas below by reasoning from publicly available material (their site, customer case studies, analyst reports). Focus on mechanics, not marketing.

Canvas Element	Your Analysis
Value Proposition *What friction does Cyberhaven remove for a security team?*	
Customer Segments *Primary buyers? Secondary stakeholders?*	
Channels *How does it reach buyers without a sales-led legacy footprint?*	
Revenue Streams *Type of income (no figures)?*	
Key Resources *Which resource is hardest for a buyer to self-build?*	

Q1: What is the single most important friction Cyberhaven removes for a regulated buyer?

Q2: How does the vendor reach new enterprise buyers without the broker network that legacy GRC suites rely on?

Q3: If Cyberhaven disappeared tomorrow, what would buyers lose that an open-source toolkit could not replace?

Activity 2: Unbundling Map — Resilience Vendors vs. the Legacy GRC Suite

Scenario: Legacy governance, risk and compliance suites bundle many resilience services into one heavy installation. A new generation of vendors attacks individual services. Match each vendor below to the resilience service it has unbundled, then answer the questions.

Vendor		Resilience Service Unbundled
Cyberhaven	____	Insider-data-flow detection
ServiceNow ITM	____	Integrated threat-and-control management
Resolver	____	Risk-event logging and IRM workflow
Riskonnect	____	Insurance-broker data orchestration
Kyndryl	____	Managed mainframe-and-platform resilience

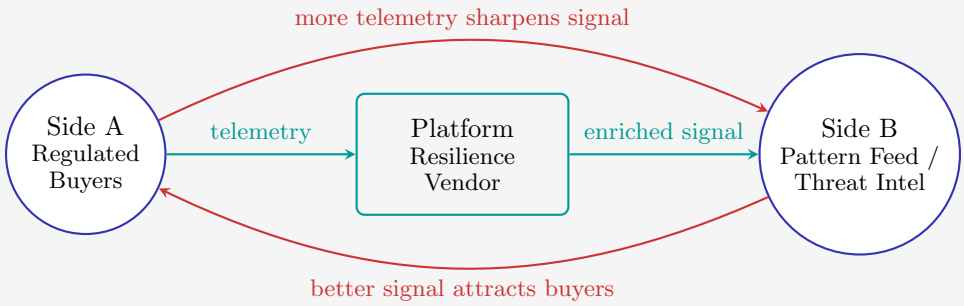
Q1: For each pair, describe in one sentence what friction the vendor removes for a regulated buyer.

Q2: Which of these vendors has started adding modules beyond its original wedge product? Name the adjacent module(s) and the original wedge.

Q3: Why might a vendor that starts with a single wedge eventually want to offer many adjacent modules to the same customer?

Activity 3: The Platform Puzzle — Cross-Customer Telemetry

Scenario: An operational-resilience vendor connects two sides of a market: regulated buyers (security and risk teams) on one side and a cross-customer pattern feed on the other. Neither side is fully useful without the other.



Q1: Why does a platform with more telemetry attract more buyers (and vice versa)?

Q2: The "cold-start problem": which side should the platform attract first, and why does the answer depend on whether the buyer can audit the signal quality before signing?

Q3: Once the platform reaches critical mass, why is it hard for a single bank's internal team to replicate the detection quality?

Solutions

Activity 1: Business Model Canvas Detective — Cyberhaven

A1: Model answer for Cyberhaven: The most important friction removed is the inability of legacy data-loss-prevention tools to reconstruct the lineage of sensitive content as it flows across endpoints, cloud apps, and external sharing channels. Cyberhaven captures the full provenance graph, which lets a security team explain how an exfiltration happened — not just that a policy was triggered.

A2: Cyberhaven reaches buyers through a combination of analyst-led category creation, customer-reference programmes, and integration partnerships with existing endpoint and identity vendors. The product itself acts as a referral channel: when a security architect at one bank evaluates the platform, peers in adjacent institutions are typically pulled into pilots through professional networks.

A3: Buyers would lose the cross-customer pattern library that no single institution can replicate. They would also lose the integrated lineage graph that connects an insider event to the chain of upstream user actions and downstream data destinations — a forensic asset that turns regulator post-mortems from speculation into a documented timeline.

Canvas elements (Cyberhaven):

- **Value Proposition:** Provable data-lineage and insider-risk evidence that withstands regulator scrutiny.
- **Customer Segments:** Primary — enterprise security teams in regulated industries; secondary — internal-audit and privacy functions that consume the same evidence.
- **Channels:** Direct enterprise sales, analyst-led category education, integration co-sell with adjacent endpoint and identity vendors.
- **Revenue Streams:** Multi-year subscription priced by data-source coverage and protected-user count.
- **Key Resources:** The cross-customer telemetry library and the lineage graph engine that turns it into searchable evidence.

Activity 2: Unbundling Map

A1: Cyberhaven → Insider-data-flow detection (removes the inability to reconstruct lineage when sensitive content moves through endpoints and clouds). ServiceNow ITM → Integrated threat-and-control management (removes the spreadsheet-based mapping between threat intelligence and control inventories). Resolver → Risk-event logging and IRM workflow (removes email-thread coordination of incident capture and follow-up). Riskonnect → Insurance-broker data orchestration (removes manual exposure-data movement between corporate risk teams and brokers). Kyndryl → Managed mainframe-and-platform resilience (removes the burden of operating supervised legacy estates with internal staff).

A2: Resolver expanded its initial logbook into integrated risk management (issues, audits, third-party risk, continuity). ServiceNow expanded its IT-service workflow platform into integrated threat management. Both illustrate **rebundling**: starting narrow with one wedge, then cross-selling adjacent modules once trust and integration footprint are established.

A3: A single-wedge vendor faces high enterprise-acquisition costs. Once a buyer trusts the platform and integrates it into operational workflow, the marginal cost of consuming an adjacent module is much lower than the cost of evaluating, procuring and integrating a separate vendor. Rebundling raises lifetime value, deepens switching costs, and pre-empts competing wedge entrants from establishing their own toehold.

Activity 3: The Platform Puzzle — Cross-Customer Telemetry

A1: This is a **cross-side network effect**: more buyer telemetry sharpens the pattern feed, which makes the platform more attractive to additional buyers. Simultaneously, more buyers expand the pattern feed's coverage of attacker techniques, which improves detection for everyone. Each side's growth reinforces the other.

A2: The **telemetry side** usually has to be attracted first — by free pilot deployments, design-partner programmes, or analyst-attended bake-offs. The reason: a buyer can audit the signal quality only after the platform has accumulated enough telemetry to demonstrate it, so early customers carry the cold-start cost in exchange for outsize influence over the product roadmap.

A3: Once critical mass is reached, the platform's pattern library reflects attacker behaviour observed across many institutions. A single bank's internal team can only see its own traffic, which is a small slice of the global pattern. The incumbent's network signal grows with every new tenant, while the internal alternative remains capped by the institution's own visibility — a structural moat that widens monotonically with platform scale.

