In-Class Exercise: Cybersecurity Business Models

Exercise 1: Structured Debate — "Is Coalition an Insurer or a Cybersecurity Vendor?"

Format: Split into two teams. Each team prepares arguments for its assigned position, then presents. After both sides speak, the class votes — but first, read the debrief questions.

Team A — "Coalition Is an Insurer"

Anchoring evidence: Coalition holds insurance carrier or surplus-lines licences in the jurisdictions where it issues policies, files actuarial submissions with regulators, maintains reserves against claim liabilities, and reinsures its book like any other carrier.

	Team A: Coalition Is an Insurer
Argument I	
Argument II	
Argument III	
Concession	*Strongest argument AGAINST your position:*
Closing	*How you address the concession:*

Team B — "Coalition Is a Cybersecurity Vendor"

Anchoring evidence: Coalition was founded by security engineers, runs continuous attack-surface scanning on every policyholder, intervenes operationally before claims crystallise, releases security tooling for free to prospects, and generates a meaningful share of its activity from defensive services rather than pure indemnity.

	Team B: Coalition Is a Cybersecurity Vendor
Argument I	
Argument II	
Argument III	
Concession	*Strongest argument AGAINST your position:*
Closing	*How you address the concession:*

Debrief Questions

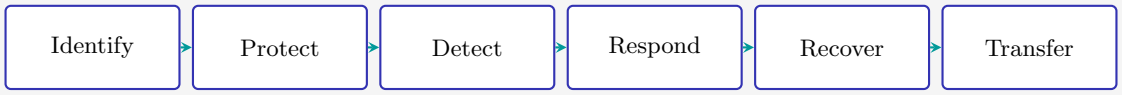
Q1: Does the answer — insurer or cybersecurity vendor — matter for how regulators should supervise Coalition? Why or why not?

Q2: Could the answer genuinely be "both"? If so, what does that imply about the usefulness of traditional industry categories?

Q3: Name another company (in any sector) that blurs established category boundaries in a similar way. What tensions does that blurring create for regulators, investors, and competitors?

Exercise 2: Defence Lifecycle Mapping

Scenario: The cyber-defence value chain can be broken into six lifecycle phases. Vendors specialise in individual phases. Your task: for each phase, identify a vendor (ideally from the lecture's slate), describe the friction it removes, and predict the long-term outcome.



Lifecycle Phase	Vendor Attacking It	Friction Removed	Replaces or Improves?	Bank Loses or Adapts?
Identify				
Protect				
Detect				
Respond				
Recover				
Transfer				

Synthesis Question

Q1: Which phase of the defence lifecycle is *most vulnerable* to vendor capture? Which is *most resistant*? Defend your reasoning with reference to switching costs, telemetry advantages, and regulatory or insurance constraints.

Facilitator Solutions

Sample answers for instructor reference. These are illustrative; student reasoning may diverge and still be valid.

Exercise 1: Debate Sample Answers

Team A (Coalition Is an Insurer) — sample arguments

Argument I. Coalition holds insurance carrier or surplus-lines licences in the jurisdictions where it operates, which legally obligates it to file actuarial submissions, hold reserves against claims, and submit to insurance-regulator supervision. A pure cybersecurity vendor has no such obligations; the regulatory perimeter Coalition sits inside is the insurance perimeter.

Argument II. Coalition's defining revenue logic is the underwriting margin — premiums collected minus claims paid minus expenses — which is the universal financial signature of an insurance carrier. The defensive-services activity is funded out of expected loss-cost reduction, not as a stand-alone product line. This is a cost-of-claims story, not a product-revenue story.

Argument III. Because Coalition issues policies, those policies create insurance-contract liabilities that fall under specific accounting and supervisory regimes. Reinsurance treaties, claim reserves, and capital-adequacy considerations all apply — none of which apply to a pure cybersecurity vendor. The presence of those balance-sheet obligations places Coalition firmly inside the insurance category.

Concession. The strongest argument against Team A is that Coalition's customer-acquisition model, telemetry-driven underwriting, and active intervention before claims all resemble a cybersecurity vendor far more than a traditional carrier.

Closing. Regulatory form follows economic substance: because Coalition issues binding insurance contracts and bears the resulting underwriting and reserve risks, the insurance classification is correct regardless of how it acquires its data or intervenes operationally.

Team B (Coalition Is a Cybersecurity Vendor) — sample arguments

Argument I. Coalition's competitive edge derives from continuous external scanning of policyholder attack surfaces — a capability that pure carriers cannot replicate without acquiring or building a security firm. The dominant value-creation mechanism is the security telemetry pipeline; the policy is just the contractual wrapper that converts that telemetry into willingness-to-pay.

Argument II. Coalition iterates on a software release cycle — vulnerability scanning rules, alerting workflows, breach-coach playbooks — at a cadence no traditional carrier operates at. The defensive-intervention pattern (warn the policyholder, push a patch, contact the breach-response team early) is operational cybersecurity, not actuarial insurance.

Argument III. Coalition has historically attracted technology-company valuation logic and InsurTech narrative framing precisely because the equity story is data and software, not premium float. The capital market treats it as a cybersecurity-driven InsurTech because its dominant moat is the data network and the active-defence capability, not deep underwriting capital.

Concession. The strongest argument against Team B is that issuing binding insurance contracts creates genuine supervisory and balance-sheet obligations that pure cybersecurity vendors never face.

Closing. Regulatory classification is a lagging indicator: the economic substance that drives most of Coalition's growth and competitive advantage is cybersecurity-platform logic, even if a slice of its revenue uses an insurance licence as the contractual wrapper.

Debrief Q1 — Regulatory supervision

Whether the regulator should treat Coalition primarily as an insurer or as a cybersecurity vendor depends on which risks the firm creates, not on which label it prefers. A firm that issues binding policies can fail to pay claims and trigger consumer-protection harm; a firm that operates active-defence tooling on client networks can cause operational disruption or mishandle sensitive telemetry. If Coalition does both, its supervisory regime should arguably draw from both perimeters — prudential rules from insurance plus operational and data-protection rules from cybersecurity. The answer matters because the supervisory toolkit (capital adequacy versus incident-reporting obligations versus breach-notification rules) is calibrated quite differently for each perimeter, and applying one regime alone would leave the other set of risks unaddressed.

Debrief Q2 — "Both" as an answer

The answer genuinely can be "both": Coalition operates a regulated insurance entity inside a cybersecurity-platform organisational structure. That duality reveals that traditional industry categories, inherited from a world where underwriting and operational risk-mitigation were performed by entirely separate firms, cannot cleanly capture a firm that bundles those functions across a single offering. If "both" is the right answer, it implies that regulators, investors and analysts need new functional classifications — focused on what risks an entity creates and what economic role it actually plays — rather than relying on the institutional label on the licence.

Debrief Q3 — Cross-sector blurring example

Tesla blurs the boundary between automotive manufacturer and technology company. It sells vehicles but derives a significant share of its market capitalisation from its proprietary software stack, over-the-air update capability, autonomous-driving data assets, and energy-storage platform. Traditional automakers are valued on capital-intensive manufacturing logic; Tesla has at times attracted software-like growth multiples. The tension this creates is acute for regulators (vehicle-safety rules versus software-update liability), for investors (which comparable set should price the equity), and for competitors (do you benchmark against legacy automakers or against software platforms?). The parallel to Coalition is direct: the blurring is not a marketing claim but a structural consequence of embedding software-platform economics inside an industry that historically had a different operating model.

Exercise 2: Defence Lifecycle Mapping Sample Answers

Lifecycle Phase	Vendor Attacking It	Friction Removed	Replaces or Improves?	Bank Loses or Adapts?
Identify	Onapsis (ERP attack-surface mapping)	Blind spot in mission-critical ERP layer that general-purpose tools miss	Improves	Bank Adapts
Protect	CrowdStrike (endpoint protection)	Inability of in-house teams to maintain detection content at attacker velocity	Replaces	Bank Adapts
Detect	BlueVoyant (managed detect and respond)	Staffing impossibility of running a continuous in-house SOC at mid-bank scale	Replaces	Bank Adapts
Respond	Specialist incident-response retainers	Lead-time problem of finding an IR firm only after an attack starts	Improves	Bank Adapts
Recover	Backup and restoration vendors	Cost and complexity of maintaining clean recovery copies for critical systems	Improves	Bank Adapts
Transfer	Coalition (active cyber-insurance)	Pricing opacity of traditional cyber-policies that lacked telemetry-grade data	Improves	Bank Adapts

Synthesis Question Sample Answer

The most vulnerable phase is Detect. Detection runs continuously, demands specialist staffing that mid-sized banks cannot afford to keep current, and benefits enormously from cross-client telemetry pooling that no single bank could replicate alone. Switching costs at the Detect layer are mostly content-tuning costs, which a competing managed-detection vendor can replicate with onboarding effort. Network effects on the vendor side compound the advantage: each new client adds telemetry that improves detection for every other client. The most resistant phase is Recover. Recovery depends on deeply integrated backup architectures, custodial control over clean copies of mission-critical data, and tightly governed change-management processes that touch core banking ledgers. Vendors can supply backup tooling, but the operational responsibility, the audit trail, and the regulatory liability all remain with the bank. Switching costs at the Recover layer are extreme because every change risks corrupting the clean-recovery posture itself.