Post-Class Summary: Cybersecurity Business Models

Key Frameworks

Business Model Canvas for Cyber-Defence Vendors

The Business Model Canvas decomposes any venture into nine interlocking elements — value proposition, customer segments, channels, revenue streams, key resources, key activities, key partners, cost structure, and customer relationships. For cyber-defence vendors, the canvas reveals a recurring pattern: the value proposition almost always centres on converting a probabilistic tail-risk loss into a predictable subscription cost, while the customer segment is reliably the CISO or enterprise risk team rather than the consumer end-user. Channels run through procurement, analyst-firm rankings and channel partners rather than through retail or app-store distribution.

Platform Economics in Cyber-Defence

Many cyber vendors operate as multi-sided platforms connecting two or more participant groups — endpoints producing telemetry on one side, hunt analysts producing detection content on the other; or policyholders generating scanning data on one side, underwriters consuming it on the other. These platforms exhibit cross-side network effects: each additional participant on one side makes the platform more valuable to the other. The central strategic challenge is the cold-start problem — attracting the first side when the other side is empty — typically solved by operating an in-house intel team or by seeding open-source feeds before any client arrives.

Unbundling–Rebundling Cycle in Cybersecurity

Christensen's disruption framework explains how cyber vendors enter: they unbundle a single capability — threat intelligence, endpoint detection, ERP scanning — from the legacy managed-services bundle and deliver it better, faster, or with richer telemetry. Over time, successful unbundlers rebundle — adding adjacent lifecycle phases once trust is established — because customer-acquisition costs are high and the renewal economics of subscription bundles are far more attractive than single-product contracts. The cycle repeats: today's rebundled cyber-platform becomes tomorrow's incumbent, ripe for a new wave of unbundling by specialist successors.

Defence-Lifecycle Value-Chain Deconstruction

Evans and Wurster argued that information-rich value chains are vulnerable to deconstruction when digital alternatives reduce the cost of coordinating across firm boundaries. In cyber-defence, the chain (Identify, Protect, Detect, Respond, Recover, Transfer) deconstructs into specialist vendors at each link. Banks defend the links where regulation, custodial control or audit-trail liability creates natural moats — typically the Recover link — and outsource the rest to vendors who can amortise the fixed cost of running the capability across many clients.

Regulatory and Underwriting Arbitrage

Some cyber vendors gain an early advantage by operating in adjacencies where regulation moves more slowly than the threat landscape. Coalition exemplifies this: cyber-policy underwriting was historically priced by traditional carriers without telemetry-grade data, leaving room for an entrant that could combine continuous scanning with insurance issuance. This arbitrage is inherently temporary — carriers eventually adopt similar telemetry, and standardised cyber-policy forms emerge. The strategic question is whether the entrant can convert the head start into a durable data-and-distribution moat before the regulatory and competitive perimeters catch up.

Company Cases Summary

Company	Value Creation Mechanism	Key Framework	What Makes It Different
CrowdStrike	Cross-client endpoint telemetry pool feeding a global detection graph	Platform Economics	The detection graph improves with every new client; a network advantage no single bank can replicate
Recorded Future	Curated threat-intelligence feed delivered as API, then rebundled into adjacent intel products	Unbundling–Rebundling	Started with a single-feed wedge, rebundled into a portfolio that resembles a managed-intel practice
BlueVoyant	Managed detect-and-respond layered onto third-party tooling the client already paid for	Value Chain Deconstruction	Owns the longest continuous lifecycle band (Detect plus Respond), capturing the deepest renewal revenue
Coalition	Active cyber-insurance combining underwriting with continuous defensive scanning	Regulatory Arbitrage → Compliance Moat	Straddles two perimeters — insurance carrier and security vendor — in a way neither incumbent could easily copy
Onapsis	Deep specialism in protecting mission-critical ERP estates that general tools miss	Depth-versus-Breadth Positioning	Wins where the protected asset is concentrated and replacement-resistant; struggles where assets are fragmented

The Five-Test Framework Applied to Cyber-Defence

Use these five tests to evaluate any cyber-defence vendor's strategic position:

1. **Friction test.** Identify the single largest friction the vendor removes from the SOC's daily work or from the CISO's board narrative.
   Application: CrowdStrike removes the impossibility of pattern-matching novel intrusions across a sprawling endpoint estate without a shared telemetry pool.

2. **Platform test.** Determine whether the vendor connects two or more sides of a market and benefits from cross-side network effects.
   Application: CrowdStrike connects endpoints (telemetry producers) and hunt analysts (content producers); each new client of either side raises value for the other.

3. **Rebundling test.** Assess whether the vendor has begun — or is likely to begin — adding adjacent lifecycle phases beyond its original wedge product.
   Application: Recorded Future entered with a single intel feed, then rebundled brand-monitoring, vulnerability triage, third-party scoring and a managed-analyst practice; a textbook rebundling arc.

4. **Depth-versus-breadth test.** Ask whether the vendor wins by going deep in a chokepoint asset or by going broad across many rails.
   Application: Onapsis wins by going deep in ERP — a concentrated, replacement-resistant asset — but cannot replicate that wedge in cloud-native fragmented estates.

5. **Arbitrage test.** Evaluate whether the vendor's edge stems from a regulatory or informational gap and, if so, whether that gap is widening or closing.
   Application: Coalition's edge over traditional cyber-carriers depends on telemetry that carriers are now adopting; the test asks whether Coalition can convert its head start into a permanent data-and-distribution moat before standardised forms close the gap.

Connections to Other Topics

The frameworks above connect directly to several other course themes. The operational-resilience material in the same lesson examines how regulators (DORA in particular) increasingly require continuous capability rather than point-in-time controls — the same demand profile that drives cyber-vendor subscription economics. The RegTech and compliance lecture in Lesson Four shares the B2B-vendor template (procurement-led customer segments, evidence-inventory key resources, subscription-plus-retainer revenue mix) and is the closest cross-lesson neighbour. Finally, the climate-risk lecture in Lesson Eight illustrates a contrasting case: where loss horizons are longer and counterparties are slower to demand telemetry, the underwriting-arbitrage edge that Coalition exploits in cyber is far harder to reproduce.

