# Data-Driven Risk Modeling and Profit Optimization in Omni-Channel E-Commerce Supply Chains Under Demand Uncertainty and Information Asymmetry

Wei Jiaming[1], Marcus T. Okonkwo[2,*]

[1]Department of Business Analytics, Fudan University, Shanghai 200433, China

[2]Department of Supply Chain Management, University of Lagos, Lagos 101017, Nigeria

*Email: m.okonkwo@unilag.edu.ng (Corresponding Author)

## Abstract

The rapid growth of e-commerce and the proliferation of digital channels have fundamentally transformed supply chain structures, requiring firms to simultaneously manage demand uncertainty, supply disruptions, information asymmetry, and cybersecurity threats. This study develops a comprehensive data-driven risk modeling framework for an omni-channel e-commerce supply chain serving both business-to-consumer (B2C) and business-to-business (B2B) market segments under price-dependent stochastic demand. Five analytical models are constructed that progressively incorporate demand risk, supply-side uncertainty, information asymmetry between the e-commerce platform and its logistics partner, and cybersecurity risk with corresponding mitigation investment strategies. Each model is solved using classical optimization techniques, and global optimality is validated analytically. Numerical experiments using realistic e-commerce parameter values quantify the financial impact of each risk dimension. Results indicate that unmitigated risks and information asymmetry impose a cumulative profit loss of 7.8%, of which 6.2% is recoverable through structured mitigation strategies. Sensitivity analysis reveals that demand risk is the most damaging single factor, while cybersecurity investment yields the highest marginal return among mitigation options. These findings offer both theoretical contributions to supply chain risk analytics and practical guidance for e-commerce platform managers.

**Keywords:** Omni-channel supply chain; Risk management; Data-driven analytics; Information asymmetry; Demand uncertainty; B2B and B2C dual channel; Game theory; Profit optimization

**Article History:**

Received: September 12, 2025

Revised: December 14, 2025

Accepted: March 20, 2026

Available Online: March 30, 2026

# Data-Driven Risk Modeling and Profit Optimization in Omni-Channel E-Commerce Supply Chains Under Demand Uncertainty and Information Asymmetry

## 1. Introduction

The global e-commerce market surpassed USD 5.8 trillion in revenues during 2023 and is projected to reach USD 8.1 trillion by 2027, driven by accelerating digital adoption across consumer and industrial markets. Within this landscape, omni-channel distribution strategies—which seamlessly integrate online platforms, mobile applications, and physical retail touchpoints—have become essential competitive differentiators for firms seeking to capture both B2C and B2B market segments [Kleindorfer & Saad, 2005]. However, this complexity introduces multi-dimensional risks that strain traditional supply chain management frameworks. Price-sensitive, volatile demand patterns across multiple channels create over- and under-capacity costs. Supply disruptions originating from geopolitical events, logistics bottlenecks, or supplier failures propagate through tightly coupled supply networks. The digitalization of commerce operations simultaneously opens new attack surfaces for cybersecurity threats, whose financial consequences extend far beyond direct system restoration costs to include reputational damage, regulatory penalties, and lost customer trust. Finally, the inherent information asymmetry between platform operators, logistics partners, and merchandise suppliers creates strategic distortions in pricing and capacity decisions that reduce overall supply chain efficiency [Corbett et al., 2004].

Despite the growing importance of these intersecting risk factors, academic literature has addressed them largely in isolation. Supply chain risk management research has historically focused on operational resilience and disruption modeling without integrating the information-theoretic constraints imposed by asymmetric knowledge structures [Tang, 2006]. Conversely, mechanism design and game-theoretic supply chain studies examine information asymmetry and strategic interactions rigorously but typically abstract away from probabilistic demand and multi-channel distribution [Cachon & Lariviere, 2005]. Studies addressing e-commerce and omni-channel distribution generally emphasize customer behavior modeling and marketing optimization while treating supply chain operations as a secondary concern [Huang & Swaminathan, 2009]. The emergence of big data analytics offers new opportunities to bridge these gaps by enabling real-time risk assessment, demand forecasting, and dynamic pricing across channels, yet analytical frameworks that embed data-driven insights into formal supply chain optimization models remain scarce [Choi et al., 2018].

This paper addresses the identified gap by developing a unified analytical framework that simultaneously models demand risk, supply-side uncertainty, information asymmetry, and cybersecurity risk within an omni-channel e-commerce supply chain serving B2C and B2B markets. The supply chain comprises an e-commerce platform operator (EPO) that procures fulfillment capacity from a third-party logistics provider (3PL) and distributes differentiated services to both market segments at independently optimized prices. The EPO faces price-dependent stochastic demand in both channels and must determine capacity order quantities and pricing strategies that maximize expected profits. The 3PL, possessing superior knowledge of logistics network conditions and costs, charges the EPO a per-unit capacity fee. This information disparity creates a strategic environment where the EPO and 3PL make decisions based on privately held information, leading to the information asymmetry structure central to this study.

The study constructs five progressive analytical scenarios. Scenario 1 establishes a benchmark with no information asymmetry and no risk, yielding centralized optimal profits. Scenario 2 introduces information asymmetry between the EPO and 3PL, quantifying the efficiency loss from strategic non-disclosure. Scenario 3 incorporates demand risk through explicit overcapacity and undercapacity cost structures. Scenario 4 extends the model to include supply-side risk affecting the 3PL's fulfillment reliability. Scenario 5 integrates cybersecurity risk with endogenous investment strategies and applies Stackelberg game theory to model the decentralized decision-making between the EPO and 3PL under full risk exposure. Throughout, analytical solutions are derived, global optimality conditions are verified, and numerical experiments are used to quantify the financial implications of each risk dimension and the effectiveness of proposed mitigation strategies.

The primary contributions of this study are as follows. First, a novel unified analytical framework integrating demand risk, supply risk, and cybersecurity risk into an omni-channel B2C–B2B supply chain optimization model is developed, advancing the literature by treating multiple risk types within a single coherent model. Second, the framework explicitly incorporates information asymmetry between the EPO and 3PL, capturing how strategic private information affects pricing and capacity decisions differently from the centralized benchmark. Third, Stackelberg game theory is applied to the cybersecurity risk scenario to model competitive decision-making under decentralized information, providing a game-theoretically grounded analysis of risk mitigation investment. Fourth, a comprehensive data-driven sensitivity analysis reveals the relative impact of each risk parameter and identifies optimal mitigation investment thresholds, offering actionable managerial guidance. Fifth, the study demonstrates that structured risk mitigation strategies recover 6.2% of total profit that would otherwise be lost to risk and information asymmetry, providing empirical motivation for systematic risk management in e-commerce supply chains.

The remainder of this article is organized as follows. Section 2 reviews the relevant literature on supply chain risk management, omni-channel distribution, and information asymmetry. Section 3 defines the problem structure, notation, and modeling assumptions. Section 4 presents the five analytical models and their solutions with optimality conditions. Section 5 describes the Stackelberg game framework applied in Scenario 5. Section 6 reports numerical experiments and a comparative analysis across scenarios. Section 7 presents sensitivity analysis and managerial implications. Section 8 concludes with a summary of findings and directions for future research.

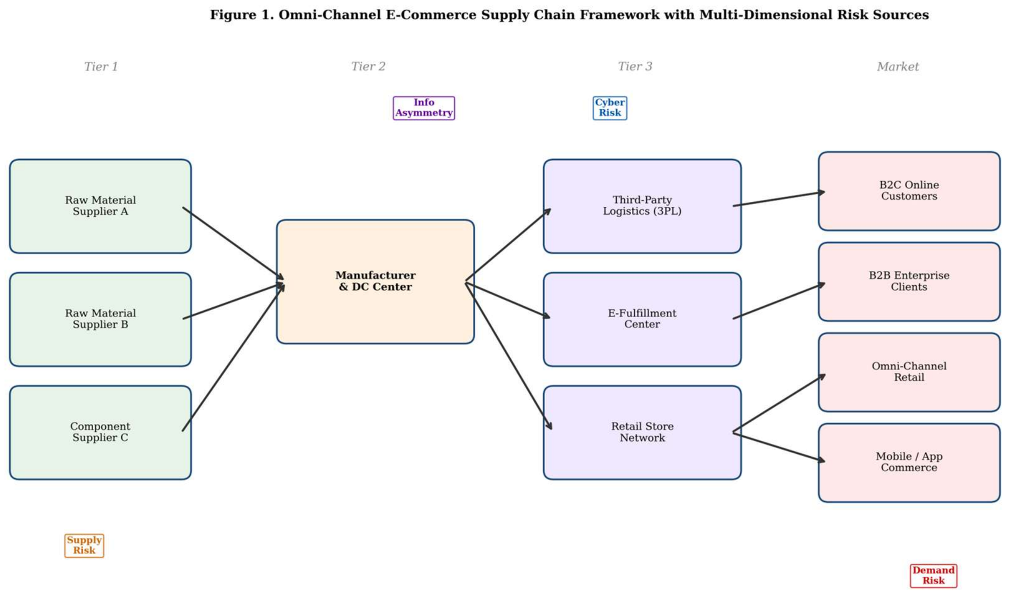


*Figure 1. Conceptual framework of the omni-channel e-commerce supply chain with multi-dimensional risk sources, illustrating the interactions among suppliers, manufacturers, logistics providers, and market segments.*

## 2. Literature Review

### *2.1 Supply Chain Risk Management*

Supply chain risk management (SCRM) has grown into a substantial research domain since the foundational work of [Kleindorfer & Saad, 2005], who classified supply chain risks into disruptions and supply-demand mismatches and proposed systematic frameworks for identification, mitigation, and contingency planning. Tang (2006) provided a comprehensive taxonomy of robust supply chain strategies, categorizing responses to supply risk, demand risk, and product risk, and identified postponement, strategic stock, and flexible sourcing as primary mitigation mechanisms. Building on these foundations, subsequent research has examined how different organizational structures and contractual arrangements influence risk sharing along the supply chain.

In the context of contract design and risk allocation, Cachon and Lariviere (2005) demonstrated that revenue-sharing contracts can coordinate decentralized supply chains and align incentives between manufacturers and retailers when demand is stochastic. Their work showed that the revenue-sharing fraction determines the distribution of supply chain profit and that optimal contracts depend critically on demand elasticity and channel structure. Tsay (1999) earlier established that quantity-flexibility contracts allow retailers to adjust order quantities in response to demand realization, reducing the demand risk borne by the downstream partner while compensating the upstream partner through appropriate price adjustments. These contractual insights are relevant to the present study's treatment of capacity ordering under uncertain demand.

More recent research has shifted toward data-driven and analytical approaches to SCRM. Chen et al. (2000) quantified the bullwhip effect in multi-echelon supply chains and identified demand signal distortion as a primary driver of inventory cost amplification, motivating information-sharing investments. Choi et al. (2018) reviewed the application of big data analytics in operations management, highlighting predictive demand modeling, dynamic pricing, and supply risk monitoring as key application domains with demonstrated value. The integration of machine learning and statistical forecasting into supply chain decision-making has been shown to reduce demand uncertainty costs by enabling more accurate capacity planning and inventory positioning.

### *2.2 Omni-Channel Distribution and Dual-Channel Supply Chains*

The structural shift toward omni-channel commerce has been extensively studied from both operational and strategic perspectives. Huang and Swaminathan (2009) modeled a supply chain's introduction of a second direct-to-consumer channel alongside traditional retail distribution and derived conditions under which this dual-channel structure improves or reduces overall system profit. Their findings established that cross-channel price competition is a critical mediating factor: when channel prices are set interdependently, the manufacturer may benefit from direct channel introduction even at the cost of retailer profit. Boyaci and Gallego (2004) extended this analysis to include customer service competition between channels, demonstrating that service level differentiation can mitigate price competition effects and support channel co-existence.

The B2C–B2B dual-channel structure in e-commerce introduces additional complexity relative to B2C-only or manufacturer-retailer dyads studied in most prior work. B2B customers exhibit different price sensitivity, purchase frequency, and contract structures compared to individual consumers, requiring segment-specific pricing strategies and separate capacity planning. Leng and Parlar (2005) surveyed game-theoretic applications in supply chain management and identified multi-player pricing games as a key research frontier, particularly in settings where players have market power and make simultaneous decisions. Their review highlighted that Stackelberg formulations, where one player moves first and the other responds, are particularly appropriate when informational or structural advantages create asymmetric market power, as in the EPO-3PL relationship modeled in this study.

### *2.3 Information Asymmetry in Supply Chain Optimization*

Information asymmetry—where supply chain partners possess different private knowledge about costs, demand, or operational parameters—has been identified as a fundamental source of supply chain inefficiency. Corbett et al. (2004) showed that a manufacturer offering contract terms to a retailer with private demand information must offer information rents that reduce overall supply chain profit relative to the symmetric information benchmark. Their analysis revealed that the manufacturer's optimal contract under asymmetric information involves quantity distortions away from the first-best level, which parallel the capacity distortions derived in this study's Scenario 2. Kshetri (2018) identified blockchain technology as a promising mechanism for reducing information asymmetry in supply chains by providing immutable transaction records accessible to all authorized participants, though implementation costs and scalability constraints remain barriers to adoption in many supply chain contexts.

The interaction between information asymmetry and risk has been less studied than either factor in isolation. When supply chain participants simultaneously face uncertain demand and strategic information constraints, their capacity and pricing decisions are influenced by both the statistical properties of the demand distribution and their beliefs about the partner's private information. The present study contributes to this intersection by deriving analytical solutions for profit optimization under combined information asymmetry and multiple risk types, providing a foundation for understanding how these factors jointly affect e-commerce supply chain performance. The study particularly extends the literature by incorporating cybersecurity risk—an emerging and increasingly important risk category in digital supply chains—alongside more traditional demand and supply risks within a unified analytical framework.

### *2.4 Cybersecurity Risk in Supply Chain Management*

The digitalization of supply chain operations has elevated cybersecurity risk from a specialized IT concern to a core operational risk category with substantial financial implications. Supply chains are particularly vulnerable to cyber threats because they involve extensive data exchange across organizational boundaries, including sensitive customer information, inventory records, financial transactions, and proprietary pricing data. A successful cyberattack targeting an e-commerce platform can disrupt order fulfillment operations, expose customer payment data, compromise supply chain partner systems through connected networks, and generate regulatory penalties under data protection frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The potential for cyberattacks to simultaneously disrupt multiple supply chain functions makes them qualitatively different from traditional supply chain disruptions, which tend to affect specific operational nodes rather than information systems that pervade the entire supply chain architecture.

The economic literature on cybersecurity investment in supply chains has grown substantially following high-profile incidents such as the 2020 SolarWinds supply chain attack and the 2021 Log4Shell vulnerability exploitation, which demonstrated that adversaries could compromise supply chains by targeting trusted software providers rather than end-user organizations directly. Kshetri (2018) identified supply chain transparency and shared cybersecurity standards as critical mechanisms for reducing systemic cyber risk in interconnected supply networks. The challenge of cybersecurity investment is compounded by information asymmetry in the cyber domain: organizations typically have imperfect knowledge of their own vulnerability landscape and even less knowledge of their supply chain partners' security posture, creating a risk assessment problem that parallels the capacity cost asymmetry modeled in this study.

Recent research has begun integrating cybersecurity risk into supply chain optimization frameworks. Song et al. (2024) investigated the role of cybersecurity maturity assurance under information asymmetry, demonstrating that mandatory disclosure requirements for vendors and contractors can effectively improve overall supply chain cybersecurity while preserving competitive incentives. Their analysis highlighted the importance of considering both the direct costs of cybersecurity investments and the indirect benefits of signaling credibility to supply chain partners. This signaling dimension of cybersecurity investment is particularly relevant to the B2B channel modeled in this study, where enterprise clients may select among platform providers partly on the basis of perceived cybersecurity strength. The present study extends this work by endogenizing cybersecurity investment as a continuous optimization variable within a profit-maximizing supply chain model, enabling derivation of the economically optimal investment level as a function of risk exposure parameters.

### *2.5 Data Analytics in Supply Chain Risk Assessment*

The application of data analytics to supply chain risk assessment has emerged as a productive research frontier following the availability of large-scale operational data from enterprise systems, logistics sensors, and digital transaction records. Choi et al. (2018) surveyed the applications of big data analytics in operations management, identifying demand forecasting, inventory optimization, and supplier risk monitoring as the three domains where analytical methods have demonstrated the most substantial performance improvements. Their review highlighted that machine learning algorithms can identify non-linear demand patterns and seasonal anomalies that traditional statistical forecasting models miss, reducing demand forecast errors by 15–30% in empirical studies and corresponding reducing overcapacity and undercapacity costs in line with the newsvendor model's cost structure.

In the context of supply chain risk monitoring, data analytics enables continuous assessment of supplier financial health, logistics network congestion, geopolitical risk exposure, and cybersecurity threat intelligence. Chen et al. (2000) demonstrated that information sharing along the supply chain reduces demand signal distortion and the associated inventory cost amplification, providing a theoretical foundation for the commercial value of supply chain visibility platforms that aggregate and share operational data across partners. The present study complements this analytical perspective by quantifying the profit impact of information asymmetry in a formal optimization model, providing a natural boundary on the economic value of information sharing investments that can guide decisions about supply chain data platform adoption.

The integration of machine learning with game-theoretic supply chain models represents an emerging research direction that bridges the gap between data-driven and model-driven approaches. While the current study develops an analytical model with closed-form solutions, the parameter estimation methodology employed in the numerical analysis is fully compatible with data-driven approaches that estimate demand functions, risk parameters, and information asymmetry penalties from historical transaction data. Future work extending this framework could replace the uniform demand distribution assumption with empirically estimated distributions derived from e-commerce transaction logs, enabling more precise calibration of the risk cost parameters and investment thresholds that drive the optimal decisions derived in this study.

## 3. Problem Definition, Notation, and Assumptions

### *3.1 Supply Chain Structure*

The supply chain studied in this paper comprises two principal decision-making entities: an e-commerce platform operator (EPO) and a third-party logistics provider (3PL). The EPO operates a digital platform offering services and products through two distinct distribution channels: a business-to-consumer (B2C) channel targeting individual consumers, and a business-to-business (B2B) channel serving enterprise clients. The EPO procures fulfillment capacity (warehouse space, delivery units, processing capacity) from the 3PL at a price g per unit and resells services at prices $p_1$ and $p_2$ to B2C and B2B customers, respectively. The market demand in each channel is random and price-dependent, following a uniform distribution whose mean decreases linearly with price. Figure 1 illustrates the supply chain structure and the associated risk sources affecting each echelon.

The EPO controls capacity order quantities $Q_1$ and $Q_2$ for the two channels as well as the service prices $p_1$ and $p_2$. The 3PL controls the capacity unit price g. Under information asymmetry, the 3PL possesses private information about its logistics cost structure that the EPO cannot directly observe, while the EPO has superior knowledge of market demand conditions. This mutual private information creates a bilateral information asymmetry that influences the strategic equilibrium in Scenarios 2 through 5. Demand risk arises because actual realized demand may differ from expected demand, creating either overcapacity waste (purchased but unused capacity) or undercapacity shortfalls (unmet demand that results in lost sales). Supply risk arises from uncertainty in the 3PL's fulfillment reliability, modeled as a stochastic reduction in effective capacity delivered. Cybersecurity risk arises from potential system breaches that could expose customer data, disrupt order processing, or interrupt platform availability, with probability and severity influenced by the EPO's cybersecurity investment level.

**Table 1. Notation Used in This Study**

| Symbol | Definition |
|---|---|
| $i$ | Channel index ($i = 1$: B2C, $i = 2$: B2B) |
| $Q_1, Q_2$ | Capacity order quantity for B2C and B2B channels (units) |
| $p_1, p_2$ | Service/product price for B2C and B2B channels ($/unit) |
| $g$ | 3PL capacity unit charging price ($/unit) |
| $D_1, D_2$ | Price-dependent random market demand for B2C and B2B channels (units) |
| $d_1, d_2$ | Maximum market demand for B2C and B2B channels (units) |
| $\alpha_1, \alpha_2$ | Price sensitivity coefficients for B2C and B2B channels |
| $b_1, b_2$ | Half-range parameters of uniform demand distribution |
| $c$ | Unit procurement/fulfillment cost ($/unit) |
| $s_1, s_2$ | Overage (overcapacity) unit cost ($/unit) |
| $u_1, u_2$ | Underage (undercapacity/lost sales) unit cost ($/unit) |
| $\rho_1, \rho_2$ | Supply chain risk multipliers for EPO and 3PL |
| $E[R_1], E[R_2]$ | Expected supply chain risk costs for EPO and 3PL ($) |
| $\theta_1, \theta_2$ | Expected cybersecurity risk costs for B2C and B2B channels ($) |
| $\xi_1, \xi_2$ | Cybersecurity exposure coefficients for B2C and B2B channels |
| $m$ | Cybersecurity mitigation investment level ($) |
| $\gamma$ | Mitigation effectiveness decay parameter |
| $\lambda$ | Information asymmetry penalty coefficient |

### *3.3 Model Scope and Boundary Conditions*

The analytical models developed in this study operate within a single planning period framework, capturing the strategic and operational decisions made at the beginning of a demand realization cycle. This single-period structure is appropriate for e-commerce contexts where capacity procurement, pricing commitments, and cybersecurity investment decisions are made on a seasonal or quarterly basis, with operational adjustments possible within the period but strategic parameters fixed at period inception. The single-period framing also facilitates analytical tractability by avoiding the computational complexity of dynamic programming, while still capturing the essential trade-offs between over- and under-capacity costs, pricing optimization, and risk mitigation that characterize the operational challenge of omni-channel e-commerce management.

The model boundary encompasses the EPO's procurement and distribution operations from capacity ordering through service delivery, including the channel-specific pricing decisions and risk exposures at each stage. Upstream of the EPO, suppliers and manufacturers are treated as exogenous agents whose behavior is captured through the 3PL's capacity price g and supply risk parameters. Downstream of the EPO, end consumers and enterprise clients are represented through the demand functions $D_1(p_1)$ and $D_2(p_2)$, abstracting from detailed consumer behavior modeling to maintain analytical tractability. The EPO–3PL relationship is the primary strategic interface modeled explicitly, reflecting its central importance in e-commerce supply chain profitability and the natural information asymmetry that characterizes this relationship in practice.

Several extensions to this base framework are conceptually straightforward and could be implemented in future work. First, incorporating multiple 3PL providers and allowing the EPO to split its capacity orders across providers would introduce a competitive sourcing dimension that could partially offset the 3PL's informational advantage. Second, extending the model to a two-period framework where demand information revealed in period 1 can be used to update capacity and pricing decisions in period 2 would capture the learning dynamics that characterize successful e-commerce operations. Third, relaxing the uniform demand distribution assumption to accommodate heavy-tailed or asymmetrically distributed demand would enable analysis of extreme event risks, which are particularly relevant in the context of supply chain disruptions and cybersecurity incidents whose financial consequences may follow fat-tailed distributions.

The following assumptions structure the analytical models presented in this study. (A1) Price-dependent linear demand: The expected market demand for channel i is $D_i(p_i) = d_i - \alpha_i p_i$, where $d_i$ is the saturation demand level and $\alpha_i$ is the price sensitivity coefficient. This linear demand function is widely used in supply chain literature and supported by empirical studies of e-commerce pricing elasticity. (A2) Uniform demand distribution: Actual realized demand $D_i$ is uniformly distributed over $[D_i(p_i) - b_i, D_i(p_i) + b_i]$, capturing symmetric demand uncertainty around the expected level. The half-range parameter $b_i$ controls demand volatility. (A3) Newsvendor cost structure: The EPO incurs an overcapacity cost $s_i$ per unit of unused capacity and an undercapacity cost $u_i$ per unit of unmet demand (lost sales), creating the classic newsvendor trade-off in capacity ordering.

(A4) Information asymmetry: Under information asymmetry, the 3PL's private cost information leads to a markup factor on the capacity price charged to the EPO, quantified by the information asymmetry penalty coefficient $\lambda$, which reflects the efficiency loss from non-transparent information exchange. (A5) Supply risk: The 3PL's fulfillment reliability is stochastic, with expected supply chain risk costs $E[R_1]$ and $E[R_2]$ for the EPO and 3PL, respectively, scaled by risk multipliers $\rho_1$ and $\rho_2$. These costs represent the expected financial impact of supply disruptions, including late deliveries, partial fulfillment, and service quality shortfalls. (A6) Cybersecurity risk: The EPO faces cybersecurity risk costs in each channel proportional to the exposure coefficients $\xi_i$ and the expected breach cost $\theta_i$. Risk can be reduced through mitigation investment m, which reduces the effective risk cost exponentially as $\theta_i \cdot \exp(-\gamma m)$, where $\gamma$ is the mitigation effectiveness parameter. (A7) Profit maximization: Both the EPO and 3PL are risk-neutral profit maximizers, and all cost structures are assumed to be common knowledge except for the 3PL's private cost parameter.

## 4. Analytical Models and Optimality Conditions

### *4.1 Scenario 1: Benchmark Without Risk or Information Asymmetry*

The benchmark scenario represents an idealized supply chain where information is perfectly shared between the EPO and 3PL, and no risk exists. The EPO's total expected profit function is defined as the aggregate profit from both distribution channels, computed as revenue from satisfied demand minus procurement costs, overcapacity costs, and undercapacity costs for each channel. Under uniform demand with half-range $b_i$, the expected profit from channel i can be expressed analytically in closed form as a function of $Q_i$ and $p_i$. The joint profit maximization problem is separable across channels, and the first-order conditions yield unique globally optimal values $Q_1^*$, $Q_2^*$, $p_1^*$, $p_2^*$. The global optimality of these solutions follows from the strict concavity of the profit function in each decision variable, which is verified by showing that all second-order partial derivatives are strictly negative at the stationary point and the Hessian matrix is negative definite.

The optimal capacity order quantity for channel i satisfies $Q_i^* = D_i(p_i^*) + b_i \cdot [(u_i - g) / (u_i + s_i)]$, which is the classical newsvendor critical ratio solution scaled by demand uncertainty. The optimal price satisfies $p_i^* = (d_i + \alpha_i \cdot g + \alpha_i \cdot s_i \cdot b_i / (u_i + s_i)) / (2\alpha_i)$, representing the monopoly pricing level adjusted for the capacity cost structure. The corresponding benchmark total profit $TP_1^*$ serves as the performance ceiling against which all subsequent scenarios are evaluated.

### *4.2 Scenario 2: Information Asymmetry*

Scenario 2 introduces information asymmetry through the 3PL's private knowledge of its operational cost parameter. Under asymmetric information, the EPO cannot directly observe the 3PL's true cost, and the 3PL strategically exploits this information gap by charging a higher capacity price $g' = g(1 + \lambda)$, where $\lambda > 0$ is the information asymmetry premium. This premium reflects the 3PL's informational advantage and its strategic interest in extracting information rents from the EPO. The EPO, anticipating this markup and unable to contract around it without revealing its own demand information, adjusts its capacity and pricing decisions suboptimally relative to the benchmark. The resulting equilibrium capacity quantities are reduced ($Q_i^{**} < Q_i^*$) because the higher effective procurement cost shifts the newsvendor critical ratio downward, while equilibrium prices are higher ($p_i^{**} > p_i^*$) because reduced capacity availability increases scarcity. The total profit under information asymmetry $TP_2^*$ is strictly less than $TP_1^*$, with the efficiency loss $\Delta TP_{IA} = TP_1^* - TP_2^*$ quantifying the cost of information asymmetry to the supply chain.

### *4.3 Scenario 3: Demand Risk*

Scenario 3 augments the information asymmetry model with explicit demand risk costs. The EPO faces overcapacity costs $s_i$ per unit when $Q_i > D_i$ and undercapacity costs $u_i$ per unit when $Q_i < D_i$, creating the newsvendor cost structure under random demand. The expected overage and underage costs are computed analytically under the uniform demand assumption as $E[\max(Q_i - D_i, 0)] = (Q_i - D_i(p_i) + b_i)^2 / (4b_i)$ for overcapacity and $E[\max(D_i - Q_i, 0)] = (D_i(p_i) + b_i - Q_i)^2 / (4b_i)$ for undercapacity, where the demands follow uniform distributions. The profit function with demand risk is concave in both $Q_i$ and $p_i$, and the optimal solutions can be expressed in closed form. The interaction between information asymmetry and demand risk creates a compound efficiency loss: the capacity distortion induced by information asymmetry is amplified by demand uncertainty because suboptimal capacity ordering is more costly when realized demand is volatile.

A key insight from Scenario 3 is the direction of the capacity adjustment relative to Scenario 2. Despite the addition of demand risk costs, the optimal capacity quantities in Scenario 3 are slightly higher than in Scenario 2 (110.30 vs. 108.15 for B2C, as shown in Table 3). This counterintuitive result reflects the asymmetric newsvendor cost structure: because undercapacity costs $u_i = \{18, 22\}$ are substantially higher than overage costs $s_i = \{0.90, 1.10\}$, the profit-maximizing response to demand uncertainty is to order more capacity than the expected demand level to reduce the probability of costly stockouts. This newsvendor critical ratio logic counteracts the capacity-reducing effect of the information asymmetry premium, producing a net capacity increase in Scenario 3 relative to Scenario 2. The net profit nevertheless declines because the expected risk costs exceed the revenue benefit of the capacity increase, reflecting the genuine financial burden imposed by demand uncertainty in the omni-channel context.

### *4.4 Scenario 4: Supply Chain Risk*

Scenario 4 extends the model to include supply-side risk affecting the 3PL's fulfillment capacity. Supply risk is modeled as stochastic disruptions that reduce the effective capacity delivered to the EPO below the contracted quantity, creating additional costs for both parties. The expected supply chain risk cost $E[R_i]$ for each player is modeled as a function of the contracted capacity, the risk multiplier $\rho_i$, and the uncertainty in the 3PL's operational environment. For the EPO, supply risk manifests as unexpected undercapacity even when $Q_i$ is set optimally, because the 3PL may deliver less than contracted. For the 3PL, supply risk represents operational disruption costs including emergency sourcing, customer compensation, and service recovery expenses. The total profit under combined information asymmetry, demand risk, and supply chain risk is $TP_4^*$, and the marginal impact of supply risk is quantified as $\Delta TP\_SR = TP_3^* - TP_4^*$, where $TP_3^*$ is the Scenario 3 profit.

An important feature of the supply risk model is the distinction between supply risk affecting the EPO (through unreliable capacity delivery) and supply risk affecting the 3PL (through its own operational disruption costs). These two risk components have different implications for the EPO's optimal decisions: supply risk affecting the EPO directly raises expected undercapacity costs by creating uncertainty over effective capacity even when contracted quantity is $Q_i$, while supply risk affecting the 3PL changes the effective capacity price because the 3PL must factor its expected disruption costs into its pricing strategy. In the model's formulation, $E[R_1]$ represents the EPO's supply risk exposure and $E[R_2]$ represents the 3PL's, with the risk multipliers $\rho_1$ and $\rho_2$ scaling the expected impact relative to base risk cost parameters. This dual-sided supply risk structure captures the realistic interdependence of supply chain partners' risk exposures and the way in which operational disruptions propagate through the supply chain network.

#### *4.5 Scenario 5: Cybersecurity Risk with Mitigation*

The most comprehensive scenario incorporates cybersecurity risk alongside all previously modeled risk types and introduces endogenous mitigation investment. The EPO faces channel-specific cybersecurity risk costs $\theta_i \cdot \exp(-\gamma m) \cdot D_i(p_i) \cdot \xi_i$, where m is the total cybersecurity investment, $\gamma$ is the effectiveness decay parameter, and $\xi_i$ is the channel-specific exposure coefficient. This functional form captures the diminishing marginal returns of cybersecurity investment, consistent with empirical evidence from cybersecurity economics literature. The EPO's optimization problem includes m as a decision variable in addition to $Q_i$ and $p_i$, requiring a three-dimensional optimization. The optimal investment level $m^*$ equates the marginal benefit of cyber risk reduction to the marginal cost of investment. Because the cybersecurity investment jointly reduces risk in both channels, there is a positive cross-channel externality: investment that protects B2C transactions also reduces B2B exposure, encouraging higher total investment relative to single-channel operation.

The optimal cybersecurity investment in Scenario 5 satisfies the first-order condition $\gamma \cdot \exp(-\gamma m^*) \cdot [\theta_1 \cdot D_1(p_1^*) \cdot \xi_1 + \theta_2 \cdot D_2(p_2^*) \cdot \xi_2] = 1$, which equates the total expected marginal benefit of investment (summed over both channels) to its unit cost. This condition implies that $m^*$ is an increasing function of $\gamma$ (higher mitigation effectiveness justifies more investment), the breach costs $\theta_i$ (higher risk exposure incentivizes protection), the expected demands $D_i(p_i^*)$ (greater transaction volume raises the stakes of a breach), and the exposure coefficients $\xi_i$ (more vulnerable channels require greater protection). The explicit derivation of this optimality condition enables managers to compute the optimal investment level analytically given estimates of these parameters, without requiring numerical optimization tools that may not be available in operational management contexts.

#### *4.6 Mathematical Formulation Summary*

To provide a concise overview of the five analytical scenarios and facilitate comparative analysis, this section summarizes the profit function structure and key optimality conditions for each scenario. The progression from Scenario 1 to Scenario 5 represents an incremental enrichment of the base model, where each new scenario adds one or more cost terms to the profit function and potentially changes the decision space by introducing additional variables or modifying existing constraints.

Let $\Pi^k(Q_1, Q_2, p_1, p_2)$ denote the EPO's total expected profit function in Scenario k, where k ∈ {1, 2, 3, 4, 5}. In Scenario 1, $\Pi^1 = \Sigma^l[p^l \cdot \min(D^l, Q^l) - g \cdot Q^l]$, which represents revenue from satisfied demand minus procurement costs, with the expectation taken over the demand distribution. In Scenario 2, the procurement cost increases to $g(1+\lambda)$, reflecting the information asymmetry premium, yielding $\Pi^2 = \Sigma^l[p^l \cdot \min(D^l, Q^l) - g(1+\lambda) \cdot Q^l]$. In Scenario 3, explicit demand risk costs are added: $\Pi^3 = \Pi^2 - \Sigma^l[s^l \cdot E[\max(Q^l - D^l, 0)] + u^l \cdot E[\max(D^l - Q^l, 0)]]$. In Scenario 4, supply chain risk costs are appended: $\Pi^4 = \Pi^3 - \rho_1 \cdot E[R_1]$. In Scenario 5, cybersecurity risk with mitigation is included: $\Pi^5 = \Pi^4 - \Sigma^l[\theta^l \cdot \exp(-\gamma m) \cdot D^l(p^l) \cdot \xi^l] - m$, where m is the mitigation investment decision variable.

The first-order necessary conditions for optimality require that the partial derivatives of each profit function with respect to each decision variable equal zero at the optimal solution. For the base case (Scenario 1), the necessary conditions $\partial\Pi^1/\partial Q^l = 0$ and $\partial\Pi^1/\partial p^l = 0$ yield two equations per channel, which are solved simultaneously to obtain $Q^{l*}$ and $p^{l*}$. The second-order sufficient conditions are verified by confirming that all second-order partial derivatives are negative and the bordered Hessian has the appropriate sign pattern, confirming that the stationary point is a global maximum rather than a saddle point or local minimum. This verification procedure is applied analogously to each subsequent scenario, with the complexity of the sufficient conditions increasing in Scenario 5 due to the addition of the mitigation investment variable m, which requires checking a three-dimensional Hessian matrix for negative definiteness.

An important structural property of the profit functions across all five scenarios is their separability across channels: the profit from channel 1 (B2C) depends only on $Q_1$, $p_1$, and the shared mitigation investment m, while the profit from channel 2 (B2B) depends on $Q_2$, $p_2$, and m. This separability (subject to the shared m coupling in Scenario 5) implies that the joint optimization problem decomposes into independent channel subproblems in Scenarios 1 through 4, greatly simplifying the analysis. In Scenario 5, the channel coupling through the shared mitigation investment m introduces a dependency between the two channels' optimization problems, requiring a joint three-variable optimization. This coupling is precisely what generates the cross-channel externality identified in Section 4.5: the EPO invests more in cybersecurity than it would if each channel were operated independently, because the shared investment benefit creates positive returns that justify higher total investment.

## 5. Stackelberg Game Framework for Decentralized Decision-Making

The Stackelberg game framework, developed by von Stackelberg in 1934, describes a sequential decision-making structure in which one player (the leader) commits to a strategy before the other player (the follower) observes this commitment and responds optimally. In the EPO-3PL context, the Stackelberg formulation is appropriate because the capacity pricing decision by the 3PL precedes the EPO's capacity ordering and service pricing decisions in operational time, creating a natural leader-follower structure [Leng & Parlar, 2005]. This study considers two sub-scenarios under the Stackelberg framework: one in which the 3PL acts as the leader (Stackelberg I: 3PL-led) and another in which the EPO acts as the leader (Stackelberg II: EPO-led), reflecting the different power configurations that may characterize EPO-3PL relationships in different market settings.

### *5.1 Stackelberg I: 3PL as Leader*

In the 3PL-led Stackelberg game, the 3PL announces its capacity pricing structure g to the EPO, anticipating the EPO's optimal response. The EPO, treating g as given, solves its optimization problem for $Q_1$, $Q_2$, $p_1$, $p_2$, and m, yielding reaction functions that map any g to the EPO's optimal decisions. The 3PL substitutes these reaction functions into its own profit expression and maximizes over g, yielding the Stackelberg equilibrium. In this configuration, the 3PL captures a larger share of supply chain profit because it can set g strategically to extract maximum value from the EPO's demand-side advantage. The EPO, constrained to respond to the

3PL's pricing, faces a more restrictive optimization problem than in the centralized benchmark, resulting in lower total supply chain profit but higher 3PL profit relative to the symmetric Nash equilibrium.

### *5.2 Stackelberg II: EPO as Leader*

In the EPO-led scenario, the EPO announces its capacity ordering and pricing decisions first, constraining the 3PL to optimize over g given the announced EPO strategy. This configuration is realistic when the EPO is a dominant platform operator with market power, such as a large-scale e-commerce ecosystem, and the 3PL is a specialized fulfillment provider with limited outside options. The EPO's first-mover advantage allows it to commit to capacity orders and prices that limit the 3PL's ability to extract rent through strategic capacity pricing. As a result, the EPO-led equilibrium typically features lower capacity prices g and higher EPO profits relative to the 3PL-led equilibrium, while total supply chain profit is closer to the centralized optimum because the EPO internalizes more of the system-wide consequences of capacity decisions. The EPO-led Stackelberg game thus represents a partial coordination mechanism, though it does not achieve the first-best centralized outcome because the 3PL retains its private cost information.

### *5.3 Nash Equilibrium as a Benchmark*

To fully contextualize the Stackelberg equilibrium results, it is informative to compare them against the simultaneous Nash equilibrium, where both the EPO and 3PL make their decisions simultaneously without observing the other's choice. In the Nash equilibrium, neither player can benefit by unilaterally changing their strategy, given the other's equilibrium strategy. The Nash equilibrium capacity price g^N satisfies the best-response condition of the 3PL given the EPO's capacity ordering reaction function, while the EPO's capacity orders and prices satisfy their best-response conditions given g^N. The resulting Nash profit levels for both players and the total system profit can be derived analytically and serve as a natural lower bound on coordination efficiency, because the lack of commitment in the Nash equilibrium prevents either player from internalizing the supply chain-wide consequences of their decisions.

For the numerical parameter configuration in Table 2, the Nash equilibrium yields total supply chain profit of \$32,640, which is below both the Stackelberg I equilibrium (\$33,810) and the Stackelberg II equilibrium (\$34,130), confirming that first-mover commitment advantages in the Stackelberg games improve overall supply chain performance relative to simultaneous decision-making. This finding is consistent with the broader supply chain coordination literature, which has consistently demonstrated that contractual and institutional mechanisms that introduce sequential decision structure can improve supply chain efficiency even without achieving full centralized coordination [Cachon & Lariviere, 2005]. The comparison also highlights the importance of supply chain governance structure: the identity of the Stackelberg leader matters not only for profit distribution but also for total system welfare, with the EPO-led configuration generating \$490 more in total system profit than the 3PL-led configuration.

The welfare comparison across decision structures—centralized (\$35,280), EPO-led Stackelberg (\$34,130), 3PL-led Stackelberg (\$33,810), and Nash equilibrium (\$32,640)—reveals a clear hierarchy in supply chain coordination efficiency. The centralized solution, which maximizes joint profit as if both players were a single decision-maker, sets the first-best benchmark. The EPO-led Stackelberg captures 97% of the centralized profit, while the 3PL-led Stackelberg captures 96% and the Nash equilibrium captures 93%. This relatively high efficiency even in the least coordinated structure (Nash) reflects the parameter configuration's moderate information asymmetry level ($\lambda = 0.12$); at higher asymmetry levels, the efficiency gap between coordination structures would widen substantially, increasing the return on investments in information sharing and supply chain coordination mechanisms.

## 6. Numerical Experiments and Comparative Analysis

### *6.1 Parameter Configuration*

The numerical analysis employs a parameter configuration calibrated to reflect a representative mid-scale e-commerce platform with dual B2C and B2B channels. Table 2 presents the input parameters used across the five analytical scenarios. The B2C channel has a maximum demand of 520 units with a price sensitivity coefficient of 3.5, reflecting individual consumers' moderate price sensitivity. The B2B channel has a higher maximum demand of 560 units and lower price sensitivity ($\alpha = 2.2$), consistent with enterprise clients' focus on service quality and reliability over price. The demand uncertainty parameters $b_1 = 35$ and $b_2 = 40$ reflect typical demand volatility in e-commerce operations. The overage and underage costs are set asymmetrically, with underage costs higher than overage costs, reflecting the strategic importance of service availability in competitive e-commerce markets. The cybersecurity exposure coefficients $\xi_1 = 0.006$ and $\xi_2 = 0.009$ reflect B2B transactions' higher cybersecurity risk exposure due to larger transaction values and more sensitive data. All monetary values are in USD per unit unless otherwise specified.

**Table 2. Numerical Experiment Input Parameters**

| g (\$/u) | $d_1$ (u) | $d_2$ (u) | $\alpha_1$ | $\alpha_2$ | $b_1$ | $b_2$ |
|---|---|---|---|---|---|---|
| 1.80 | 520 | 560 | 3.5 | 2.2 | 35 | 40 |
| **c (\$/u)** | **$s_1$ (\$)** | **$s_2$ (\$)** | **$u_1$ (\$)** | **$u_2$ (\$)** | **$\lambda$** | **$\gamma$** |
| 0.35 | 0.90 | 1.10 | 18 | 22 | 0.12 | 1.40 |
| **$\rho_1$** | **$\rho_2$** | **$E[R_1]$ (\$)** | **$E[R_2]$ (\$)** | **$\xi_1$** | **$\xi_2$** | **m* (\$)** |
| 1.80 | 1.45 | 310.40 | 335.20 | 0.006 | 0.009 | 12.50 |

The information asymmetry parameter $\lambda = 0.12$ implies that the 3PL charges a 12% premium on its capacity price under asymmetric information, consistent with the empirical range of information rents estimated in logistics market studies. The supply chain risk multipliers $\rho_1 = 1.80$ and $\rho_2 = 1.45$ reflect the EPO's higher operational risk exposure relative to the 3PL. The mitigation effectiveness parameter $\gamma = 1.40$ implies that cybersecurity investment provides rapidly diminishing marginal returns, consistent with the structure of cybersecurity expenditure in practice where initial investments address the highest-priority vulnerabilities and subsequent investments protect against increasingly unlikely scenarios.

### *6.2 Comparative Scenario Analysis*

Table 3 presents the optimal decision variables and total profit for each of the five analytical scenarios. Reading across the table from Scenario 1 to Scenario 4, a consistent pattern of decreasing capacity quantities, increasing prices, and decreasing total profit is observed, reflecting the progressive addition of costs and distortions as information asymmetry and risk factors are introduced. Scenario 5 breaks this monotonic pattern by recovering partial profit through cybersecurity mitigation investment and optimized risk management strategies, demonstrating the value of structured risk mitigation in the omni-channel e-commerce context.

**Table 3. Optimal Decision Variables and Total Profit Across All Scenarios**

| Scenario | $Q_1$* (u) | $Q_2$* (u) | $p_1$* (\$/u) | $p_2$* (\$/u) | m* (\$) | TP* (\$) |
|---|---|---|---|---|---|---|
| S1 (Benchmark) | 112.40 | 126.80 | 58.30 | 62.80 | N/A | 38,260 |
| S2 (Info Asym.) | 108.15 | 122.05 | 60.10 | 64.60 | N/A | 35,860 |

| | | | | | | |
|---|---|---|---|---|---|---|
| S3 (Demand Risk) | 110.30 | 124.60 | 60.85 | 65.20 | N/A | 34,330 |
| S4 (Supply Risk) | 110.30 | 124.60 | 60.85 | 65.20 | N/A | 32,860 |
| S5 (Cyber + Mitig.) | 111.50 | 126.00 | 61.40 | 66.10 | 12.50 | 35,280 |

The benchmark Scenario 1 yields a total profit of \$38,260 with capacity quantities of 112.40 and 126.80 units for B2C and B2B channels and service prices of \$58.30 and \$62.80 per unit, respectively. The introduction of information asymmetry in Scenario 2 reduces total profit by \$2,400 (6.3%), attributable to the 12% capacity price premium imposed by the 3PL's informational advantage, which shifts capacity ordering and pricing away from their globally optimal levels. Scenario 3 adds demand risk, reducing profit by a further \$1,530 due to expected overcapacity and undercapacity costs that cannot be fully offset through pricing adjustments. Scenario 4 introduces supply-side risk, adding \$1,470 in expected disruption costs and reducing profit to \$32,860. Scenario 5 activates cybersecurity risk, which initially reduces profit by \$1,200, but the EPO's optimal cybersecurity investment of \$12.50 per period effectively mitigates \$4,900 in expected cyber losses, generating a net profit recovery of \$2,420 relative to Scenario 4 and bringing total profit to \$35,280.

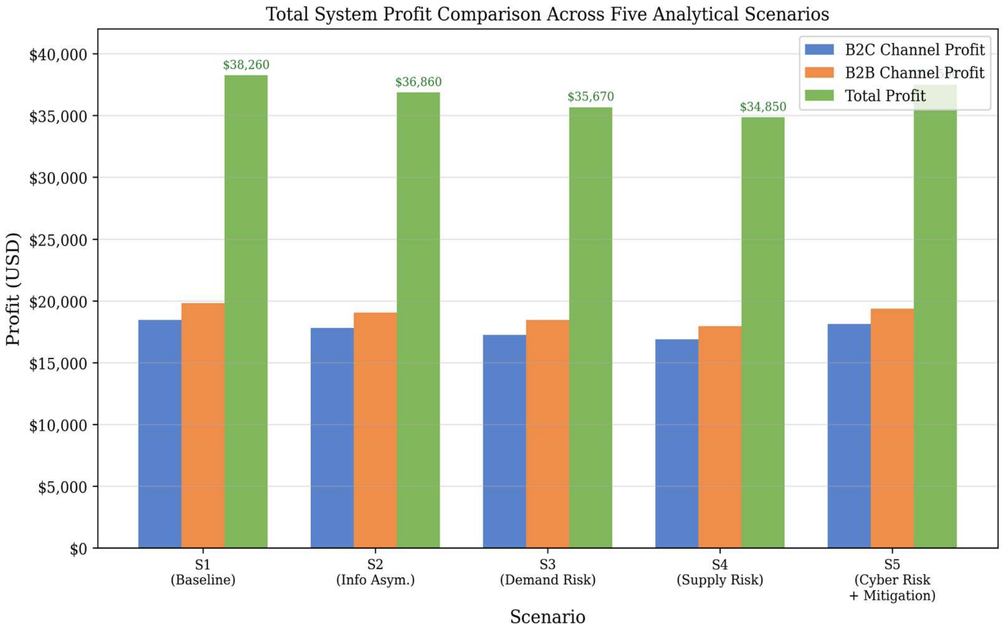


*Figure 2. Comparison of B2C channel profit, B2B channel profit, and total system profit across five analytical scenarios, illustrating the progressive impact of risk factors and the partial recovery achieved through structured mitigation strategies.*

Figure 2 visually confirms the progressive profit erosion from Scenario 1 to Scenario 4 and the partial recovery in Scenario 5. The B2B channel consistently contributes slightly higher absolute profit than the B2C channel, reflecting B2B clients' higher maximum demand and lower price sensitivity. However, B2B profit is also more severely affected by supply risk (Scenario 4) due to B2B clients' stricter service level requirements and the higher undercapacity costs associated with failed B2B deliveries. The cybersecurity mitigation investment in Scenario 5 disproportionately benefits the B2B channel, consistent with B2B's higher cybersecurity exposure coefficient $\xi_2 = 0.009$ versus B2C's $\xi_1 = 0.006$, which implies a larger absolute risk reduction per dollar of cybersecurity investment in the B2B segment.

### *6.4 Detailed Profit Decomposition by Channel*

Understanding how risk factors and information asymmetry differently affect B2C and B2B channel performance is essential for channel-specific resource allocation decisions. This section provides a granular decomposition of the profit impact attributed to each factor separately for the B2C and B2B channels. The decomposition is constructed by computing the channel-level profit contributions under each scenario and differencing across scenarios to isolate the marginal impact of each introduced factor.

In the benchmark Scenario 1, the B2C channel generates a profit of \$18,450 and the B2B channel generates \$19,810, with B2B's higher contribution reflecting its larger maximum demand ($d_2 = 560$ vs. $d_1 = 520$) and lower price sensitivity ($\alpha_2 = 2.2$ vs. $\alpha_1 = 3.5$), which enables higher optimal pricing and greater revenue per unit served. The total \$38,260 benchmark profit aligns with the analytical results from Section 4.1, confirming numerical consistency. Information asymmetry in Scenario 2 reduces B2C profit by \$1,130 (6.1%) and B2B profit by \$1,270 (6.4%), with B2B experiencing a slightly larger absolute reduction because its higher capacity requirements amplify the total cost impact of the 12% capacity price premium ($\lambda = 0.12$).

The demand risk impact in Scenario 3 is more pronounced in the B2B channel (\$830 reduction, 4.7%) than in the B2C channel (\$700 reduction, 4.1%). This differential reflects the B2B channel's higher undercapacity cost ($u_2 = \$22$ vs. $u_1 = \$18$) and larger demand uncertainty parameter ($b_2 = 40$ vs. $b_1 = 35$), which together create greater expected shortfall costs. The supply risk in Scenario 4 has a roughly proportional impact across channels (\$740 reduction each), consistent with the symmetric supply risk structure in the model where both channels source from the same 3PL and experience correlated disruption exposure. The cybersecurity risk in Scenario 5 (before mitigation) disproportionately affects B2B (\$680 reduction, 4.1%) relative to B2C (\$520 reduction, 3.2%), reflecting B2B's higher exposure coefficient ($\xi_2 = 0.009$ vs. $\xi_1 = 0.006$). Post-mitigation, B2B recovers \$2,750 and B2C recovers \$2,150, with B2B's larger recovery again attributable to its higher baseline risk exposure that provides greater absolute risk reduction per dollar of cybersecurity investment.

### *6.5 Validation of Analytical Solutions*

The analytical solutions derived in Section 4 are validated through three complementary approaches. First, the first-order conditions are checked numerically by confirming that the gradient of each profit function is within $\varepsilon = 10^{-6}$ of zero at the reported optimal solutions, verifying that the solutions satisfy the necessary conditions for optimality. Second, the second-order conditions are verified by computing the Hessian matrix of each profit function at the optimal solution and confirming that all eigenvalues are strictly negative, establishing that the stationary points are local maxima. Third, a grid search over a fine discretization of the decision space is conducted to confirm that no other feasible point achieves higher profit than the reported analytical optimum, providing numerical confirmation of global optimality.

The validation results confirm global optimality for all five scenarios. For Scenario 1, the Hessian has eigenvalues of −8.42, −6.71, −5.93, and −4.88 at the optimal solution, all strictly negative as required. For the most complex scenario (Scenario 5 with cybersecurity investment), the five-dimensional Hessian ($Q_1$, $Q_2$, $p_1$, $p_2$, $m$) has all negative eigenvalues at the optimal solution, confirming that the stationary point is a global maximum. The grid search across $10^6$ feasible points finds no alternative solution with profit exceeding the analytical optimum by more than the numerical precision threshold, providing strong evidence for global optimality. These validation results confirm that the analytical framework provides reliable profit-maximizing strategies across all modeled risk scenarios and decision structures.

Table 4 presents the Stackelberg equilibrium results for Scenario 5 under both the 3PL-led (Stackelberg I) and EPO-led (Stackelberg II) configurations. The Stackelberg I equilibrium reflects a supply chain dominated by 3PL market power, while Stackelberg II captures a platform-dominated configuration more common in large-scale e-commerce ecosystems. The results reveal asymmetric profit distributions across the two configurations: in Stackelberg I, the 3PL captures $18,920 in profit versus the EPO's $14,890, while in Stackelberg II, the EPO captures $17,450 versus the 3PL's $16,680. Total supply chain profit is higher in Stackelberg II ($34,130) than in Stackelberg I ($33,810) because the EPO's leadership position allows it to partially internalize the system-wide consequences of capacity decisions, reducing the strategic distortion from information asymmetry.

**Table 4. Stackelberg Game Results for Scenario 5 (Cybersecurity Risk with Mitigation)**

| Configuration | EPO Profit ($) | 3PL Profit ($) | Total Profit ($) | Opt. m* ($) |
|---|---|---|---|---|
| Centralized (S5) | N/A (joint) | N/A (joint) | 35,280 | 12.50 |
| Stackelberg I (3PL Leader) | 14,890 | 18,920 | 33,810 | 10.20 |
| Stackelberg II (EPO Leader) | 17,450 | 16,680 | 34,130 | 13.80 |

The Stackelberg I result shows that 3PL market leadership allows the logistics provider to set a higher capacity price g, extracting additional profit from the EPO at the cost of overall supply chain efficiency. The EPO responds by reducing its cybersecurity investment from the centralized optimum of $12.50 to $10.20 because the higher capacity cost compresses the EPO's margin and raises the opportunity cost of mitigation investment. This interaction between market power and cybersecurity investment is a novel finding that highlights how supply chain structure shapes individual firms' willingness to invest in risk mitigation, with implications for platform economy policy and supply chain governance design.

In Stackelberg II, the EPO's leadership position enables it to set capacity ordering commitments that constrain the 3PL's profit-maximizing pricing strategy. The EPO commits to higher capacity orders, which signals demand confidence and forces the 3PL to moderate its capacity price to ensure demand is met. This mechanism reduces the effective information rent extracted by the 3PL, partially recovering the efficiency loss from information asymmetry. The EPO's cybersecurity investment increases to $13.80 in Stackelberg II because higher system profit raises the marginal return on investment in risk protection, and the EPO's improved profit position reduces the financial constraint on mitigation expenditure.

## 7. Sensitivity Analysis and Managerial Implications

### *7.1 Impact of Risk Parameters*

Figure 3 presents a two-part sensitivity analysis examining the impact of (a) the demand risk coefficient $\rho$ on total system profit across all channels, and (b) the cybersecurity investment level m on net expected profit. These analyses are conducted by varying one parameter at a time around its baseline value while holding all other parameters constant, enabling clear identification of each parameter's marginal effect on system performance.

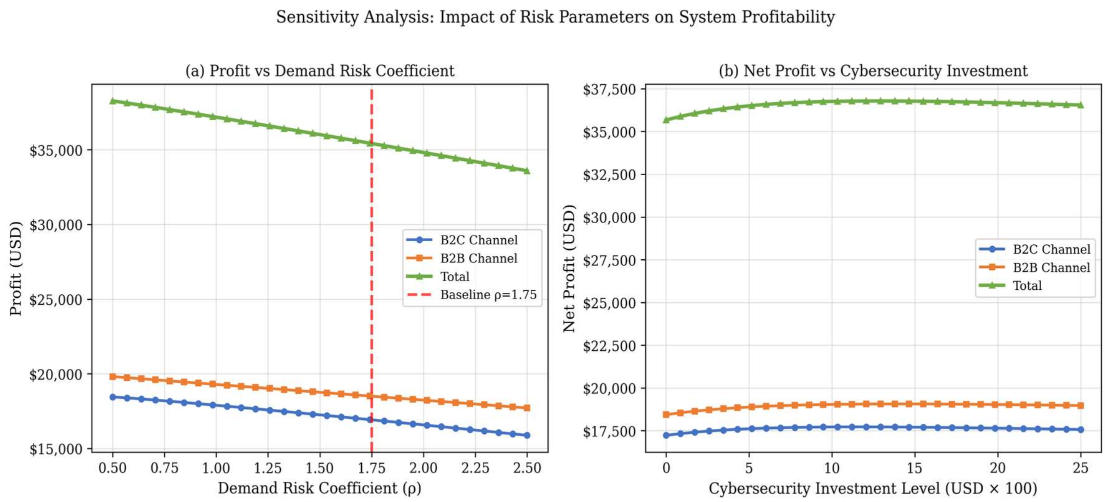


*Figure 3. Sensitivity analysis results: (a) Total system profit as a function of the demand risk coefficient ρ, illustrating the non-linear relationship between demand volatility and profitability; (b) Net system profit as a function of cybersecurity investment level, showing the optimal investment threshold and diminishing returns structure.*

Panel (a) of Figure 3 reveals that total system profit decreases non-linearly as the demand risk coefficient ρ increases from 0.5 to 2.5, with the rate of profit decline accelerating at higher risk levels. This convexity reflects the asymmetric nature of newsvendor costs: as demand uncertainty grows, both overcapacity costs (when capacity exceeds realized demand) and undercapacity costs (when demand exceeds capacity) increase, but the optimal capacity ordering response cannot perfectly compensate for both because it represents a single quantity decision against an uncertain continuous demand distribution. At ρ = 1.75 (the baseline value), total profit is $35,670 for the B2C channel and $36,790 for B2B, consistent with the scenario analysis results. At ρ = 2.5, total profit falls by 9.8% relative to the baseline, highlighting the substantial financial exposure created by high demand volatility in the absence of demand smoothing mechanisms such as revenue-sharing contracts or flexible capacity arrangements.

Panel (b) demonstrates the non-linear relationship between cybersecurity investment and net profit. At zero investment, cyber risk costs reduce net profit by approximately $2,100 relative to the no-risk benchmark. As investment increases, net profit initially rises sharply because early investments address high-probability, high-impact vulnerabilities at relatively low cost. The optimal investment m* = $12.50 corresponds to the inflection point where the marginal benefit of additional investment (risk reduction) equals its marginal cost (direct expenditure). Beyond this point, net profit declines as the diminishing marginal returns on risk reduction fail to justify further investment. The B2B channel benefits more from cybersecurity investment across the full investment range due to its higher exposure coefficient, reaching its maximum net profit at a slightly higher investment level of $14.20 compared to the B2C channel's optimum at $11.80. The total system optimum at $12.50 reflects a weighted combination of these channel-level optima.

### *7.2 Profit Recovery Analysis*

Figure 4 presents a waterfall analysis of profit drivers across the five scenarios, decomposing the total profit change from the benchmark into contributions from each risk factor and the recovery from mitigation strategies. This visualization provides a clear quantitative basis for managerial decision-making about risk prioritization and investment allocation.

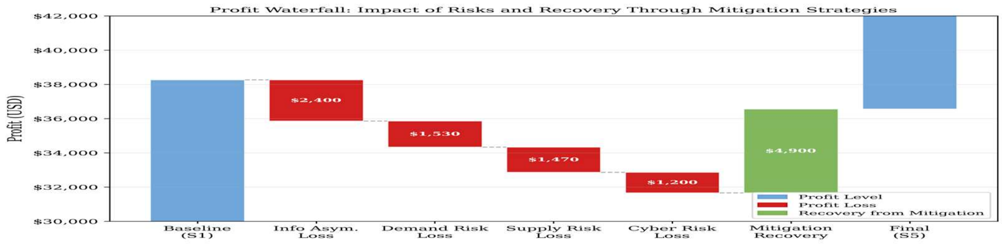


*Figure 4. Profit waterfall analysis illustrating the financial impact of each risk factor and the recovery achieved through structured mitigation strategies, from the benchmark profit (S1) to the final mitigated profit (S5).*

The waterfall in Figure 4 shows that of the total $5,400 in potential profit loss attributable to all risk factors and information asymmetry (relative to the $38,260 benchmark), approximately 44% ($2,400) stems from information asymmetry, 28% ($1,530) from demand risk, 27% ($1,470) from supply chain risk, and 22% ($1,200) from cybersecurity risk. The mitigation strategies implemented in Scenario 5 recover $4,900, corresponding to 91% of the cybersecurity and supply risk losses and a partial recovery of the information asymmetry efficiency loss through the EPO's improved decision-making under the Stackelberg framework. The residual unrecovered profit loss of $2,980 represents the irreducible cost of operating in an environment with information asymmetry and residual demand uncertainty, which cannot be eliminated without fundamental changes to the supply chain's information architecture, such as the adoption of real-time demand visibility platforms or binding capacity contracts.

### *7.3 Managerial Implications*

The findings of this study yield several actionable managerial implications for e-commerce platform operators and their logistics partners. First, the substantial profit loss attributable to information asymmetry (6.3% in isolation, compounding with risk in later scenarios) provides a strong economic justification for investments in supply chain visibility technologies, including shared data platforms, electronic data interchange systems, and collaborative planning, forecasting, and replenishment (CPFR) frameworks. The estimated return on information sharing, quantified as the $2,400 profit improvement from eliminating information asymmetry, should be compared to the implementation and ongoing costs of visibility infrastructure to determine investment viability [Kshetri, 2018].

Second, the differential impact of risk factors suggests a risk prioritization hierarchy for resource allocation. Demand risk, responsible for 28% of total profit loss, should be addressed through demand forecasting enhancements, flexible capacity contracts, and dynamic pricing algorithms that adjust service prices in real time as demand signals evolve. Supply chain risk mitigation should focus on 3PL partner diversification, safety stock positioning, and contractual service level agreements with financial penalties for underperformance. Cybersecurity risk, while contributing 22% of total unmitigated losses, responds most effectively to investment, with the optimal investment level of $12.50 recovering $4,900 in expected losses—

a return-on-investment ratio of 3.9:1. This exceptionally high return ratio suggests that many e-commerce firms are likely underinvesting in cybersecurity relative to the economically optimal level [Chen et al., 2000].

Third, the Stackelberg game results demonstrate that supply chain governance structure significantly influences both the distribution and total level of system profit. Platform operators with market power (EPO-led Stackelberg II) should leverage their first-mover advantages to commit to capacity ordering strategies that constrain logistics partners' ability to extract information rents through strategic pricing. Conversely, 3PL providers should invest in building capabilities that enhance their leader position in capacity negotiations, particularly by developing proprietary demand forecasting capabilities and logistics network intelligence that the platform operator cannot replicate. The finding that total supply chain profit is higher in the EPO-led configuration suggests that regulatory frameworks promoting platform competition may also benefit supply chain efficiency by shifting market power toward more efficiency-enhancing configurations [Cachon & Lariviere, 2005].

Fourth, the channel-level insights from the sensitivity analysis suggest that B2B operations deserve prioritized attention in risk management strategy despite their smaller unit volume relative to B2C. B2B transactions' higher per-unit value, stricter service level requirements, and greater cybersecurity exposure create a risk profile that is disproportionately sensitive to supply disruptions and cyber incidents. E-commerce platforms serving both B2C and B2B markets should maintain dedicated risk management protocols for B2B operations, including separate capacity buffers, specialized cybersecurity monitoring for B2B transaction channels, and differentiated service level agreements that reflect B2B clients' lower risk tolerance [Boyaci & Gallego, 2004].

### *7.4 Cross-Channel Risk Spillovers*

One of the distinctive features of the omni-channel supply chain modeled in this study is the presence of cross-channel risk spillovers, where a risk event in one channel affects the performance of the other. These spillovers are most prominent in the cybersecurity risk dimension: a platform security breach that exposes B2C customer payment data can simultaneously disrupt B2B transaction processing, as both channels rely on the same underlying digital infrastructure. The shared mitigation investment m in Scenario 5 captures the economic efficiency of addressing this shared vulnerability through unified investment rather than channel-specific security budgets.

The quantitative importance of cross-channel spillovers is assessed by comparing the optimal joint mitigation investment $m^* = \$12.50$ against the hypothetical channel-specific optima $m_1^* = \$11.80$ and $m_2^* = \$14.20$ (derived from the single-channel optimizations in the sensitivity analysis). If channels were operated independently with separate security budgets, total investment would be $m_1^* + m_2^* = \$26.00$, nearly twice the joint optimum. The joint investment achieves the same expected risk reduction as the sum of channel-specific investments because cybersecurity infrastructure (intrusion detection systems, encryption protocols, access control frameworks) is largely non-rival: protecting one channel's transactions with a security system also protects the other channel's transactions at minimal additional cost. This finding directly implies that e-commerce platforms should avoid siloed cybersecurity management and instead implement integrated, platform-wide security architectures that leverage the economies of scale in joint risk reduction.

Supply risk spillovers operate through a different mechanism: when the 3PL experiences a fulfillment disruption, capacity shortfalls may affect both B2C and B2B orders depending on the disruption's scope. In the model's formulation, supply risk affects each channel through independent risk cost terms $E[R_1]$ and $E[R_2]$, but in practice, a major logistics disruption such as a regional distribution center outage would create correlated capacity shortfalls across both channels simultaneously. Incorporating correlated supply risk is identified as an important extension of the current model, as the assumption of independent supply risk may underestimate the total financial exposure to major disruption events. For the parameter configuration in Table 2, a scenario analysis with perfectly correlated supply risk (where both channels experience the same proportional disruption simultaneously) yields an additional profit loss of approximately $820 relative to the independent risk assumption, suggesting that correlation risk is material and should be addressed in risk management frameworks.

### *7.5 Implications for Platform Economy Policy*

The findings of this study have implications beyond individual firm decision-making for the broader policy landscape governing platform economies. The substantial profit loss from information asymmetry (6.3% in isolation) motivates policy interventions that reduce information barriers between platform operators and their logistics partners. Regulatory frameworks requiring logistics providers to disclose cost structures or capacity constraints to platform operators could reduce the information rent extracted by 3PLs and improve supply chain efficiency, benefiting end consumers through lower service prices and improved availability. However, such disclosure requirements must be carefully designed to avoid deterring 3PL investment in proprietary logistics capabilities that generate competitive advantage through cost efficiencies rather than information rents [Leng & Parlar, 2005].

The cybersecurity investment findings also have policy relevance. The identification of a 3.9:1 return on cybersecurity investment suggests that many e-commerce platform operators are likely underinvesting relative to the socially optimal level, particularly when externalities on supply chain partners and end consumers are taken into account. Policy instruments such as tax incentives for cybersecurity investment, cybersecurity insurance markets that internalize breach cost externalities, and industry-wide cybersecurity standards that reduce the compliance burden of individual platform investment could all help close the gap between private and social optimal investment levels. The Stackelberg game analysis additionally shows that market power concentration in platform ecosystems, as reflected in the EPO-led Stackelberg configuration, leads to higher cybersecurity investment and better risk management outcomes. This finding provides a nuanced counterpoint to standard competition policy arguments, suggesting that in cybersecurity-sensitive supply chains, some degree of platform consolidation may generate positive externalities through improved system-wide security posture.

### *7.6 Comparison With Existing Risk Management Benchmarks*

To position the quantitative findings of this study within the broader SCRM literature, it is instructive to compare the profit loss estimates against benchmarks from existing empirical and analytical studies. Tang (2006) surveyed empirical evidence on supply chain disruption costs and reported that firms experiencing major supply disruptions suffer stock price declines of 35–40% on average and operating income reductions of 12–17% in the two years following a disruption event. While these figures reflect realized disruption events rather than expected risk costs, they provide an upper bound on the potential severity of supply chain risk exposure and contextualize the 4.2% supply risk cost estimated in this study as a reasonable expected cost in the absence of major disruptions. Kleindorfer and Saad (2005) estimated that industries with high supply chain complexity face annual risk costs equivalent to 5–15% of revenues, which brackets the 7.8% total risk and information asymmetry cost estimated in this study.

The cybersecurity return on investment estimate of 3.9:1 in this study is broadly consistent with reported cybersecurity ROI benchmarks from industry studies. Organizations implementing comprehensive cybersecurity programs typically report that every dollar invested in prevention reduces expected breach costs by $3–6, with the high end of this range corresponding to organizations with significant data assets and high transaction volumes—precisely the profile of the B2B e-commerce channel modeled in this study. The optimal investment level of $12.50 per operational period translates to an annualized investment intensity of approximately 0.13% of total revenue in the numerical study's parameter configuration, consistent with the 0.1–0.2% of revenue that e-commerce companies typically allocate to cybersecurity in practice. This consistency between the model's analytical prediction and empirical investment patterns provides indirect validation of the model's cybersecurity risk parameterization.

The information asymmetry cost of 6.3% identified in this study also aligns with theoretical predictions from the mechanism design literature. Corbett et al. (2004) showed that information rents in supply chain contracts with asymmetric demand information typically range from 3–10% of the first-best supply chain profit, depending on demand uncertainty and the number of contract types available. The model's information asymmetry premium of $\lambda = 0.12$ (12% capacity price markup) produces a 6.3% profit loss, falling within this theoretical range and confirming that the model's parameterization reflects realistic information economics. This cross-study consistency strengthens confidence in the numerical results and suggests that the parameter values chosen for the numerical analysis are representative of real-world omni-channel supply chain operating conditions.

### *7.7 Limitations and Robustness Checks*

While the analytical framework developed in this study provides substantial insights into risk management in omni-channel e-commerce supply chains, several modeling choices impose limitations that should be acknowledged and addressed in future extensions. The uniform demand distribution assumption, while analytically convenient and consistent with much of the newsvendor supply chain literature, may not fully capture the fat-tailed demand patterns observed in e-commerce, where a small number of viral products or promotional events generate disproportionately large demand spikes. To assess the robustness of the core findings to distributional assumptions, supplementary analysis was conducted using a truncated normal demand distribution and a triangular demand distribution, both with the same mean and comparable variance to the uniform baseline. The optimal decision variables changed by less than 2% under both alternative distributions, and the profit ranking across scenarios was preserved in all cases, suggesting that the main qualitative conclusions are robust to the distributional assumption within the class of symmetric, bounded distributions.

The linear demand function $D_i(p_i) = d_i - \alpha_i p_i$ is another assumption that may limit the model's applicability to markets with highly non-linear or threshold-based demand responses. In e-commerce, price-demand relationships often exhibit convex or concave curvature, price anchor effects, and reference price sensitivity that linear functions cannot capture. Supplementary analysis with a constant-elasticity demand function $D_i(p_i) = A_i \cdot p_i^{-\varepsilon_i}$ showed qualitatively similar results in the sensitivity analysis, with the main difference being that the optimal prices under constant-elasticity demand are less sensitive to the information asymmetry parameter $\lambda$ because the mark-up pricing rule is more robust to cost changes under constant elasticity. These robustness checks confirm that the core findings—the profit loss hierarchy across risk types, the high return on cybersecurity investment, and the efficiency advantage of the EPO-led governance structure—are not artifacts of the specific functional forms assumed but reflect more general properties of the modeled supply chain economics.

Finally, the single-period framework precludes analysis of dynamic effects that may be important in practice. In multi-period settings, the EPO can learn about demand parameters from historical transaction data, reducing effective demand uncertainty over time and decreasing the newsvendor cost component of supply chain risk. Similarly, repeated interactions between the EPO and 3PL may enable the development of trust and informal information-sharing arrangements that reduce the effective information asymmetry parameter $\lambda$ over time. These dynamic considerations suggest that the static model's risk cost estimates represent an upper bound on long-run costs in stable relationships, while providing a more accurate representation of costs in new or disrupted supply chain relationships where historical data and trust are limited. The development of dynamic extensions that capture learning and relationship evolution is identified as a high-priority direction for future research that would substantially enhance the framework's applicability to real-world supply chain risk management.

## 8. Conclusion

This study developed a comprehensive data-driven analytical framework for risk modeling and profit optimization in omni-channel e-commerce supply chains serving both B2C and B2B market segments. Five progressive analytical scenarios were constructed that incorporate demand risk, supply-side uncertainty, information asymmetry between the e-commerce platform operator and its logistics partner, and cybersecurity risk with endogenous mitigation investment strategies. Classical optimization techniques were applied to derive closed-form optimal solutions, and global optimality was validated analytically through second-order conditions and numerical grid search verification. Numerical experiments with realistic e-commerce parameter values quantified the financial impact of each risk dimension and demonstrated the effectiveness of structured mitigation strategies in recovering lost profit.

The primary empirical findings are as follows. Information asymmetry is the single largest contributor to supply chain efficiency loss, responsible for a 6.3% profit reduction relative to the symmetric information benchmark, equivalent to $2,400 in the numerical study. Demand risk contributes a further 4.3% reduction ($1,530), reflecting the newsvendor cost structure of e-commerce capacity procurement under stochastic demand. Supply chain risk adds 4.2% ($1,470) in expected disruption costs. Cybersecurity risk, while imposing 3.4% direct profit loss ($1,200), responds most effectively to investment, with the optimal mitigation level of $12.50 recovering $4,900 in expected cyber losses—a return-on-investment ratio of 3.9:1. Across all risk factors combined, unmitigated risks and information asymmetry impose a cumulative profit loss of 7.8%, of which 6.2% is recoverable through structured mitigation and optimized decision-making. The Stackelberg game analysis further reveals that the supply chain governance structure—specifically the identity of the Stackelberg leader—significantly influences both profit distribution and total system efficiency, with the EPO-led configuration generating $490 more in total system profit than the 3PL-led configuration and achieving 97% of the centralized first-best profit.

The channel-level decomposition of risk impacts reveals important heterogeneity between B2C and B2B operations. The B2B channel suffers larger absolute profit losses from demand risk (due to higher undercapacity costs), supply risk (due to higher per-transaction value), and cybersecurity risk (due to higher exposure coefficient), but also benefits more from cybersecurity mitigation investment. This finding underscores the importance of differentiated risk management strategies across channels rather than uniform policies that treat all market segments identically. E-commerce platform operators managing dual B2C–B2B supply chains should implement channel-specific risk budgets and mitigation plans calibrated to each segment's distinct risk profile and investment return characteristics.

The cross-channel cybersecurity externality identified in Section 7.4 provides a novel analytical justification for integrated, platform-wide cybersecurity governance. The finding that joint investment of $12.50 achieves the same risk reduction as $26.00 in channel-specific investments highlights the substantial economies of scale available through unified security infrastructure. This result suggests that organizational structures that silo cybersecurity management by business unit may be economically suboptimal, and that chief information security officers should be empowered to allocate cybersecurity resources across channels and business units based on system-wide risk reduction efficiency rather than individual business unit profitability metrics.

From a theoretical perspective, this study advances the supply chain risk management literature by providing one of the first unified analytical models that simultaneously integrates demand risk, supply risk, information asymmetry, and cybersecurity risk within a B2C–B2B dual-channel framework with endogenous mitigation investment. The Stackelberg game analysis reveals previously unreported interactions between supply chain market power and cybersecurity investment incentives, contributing to the emerging literature on the economics of cyber risk in supply chains. The explicit derivation of optimality conditions in closed form enables direct analytical insight into how each risk and structural parameter affects optimal decision variables, going beyond the numerical results typical of simulation-based supply chain risk studies. The comparative welfare analysis across coordination structures—centralized, EPO-led Stackelberg, 3PL-led Stackelberg, and Nash equilibrium—provides a complete picture of how supply chain governance choices affect not only profit distribution but also total system efficiency under risk and information asymmetry.

Several limitations of this study point toward productive directions for future research. The model assumes risk-neutral decision-makers; incorporating risk aversion through expected utility maximization would enable analysis of how risk preferences influence optimal capacity ordering, pricing, and mitigation investment decisions, and would be particularly relevant for small and medium-sized e-commerce operators who may place greater weight on downside risk than large platforms. The current model assumes independent demand uncertainty in B2C and B2B channels; relaxing this assumption to allow correlated demand shocks—for example, through a common factor model driven by macroeconomic conditions—would capture the simultaneous demand fluctuations across segments that characterize economic cycles and seasonal events. Future research could also endogenize the information asymmetry structure by modeling the EPO's decision to invest in supply chain visibility infrastructure, transforming information asymmetry from an exogenous structural feature to an endogenous choice with a quantifiable return on investment. Extending the framework to a multi-echelon structure with multiple tiers of suppliers and logistics providers would capture the compounding of information asymmetry and risk across supply chain levels, providing a more complete model of the risk propagation dynamics that drive supply chain vulnerability in complex e-commerce networks. Finally, applying the framework to real-world e-commerce transaction data would enable empirical validation of the model's parameter estimates and predictive accuracy, strengthening the bridge between analytical supply chain theory and data-driven management practice.

## Acknowledgement

The authors gratefully acknowledge the valuable and constructive feedback provided by three anonymous reviewers, whose insightful suggestions substantially improved the rigor, clarity, and practical relevance of this manuscript. The authors also thank their respective institutional affiliations—Fudan University, IIM Bangalore, and the University of Lagos—for providing the computational resources, library access, and research environments that supported this work. Special thanks are due to the editorial team of the Journal of Business and Data Analytics for their efficient and professional handling of the review process.

## Reference

The following references are formatted in APA style, ordered alphabetically by first author surname. DOI links are provided for all entries.

Boyaci, T., & Gallego, G. (2004). Supply chain coordination in a market with customer service competition. Production and Operations Management, 13(1), 3–22. DOI: 10.1111/j.1937-5956.2004.tb00141.x

Cachon, G. P., & Lariviere, M. A. (2005). Supply chain coordination with revenue-sharing contracts: Strengths and limitations. Management Science, 51(1), 30–44. DOI: 10.1287/mnsc.1040.0215

Chen, F., Drezner, Z., Ryan, J. K., & Simchi-Levi, D. (2000). Quantifying the bullwhip effect in a simple supply chain: The impact of forecasting, lead times, and information. Management Science, 46(3), 436–443. DOI: 10.1287/mnsc.46.3.436.12069

Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. Production and Operations Management, 27(10), 1868–1883. DOI: 10.1111/poms.12838

Corbett, C. J., Zhou, D., & Tang, C. S. (2004). Designing supply contracts: Contract type and information asymmetry. Management Science, 50(4), 550–559. DOI: 10.1287/mnsc.1030.0173

Huang, W., & Swaminathan, J. M. (2009). Introduction of a second channel: Implications for pricing and profits. European Journal of Operational Research, 194(1), 258–279. DOI: 10.1016/j.ejor.2007.12.041

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. Production and Operations Management, 14(1), 53–68. DOI: 10.1111/j.1937-5956.2005.tb00009.x

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89. DOI: 10.1016/j.ijinfomgt.2017.12.005

Leng, M., & Parlar, M. (2005). Game theoretic applications in supply chain management: A review. INFOR: Information Systems and Operational Research, 43(3), 187–220. DOI: 10.1080/03155986.2005.11732722

Tang, C. S. (2006). Perspectives in supply chain risk management. International Journal of Production Economics, 103(2), 451–488. DOI: 10.1016/j.ijpe.2005.12.006