



## STRATEGIC RESILIENCE INVESTMENT FOR A METAVERSE SUPPLY CHAIN

YARU HAO , BAOGUI XIN\*  AND WEI PENG

**Abstract.** Technological advances enable firms to operate virtually through the metaverse, yet data security risks threaten platform resilience. This study examines the resilience-cost trade-off in metaverse supply chains using a risk-attitude-based decision model. Combining mean-variance theory and Stackelberg game analysis, we derive optimal pricing and resilience strategies, validated with *Meta* case data. We find that: (i) Consumer data security concerns and hacking probabilities suppress product demand through risk disutility, prompting supply chain adjustments in resilience investments and pricing strategies. (ii) Platform risk aversion simultaneously reduces both resilience investments and pricing levels, whereas firm risk aversion operates solely through price channels, with Pareto optimal equilibrium achievable under risk-neutral conditions. (iii) Incorporating digital asset losses enhances platform resilience investments and firm profit. Interestingly, platforms derive greater benefits from higher resilience cost coefficients and digital asset losses. Further analysis reveals that a threshold effect of consumer data security risk may impose an upper bound on platform resilience investments, while firm risk attitude and consumer trust jointly shape resilience strategies for incumbent platforms in dual-platform competitive environments. Our findings provide new insights on how to strategically enhance platform resilience, as well as guidance on how governments can better encourage the security of the metaverse.

**Mathematics Subject Classification.** 90B25, 91A35.

Received April 16, 2024. Accepted July 19, 2025.

### 1. INTRODUCTION

With the development of technology and evolving consumer demand, the metaverse has shown profound commercial value and will completely change the retail format [1]. Within an interactive virtual space, consumers can travel through the metaverse *via* digital avatars and interact with other avatars [2]. The employment of immersive technology within the metaverse enables users to have a multidimensional experience [3], surpassing the limitations of time and space. Related research has shown that consumers spend significantly more time shopping in immersive environments than in traditional online and offline channels, significantly increasing the purchase potential<sup>1</sup>. Presently, a number of distinguished companies, such as *Nike* and *Gucci*, have launched

---

*Keywords.* Metaverse retail, platform resilience, digital asset losses, risk aversion, data security.

College of Economics and Management, Shandong University of Science and Technology, Qingdao 266590, P.R. China.

\*Corresponding author: [xin@sdust.edu.cn](mailto:xin@sdust.edu.cn).

<sup>1</sup> <https://venturebeat.com/datadecisionmakers/metaverse-shopping-retailers-new-reality/>.

© The authors. Published by EDP Sciences, ROADEF, SMAI 2025

branded products in the metaverse. The metaverse has become an essential element of marketing strategies for retailers and brand companies [4].

While the metaverse enhances the shopping experience for consumers due to its unique features, capturing and sharing consumer behavior digitally within the metaverse raises data security complications [5]. For instance, the *Meta* (previously known as *Facebook*) once fell victim to a hack which brought the personal data of about 500 million users to light. Following this event, *Meta*'s share price fell to its lowest point, wiping out \$134 billion in market value<sup>2</sup>. To prevent similar incidents from occurring, metaverse platforms should improve security systems to cope with hacker attacks, known as platform resilience. Platform resilience is the capability of a platform to anticipate and withstand external attacks, swiftly recovering to its initial state [6]. To ensure the metaverse's sustainable growth, the platform is actively developing protection technologies, strengthening its resilience and security to achieve operational excellence. However, resilience investment inevitably results in additional costs, which heightens the financial pressure [7]. Continuously maintaining current security systems increases the possibility of an attack and potentially substantial digital asset losses in the future. The crucial challenge for metaverse platforms is to strike a balance between the investment costs, enhanced resilience and potential loss of digital assets.

As an emerging economy, notably, the metaverse faces significant uncertainty. The unpredictable market demand and sustained high investment in the initial construction process increase operational risks [8]. For the participants in the metaverse, they need to consider their own risk tolerance when making relevant investment and pricing decisions [9]. The impact of risk attitudes on decision-making is stronger if the participants are more sensitive to risk perception [10]. Hence, it is essential to consider the risk averse behavior of supply chain members while making relevant decisions under uncertain demand. Based on the above analysis, this paper explores the following three major issues from a risk aversion perspective:

- (i) What are the most effective resilience investment and pricing strategies for the metaverse platform and firm respectively? What is the connection between consumer data security concerns and the optimal decisions?
- (ii) How does the loss of digital assets affect the efficiency of supply chain systems? Could the platform resilience be improved?
- (iii) To what extent do the risk attitudes of supply chain members affect their strategic decision-making and which attitude proves more advantageous for the system?

To address the questions outlined earlier, we first construct a basic model that includes a metaverse platform, a metaverse firm, and consumers. Through adjusting the risk attitudes of the members, we identify the optimal resilience investment and pricing decision for the metaverse members. Secondly, we include digital asset losses in our analytical framework to derive the Stackelberg game equilibrium solution for the supply chain members. Following a comparative analysis, the ideal conditional threshold for the supply chain system is obtained. Lastly, we use *Meta* for case analysis, to validate the robustness of the conclusions. The framework is shown in Figure 1.

The rest of the paper is organized as follows. Section 2 reviews the relevant literature. Section 3 presents the model assumptions and performs equilibrium solutions. Section 4 analyzes and discusses the model. Section 5 uses *Meta*'s data for case analysis. Section 6 concludes.

## 2. LITERATURE REVIEW

### 2.1. Metaverse retail and privacy protection

Through the synergistic integration of technologies such as virtual reality (VR), augmented reality (AR), and artificial intelligence (AI) [11], the metaverse is driving a shift in business models, giving rise to novel consumption scenarios like virtual tourism [12] and immersive retail [13]. In retail, metaverse technologies enable consumers to interact with products and engage in virtual try-ons through avatars, with their immersive nature significantly reshaping customer experience [4, 14, 15]. Existing research has examined the metaverse's economic

<sup>2</sup> <https://www.cbsnews.com/news/facebook-stock-price-recovers-all-134-billion-lost-in-after-cambridge-analytica-datascandal/>.

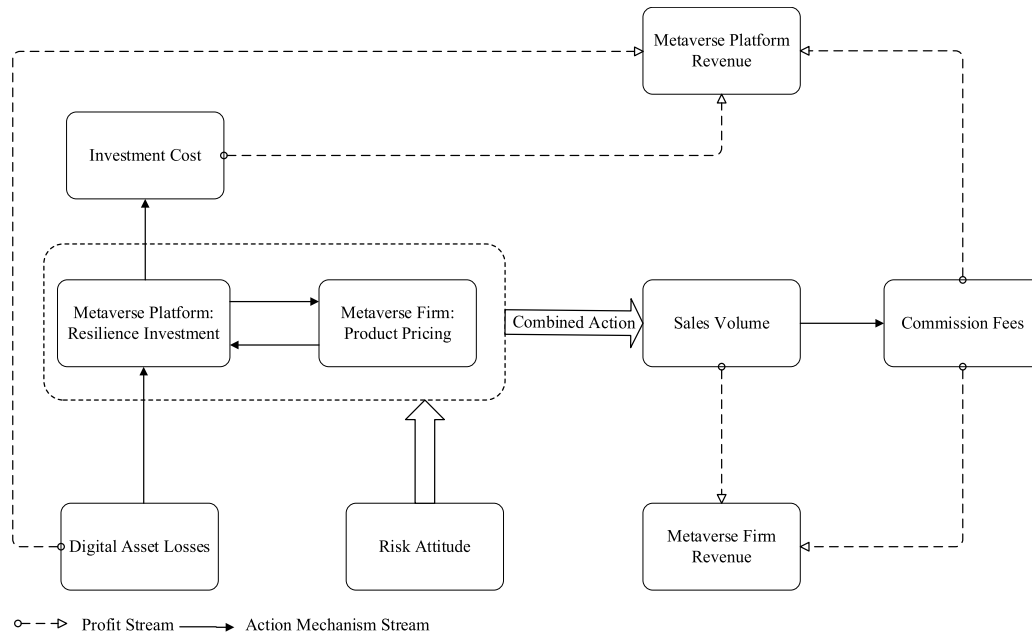


FIGURE 1. Research framework.

potential from a behavioral economics perspective, with consumer purchase decision mechanisms emerging as a core topic. Grounded in self-expansion theory, Ahn *et al.* [16] demonstrated that perceived interactivity positively influences virtual product purchase intention by enhancing the perception of expanded self. Payal *et al.* [17] further revealed that virtual interactions indirectly drive real-world consumption conversion by strengthening brand attachment and trust. Scholars also emphasize the metaverse's inherent capacity to enhance user interactivity [18], with technology-enabled user-generated content (UGC) and presence enhancement mechanisms proven to boost engagement [19].

While the metaverse offers substantial commercial benefits, extant research has not adequately addressed data security risks within its ecosystem [20]. Studies identify identity authentication vulnerabilities, access control flaws, and session management failures as primary threats to privacy security [21], with flawed identity mechanisms directly leading to user information leakage and identity theft. Gupta *et al.* [22] proposed self-sovereign identity management to mitigate platform tracking, yet its decentralized nature may hinder the tracing and accountability of user misconduct [23]. Meanwhile, the metaverse's personalized service optimization relying on fine-grained user data creates a structural contradiction with user privacy protection needs [24]. Cross-platform interconnection of multimodal sensor data from avatars – such as biometrics and behavioral trajectories – exacerbates privacy leakage risks [25], underscoring the need for collaborative technical ethics and data governance.

Addressing this contradiction, this paper proposes from a technical governance perspective that enhancing technical resilience investments in metaverse platforms can effectively defend against hacker attacks and reduce data breach risks. Analysis based on a supply chain game model shows that platform technical investments can share costs through commission compensation mechanisms, while improved resilience generates demand increments. This bidirectional synergy drives the construction of a secure metaverse environment. Table 1 summarizes the research gaps relative to existing literature.

TABLE 1. Metaverse retailing and privacy protection.

Paper	Research focus	Security and privacy	Main methods
Shin and Kang [12]	The experience value of metaverse travel and both virtual and actual travel intentions	No	Interview; Questionnaire
Chakraborty et al. [13]	Consumers' continuance intention towards metaverse-based virtual stores	No	Grounded theory; Structural equation modelling
Ahn et al. [16]	Purchase intention of virtual products	No	Questionnaire
Payal et al. [17]	The spillover effect of brand participation in the metaverse on the real-world	No	Experimental study
Dwivedi et al. [20]	Opportunities and challenges in the metaverse	Yes	Multi-perspective approach
Otoum et al. [21]	The security and privacy challenges of using machine learning models in the metaverse	Yes	Systematic literature review
Gupta et al. [22]	Different aspects and challenges that need to be addressed in the future metaverse	Yes	Multi-perspective approach
Alkaeed et al. [24]	Privacy challenges and solutions in the metaverse	Yes	Systematic literature review
<b>Our Study</b>	<b>Resilience investment of metaverse platform reduces security risks</b>	<b>Yes</b>	<b>Game theory</b>

## 2.2. Data security and supply chain resilience

### 2.2.1. The impact of data security on supply chains

Against the backdrop of technology-driven supply chain digital transformation, data security issues merit critical attention [26,27]. Research demonstrates that data breaches and cyberattacks across supply chain nodes destabilize systems through dual pathways: First, consumer trust plummets due to privacy violations [28], reducing purchase intent and repurchase rates [29–31], which in turn weakens firms' market competitiveness [32]. Second, eroded corporate reputation and diminished brand value [33,34] can trigger a chain effect of supply chain disruptions [35]. Additionally, surging compliance costs from data security incidents [36] not only squeeze profit margins [37] but also exert persistent negative impacts on stock price volatility [38]. While extant studies primarily focus on empirical analyses of data breach impacts, few explore how security technology integration can optimize supply chain resilience architectures.

### 2.2.2. Supply chain resilience

The academic community defines supply chain resilience as the ability to withstand disruptions and recover to a stable or improved state [39]. Early research in this field identified key resilience drivers, including market sensitiveness [40], adaptive capability [6] and risk management infrastructure [41]. Building on these frameworks, recent studies have systematically explored diverse resilience-enhancing pathways – from traditional governance tools like collaborative contract design [42] to innovative applications of emerging digital technologies. Technologies such as blockchain [43], artificial intelligence [44], and distributed ledger technology [45] have been validated to significantly improve supply chain transparency and risk resistance, while enterprise resource planning (ERP) systems enhance resilience by reducing process complexity [46]. Institutionally, governments incentivize security practices through data regulatory constraints [47,48] and punitive regulations [49], whereas price contract design among supply chain members [50] provides market-driven incentives for security investments. However, existing research remains largely confined to traditional supply chain contexts, with limited

TABLE 2. Data security and supply chain resilience.

Paper	Research theme	Security	Resilience	Main methods
Choi <i>et al.</i> [31]	Privacy leakage remediation and user behavior	Yes	No	Questionnaire
Chan and Palmeira [34]	Brand apology and consumer response	Yes	No	Experimental study
Nijssen <i>et al.</i> [33]	Customer privacy and supplier profitability	Yes	No	Questionnaire
Luo and Choi [49]	Cyber-security in e-commerce supply chains	Yes	No	Game theory
Uddin <i>et al.</i> [27]	Data breach protection framework	Yes	No	Systematic literature review
Alharbi and Alkhalifah [28]	The security factors of online comments and website trust	Yes	No	Questionnaire
Laradi <i>et al.</i> [32]	Social media purchase intention	Yes	No	Questionnaire
Kim <i>et al.</i> [47]	Regulatory laws and the incidence of company security incidents	Yes	No	Difference-in-differences
Soni <i>et al.</i> [39]	Measuring supply chain resilience	No	Yes	Deterministic modeling approach
Ambulkar <i>et al.</i> [41]	Supply chain interruption and enterprise response	No	Yes	Questionnaire
Modgil <i>et al.</i> [44]	AI technologies and extreme disruptions	No	Yes	Grounded theory
Sadeghi <i>et al.</i> [6]	Supply chain cyber-resilience	No	Yes	Experimental study
Narwane <i>et al.</i> [43]	Supply chain risks	Yes	Yes	Grey-DEMATEL
Sadeghi <i>et al.</i> [46]	Enterprise resource planning and supply chain resilience	Yes	Yes	Empirical research
<b>Our Study</b>	<b>Data breach and resilience investment of the metaverse platform</b>	<b>Yes</b>	<b>Yes</b>	<b>Game theory</b>

exploration of platform security mechanisms, risk-sharing strategies, and resilience investment games within emerging digital ecosystems like the metaverse.

As outlined in Table 2, this study takes data security in metaverse platforms as its entry point, examining how digital asset losses influence platform resilience strategies. By integrating game theory models and dynamic optimization frameworks, it not only expands the applicability of supply chain resilience theory but also offers a novel analytical paradigm for risk governance in phygital economic systems.

### 2.3. Supply chain management considering risk aversion

Against the backdrop of accelerated digital and intelligent transformation, research on the risk preferences of decision-makers in supply chain risk management has emerged as a core topic in operations management, establishing a robust theoretical framework [51–53]. Academic research on risk measurement methods has evolved along multidimensional paths, with current mainstream paradigms focusing on three approaches: value-at-risk (VaR) [54–56], conditional value-at-risk (CVaR) [57–59], and mean-variance (MV) [60, 61]. The MV approach,

TABLE 3. Risk avoidance supply chain using mean-variance method.

Paper	Supply chain theme	Risk aversion party	Decision
Wei and Choi [65]	Wholesale pricing and profit-sharing schemes	Retailer	Order quantity
Chiu <i>et al.</i> [52]	Channel coordination; Target sales rebate (TSR) contracts	Retailer	Order quantity
Li <i>et al.</i> [66]	Fast fashion supply chains; Returns policy	Retailer	Order quantity; Wholesale price; Buyback price
Liu <i>et al.</i> [67]	Dual-channel supply chain; Asymmetric information	Manufacturer; Retailer	Wholesale price; Retail price
Zhuo <i>et al.</i> [68]	Option contracts; Supply chain coordination	Retailer; Supplier	Option price; Exercise price; Order quantity
Wen and Siqin [69]	Quality uncertainty in sharing platforms	Platform; Consumers	Product quality level; Product price
Yang <i>et al.</i> [60]	Wholesale price contracts; Financing equilibrium	Retailer; Supplier	Wholesale price; Order quantity
Zhang and Xu [70]	Platform goodwill; Agency contracts with incentive mechanism	Supplier	Product price; Quality effort; Service effort
Chen <i>et al.</i> [71]	Demand information sharing	Supplier	Wholesale price; Selling prices
Zhou <i>et al.</i> [63]	WEEE closed-loop supply chain	Manufacturer	Unit wholesale price of EEE; Unit retail price of EEE; Return rate of WEEE
<b>Our Study</b>	<b>Metaverse supply chain; Data asset losses</b>	<b>Platform; Firm</b>	<b>Product prices; Resilience investment</b>

**Notes.** WEEE (waste electrical and electronic equipment); EEE (electrical and electronic equipment).

prized for its mathematical tractability and economic interpretability, has demonstrated significant advantages in supply chain coordination research, extending its applications from traditional supply chains to emerging domains such as smart supply chains [9], green supply chains [62], and closed-loop supply chains [63, 64].

Table 3 systematically outlines the research progress of the MV approach in risk-averse supply chains, primarily unfolding along two dimensions: pricing strategy optimization and coordination mechanism design. Along the pricing dimension, Liu *et al.* [67] analyzed the impact of risk-averse behavior on members' pricing strategies within a dual-channel supply chain framework. Wen and Siqin [69] explored quality-price decision mechanisms for sharing economy platforms, while Yang *et al.* [60] examined wholesale price contracts and optimal financing models under risk constraints for capital-constrained retailers. Chen *et al.* [71] revealed the interactive effects of information precision and risk aversion on supply chain pricing, and Zhou *et al.* [63] confirmed a positive dynamic association between manufacturers' risk aversion levels and wholesale/retail prices of waste electrical and electronic equipment (WEEE) in closed-loop scenarios. In terms of coordination mechanism design, scholars have proposed diverse solutions [66], with contract design dominating the landscape. Studies have systematically validated the risk-mitigation efficacy of tools such as target sales rebate (TSR) contracts [52], TSR contracts with fixed order quantity (TSR-FOQ) [53], option contracts [68], wholesale price contracts [60], and agency contracts with incentive mechanisms [70].

Notably, extant research has not sufficiently explored the role of risk attitudes in metaverse supply chain optimization – specifically, the interactive effects between platform resilience investments and risk-averse behaviors. This study constructs a metaverse supply chain model incorporating risk attitudes, aiming to investigate how decision-makers' risk preferences influence platform security investment strategies and provide theoretical support for resilience building in intelligent supply chains.

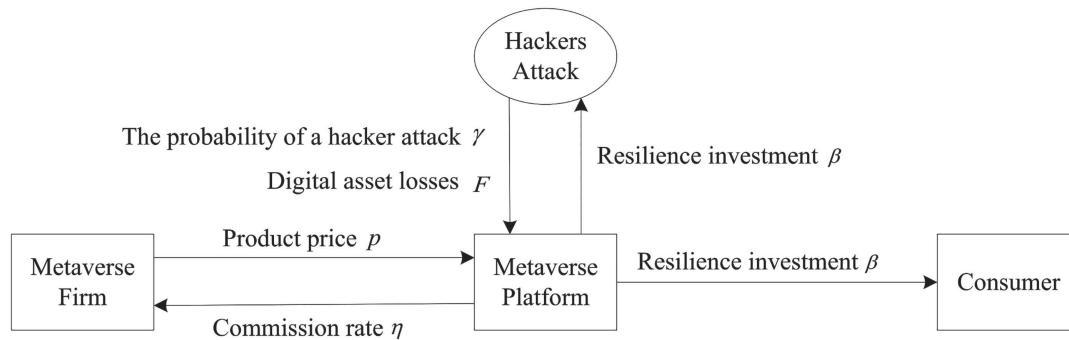


FIGURE 2. Metaverse supply chain structure.

## 2.4. Our contribution

This study synthesizes three theoretical streams: (i) privacy protection in metaverse retail scenarios; (ii) data security and supply chain resilience construction; and (iii) risk-averse supply chain decision-making within a mean-variance framework. Building on this foundation, we construct a dynamic game model involving multi-party decision-makers, systematically analyzing how risk attitude parameters influence both pricing strategies and resilience investments. By characterizing the dual impacts of risk preferences on supply chain optimization under demand uncertainty, the research reveals critical pathways for operational resilience. Specifically, the model innovatively incorporates a digital asset loss variable to quantify the security-enhancing effects of resilience investments on metaverse platforms. The findings not only provide theoretical foundations for strategic decisions by supply chain members but also offer quantifiable policy tools for regulatory authorities through parameter sensitivity analysis, enabling the formulation of science-based security standards for metaverse ecosystems.

## 3. PROBLEM DESCRIPTION AND MODEL

### 3.1. Problem description

This study constructs a two-tier supply chain system comprising a metaverse platform and firm (platform tenants), focusing on the platform's security resilience investment strategies and firm's pricing decisions amid data breach risks. In metaverse environments, the multi-dimensional storage and transmission of data amplify hacking risks [25]. The platform must invest in technical resilience to mitigate these risks, while firms access platform services by paying a commission fee. The research aims to uncover how heterogeneous risk attitudes shape the interactive decision-making between the two parties, with the supply chain structure illustrated in Figure 2.

### 3.2. Model assumptions

Table 4 summarizes the definitions of key parameters, with the following specific assumptions:

#### 3.2.1. Game structure specification

- (i) Stackelberg leadership: Adopting a sequential game framework, the platform acts as the leader and firms act as followers, reflecting the platform's real-world dominance in setting technical standards and security protocols [72].
- (ii) Complete information: Both parties fully observe each other's cost parameters and market demand functions to ensure the existence of game equilibrium solutions.

TABLE 4. Notations.

Notation	Definition	Notation	Definition
$p$	The price of products sold by metaverse firms.	$r$	Metaverse firm.
$\beta$	Resilience investment in metaverse platforms.	$sc$	Metaverse supply chain system.
$c$	The construction cost of immersion generated by unit metaverse transactions.	<b>Superscript</b>	
$k$	Cost coefficient of metaverse platform resilience investment.	$N$	Ignore digital asset losses.
$\gamma$	The probability of a hacker attack.	$Y$	Consider digital asset losses.
$\alpha$	Consumer data security concern coefficient.	$A$	The risk aversion of all members.
$b$	The benefits of immersion for consumers.	$R$	Firm risk aversion.
$\eta$	The commission ratio extracted by the metaverse platform for transactions.	$O$	Platform risk aversion.
$F$	Data asset losses caused by hacker attacks on the metaverse platform.	$M$	Risk neutrality.
$\varepsilon$	Stochastic demand, meeting $\varepsilon \sim N(0, \sigma^2)$ .	<b>Model summary</b>	
$\sigma$	Stochastic demand standard deviation.	$MN$	$\lambda_o = \lambda_r = 0$ and $F = 0$ .
$\lambda_i$	Risk aversion coefficient, where $i \in (o, r)$ .	$RN$	$\lambda_o = 0, \lambda_r > 0$ and $F = 0$ .
$\pi_i$	The random returns of each member in the supply chain system, where $i \in (o, r, sc)$ .	$ON$	$\lambda_o > 0, \lambda_r = 0$ and $F = 0$ .
$E(\pi_i)$	The expectation of random returns for each member in a supply chain system, where $i \in (o, r, sc)$ .	$AN$	$\lambda_o > 0, \lambda_r > 0$ and $F = 0$ .
$Var(\pi_i)$	The variance of random returns for each member in a supply chain system, where $i \in (o, r)$ .	$MY$	$\lambda_o = \lambda_r = 0$ and $F > 0$ .
$U(\pi_i)$	The utility of random returns for each member in a supply chain system, where $i \in (o, r)$ .	$RY$	$\lambda_o = 0, \lambda_r > 0$ and $F > 0$ .
<b>Subscript</b>		$OY$	$\lambda_o > 0, \lambda_r = 0$ and $F > 0$ .
$o$	Metaverse platform.	$AY$	$\lambda_o > 0, \lambda_r > 0$ and $F > 0$ .

(iii) Decision sequence: As the leader, the platform first determines its resilience investment level  $\beta$ ; upon observing  $\beta$ , the firm sets the retail price  $p$ . After the transaction is completed, the firm pays commission according to the sales ratio  $\eta$ .

3.2.2. Operational environment assumptions

- (i) Production cost: The firm’s per-unit production cost is normalized to zero to focus on strategic decision-making and risk attitude analysis.
- (ii) Commission mechanism: Firms pay the platform a commission rate  $\eta \in (0, 1)$  based on sales revenue.
- (iii) Immersion cost: Metaverse immersion directly impacts consumer experience and purchase intent [2]. We assume the platform incurs a constant per-unit immersion cost  $c$ .
- (iv) Attack probability and resilience investment: The probability of a hacker attack is  $\gamma \in (0, 1)$ . The platform invests resilience effort  $\beta$  mitigate risks, where  $\gamma\beta$  represents the degree of successful attack defense, and  $\gamma(1 - \beta)$  denotes the probability of defense failure [49]. Resilience investment incurs a cost  $\frac{1}{2}k\beta^2$ , where  $k > 0$  represents the cost coefficient of resilience investment. This setting aligns with the characteristic of increasing marginal costs for safety enhancement and has been widely adopted in numerous studies [73, 74].
- (v) Digital asset losses: When a defense failure occurs, the platform may incur digital asset losses  $F \geq 0$ . Based on this, we propose two models: Model  $N$  that ignores digital asset losses and Model  $Y$  that considers digital asset losses.

### 3.2.3. Demand function

Based on consumer utility theory, a linear demand function is specified as:

$$d = \varepsilon + \int_{p+\alpha\gamma(1-\beta)-b}^1 f(v) dv = 1 - p - \alpha\gamma(1 - \beta) + b + \varepsilon. \quad (1)$$

The specific composition of this equation is as follows:

- (i) Base utility: Consumers' heterogeneous valuation of the product is denoted as  $v \sim U[0, 1]$ , with a probability density function  $f(v)$ .
- (ii) Price disutility: Negative utility from the payment price  $p$ .
- (iii) Security risk disutility: If the platform fails to defend against the attack (with probability  $\gamma(1 - \beta)$ ), consumers experience a disutility of  $\alpha\gamma(1 - \beta)$  due to data breaches, where  $\alpha > 0$  represents the consumer's security concern coefficient.
- (iv) Immersion utility: The platform enhances user experience through immersion-building efforts [75,76], resulting in a demand increment of  $b$ .
- (v) Market uncertainty: The market demand exhibits uncertainty  $\varepsilon \sim N(0, \sigma^2)$  to reflect the emerging characteristics of the metaverse domain.

### 3.2.4. Mean-Variance risk measurement

- (i) Risk utility specification.

The study employs the mean-variance model to quantify risk-averse preferences [65]. For a risk-averse platform, the utility function is:

$$U(\pi_o) = E(\pi_o) - \lambda_o \sqrt{Var(\pi_o)} \quad (2)$$

where  $Var(\pi_o) = E[\pi_o - E(\pi_o)]^2$  and  $\pi_o$  is the platform's random profit;  $E(\pi_o)$  and  $Var(\pi_o)$  denote the profit's expected value and variance;  $\lambda_o \geq 0$  is the platform's risk aversion parameter ( $\lambda_o = 0$  for risk neutrality,  $\lambda_o > 0$  for risk aversion, with higher values indicating stronger aversion).

Similarly, the firm's utility function under risk aversion is:

$$U(\pi_r) = E(\pi_r) - \lambda_r \sqrt{Var(\pi_r)} \quad (3)$$

where  $Var(\pi_r) = E[\pi_r - E(\pi_r)]^2$  and  $\lambda_r \geq 0$  is the firm's risk aversion parameter, treated as an exogenous variable consistent with mean-variance model assumptions.

- (ii) Risk attitude combinations.

To account for potential asymmetries in participants' risk attitudes, we systematically examine all possible combinations of risk profiles to analyze decision-making variations:

Scenario 1: Both platform and firm are risk-neutral (superscript  $M$ ).

Scenario 2: Platform risk-averse, firm risk-neutral (superscript  $O$ ).

Scenario 3: Firm risk-averse, platform risk-neutral (superscript  $R$ ).

Scenario 4: Both risk-averse (superscript  $A$ ).

By integrating the four risk-attitude combinations with two digital asset loss models ( $N/Y$ ), we develop a comprehensive framework comprising eight analytical scenarios (see Tab. 4). This systematic approach enables precise identification and isolation of decision-making impacts arising from heterogeneous risk preferences across different market participants.

### 3.2.5. Game dynamics and model interaction

By integrating the mean-variance framework with the Stackelberg game, the study analyzes dynamic decision-making under risk attitude disparities. As the Stackelberg leader, the platform first chooses resilience investment  $\beta$  to maximize its mean-variance utility (see Eq. (2)), with risk aversion quantified through the variance penalty

term (*i.e.*,  $-\lambda_o\sqrt{Var(\pi_o)}$ ). The firm, as a follower, sets price  $p$  based on  $\beta$ , with its risk attitude reflected in equation (3). This sequential game structure translates risk attitudes into quantifiable strategic differences, capturing the forward-looking nature of the platform’s resilience investments while reflecting the firm’s market response flexibility through pricing adjustments. Ultimately, the equilibrium solution is obtained through backward induction. The core of model coupling lies in the platform’s initial decisions directly shaping the firm’s market environment through the demand function (*i.e.*, Eq. (1)), while the firm’s pricing feedback reacts on the platform’s profits, forming a bidirectional dynamic equilibrium.

### 3.3. Equilibrium characteristics

Firstly, in the case of all members being risk averse, we conduct an equilibrium analysis using the presence of data asset losses as an example, *i.e.*,  $AY$  model. The random returns of the platform and the firm are given by

$$\begin{aligned} \pi_o^{AY} &= (\eta p - c)d - F\gamma(1 - \beta) - \frac{k\beta^2}{2} \\ &= (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b + \varepsilon) - F\gamma(1 - \beta) - \frac{k\beta^2}{2} \end{aligned} \tag{4}$$

$$\begin{aligned} \pi_r^{AY} &= (1 - \eta)pd \\ &= (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b + \varepsilon). \end{aligned} \tag{5}$$

We then can obtain the target decision-making issues for the platform and the firm:

$$\begin{aligned} \max_{\beta} U(\pi_o^{AY}) &= E(\pi_o^{AY}) - \lambda_o\sqrt{Var(\pi_o^{AY})} \\ &= (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - F\gamma(1 - \beta) - \frac{k\beta^2}{2} - \lambda_o(\eta p - c)\sigma \end{aligned} \tag{6}$$

$$\begin{aligned} \max_p U(\pi_r^{AY}) &= E(\pi_r^{AY}) - \lambda_r\sqrt{Var(\pi_r^{AY})} \\ &= (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b) - \lambda_r(1 - \eta)p\sigma. \end{aligned} \tag{7}$$

By adjusting the risk aversion coefficient  $\lambda_i$ , the objective functions of supply chain members can be obtained under different risk attitudes. Additionally, while ignoring data asset losses, the decision function of supply chain members can be analyzed using the parameter  $F = 0$ , which is summarized in Table 5. By implementing the backward induction method, equilibrium solutions for various situations can be obtained and displayed in Tables 6 and 7.

## 4. ANALYSIS AND DISCUSSION

Based on the equilibrium results presented in Tables 6 and 7, this section provides the essential analysis. Section 4.1 includes a sensitivity analysis to investigate the influence of relevant parameters on the equilibrium strategy. The comparative analysis is presented in Section 4.2, which conducts a comparative analysis of data asset losses and risk attitudes to examine their impact on the equilibrium decision-making of supply chain members. Section 4.3 further extends the model framework to investigate the robustness of research conclusions under different model specifications. The findings provide a reference for pricing and resilience investment decisions by metaverse supply chain members, and theoretical guidance for government to regulate and promote the healthy development of the metaverse.

### 4.1. Sensitivity analysis

**Proposition 1.** *Table 8 illustrates the impact of relevant parameters on the equilibrium price, resilience investment, and demand of the metaverse supply chain.*

TABLE 5. Summary of objective functions.

Model	Objective functions
MN	$\max_{\beta} U(\pi_o^{MN}) = E(\pi_o^{MN}) = (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - \frac{k\beta^2}{2}$
	$\max_p U(\pi_r^{MN}) = E(\pi_r^{MN}) = (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b)$
MY	$\max_{\beta} U(\pi_o^{MY}) = E(\pi_o^{MY}) = (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - F\gamma(1 - \beta) - \frac{k\beta^2}{2}$
	$\max_p U(\pi_r^{MY}) = E(\pi_r^{MY}) = (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b)$
RN	$\max_{\beta} U(\pi_o^{RN}) = E(\pi_o^{RN}) = (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - \frac{k\beta^2}{2}$
	$\max_p U(\pi_r^{RN}) = E(\pi_r^{RN}) - \lambda_r \sqrt{Var(\pi_r^{RN})} = (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b) - \lambda_r(1 - \eta)p\sigma$
RY	$\max_{\beta} U(\pi_o^{RY}) = E(\pi_o^{RY}) = (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - F\gamma(1 - \beta) - \frac{k\beta^2}{2}$
	$\max_p U(\pi_r^{RY}) = E(\pi_r^{RY}) - \lambda_r \sqrt{Var(\pi_r^{RY})} = (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b) - \lambda_r(1 - \eta)p\sigma$
ON	$\max_{\beta} U(\pi_o^{ON}) = E(\pi_o^{ON}) - \lambda_o \sqrt{Var(\pi_o^{ON})} = (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - \frac{k\beta^2}{2} - \lambda_o(\eta p - c)\sigma$
	$\max_p U(\pi_r^{ON}) = E(\pi_r^{ON}) = (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b)$
OY	$\max_{\beta} U(\pi_o^{OY}) = E(\pi_o^{OY}) - \lambda_o \sqrt{Var(\pi_o^{OY})} = (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - F\gamma(1 - \beta) - \frac{k\beta^2}{2} - \lambda_o(\eta p - c)\sigma$
	$\max_p U(\pi_r^{OY}) = E(\pi_r^{OY}) = (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b)$
AN	$\max_{\beta} U(\pi_o^{AN}) = E(\pi_o^{AN}) - \lambda_o \sqrt{Var(\pi_o^{AN})} = (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - \frac{k\beta^2}{2} - \lambda_o(\eta p - c)\sigma$
	$\max_p U(\pi_r^{AN}) = E(\pi_r^{AN}) - \lambda_r \sqrt{Var(\pi_r^{AN})} = (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b) - \lambda_r(1 - \eta)p\sigma$
AY	$\max_{\beta} U(\pi_o^{AY}) = E(\pi_o^{AY}) - \lambda_o \sqrt{Var(\pi_o^{AY})} = (\eta p - c)(1 - p - \alpha\gamma(1 - \beta) + b) - F\gamma(1 - \beta) - \frac{k\beta^2}{2} - \lambda_o(\eta p - c)\sigma$
	$\max_p U(\pi_r^{AY}) = E(\pi_r^{AY}) - \lambda_r \sqrt{Var(\pi_r^{AY})} = (1 - \eta)p(1 - p - \alpha\gamma(1 - \beta) + b) - \lambda_r(1 - \eta)p\sigma$

TABLE 6. Equilibrium solutions.

Model	$p$	$\beta$	$d$
MN	$\frac{2k(1 + b - \alpha\gamma) - c\alpha^2\gamma^2}{2(2k - \alpha^2\gamma^2\eta)}$	$\frac{\alpha\gamma(\eta(1 + b - \alpha\gamma) - c)}{2k - \alpha^2\gamma^2\eta}$	$\frac{2k(1 + b - \alpha\gamma) - c\alpha^2\gamma^2}{2(2k - \alpha^2\gamma^2\eta)}$
MY	$\frac{\alpha(2F - c\alpha)\gamma^2 + 2k(1 + b - \alpha\gamma)}{4k - 2\alpha^2\gamma^2\eta}$	$\frac{\gamma(2F - \alpha(c - \eta(1 + b - \alpha\gamma)))}{2k - \alpha^2\gamma^2\eta}$	$\frac{\alpha(2F - c\alpha)\gamma^2 + 2k(1 + b - \alpha\gamma)}{4k - 2\alpha^2\gamma^2\eta}$
RN	$\frac{2k(1 + b - \alpha\gamma - \lambda_r\sigma) - \alpha^2\gamma^2(c - \eta\lambda_r\sigma)}{4k - 2\alpha^2\gamma^2\eta}$	$\frac{\alpha\gamma(\eta(1 + b - \alpha\gamma) - c)}{2k - \alpha^2\gamma^2\eta}$	$\frac{2k(1 + b - \alpha\gamma + \lambda_r\sigma) - \alpha^2\gamma^2(c + \eta\lambda_r\sigma)}{4k - 2\alpha^2\gamma^2\eta}$
RY	$\frac{2k(1 + b - \alpha\gamma - \lambda_r\sigma) + \alpha\gamma^2(2F - c\alpha + \eta\lambda_r\sigma)}{4k - 2\alpha^2\gamma^2\eta}$	$\frac{\gamma(2F - \alpha(c - \eta(1 + b - \alpha\gamma)))}{2k - \alpha^2\gamma^2\eta}$	$\frac{2k(1 + b - \alpha\gamma + \lambda_r\sigma) + \alpha\gamma^2(2F - \alpha(c + \eta\lambda_r\sigma))}{4k - 2\alpha^2\gamma^2\eta}$
ON	$\frac{2k(1 + b - \alpha\gamma) - \alpha^2\gamma^2(c + \eta\lambda_o\sigma)}{4k - 2\alpha^2\gamma^2\eta}$	$\frac{\alpha\gamma(\eta(1 + b - \alpha\gamma - \lambda_o\sigma) - c)}{2k - \alpha^2\gamma^2\eta}$	$\frac{2k(1 + b - \alpha\gamma) - \alpha^2\gamma^2(c + \eta\lambda_o\sigma)}{4k - 2\alpha^2\gamma^2\eta}$
OY	$\frac{2k(1 + b - \alpha\gamma) + \alpha\gamma^2(2F - \alpha(c + \eta\lambda_o\sigma))}{4k - 2\alpha^2\gamma^2\eta}$	$\frac{\gamma(2F - \alpha(c - \eta(1 + b - \alpha\gamma - \lambda_o\sigma)))}{2k - \alpha^2\gamma^2\eta}$	$\frac{2k(1 + b - \alpha\gamma) + \alpha\gamma^2(2F - \alpha(c + \eta\lambda_o\sigma))}{4k - 2\alpha^2\gamma^2\eta}$
AN	$\frac{2k(1 + b - \alpha\gamma - \lambda_r\sigma) - \alpha^2\gamma^2(c + \eta(\lambda_o - \lambda_r)\sigma)}{4k - 2\alpha^2\gamma^2\eta}$	$\frac{\alpha\gamma(\eta(1 + b - \alpha\gamma - \lambda_o\sigma) - c)}{2k - \alpha^2\gamma^2\eta}$	$\frac{2k(1 + b - \alpha\gamma + \lambda_r\sigma) - \alpha^2\gamma^2(c + \eta(\lambda_o + \lambda_r)\sigma)}{4k - 2\alpha^2\gamma^2\eta}$
AY	$\frac{2k(1 + b - \alpha\gamma - \lambda_r\sigma) + \alpha\gamma^2(2F - \alpha(c + \eta(\lambda_o - \lambda_r)\sigma))}{4k - 2\alpha^2\gamma^2\eta}$	$\frac{\gamma(2F - \alpha(c - \eta(1 + b - \alpha\gamma - \lambda_o\sigma)))}{2k - \alpha^2\gamma^2\eta}$	$\frac{2k(1 + b - \alpha\gamma + \lambda_r\sigma) + \alpha\gamma^2(2F - \alpha(c + \eta(\lambda_o + \lambda_r)\sigma))}{4k - 2\alpha^2\gamma^2\eta}$

TABLE 7. Equilibrium profits.

Model	Metaverse platform profit	Metaverse firm profit
MN	$\frac{c^2\alpha^2\gamma^2 - 4ck(1+b-\alpha\gamma) + 2k(1+b-\alpha\gamma)^2\eta}{8k - 4\alpha^2\gamma^2\eta}$	$\frac{(c\alpha^2\gamma^2 - 2k(1+b-\alpha\gamma))^2(1-\eta)}{4(2k - \alpha^2\gamma^2\eta)^2}$
MY	$\frac{c^2\alpha^2\gamma^2 - 4F\gamma(2k - F\gamma) - 4c(F\alpha\gamma^2 + k(1+b-\alpha\gamma)) + 4(1+b)F\alpha\gamma^2\eta + 2k(1+b-\alpha\gamma)^2\eta}{8k - 4\alpha^2\gamma^2\eta}$	$\frac{(\alpha(2F - c\alpha)\gamma^2 + 2k(1+b-\alpha\gamma))^2(1-\eta)}{4(2k - \alpha^2\gamma^2\eta)^2}$
RN	$\frac{c^2\alpha^2\gamma^2 + 2k(1+b-\alpha\gamma)^2\eta + 2c\alpha^2\gamma^2\eta\lambda_r\sigma - \eta(2k - \alpha^2\gamma^2\eta)\lambda_r^2\sigma^2 - 4ck(1+b-\alpha\gamma + \lambda_r\sigma)}{4(2k - \alpha^2\gamma^2\eta)}$	$\frac{(1-\eta)(2k(1+b-\alpha\gamma - \lambda_r\sigma) - \alpha^2\gamma^2(c - \eta\lambda_r\sigma)) \cdot (2k(1+b-\alpha\gamma + \lambda_r\sigma) - \alpha^2\gamma^2(c + \eta\lambda_r\sigma))}{4(2k - \alpha^2\gamma^2\eta)^2}$
RY	$\frac{c^2\alpha^2\gamma^2 + 4F\gamma(F\gamma - 2k) + 4(1+b)F\alpha\gamma^2\eta + 2k(1+b-\alpha\gamma)^2\eta - \eta(2k - \alpha^2\gamma^2\eta)\lambda_r^2\sigma^2 - 2c(2k(1+b-\alpha\gamma + \lambda_r\sigma) + \alpha\gamma^2(2F - \alpha\eta\lambda_r\sigma))}{8k - 4\alpha^2\gamma^2\eta}$	$\frac{(1-\eta)(2k(1+b-\alpha\gamma - \lambda_r\sigma) + \alpha\gamma^2(2F - c\alpha + \alpha\eta\lambda_r\sigma)) \cdot (2k(1+b-\alpha\gamma + \lambda_r\sigma) + \alpha\gamma^2(2F - \alpha(c + \eta\lambda_r\sigma)))}{4(2k - \alpha^2\gamma^2\eta)^2}$
ON	$\frac{c^2\alpha^2\gamma^2 - 4ck(1+b-\alpha\gamma) + \eta(2k(1+b-\alpha\gamma)^2 - \alpha^2\gamma^2\eta\lambda_o^2\sigma^2)}{8k - 4\alpha^2\gamma^2\eta}$	$\frac{(1-\eta)(2k(1+b-\alpha\gamma) - \alpha^2\gamma^2(c + \eta\lambda_o\sigma))^2}{4(2k - \alpha^2\gamma^2\eta)^2}$
OY	$\frac{4F^2\gamma^2 + c^2\alpha^2\gamma^2 - 4c(F\alpha\gamma^2 + k(1+b-\alpha\gamma)) + 4F\gamma((1+b)\alpha\gamma\eta - 2k) + \eta(2k(1+b-\alpha\gamma)^2 - \alpha^2\gamma^2\eta\lambda_o^2\sigma^2)}{8k - 4\alpha^2\gamma^2\eta}$	$\frac{(1-\eta)(2k(1+b-\alpha\gamma) + \alpha\gamma^2(2F - \alpha(c + \eta\lambda_o\sigma)))^2}{4(2k - \alpha^2\gamma^2\eta)^2}$
AN	$\frac{c^2\alpha^2\gamma^2 + 2k(1+b-\alpha\gamma)^2\eta + \eta(\alpha^2\gamma^2\eta(\lambda_r^2 - \lambda_o^2) - 2k\lambda_r^2)\sigma^2 + c(2\alpha^2\gamma^2\eta\lambda_r\sigma - 4k(1+b-\alpha\gamma + \lambda_r\sigma))}{8k - 4\alpha^2\gamma^2\eta}$	$\frac{(1-\eta)(2k(1+b-\alpha\gamma - \lambda_r\sigma) + \alpha^2\gamma^2(c + \eta(\lambda_o - \lambda_r)\sigma)) \cdot (2k(1+b-\alpha\gamma + \lambda_r\sigma) - \alpha^2\gamma^2(c + \eta(\lambda_o + \lambda_r)\sigma))}{4(2k - \alpha^2\gamma^2\eta)^2}$
AY	$\frac{c^2\alpha^2\gamma^2 + 4F\gamma(F\gamma - 2k) + 4(1+b)F\alpha\gamma^2\eta + 2k(1+b-\alpha\gamma)^2\eta + \eta(\alpha^2\gamma^2\eta(\lambda_r^2 - \lambda_o^2) - 2k\lambda_r^2)\sigma^2 - 2c(2k(1+b-\alpha\gamma + \lambda_r\sigma) + \alpha\gamma^2(2F - \alpha\eta\lambda_r\sigma))}{8k - 4\alpha^2\gamma^2\eta}$	$\frac{(1-\eta)(2k(1+b-\alpha\gamma - \lambda_r\sigma) + \alpha\gamma^2(2F - \alpha(c + \eta(\lambda_o - \lambda_r)\sigma))) \cdot (2k(1+b-\alpha\gamma + \lambda_r\sigma) + \alpha\gamma^2(2F - \alpha(c + \eta(\lambda_o + \lambda_r)\sigma)))}{4(2k - \alpha^2\gamma^2\eta)^2}$

This study first investigates the impact of the consumer data security concern coefficient  $\alpha$  on the equilibrium solution. Despite heterogeneous risk attitudes, the overall equilibrium remains stable, with only minor shifts in critical thresholds. Specifically, when ignoring digital asset losses: in scenarios with low resilience investment cost coefficients  $k$  or immersion costs  $c$ , an increase in  $\alpha$  directly boosts platform resilience investments. The underlying mechanism lies in the platform’s ability to mitigate security risk disutility (term  $-\alpha\gamma(1 - \beta)$  in the demand function) at limited costs, thereby driving commission revenue growth through demand expansion. Notably, this positive effect attenuates when the platform exhibits risk aversion ( $c_1 > c_3$ ). Under higher cost constraints, however, demand increments from immersion and resilience investments fail to cover marginal costs, prompting the platform to reduce security inputs for operational balance. Incorporating digital asset losses complicates the platform’s cost structure: expected high losses incentivize larger resilience investments to mitigate future cash flow volatility.

In the Stackelberg framework, the pricing decisions of follower firms are significantly constrained by resilience cost coefficient  $k$ . As  $\alpha$  increases, the weight of security risk disutility in the demand function rises. Under conditions of a low resilience cost coefficient, increasing resilience investment by the platform effectively hedges against this negative utility, enabling firms to achieve revenue maximization through price increases and demand growth. When facing a high resilience cost coefficient, the platform reduces resilience investment to cut cost expenditures. However, the superimposed effect of the negative utility of security risks – where smaller values of  $\beta$  and increasing values of  $\alpha$  lead to a larger absolute value of  $-\alpha\gamma(1 - \beta)$  – forces firms to adopt a price reduction strategy to mitigate demand decline, though with limited effectiveness. Notably, after incorporating the loss of data assets, both the space for price increases and the potential for demand growth expand for firms.

Further analysis explores the mechanism through which hacking probability  $\gamma$  influences equilibrium solutions. As  $\gamma$  increases, transaction environment vulnerability intensifies, prompting the platform to adjust resilience strategies under given immersion and cost constraints to hedge the rising security risk disutility. Notably, platform risk aversion may dampen investment willingness. Including digital asset losses directly increases

TABLE 8. Summary of sensitivity analysis of equilibrium results.

	Model	$p$	$\beta$	$d$
$\alpha \uparrow$	$MN/RN$	$\uparrow: \underline{k} < k < k_1$ $\downarrow: k > k_1$	$\uparrow: c < c_1;$ $c > c_1, \underline{k} < k < k_2$ $\downarrow: c > c_1, k > k_2$	$\uparrow: \underline{k} < k < k_1$ $\downarrow: k > k_1$
	$MY/RY$	$\uparrow: \underline{k} < k < k_1;$ $k > k_1, F > F_1$ $\downarrow: k > k_1, F < F_1$	$\uparrow: c < c_1;$ $c_1 < c < c_2, k < k_2;$ $c_1 < c < c_2, k > k_2, F > F_2$ $\downarrow: c_1 < c < c_2, k > k_2, F < F_2$	$\uparrow: \underline{k} < k < k_1;$ $k > k_1, F > F_1$ $\downarrow: k > k_1, F < F_1$
	$ON/AN$	$\uparrow: \underline{k} < k < k_3$ $\downarrow: k > k_3$	$\uparrow: c < c_3;$ $c > c_3, \underline{k} < k < k_4$ $\downarrow: c > c_3, k > k_4$	$\uparrow: \underline{k} < k < k_3$ $\downarrow: k > k_3$
	$OY/AY$	$\uparrow: \underline{k} < k < k_3;$ $k > k_3, F > F_3$ $\downarrow: k > k_3, F < F_3$	$\uparrow: c < c_3;$ $c_3 < c < c_4, k < k_4;$ $c_3 < c < c_4, k > k_4, F > F_4$ $\downarrow: c_3 < c < c_4, k > k_4, F < F_4$	$\uparrow: \underline{k} < k < k_3;$ $k > k_3, F > F_3$ $\downarrow: k > k_3, F < F_3$
$\gamma \uparrow$	$MN/RN$	$\uparrow: \underline{k} < k < k_1$ $\downarrow: k > k_1$	$\uparrow: c < c_1;$ $c > c_1, \underline{k} < k < k_2$ $\downarrow: c > c_1, k > k_2$	$\uparrow: \underline{k} < k < k_1$ $\downarrow: k > k_1$
	$MY/RY$	$\uparrow: \underline{k} < k < k_1;$ $k > k_1, F > F_5$ $\downarrow: k > k_1, F < F_5$	$\uparrow: c < c_1;$ $c_1 < c < c_5, k < k_2;$ $c_1 < c < c_5, k > k_2, F > F_6$ $\downarrow: c_1 < c < c_5, k > k_2, F < F_6$	$\uparrow: \underline{k} < k < k_1;$ $k > k_1, F > F_5$ $\downarrow: k > k_1, F < F_5$
	$ON/AN$	$\uparrow: \underline{k} < k < k_3$ $\downarrow: k > k_3$	$\uparrow: c < c_3;$ $c > c_3, \underline{k} < k < k_4$ $\downarrow: c > c_3, k > k_4$	$\uparrow: \underline{k} < k < k_3$ $\downarrow: k > k_3$
	$OY/AY$	$\uparrow: \underline{k} < k < k_3;$ $k > k_3, F > F_7$ $\downarrow: k > k_3, F < F_7$	$\uparrow: c < c_3;$ $c_3 < c < c_4, k < k_4;$ $c_3 < c < c_4, k > k_4, F > F_8$ $\downarrow: c_3 < c < c_4, k > k_4, F < F_8$	$\uparrow: \underline{k} < k < k_3;$ $k > k_3, F > F_7$ $\downarrow: k > k_3, F < F_7$
$k \uparrow$	$MN/RN/ON/AN/$ $MY/RY/OY/AY$	$\downarrow$	$\downarrow$	$\downarrow$
$\eta \uparrow$	$MN/RN/ON/AN/$ $MY/RY/OY/AY$	$\uparrow$	$\uparrow$	$\uparrow$
$\lambda_r \uparrow$	$RN/AN/RY/AY$	$\downarrow$	—	$\uparrow$
$\lambda_o \uparrow$	$ON/AN/OY/AY$	$\downarrow$	$\downarrow$	$\downarrow$
$\sigma \uparrow$	$RN/RY$	$\downarrow$	—	$\uparrow$
	$ON/OY$	$\downarrow$	$\downarrow$	$\downarrow$
	$AN/AY$	$\downarrow$	$\downarrow$	$\uparrow: k > k_5$ $\downarrow: \underline{k} < k < k_5$

**Notes.** “ $\uparrow$ ” means increase; “ $\downarrow$ ” means decrease; “—” means unaffected. The critical point values are shown in the Appendix A.

the platform's expected cost function as  $\gamma$  rises, reinforcing investment incentives through cost transmission mechanisms. From the firm's perspective, the resilience cost coefficient  $k$  acts as a core constraint on pricing: low  $k$  enables high-intensity investments to significantly reduce the probability of successful attacks, offsetting risk utility losses from rising  $\gamma$  – this transmission through the demand function's security disutility term facilitates price increases for profit improvement. Under high  $k$ , however, the dual effects of increasing  $\gamma$  and decreasing investments  $\beta$  accelerate security risk disutility accumulation, leading firms alleviate the decline in demand through price discounts.

As shown in Table 8, the relationship between the resilience investment cost coefficient  $k$  and equilibrium solutions exhibits notable stability, unaffected by digital asset losses or supply chain risk attitude heterogeneity. Specifically, higher  $k$  increases the marginal cost of resilience investments, requiring the platform to balance demand-stimulating effects (reducing security risk disutility to boost demand and commission revenue) against rising costs. As  $k$  grows, the steeper marginal cost curve drives optimal investment levels to lower intervals to avoid excessive costs, prompting firms to reduce prices through the demand function to fill demand gaps from reduced investments. However, the increasing weight of consumer security risk disutility outweighs price adjustment benefits, contracting total market demand. An increase in the commission rate  $\eta$  strengthens the platform's motivation to boost demand through resilience investment while prompting firms to raise prices to alleviate profit pressures. Although price increases may suppress part of the demand, the substantial increase in platform investment reduces the negative utility of security risks, leading to a net upward trend in demand. This dynamic equilibrium relationship holds under different risk preferences, reflecting the cooperative adjustment of supply chain members to changes in revenue distribution.

This study further investigates the mechanism through which the risk aversion coefficient influences equilibrium decisions. Within the analytical framework where supply chain members make strategic choices based on the mean-variance utility function, an increase in the risk aversion coefficient significantly amplifies the negative utility of profit volatility. Specifically, when the platform's risk aversion coefficient  $\lambda_o$  rises, the platform tends to reduce its resilience investment level to minimize profit variance. This decision is transmitted to the consumer side through the negative utility term of security risk in the demand function, thereby leading to a contraction in market demand. In response, firms typically adopt a price reduction strategy; however, the demand growth driven by price cuts is insufficient to offset the weakened consumer purchase intention caused by reduced security utility. Consequentially, this results in a downward trend in the market equilibrium demand level. When firms exhibit risk aversion, the variance term in their utility function gains weight, prompting low-margin strategies to diversify risks. Importantly, in the Stackelberg framework, the platform's first-mover advantage in resilience investment decisions means firm risk aversion can only influence equilibrium through price adjustments, unable to reverse platform investments. Thus, deepening firm risk aversion leaves platform investment levels unchanged but induces local demand changes through price decreases. This mechanism reveals asymmetric risk transmission: the leader's (platform) risk attitudes have global impacts through investment decisions, while the follower's (firm) risk aversion only triggers local price adjustments. This finding highlights that excessive platform risk aversion may lead to systemic resilience investment shortfalls, necessitating institutional designs for risk-sharing mechanisms.

The impact of demand uncertainty on equilibrium solutions varies depending on different forms of risk aversion. Specifically, when firms are risk-averse, an increase in demand uncertainty is not related to the platform's investment. Risk-averse firms implement price reductions to generate more sales and avoid the risk of inventory backlogs caused by demand uncertainty. Platforms with risk aversion reduce their investment due to high demand uncertainty implies the risk of low transaction volumes and difficulty in recovering investment costs. Ensuring safety is a challenging task that may impede sales. However, reducing prices cannot prevent performance losses due to insufficient platform resilience in the trading environment. Under the influence of risk aversion among all members, the positive stimulating effect on demand of lowering the selling price outweighs the negative effect of cutting investment intensity when the cost coefficient of resilience investment is low, enabling the firm to maintain higher demand; otherwise, the dominant relationship is reversed and demand decreases.

## 4.2. Comparative analysis

Next, we use the equilibrium outcomes extracted from Tables 6 and 7 to investigate the mechanism by which risk attitudes and data asset losses affect member strategies.

### 4.2.1. Comparative analysis of data asset losses

We examine the effect of data asset losses on the equilibrium decisions of supply chain members under a deterministic risk attitude. We employ  $\Delta X^Z$  to represent the difference in equilibrium results  $X \in \{p, \beta, d, E(\pi_r), E(\pi_o), E(\pi_{sc})\}$  considering and ignoring data asset losses under risk attitude  $Z \in \{M, O, R, A\}$ , which is  $\Delta X^Z = X^{ZY} - X^{ZN}$ .

**Proposition 2.** *Comparison of Equilibrium Solutions*

- (i)  $\Delta p^M = \Delta p^O = \Delta p^R = \Delta p^A > 0$ ;
- (ii)  $\Delta \beta^M = \Delta \beta^O = \Delta \beta^R = \Delta \beta^A > 0$ ;
- (iii)  $\Delta d^M = \Delta d^O = \Delta d^R = \Delta d^A > 0$ .

Proposition 2 implies that the equilibrium decisions of supply chain members, whether data asset losses are considered or ignored, remain unaffected by the risk aversion coefficient. Indeed, Table 8 indicates that data asset losses fail to change the direction of the impact of the risk aversion coefficient on equilibrium results. Furthermore, losses of data assets potentially escalate the platform’s future financial risks, and significant losses drive the platform to improve system security to a higher level. Additionally, high safety elevates the appeal of products to consumers and provides additional room for firms to raise product prices.

**Proposition 3.** *Profit Comparison of Firm.*

*Regardless of the risk attitude, we have  $\Delta E(\pi_r^M) = \Delta E(\pi_r^R) > \Delta E(\pi_r^O) = \Delta E(\pi_r^A) > 0$ .*

Proposition 2 highlights that incorporating data asset losses into the model leads to a double increase in product prices and demand, compared to ignoring data asset losses. This could be considered beneficial for firms as their profit margins increase without any additional financial pressure, and the firms have always benefited. Moreover, our research highlights that under risk neutrality and self-risk aversion, firms benefit more. This is because platform risk aversion weakens the capacity for resilience improvement, which is manifested in the double reduction of sales price and sales volume at the sales level, and the profit margin of firms is severely compressed. In contrast, a firm’s risk aversion and resilience investment remain independent, ensuring that demand is not lost due to inadequate security. Consequently, firms can uphold relatively high profits.

**Proposition 4.** *Profit Comparison of Platform.*

*Regardless of the risk attitude, we have  $\Delta E(\pi_o^M) = \Delta E(\pi_o^O) = \Delta E(\pi_o^R) = \Delta E(\pi_o^A) > 0$  when  $\underline{k} < k < k_6$  or  $k > k_6, F > F_9$ , and  $\Delta E(\pi_o^M) = \Delta E(\pi_o^O) = \Delta E(\pi_o^R) = \Delta E(\pi_o^A) < 0$  when  $k > k_6, F < F_9$ .*

From a platform perspective, the influencing factors are varied. As the commission recipient, the platform benefits from an increase in sales and selling prices, but also incurs the cost of investing in resilience and potential data asset losses. If the cost coefficient is low, the platform is able to significantly improve the security of the metaverse trading environment and platform resilience with minimal expenditure. The commissions dominate the resilience costs and data asset losses at this point, leading to an increase in profits. When the cost coefficient of resilience investment is high, data asset losses play a vital role in determining the profitability of the platform. Although one may assume that data asset losses have a negative effect on profits and that the impact is greater with higher losses, our research indicates that the platform benefits under the compound influence of high resilience cost coefficients and high data asset losses. High data asset losses increase the risk of defense failure and can induce greater endeavors to enhance platform resilience. A more propitious trading environment begets amplified sales, counterbalancing expenses while boosting profits for the platform. Conversely, lower potential data asset losses do not yield a potent incentive for platforms to enhance the trading atmosphere, thereby

increasing the chances of underinvestment in resilience. Poor security performance makes it difficult to motivate customers to make effective purchases. Increasing commissions proves insufficient to cover costs and data asset losses, ultimately reducing platform profits.

**Proposition 5.** *Profit Comparison of Supply Chain System*

- (i) When risk neutrality or firm risk aversion is present,  $\Delta E(\pi_{sc}^M) = \Delta E(\pi_{sc}^R) > 0$  exists when  $\underline{k} < k < k_7$  or  $k > k_7, F > F_{10}$  is met, and  $\Delta E(\pi_{sc}^M) = \Delta E(\pi_{sc}^R) < 0$  holds when  $k > k_7, F < F_{10}$  is satisfied.
- (ii) When platform or full-member risk aversion is present,  $\Delta E(\pi_{sc}^O) = \Delta E(\pi_{sc}^A) > 0$  exists when  $\underline{k} < k < k_8$  or  $k > k_8, F > F_{11}$  is met, and  $\Delta E(\pi_{sc}^O) = \Delta E(\pi_{sc}^A) < 0$  holds when  $k > k_8, F < F_{11}$  is satisfied.

According to Proposition 3, incorporating data asset losses into the analysis framework is always advantageous for the firm compared to ignoring them, and this effect is more pronounced under risk neutrality and firm risk aversion. When the resilience cost coefficient is low, or both the resilience cost coefficient and the data asset losses are high, the platform benefits; on the contrary, the platform suffers as a result. The profit generated by the supply chain system, which combines the profits of the platform and the firm, represents the relationship between the two and their corresponding changes objectively. Compared to platform profits, incorporating data asset losses into the analysis framework benefits system profits to a greater extent. The system profits increase when the rise in firm profits exceeds the drop in platform profits, which is reasonable. Therefore, to attain the objective of maximizing profits in the supply chain system, the government should strictly monitor data security issues and actively promote their serious consequences, to make all parties fully realize the importance of system security.

4.2.2. *Comparative analysis of risk attitudes*

Now we consider how risk attitudes affect the equilibrium decisions and profits of supply chain members.

**Proposition 6.** *Comparison of Equilibrium Solutions.*

Whether or not data asset losses are taken into account, the following results are valid:

- (i)  $\beta^A = \beta^O < \beta^R = \beta^M$ .
- (ii)  $p^A < p^O < p^R < p^M$  exists when  $\underline{k} < k < k_5$  is met, and  $p^A < p^R < p^O < p^M$  holds when  $k > k_5$  is satisfied.
- (iii)  $d^O < d^A < d^M < d^R$  exists when  $\underline{k} < k < k_5$  is met, and  $d^O < d^M < d^A < d^R$  holds when  $k > k_5$  is satisfied.

According to Proposition 1, the risk aversion coefficient of the firm remains independent of the resilience investment level. With an increase in the platform's risk aversion coefficient, resilience investment decreases, ultimately leading to a situation of  $\beta^A = \beta^O < \beta^R = \beta^M$ . Due to risk aversion, firms are motivated to sell products at lower prices, with product prices being the lowest when members are fully risk averse and highest when they are risk neutral. Within a certain range of  $k$ , the platform's risk aversion effect is stronger; otherwise, firm risk aversion predominates, making  $p^R < p^O$  feasible. Additionally, the risk aversion attitudes of various members have differing impacts on sales. Specifically, a rise in the firm's risk aversion coefficient encourages sales growth whilst the reverse is true for platform risk aversion. When the resilience investment cost coefficient is low, the platform has more room for maneuver and the overall effect is mainly inhibitory, *i.e.*,  $d^O < d^A < d^M < d^R$ . With the increase in  $k$ , the increase in sales caused by firm risk aversion becomes the main force, and  $d^O < d^M < d^A < d^R$  represents the end result.

**Proposition 7.** *Profit Comparison of Firm*

- (i) If ignoring data asset losses,  $E(\pi_r^{AN}) < E(\pi_r^{ON}) < E(\pi_r^{RN}) < E(\pi_r^{MN})$  exists when  $\underline{k} < k < k_9$  is met, and  $E(\pi_r^{AN}) < E(\pi_r^{RN}) < E(\pi_r^{ON}) < E(\pi_r^{MN})$  holds when  $k > k_9$  is satisfied.

- (ii) *If considering data asset losses,  $E(\pi_r^{AY}) < E(\pi_r^{OY}) < E(\pi_r^{RY}) < E(\pi_r^{MY})$  exists when  $\underline{k} < k < k_9$  or  $k > k_9, F > F_{12}$  is met, and  $E(\pi_r^{AY}) < E(\pi_r^{RY}) < E(\pi_r^{OY}) < E(\pi_r^{MY})$  holds when  $k > k_9, F < F_{12}$  is satisfied.*

Firm’s profit is the result of the combined effect of product price and sales volume. Observing Propositions 6 and 7, we find that the comparison of firm’s profit and product prices under different risk attitudes is similar, indicating that the impact of product prices on profits is much greater than the impact of sales. When  $k$  is small, risk neutrality permits firms to sell products at higher prices, subsequently generating significant profits. Risk aversion prompts firms to adopt a cautious approach and reduce prices to hold onto their market position. Under the leading role of product prices, profits decrease. If the risk aversion effect of the platform is stronger,  $E(\pi_r^{AN}) < E(\pi_r^{ON}) < E(\pi_r^{RN}) < E(\pi_r^{MN})$  is established. Otherwise, the firm’s risk aversion pattern dominates, making  $p^R < p^O$  possible and eventually stabilizing at  $E(\pi_r^{AN}) < E(\pi_r^{RN}) < E(\pi_r^{ON}) < E(\pi_r^{MN})$ . Furthermore, compared to ignoring data asset losses, incorporating data asset losses into the model effectively encourages the platform to enhance system security and platform resilience. The risk-averse firms can attain the initial outcome by suitably reducing the discount, making  $E(\pi_r^{OY}) < E(\pi_r^{RY})$  feasible on a greater extent.

**Proposition 8.** *Profit Comparison of Platform.*

*Whether or not data asset losses are taken into account, the following results are valid:  $E(\pi_o^A) < E(\pi_o^O) < E(\pi_o^R) < E(\pi_o^M)$  exists when  $\underline{k} < k < k_{10}$  is met, and  $E(\pi_o^A) < E(\pi_o^R) < E(\pi_o^O) < E(\pi_o^M)$  holds when  $k > k_{10}$  is satisfied.*

Whatever the cost coefficient of resilience investment and data asset losses, Proposition 7 demonstrates that greater sales can be attained through risk neutrality, while the firm’s least advantage accrues from total risk aversion among its members, which indirectly leads to the results of  $E(\pi_o^A)$  minimum and  $E(\pi_o^M)$  optimal. While comparing  $E(\pi_o^R)$  and  $E(\pi_o^O)$ , commission fees, resilience investment costs, and data asset losses are the primary constraints under consideration. Proposition 6 implies  $\beta^O < \beta^R$ , indicating that the total amount of resilience investment costs is greater when the firm is risk-averse. When the resilience investment cost coefficient is small enough, the profit increase brought by commission fees fully covers the resilience costs and data asset losses, and  $E(\pi_o^O) < E(\pi_o^R)$  is established; on the contrary, the resilience costs dominate the overall effect, leading to  $E(\pi_o^R) < E(\pi_o^O)$ . We should note that as a direct target of data asset losses, the impact of losses on the platform can be ignored and there is no fundamental impact on the profit comparison of platforms with different risk attitudes.

**Proposition 9.** *Profit Comparison of Supply Chain Systems*

- (i) *If ignoring data asset losses,  $E(\pi_{sc}^{AN}) < E(\pi_{sc}^{ON}) < E(\pi_{sc}^{RN}) < E(\pi_{sc}^{MN})$  exists when  $\underline{k} < k < k_{11}$  is met, and  $E(\pi_{sc}^{AN}) < E(\pi_{sc}^{RN}) < E(\pi_{sc}^{ON}) < E(\pi_{sc}^{MN})$  holds when  $k > k_{11}$  is satisfied.*
- (ii) *If considering data asset losses,  $E(\pi_{sc}^{AY}) < E(\pi_{sc}^{OY}) < E(\pi_{sc}^{RY}) < E(\pi_{sc}^{MY})$  exists when  $\underline{k} < k < k_{11}$  or  $k > k_{11}, F > F_{13}$  is met, and  $E(\pi_{sc}^{AY}) < E(\pi_{sc}^{RY}) < E(\pi_{sc}^{OY}) < E(\pi_{sc}^{MY})$  holds when  $k > k_{11}, F < F_{13}$  is satisfied.*

Propositions 7 and 8 illustrate that the magnitude of the profits of the platform and the firm maintains its consistency across varying risk attitudes. Specifically, when the resilience investment cost coefficient is low, the profits of supply chain members decrease sequentially under risk neutrality, firm risk aversion, platform risk aversion, and full member risk aversion. If the cost coefficient is high, there is a reversal in the supply chain members’ profits under firm risk aversion and platform risk aversion. The supply chain system profits also correspondingly change as the platform and firm operate in dual roles. With the loss of digital assets included,  $E(\pi_r^{OY}) < E(\pi_r^{RY})$  appears on a broader range, while the platform’s profits remain steady. Consequently, the combined profits of the firm and platform establish a larger scale of  $E(\pi_{sc}^{OY}) < E(\pi_{sc}^{RY})$ , and achieve a perfect win-win scenario for supply chain members.

### 4.3. Model extension

#### 4.3.1. Platform competition

The baseline model examines decision-making under a monopolistic metaverse platform, neglecting potential impacts of inter-platform competition on supply chain strategies. To address this theoretical gap, this section extends the model to a competitive scenario (superscript  $C$ ), considering two competing metaverse platforms (platform 1 as the incumbent and platform 2 as the entrant). Assume firms sell products on both platforms, where platform 1 has a consumer-perceived value  $v$  and platform 2 has a consumer-perceived value  $\theta v$ , with  $\theta \in (0, 1)$  denoting the consumer trust coefficient for the entrant. Consumer utility functions on the two platforms are defined as:

$$U_1 = v - p_1 - \alpha\gamma(1 - \beta_1) + b \tag{8}$$

$$U_2 = \theta v - p_2 - \alpha\gamma(1 - \beta_2) + b. \tag{9}$$

Consumers choose platform 1 if  $U_1 \geq U_2$  and  $U_1 > 0$ , and switch to platform 2 if  $U_2 \geq U_1$  and  $U_2 > 0$ . Incorporating demand uncertainty, the derived demand functions are:

$$d_1 = \varepsilon + \int_{\frac{p_1 - p_2 + \alpha\gamma(\beta_2 - \beta_1)}{1 - \theta}}^1 f(v) \, dv \tag{10}$$

$$d_2 = \varepsilon + \int_{\frac{p_2 + \alpha\gamma(1 - \beta_2) - b}{\theta}}^{\frac{p_1 - p_2 + \alpha\gamma(\beta_2 - \beta_1)}{1 - \theta}} f(v) \, dv. \tag{11}$$

To address the core research question, we posit that the stochastic demand term  $\varepsilon \sim N(0, \sigma^2)$  follows an identical probability distribution across both platforms, with symmetric immersion parameters. Given the technological maturity advantage of the incumbent platform (platform 1), we specify its resilience investment cost coefficient as  $k \in (0, 1)$ , while normalizing the corresponding coefficient for the emerging platform (platform 2) to unity. Under the assumption of embedded data asset losses and risk-averse supply chain members, the profit functions for each agent can be expressed as follows:

$$\pi_{o1}^{AYC} = (\eta p_1 - c)d_1 - F\gamma(1 - \beta_1) - \frac{k\beta_1^2}{2} \tag{12}$$

$$\pi_{o2}^{AYC} = (\eta p_2 - c)d_2 - F\gamma(1 - \beta_2) - \frac{\beta_2^2}{2} \tag{13}$$

$$\pi_r^{AYC} = (1 - \eta)(p_1 d_1 + p_2 d_2) \tag{14}$$

and the decision objectives are

$$\begin{aligned} \max_{\beta_1} U(\pi_{o1}^{AYC}) &= E(\pi_{o1}^{AYC}) - \lambda_{o1} \sqrt{Var(\pi_{o1}^{AYC})} \\ &= (\eta p_1 - c) \cdot E(d_1) - F\gamma(1 - \beta_1) - \frac{k\beta_1^2}{2} - \lambda_{o1}(\eta p_1 - c)\sigma \end{aligned} \tag{15}$$

$$\begin{aligned} \max_{\beta_2} U(\pi_{o2}^{AYC}) &= E(\pi_{o2}^{AYC}) - \lambda_{o2} \sqrt{Var(\pi_{o2}^{AYC})} \\ &= (\eta p_2 - c) \cdot E(d_2) - F\gamma(1 - \beta_2) - \frac{\beta_2^2}{2} - \lambda_{o2}(\eta p_2 - c)\sigma \end{aligned} \tag{16}$$

$$\begin{aligned} \max_{p_1, p_2} U(\pi_r^{AYC}) &= E(\pi_r^{AYC}) - \lambda_r \sqrt{Var(\pi_r^{AYC})} \\ &= (1 - \eta)(p_1 \cdot E(d_1) + p_2 \cdot E(d_2)) - \lambda_r(1 - \eta)(p_1 + p_2)\sigma \end{aligned} \tag{17}$$

where  $\lambda_{o1}$  and  $\lambda_{o2}$  represent the risk aversion coefficients of the two platforms, respectively. By varying the values of  $\lambda_{o1}$ ,  $\lambda_{o2}$ , and  $\lambda_r$ , we can analytically derive the equilibrium strategies under different risk combinations. When  $F = 0$ , the model reduces to the special case without data asset losses.

**Proposition 10.** *Sensitivity Analysis of Platform Resilience Investments*

(i) *Consumer trust coefficient  $\theta$ .*

*Regardless of whether platforms are risk-averse or embedded with data asset losses, the following two scenarios emerge:*

*When firms are risk-averse, an increase in the consumer trust coefficient  $\theta$  leads to a decline in the resilience investment levels of both platforms ( $\frac{\partial \beta_1}{\partial \theta} < 0$  and  $\frac{\partial \beta_2}{\partial \theta} < 0$ ).*

*When firms are risk-neutral, an increase in the consumer trust coefficient  $\theta$  drives the resilience investment of incumbent platforms to rise monotonically ( $\frac{\partial \beta_1}{\partial \theta} > 0$ ), while the resilience investment of emerging platforms exhibits a U-shaped pattern of first decreasing and then increasing ( $\frac{\partial \beta_2}{\partial \theta} < 0 \rightarrow \frac{\partial \beta_2}{\partial \theta} > 0$ ).*

(ii) *Resilience investment cost coefficient  $k$ .*

*As the resilience investment cost coefficient  $k$  increases, the resilience investment of incumbent platforms decreases ( $\frac{\partial \beta_1}{\partial k} < 0$ ), while that of emerging platforms increases ( $\frac{\partial \beta_2}{\partial k} > 0$ ).*

Risk-averse firms’ decisions are constrained by the negative utility of profit variance, leading to conservative pricing to mitigate uncertainty. As the consumer trust coefficient  $\theta$  increases, emerging platforms have directly boosted demand due to the alleviation of trust disadvantages, weakening the necessity for resilience investment. The incumbent platform’s shrinking market share reduces commission revenues, making it difficult to cover investment costs. Consequently, both platforms reduce resilience investment to control expenses. In the risk-neutral scenario, firms prioritize profit maximization over risk avoidance. The incumbent platform leverages its lower resilience investment cost coefficient  $k$  to reduce consumer security risk disutility through investment, offsetting the decline in competitive advantage caused by rising  $\theta$ . For emerging platforms, resilience investment exhibits distinct stage characteristics: at lower  $\theta$ , limited market scale and high unit investment costs (with the cost coefficient normalized to 1) make marginal costs exceed marginal benefits, prompting cost-control through reduced investment. As  $\theta$  rises, demand-driven revenue growth surpasses investment costs, leading platforms to increase resilience investment to mitigate security risk disutility, forming a demand-induced U-shaped investment curve. From a cost advantage perspective, an increase in the resilience cost investment coefficient  $k$  erodes the incumbent platform’s technological edge. Rising marginal costs dampen its investment incentives, while narrowing cost disadvantages for emerging platforms lower their opportunity costs of resilience investment. This motivates emerging platforms to attract security sensitive consumers through enhanced investment, expanding competitive advantages on the demand side.

4.3.2. *Threshold effect of consumer data security risk*

In the baseline model, consumers’ disutility from security risk is captured as a subtractive term  $\alpha\gamma(1 - \beta)$  in the demand function. This term indicates that as platforms increase resilience investment to raise security coefficients, perceived risks decrease, thereby boosting demand. However, consumer perception of data security may exhibit a threshold effect: when platform resilience investment reaches a specific level (psychological threshold  $\beta_0$ ), consumers consider security expectations met, and their purchase decisions no longer depend on security risks. We now focus on this critical mechanism.

We assume a psychological threshold  $\beta_0$  for consumers’ data security concern: security risks are excluded from consumer decisions when platform resilience investment  $\beta \geq \beta_0$ , whereas consumers remain highly sensitive to security risks (incurring a utility deduction  $\alpha\gamma(1 - \beta)$ ) when  $\beta < \beta_0$ . Based on consumer utility theory with demand uncertainty, the demand function is modeled as a piecewise form:

$$d = \begin{cases} 1 - p - \alpha\gamma(1 - \beta) + b + \varepsilon, & \text{if } \beta < \beta_0 \\ 1 - p + b + \varepsilon, & \text{if } \beta \geq \beta_0. \end{cases} \tag{18}$$

**Proposition 11.** *Without considering data asset loss, the optimal platform resilience investment  $\beta^*$  is constrained by the consumer psychological threshold, i.e.,  $\beta^* \leq \beta_0$ . When data asset loss is embedded, platform resilience investment may exceed the threshold ( $\beta^* > \beta_0$ ) if and only if the consumer psychological threshold is low ( $\beta_0 < \frac{F\gamma}{k}$ ); otherwise,  $\beta_0$  remains the upper bound of resilience investment.*

Proposition 11 highlights that  $\beta_0$  serves as the core constraint for resilience investment in scenarios without data asset loss. This arises from the structural shift in the demand function at the threshold: when  $\beta \geq \beta_0$ , demand decouples from resilience investment, and additional investment only increases costs. With data asset loss introduced, although a low  $\beta_0$  implies less demand sensitivity to security risks, the extra risk costs from potential data loss compel platforms to increase investment to mitigate losses. This finding suggests that metaverse platforms should prioritize resilience investment within a reasonable range bounded by  $\beta_0$ , optimizing resource allocation while meeting consumers' psychological security expectations.

#### 4.3.3. Nash game

This study employs a two-stage modeling framework to analyze the supply chain decision mechanism. In the baseline model, a Stackelberg sequential game model is constructed: metaverse platforms, as leaders, first determine resilience investment levels, while firms, as followers, implement product pricing strategies after observing platform decisions. This section extends the research framework to a simultaneous-decision context, establishing a Nash game model to examine the dynamic evolution of equilibrium states.

**Proposition 12.** *Equilibrium analysis under the Nash game framework reveals the following characteristic changes:*

- (i) *The platform's risk-aversion coefficient has no significant impact on the strategic choices of supply chain members.*
- (ii) *Introducing the data asset loss parameter consistently increases firm profits.*
- (iii) *Firms' risk-averse behavior simultaneously reduces resilience investment levels and the expected profits of metaverse supply chain members.*

Theoretical analysis shows that the Nash game structure eliminates the platform's first-mover advantage, blocking the transmission path through which risk aversion parameters affect pricing strategies through investment decisions. The introduction of data asset loss motivates platforms to increase resilience investment to minimize expected losses, thereby reducing consumer security risk disutility and increasing demand, creating pricing room for firms. Firms can transfer part of the security costs to end markets through price adjustments, a profit-enhancing mechanism that holds across all combinations of risk attitudes. Notably, firms' risk aversion triggers systemic efficiency losses: an increase in the risk-aversion coefficient not only leads to pricing deviations from the optimal equilibrium but also dampens platform investment incentives by reducing expected commission revenues. The results indicate that firms' risk-averse behavior initiates a vicious cycle of "low investment – low pricing – low profits", ultimately causing synchronous declines in the expected profits of both platforms and firms. This finding reveals the negative externality transmission mechanism of risk attitudes within a decentralized decision-making framework from a game-theoretic perspective.

#### 4.3.4. Resilience evaluation metrics

In this section, a supply chain model is constructed by setting resilience investment parameter  $\beta = 0$ , providing a reference for analyzing the economic effects of platform resilience investment. Specifically, when platform resilience investment  $\beta = 0$ , the demand function is expressed as:

$$d = \varepsilon + \int_{p+\alpha\gamma-b}^1 f(v) dv = 1 - p - \alpha\gamma + b + \varepsilon. \quad (19)$$

This expression is obtained by performing a parameter transformation of  $\beta = 0$  on the basic model equation (1). The profit and utility functions for metaverse platforms and firms follow the baseline model specifications

TABLE 9. Parameter assignment and sources.

Notation	Definition	Assignment	Sources
$\alpha$	Consumer data security concern coefficient	0.18	Meta quarterly financial report
$\eta$	The commission ratio extracted by the metaverse platform for transactions	47.5%	Media reports
$F$	Data asset losses caused by hacker attacks on the metaverse platform	[0, 3]	Ireland's Data Protection Commission
$\lambda_i$	Risk aversion coefficient, where $i \in (o, r)$	0.5	Yan <i>et al.</i> [77]
$\sigma$	Stochastic demand standard deviation	1	Wang <i>et al.</i> [78]
$\gamma$	The probability of a hacker attack	0.18	Luo and Choi [49]
$b$	The benefits of immersion for consumers	0.7	Novak <i>et al.</i> [79]; Kim and Ko [80]; Cha <i>et al.</i> [81]
$c$	The construction cost of immersion generated by unit metaverse transactions	0.25	Combined with data analysis company report comprehensive setting.

(see Tab. 5), with differences only in the value of the resilience investment parameter  $\beta$ . Based on the above setup, this study further develops a profit difference ( $PD$ ) metric, mathematically defined as:

$$PD^H = \pi_o((\beta^*)^H) - \pi_o((\beta = 0)^H) \quad (20)$$

where  $\pi_o((\beta^*)^H)$  represents platform profits under resilience investment, corresponding to the eight game combinations in the baseline model (four risk attitudes  $\times$  two data asset loss states);  $\pi_o((\beta = 0)^H)$  denotes profits under non-resilience investment, *i.e.*, the eight game combinations in the extended non-resilience scenario. Since the platform's profit function already includes resilience investment costs  $\frac{k\beta^2}{2}$ , this metric directly reflects the net contribution of investment behavior to platform profits.

**Proposition 13.** *Platform resilience investment always generates positive benefits.*

Proposition 13 indicates that resilience investment significantly increases platform profits ( $PD > 0$ ) regardless of whether supply chain members exhibit risk-averse characteristics or face data asset loss risks. The result reveals that synergistic benefits from resilience investment not only cover initial input costs but also effectively expand platform commission revenue through optimized resource allocation mechanisms.

## 5. CASE STUDY

To further demonstrate the impact of various risk attitudes and data asset losses on the equilibrium decisions of the metaverse supply chain, we employ the case of *Meta* to visually illustrate the essential propositions above and provide further management insights.

### 5.1. Case details and parameter assignments

Based on existing literature and industry empirical data, this study systematically assigns values to each parameter, with detailed settings summarized in Table 9. The derivation processes and rationales for parameterization are elaborated as follows:

- (i) Consumer data security concern coefficient  $\alpha$ .  
Responsible for virtual reality and metaverse businesses, *Meta's* Reality Labs reported Q1 2022 revenue of \$695 million, a significant increase from \$534 million in the same period of 2021. Concurrently, operating costs surged from \$2.4 billion to \$3.7 billion. Given *Meta's* lack of detailed cost disclosures, this study assumes that the division's high costs are equally allocated to metaverse platform resilience construction and technological investment (50% each), a proportion that cancels out in calculations and thus does not affect results. Using this assumption, the revenue growth driven by platform resilience investment in Q1 2022 is estimated as  $\frac{(6.95-5.34) \times 50\%}{(37-24) \times 50\%}$ <sup>3</sup>. A similar quantitative analysis for Q2 yields  $\frac{(4.52-3.05) \times 50\%}{(33-27) \times 50\%}$ <sup>4</sup>. To enhance robustness, the arithmetic average of the two quarters, *i.e.*,  $\left(\frac{(6.95-5.34) \times 50\%}{(37-24) \times 50\%} + \frac{(4.52-3.05) \times 50\%}{(33-27) \times 50\%}\right) / 2 \approx 0.18$ , serves as the benchmark. Motivated by consumers' high sensitivity to data security, we posit that resilience investment strengthens perceived security, translating into revenue growth. The consumer security concern coefficient is therefore set at  $\alpha = 0.18$ .
- (ii) Commission rate  $\eta$ .  
Drawing on publicly reported data, *Meta* charges a 47.5% commission fee for virtual asset transactions, a transparent and widely adopted structure<sup>5</sup>. This study sets the platform's commission rate parameter as  $\eta = 47.5\%$ .
- (iii) Data asset losses  $F$ .  
In November 2022, Ireland's Data Protection Commission fined *Meta* €265 million ( $\approx$ \$276 million) for a software vulnerability causing over 500 million user data leaks<sup>6</sup>. Given the significant measurement difficulties in assessing digital asset losses and the fact that this case exhibits typical characteristics of a data security incident, this study draws reference from this authoritative regulatory penalty case to set the value range for data asset losses as  $F \in [0, 3]$ .
- (iv) Risk aversion coefficient  $\lambda_i$ ,  $i \in (o, r)$ .  
Following Yan *et al.*'s [77] framework for supply chain risk preferences, the risk aversion coefficient is set at  $\lambda_i = 0.5$  to quantify stakeholders' risk attitudes.
- (v) Stochastic demand standard deviation  $\sigma$ .  
Adopting the standard deviation proposed by Wang *et al.* [78], the stochastic demand standard deviation is specified as  $\sigma = 1$ , capturing market demand uncertainty accurately.
- (vi) The probability of a hacker attack  $\gamma$ .  
Referring to Luo and Choi's [49] research on platform security risks, the probability of a hacker attack is set at  $\gamma = 0.18$ .
- (vii) The benefits of immersion for consumers  $b$ .  
Empirical studies show that virtual technologies influence user behavior through immersion and flow experiences, with path coefficients ranging from 0.6 to 0.8 [79–81]. Using the midpoint for representativeness, the immersion technology coefficient is set at  $b = 0.7$ .
- (viii) The construction cost of immersion  $c$ .  
This study uses the cost of *Meta's* leading consumer-grade VR device Quest 2 as a proxy variable for investment in immersion construction, primarily based on the following research considerations: (a) limited industry-level cost data in the early metaverse development stage; (b) *Meta's* representative cost structure as an industry leader; and (c) the positive correlation between hardware configuration and immersion experience. Counterpoint Research reports a bill of materials (BOM) cost of \$264.2<sup>7</sup>, while

<sup>3</sup> <https://www.uploadvr.com/meta-q1-2022-earnings-costs-revenue/>.

<sup>4</sup> <https://www.uploadvr.com/meta-revenue-now-growing-faster-than-costs/>.

<sup>5</sup> <https://www.cnbc.com/2022/04/13/meta-plans-to-take-a-nearly-50percent-cut-on-nft-sales-in-its-metaverse.html>.

<sup>6</sup> <https://www.theverge.com/2022/11/28/23481786/meta-fine-facebook-data-leak-ireland-dpc-gdpr>.

<sup>7</sup> <https://xrdailynews.com/quest-3-bom-production-costs-revealed/>.

Nikkei Asia estimates core component costs at \$182<sup>8</sup>. After weighting these sources and calibrating with the market price (\$299)<sup>9</sup>, the unit immersion cost parameter is standardized to  $c = 0.25$ . This value lies within the actual cost range and, through sensitivity analysis, ensures non-negative equilibrium solutions, safeguarding result robustness.

## 5.2. Example analysis

Firstly, we investigate the impact of data asset losses on the equilibrium decision. Figure 3a demonstrates that the data asset losses are beneficial for firms irrespective of the members' risk attitude, thus verifying the correctness of Proposition 3. Figure 3b shows that there is no correlation between the risk aversion coefficient and the changes in profits due to data asset losses, *i.e.*,  $\Delta E(\pi_o^M) = \Delta E(\pi_o^O) = \Delta E(\pi_o^R) = \Delta E(\pi_o^A)$ . We also observe in Figure 3b that the resilience investment cost coefficient limits the direction of the effect of data asset losses on platform profits. When the coefficient is high and losses are moderate, platform profits are negatively affected, *i.e.*,  $\Delta E(\pi_o^M) = \Delta E(\pi_o^O) = \Delta E(\pi_o^R) = \Delta E(\pi_o^A) < 0$  applies when  $k > k_6$  and  $F < F_9$  occurs. To further explore the impact of data asset losses on the supply chain system in the metaverse, we present Figure 3c. Figure 3c indicates that the losses are beneficial for the supply chain system when the cost coefficient is low or when both the coefficient and losses are high, which is the result revealed by Proposition 5.

Next, we analyze how risk attitudes impact supply chain equilibrium. Figures 4 and 5 demonstrates the effect of various risk attitudes on the profits of both the supply chain members and the system, considering (ignoring) the loss of data assets. From Figures 4a and 5a, we observe that regardless of considering or ignoring data asset losses, firms always benefit the most under risk neutrality and the least under full member risk aversion. Meanwhile, Figure 4a shows that under the conditions of firm risk aversion and platform risk aversion, the magnitude relationship between firm's profits alternates within different resilience investment cost coefficients, namely  $E(\pi_r^{ON}) < E(\pi_r^{RN})$  holds when  $\underline{k} < k < k_9$ ; otherwise,  $E(\pi_r^{ON}) > E(\pi_r^{RN})$  holds. Similar results can also be found in Figure 5a. In addition, high data asset losses can help firms achieve higher returns when self-risk aversion is presented. In other words,  $F > F_{12}$  can transform  $E(\pi_r^{OY}) > E(\pi_r^{RY})$  into  $E(\pi_r^{OY}) < E(\pi_r^{RY})$  when  $k > k_9$ . This result can be observed in Figure 5b.

Figures 4b and 5c demonstrate the impact of varying risk attitudes on platform profitability. Similar to firms, platforms generate the greatest profit when risk neutrality prevails, regardless of whether data asset losses are considered or not. Differing from firms, the sole limiting factor on platform's profit is the resilience investment cost coefficient. From Figures 4b and 5c, it is evident that the platform can generate considerable profits through reduced cost coefficient when firms are risk averse; otherwise, it benefits more from self-risk aversion. As Proposition 8 illustrates,  $E(\pi_o^A) < E(\pi_o^O) < E(\pi_o^R) < E(\pi_o^M)$  exists when  $\underline{k} < k < k_{10}$  is met; otherwise,  $E(\pi_o^A) < E(\pi_o^R) < E(\pi_o^O) < E(\pi_o^M)$  holds.

We also investigate the effect of various risk attitudes on the benefits of the metaverse supply chain system and present the outcomes in Figures 4c and 5d. As shown in Figure 4c, when the resilience investment cost coefficient is low, the system obtains the highest benefit from risk neutrality, followed by firm risk aversion, platform risk aversion and full member risk aversion. The elevated cost coefficient leads to a reversal of the system's profit situation under firm risk aversion and platform risk aversion, *i.e.*,  $E(\pi_{sc}^{AN}) < E(\pi_{sc}^{RN}) < E(\pi_{sc}^{ON}) < E(\pi_{sc}^{MN})$  holds when  $k > k_{11}$ . Similar results can also be found in Figure 5d. Furthermore, it has been shown by Figure 5b that high losses in data assets can result in greater profits for firms with self-risk aversion. As the profit total of firm and platform, system profits have the potential to reach  $E(\pi_{sc}^{AY}) < E(\pi_{sc}^{OY}) < E(\pi_{sc}^{RY}) < E(\pi_{sc}^{MY})$  on a greater magnitude, as evidenced by Figure 5e, and corresponds with the theoretical findings of Proposition 9.

## 5.3. Platform scale analysis

This study selects *Meta* as a case due to its representative technological investments, user base, and industry influence in the metaverse domain. However, as a large technology platform, *Meta*'s resource endowments, risk

<sup>8</sup> <https://mixed-news.com/en/meta-quest-pro-bill-of-materials-cost/>.

<sup>9</sup> <https://www.pcgamer.com/oculus-quest-2-officially-revealed-at-dollar299-preorders-are-live-now/>.

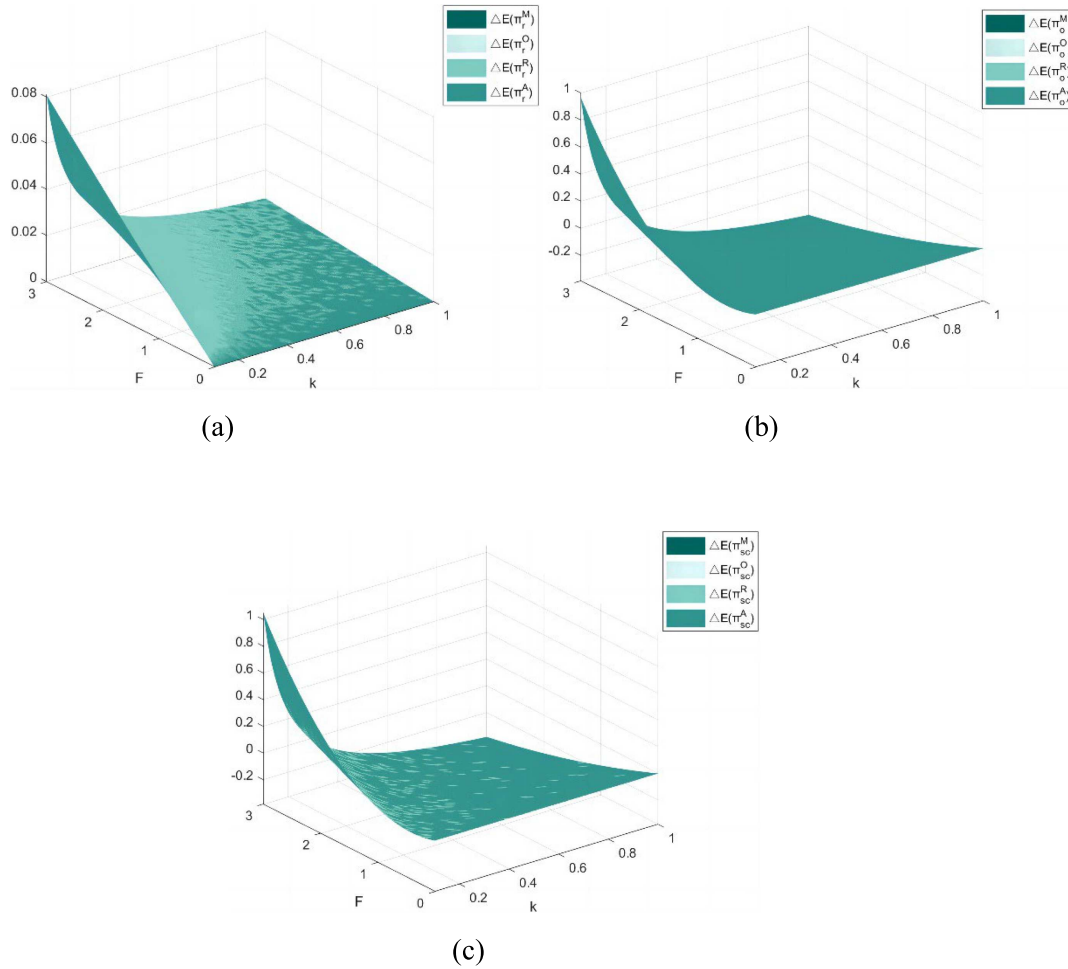


FIGURE 3. The impact of data asset losses on the profits of the metaverse supply chain. (a) Profit comparison of firm. (b) Profit comparison of platform. (c) Profit comparison of supply chain system.

preferences, and market position may differ from those of smaller or emerging platforms. Thus, generalization of research findings requires contextual consideration. Specifically, compared with *Meta*, emerging platforms may exhibit the following differences:

- (i) Resource asymmetry: As an industry leader, *Meta* likely faces lower marginal costs of technological investment (*i.e.*, a smaller  $k$ ), whereas smaller or emerging platforms may have a larger  $k$  due to capital constraints.
- (ii) Risk attitudes: The large platforms like *Meta*, with robust financial reserves and diversified revenue streams, can absorb short-term investment losses or financial shocks from security incidents. In contrast, smaller platforms' limited budgets make them unable to withstand direct losses from high investment failures or security events, leading to more conservative decision-making and stronger risk aversion (*i.e.*, a larger  $\lambda_o$ ).
- (iii) Consumer trust levels: As a well-established brand, *Meta* benefits from a loyal customer base and strong reputation, which may reduce consumers' sensitivity to security risks (*i.e.*, a lower  $\alpha$ ). Consumers of smaller

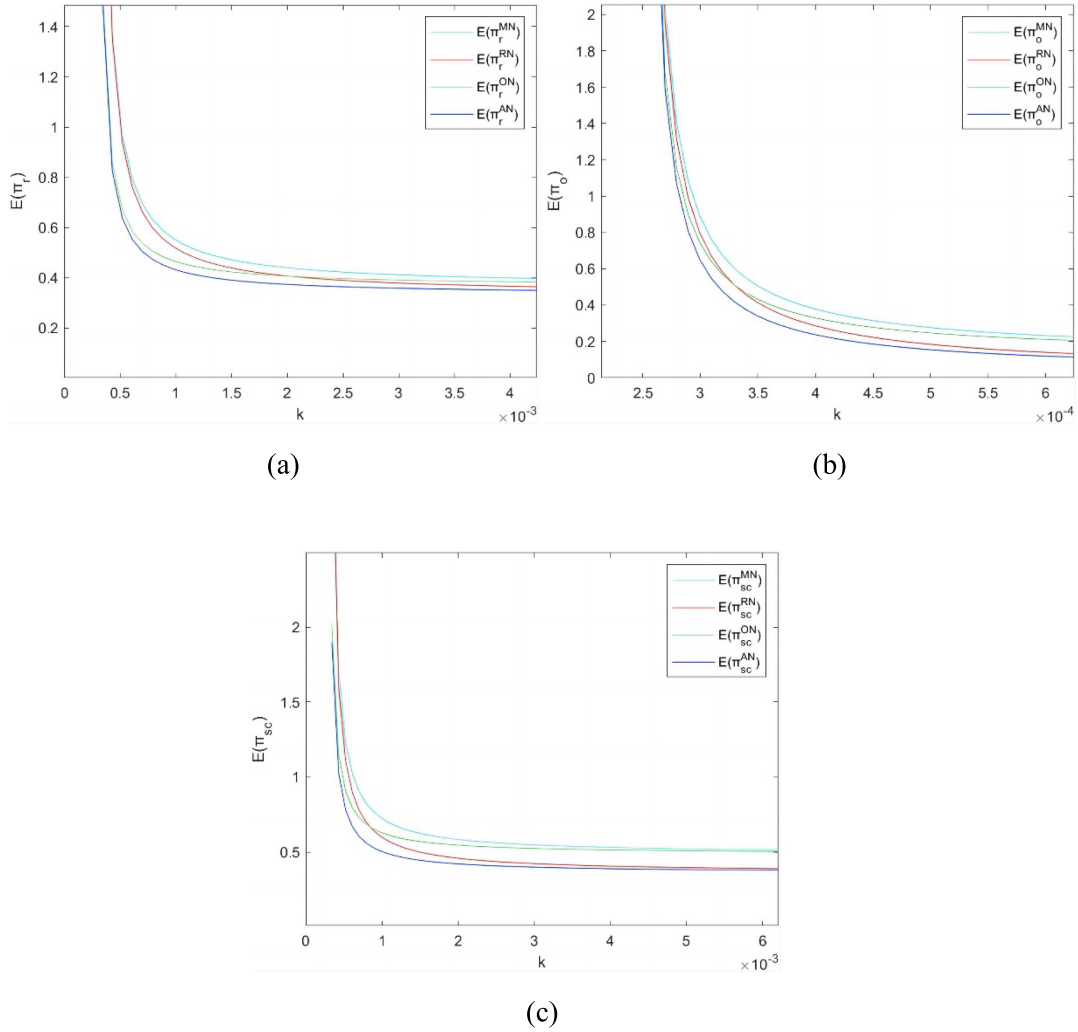


FIGURE 4. The impact of risk attitudes on metaverse supply chain profits under ignoring data asset losses. (a) Profit comparison of firm. (b) Profit comparison of platform. (c) Profit comparison of supply chain system.

or emerging platforms, however, are likely more sensitive to data security (*i.e.*, a higher  $\alpha$ ), increasing the dependency of the demand function on resilience investment levels  $\beta$ .

Based on the sensitivity analysis in Proposition 1, increases in  $k$  and  $\lambda_o$  lead to lower platform resilience investment, reduced product prices, and smaller demand scales. Additionally, a higher  $k$  makes it easier to exceed the critical threshold  $k_j, j \in \{1, 2, \dots, 11\}$ , causing the impact of increased  $\alpha$  on equilibrium solutions to decline across a broader range. A higher  $k$  also exacerbates the negative effects of data asset loss on platform and supply chain profits, meaning that within a wider parameter space, profits considering data asset loss are lower than those without. Importantly, regardless of whether data asset loss is included in the model, a higher  $k$  does not alter the conclusion that the “full-member risk neutrality” scenario yields maximum benefits for platforms, firms, and the supply chain system. However, it does strengthen the suboptimal position of all parties when only the platform exhibits risk aversion.

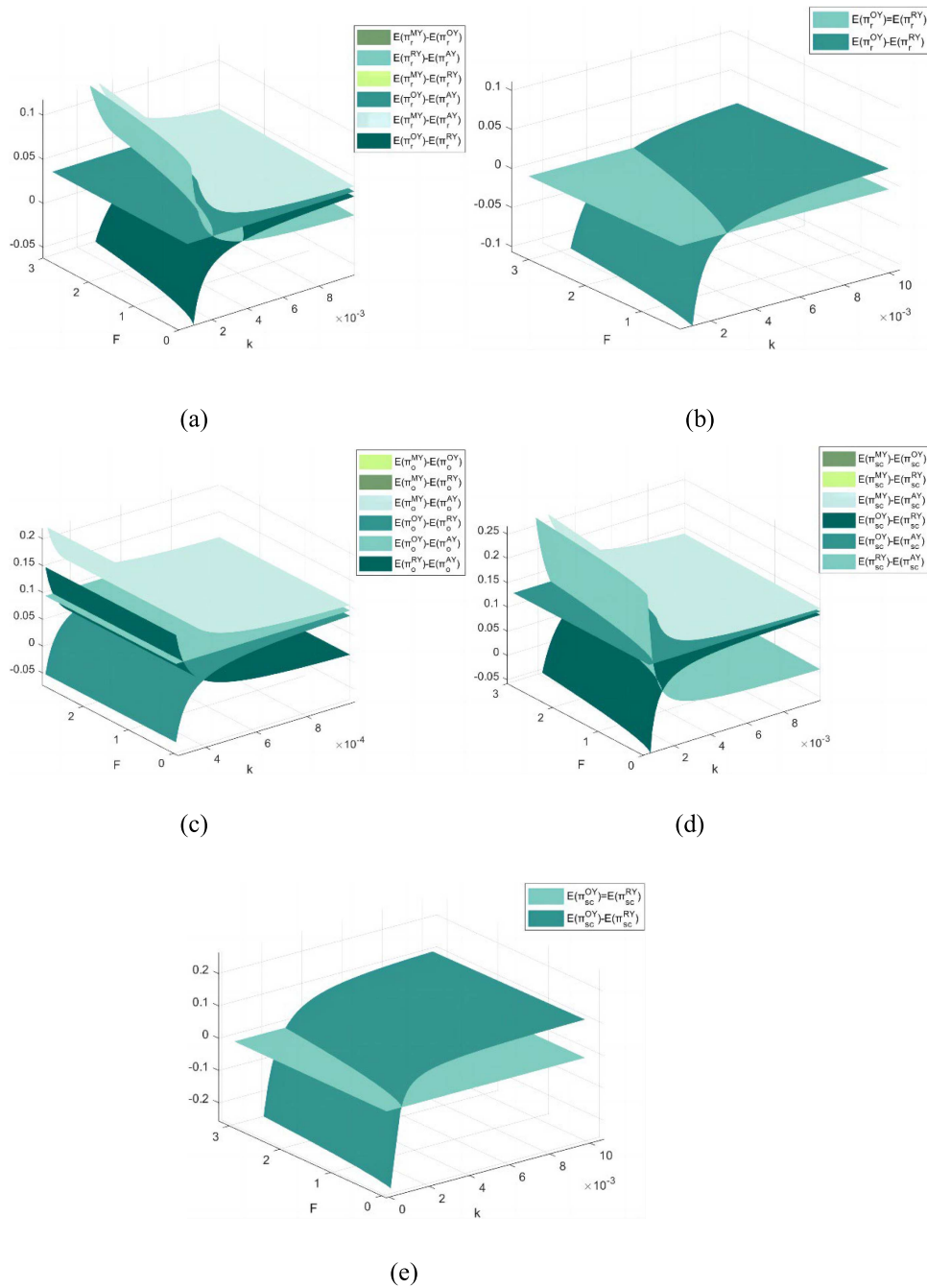


FIGURE 5. The impact of risk attitudes on metaverse supply chain profits under considering data asset losses. (a) Profit comparison of firm. (b) Profit comparison of  $E(\pi_r^{OY})$  and  $E(\pi_r^{RY})$ . (c) Profit comparison of platform. (d) Profit comparison of supply chain system. (e) Profit comparison of  $E(\pi_{sc}^{OY})$  and  $E(\pi_{sc}^{RY})$ .

## 6. CONCLUSION

By integrating data security and supply chain resilience, we construct a metaverse supply chain model to explore the optimal resilience investment and pricing decisions. Our analysis combines risk attitudes and data asset losses, examining how risk aversion behavior impacts metaverse equilibrium decisions, concentrating on examining the effect of data asset losses in enhancing platform resilience. In addition, we analyze the impact of crucial parameters on equilibrium outcomes and test our conclusions through case analysis.

### 6.1. Main findings

- (i) **The Role of Data Asset Losses:** Integrating data asset loss into the model not only promotes platform security resilience but also enhances firm profitability through price-demand synergies, particularly under risk-neutral and firm risk-averse scenarios. For platforms, when the resilience investment cost coefficient exceeds a critical threshold or moderate data asset losses occur, platform profits may decline. Notably, in contexts where improved transaction environments boost commission revenues, higher cost constraints combined with significant data asset losses can paradoxically generate excess platform profits, illustrating the complex interplay between security investments and commercial returns.
- (ii) **The Influence of Risk Attitudes:** Heterogeneous risk attitudes exert differentiated effects on supply chain decisions. Platform risk aversion simultaneously dampens resilience investment and product pricing, whereas firm risk aversion influences only the pricing channel. Risk-averse behavior significantly lowers product prices, creating a price trough under full-member risk aversion and a price peak under full-member risk neutrality. Specifically, high resilience investment costs amplify price concessions driven by firm risk aversion, while platform risk aversion dominates price declines under low-cost conditions. Similar patterns emerge in the interaction between risk preference and the profits of metaverse platforms and firms, with the Pareto optimal state achieved under full-member risk neutrality.
- (iii) **The Impact of Key Parameters:** Consumer data security concern and hacker attack probability compel platforms to increase resilience investment by intensifying security risk disutility. The lower cost coefficients motivate platforms to proactively invest in risk mitigation, driving synchronized growth in prices and demand – an effect weakened by platform risk aversion. Under high-cost constraints, limited resilience investment makes it difficult to reverse demand slumps even through price cuts. Further analysis reveals that rising resilience investment costs inhibit platform investment, while higher commission rates enhance platform revenue expectations, effectively incentivizing security investments and prompting firms to adjust prices in tandem. Demand uncertainty is negatively correlated with firm pricing, while its impact on platform strategy shows a significant dependence on risk attitude. When firms avoid risks, demand uncertainty and platform resilience investment remain independent, while under other risk attitudes, the increase in demand uncertainty will directly reduce the platform’s investment motivation. In addition, the risk attitudes of supply chain members exhibit a divergent transmission path, manifested as platform risk aversion simultaneously suppressing resilience investment and product pricing, while firm risk aversion acts solely through the pricing channel.
- (iv) **Dynamic Equilibrium Characteristics of Resilience Investment:** Firms’ risk attitudes significantly impact dual-platform resilience strategies, manifested in the fact that when firms are risk aversion, higher consumer trust coefficients reduce both platforms’ resilience investment synchronously; under firm risk neutrality, rising trust drives incumbent platforms’ investment to grow monotonically while emerging platforms’ investment follows a U-shaped trajectory of first decreasing then increasing. An increase in the investment cost coefficient reduces the incumbent platform’s incentive for resilience investment, whereas the emerging platform, benefiting from a narrowed cost disadvantage, tends to intensify resilience investment to achieve market expansion. Mechanistic analysis of data asset loss shows that without data loss, platform investment is strictly bounded by the consumer psychological threshold; with data loss embedded, investment may exceed this threshold only when the psychological threshold is low, otherwise it remains an upper bound. Equilibrium analysis in the Nash game framework indicates that platform risk aversion coefficients

do not affect supply chain members' strategic choices, while data asset loss consistently increases firm profits. Firm risk aversion, however, simultaneously reduces resilience investment and expected profits for metaverse supply chain members. Importantly, regardless of risk attitude combinations or data asset loss inclusion, platform resilience investment always generates positive benefits by enhancing consumer security perceptions.

## 6.2. Management insights

Based on the research findings, the following stratified recommendations are proposed for metaverse platforms, metaverse firms, and policymakers:

### 6.2.1. Metaverse platforms

- (i) **Develop a Data Asset Loss Risk Quantification Model:** Platform operators should integrate historical operational data and industry benchmark cases to establish a framework for quantifying data asset loss risks. Through market surveys and user behavior analysis, core parameters such as consumer data security concern coefficients, hacker attack probabilities, and resilience investment cost coefficients can be systematically estimated. Substituting these parameters into the equilibrium analysis model (see Tab. 6) enables determination of optimal resilience investment levels under differentiated operational scenarios.
- (ii) **Implement Graded Resilience Investment Strategies:** Differentiated investment strategies should be adopted based on resilience investment cost coefficients. When costs are low, platforms should proactively increase resilience investment to attract security sensitive users through enhanced data security, thereby synchronously improving pricing power and market demand. When costs exceed critical thresholds, collaborative mechanisms such as cost-sharing contracts (*e.g.*, joint investment with metaverse firms) and revenue-sharing agreements (*e.g.*, linking resilience investment to commission rates) should be established to foster multi-party collaboration in securing transaction environments, preventing excessive contraction of resilience investment due to unilateral cost pressures.
- (iii) **Promote Risk Assessment Collaboration and Strategic Alliances:** Given the dampening effects of risk aversion on platform resilience and profitability, leading platforms can initiate "risk-neutral strategic alliances" to share risk assessment tools and supply chain risk data. Such initiatives reduce systemic uncertainty and facilitate the achievement of Pareto optimal equilibria.

### 6.2.2. Metaverse firms

- (i) **Quantify Risk Aversion Coefficients and Optimize Pricing:** Firms should use historical transaction data to quantify how their risk attitudes influence pricing strategies, avoiding profit losses from excessive unilateral price reductions under high resilience investment costs.
- (ii) **Establish Risk-Sharing and Cost-Allocation Mechanisms:** Enter into risk-sharing agreements with platforms to define clear rules for allocating resilience investment costs, while negotiating commission rate discounts or traffic support as compensation. These measures mitigate capital risks for both parties and prevent profit erosion caused by excessive risk aversion in the supply chain.
- (iii) **Adopt Data-Security-Based Product Differentiation Pricing:** In response to consumer data security concerns, firms should explicitly disclose their own and platform's data protection measures (*e.g.*, blockchain technology) in product detail pages and implement tiered pricing strategies based on security levels.

### 6.2.3. Policymakers

- (i) **Build a Regulatory Framework for Data Asset Loss Quantification:** Governments should establish uniform policies to clarify liability standards, loss assessment methodologies, and compensation mechanisms for data security incidents. This prevents platforms from neglecting long-term resilience due to short-term financial pressures and imposes strict penalties on entities failing to meet resilience investment standards.
- (ii) **Strengthen Information Disclosure and Decision Coordination:** Enforce policies requiring platforms to regularly disclose resilience investment scales, data asset loss contingency plans, and risk preference parameters,

enhancing supply chain transparency. Additionally, promote the creation of risk information-sharing platforms to facilitate coordination in pricing and investment decisions among metaverse participants, reducing market inefficiencies caused by information asymmetry.

- (iii) Provide Fiscal Incentives to Lower Investment Barriers: To address the disincentive effects of high resilience investment costs, governments should offer fiscal subsidies, tax reductions, and other incentives to platforms that proactively enhance security resilience. These measures lower platforms' marginal investment costs and promote sustainable growth in security investments.

### 6.3. Future research

While this study contributes to metaverse supply chain optimization, several limitations warrant future exploration. First, the research assumes platforms independently bear resilience investment costs, whereas real-world scenarios may involve specialized service providers sharing these functions. Future studies could investigate resilience strategies across different stakeholders (in-house *vs.* third-party investments) and how to achieve Pareto optimality between security and economic efficiency. Second, existing literature highlights that consumer purchase intent for metaverse products may boost sales of real-world goods [17], but this study does not address the synergistic effects between virtual and physical product sales. Exploring dynamic pricing and marketing allocation strategies across virtual and physical products, and their impacts on overall supply chain efficiency, represents a promising research avenue.

#### FUNDING

This work was supported by the National Office of Philosophy and Social Science of China (Grant No. 24AJY030).

#### DATA AVAILABILITY STATEMENT

The research data associated with this article are included in the article.

#### REFERENCES

- [1] H. Wang, H. Ning, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding and M. Daneshmand, A survey on the metaverse: the state-of-the-art, technologies, applications, and challenges. *IEEE Int. Things J.* **10** (2023) 14671–14688.
- [2] K. Yoo, R. Welden, K. Hewett and M. Haenlein, The merchants of meta: a research agenda to understand the future of retailing in the metaverse. *J. Retail.* **99** (2023) 173–192.
- [3] S. Richter and A. Richter, What is novel about the metaverse? *Int. J. Inf. Manag.* **73** (2023) 102684.
- [4] H. Park and R.E. Lim, Fashion and the metaverse: clarifying the domain and establishing a research agenda. *J. Retail. Consum. Serv.* **74** (2023) 103413.
- [5] Y. Fu, C. Li, F.R. Yu, T.H. Luan, P. Zhao and S. Liu, A survey of blockchain and intelligent networking for the metaverse. *IEEE Int. Things J.* **10** (2023) 3587–3610.
- [6] R.K. Sadeghi, A. Azadegan and D. Ojha, A path to build supply chain cyber-resilience through absorptive capacity and visibility: two empirical studies. *Ind. Mark. Manag.* **111** (2023) 202–215.
- [7] Q. Bai, J. Xu and S.S. Chauhan, Effects of sustainability investment and risk aversion on a two-stage supply chain coordination under a carbon tax policy. *Comput. Ind. Eng.* **142** (2020) 106324.
- [8] C. Liu, H. Ji and J. Wei, Smart supply chain risk assessment in intelligent manufacturing. *J. Comput. Inf. Syst.* **62** (2022) 609–621.
- [9] B. Xin and Y. Xu, Optimal subsidy strategies in a smart supply chain driven by dual innovation. *Int. J. Ind. Eng. Comput.* **13** (2022) 557–572.
- [10] Q. Li, B. Li, P. Chen and P. Hou, Dual-channel supply chain decisions under asymmetric information with a risk-averse retailer. *Ann. Oper. Res.* **257** (2017) 423–447.
- [11] A. Bilgihan, A. M. W. Leong, F. Okumus and J. Bai, Proposing a metaverse engagement model for brand development. *J. Retail. Consum. Serv.* **78** (2024) 103781.
- [12] H. Shin and J. Kang, How does the metaverse travel experience influence virtual and actual travel behaviors? Focusing on the role of telepresence and avatar identification. *J. Hosp. Tour. Manag.* **58** (2024) 174–183.

- [13] D. Chakraborty, A. Polisetty and N.P. Rana, Consumers' continuance intention towards metaverse-based virtual stores: a multi-study perspective. *Technol. Forecast. Soc. Chang.* **203** (2024) 123405.
- [14] K.G. Barrera and D. Shah, Marketing in the metaverse: conceptual understanding, framework, and research agenda. *J. Bus. Res.* **155** (2023) 113420.
- [15] A. Mehrotra, R. Agarwal, A. Khalil, E.A. Alzeiby and V. Agarwal, Nitty-gritties of customer experience in metaverse retailing. *J. Retail. Consum. Serv.* **79** (2024) 103876.
- [16] S. Ahn, B.E. Jin and H. Seo, Why do people interact and buy in the metaverse? Self-Expansion perspectives and the impact of hedonic adaptation. *J. Bus. Res.* **175** (2024) 114557.
- [17] R. Payal, N. Sharma and Y.K. Dwivedi, Unlocking the impact of brand engagement in the metaverse on real-world purchase intentions: analyzing pre-adoption behavior in a futuristic technology platform. *Electron. Commer. Res. Appl.* **65** (2024) 101381.
- [18] D. Buhalis, M.S. Lin and D. Leung, Metaverse as a driver for customer experience and value co-creation: implications for hospitality and tourism management and marketing. *Int. J. Contemp. Hosp. Manag.* **35** (2023) 701–716.
- [19] P.B. Lowry, W.F. Boh, S. Petter and J.M. Leimeister, Long live the metaverse: identifying the potential for market disruption and future research. *J. Manag. Inform. Syst.* **42** (2025) 3–38.
- [20] Y.K. Dwivedi, L. Hughes, A.M. Baabdullah, S. Ribeiro-Navarrete, M. Giannakis, M.M. Al-Debei, D. Dennehy, B. Metri, D. Buhalis, C.M.K. Cheung, K. Conboy, R. Doyle, R. Dubey, V. Dutot, R. Felix, D.P. Goyal, A. Gustafsson, C. Hinsch, I. Jebabli, M. Janssen, Y.-G. Kim, J. Kim, S. Koos, D. Kreps, N. Kshetri, V. Kumar, K.-B. Ooi, S. Papagiannidis, I.O. Pappas, A. Polyviou, S.-M. Park, N. Pandey, M.M. Queiroz, R. Raman, P.A. Rauschnabel, A. Shirish, M. Sigala, K. Spanaki, G.W.-H. Tan, M.K. Tiwari, G. Viglia and S.F. Wamba, Metaverse beyond the hype: multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Int. J. Inf. Manag.* **66** (2022) 102542.
- [21] Y. Otoum, N. Gottimukkala, N. Kumar and A. Nayak, Machine learning in metaverse security: current solutions and future challenges. *ACM Comput. Surv.* **56** (2024). 1–36
- [22] A. Gupta, S. Sawhney and K. Kompella, The first principles: setting the context for a safe and secure metaverse. *ACM Comput. Surv.* **56** (2024) 1–29.
- [23] Y. Bai, H. Lei, S. Li, H. Gao, J. Li, L. Li and I.C. Soc, Decentralized and self-sovereign identity in the era of blockchain: a survey, in 5th IEEE International Conference on Blockchain (Blockchain). Espoo, Finland (2022) 500–507.
- [24] M. Alkaeed, A. Qayyum and J. Qadir, Privacy preservation in Artificial Intelligence and Extended Reality (AI-XR) metaverses: a survey. *J. Netw. Comput. Appl.* **231** (2024) 103989.
- [25] G. Kang, J. Koo and Y.-G. Kim, Security and privacy requirements for the metaverse: a metaverse applications perspective. *IEEE Commun. Mag.* **62** (2024) 148–154.
- [26] A. McLeod and D. Dolezel, Cyber-analytics: modeling factors associated with healthcare data breaches. *Decis. Support Syst.* **108** (2018) 57–68.
- [27] M.R. Uddin, S. Akter and W.J.T. Lee, Developing a data breach protection capability framework in retailing. *Int. J. Prod. Econ.* **271** (2024) 109202.
- [28] K. Alharbi and A. Alkhalifah, Examining the role of trust and privacy effects through online reviews in social commerce using an integrated model and hybrid approach analysis. *IEEE Trans. Eng. Manag.* **71** (2024) 10943–10965.
- [29] Y. Wang and C. Herrando, Does privacy assurance on social commerce sites matter to millennials? *Int. J. Inf. Manag.* **44** (2019) 164–177.
- [30] R. Janakiraman, J.H. Lim and R. Rishika, The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer. *J. Mark.* **82** (2018) 85–105.
- [31] B.C.F. Choi, S.S. Kim and Z. Jiang, Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *J. Manag. Inf. Syst.* **33** (2016) 904–933.
- [32] S. Laradi, M. Alrawad, A. Lutfi and G. Agag, Understanding factors affecting social commerce purchase behavior: a longitudinal perspective. *J. Retail. Consum. Serv.* **78** (2024) 103751.
- [33] E.J. Nijssen, M. van der Borgh and D. Totzek, Dealing with privacy concerns in product-service system selling: value-based selling as fair treatment practice. *Ind. Mark. Manag.* **105** (2022) 60–71.
- [34] E.Y. Chan and M. Palmeira, Political ideology moderates consumer response to brand crisis apologies for data breaches. *Comput. Hum. Behav.* **121** (2021) 106801.
- [35] W.-P. Wong, K.H. Tan, K. Govindan, D. Li and A. Kumar, A conceptual framework for information-leakage-resilience. *Ann. Oper. Res.* **329** (2023) 931–951.

- [36] M.S. Hossain, H. Belina, M.M. Hasan and M.M. Kim, The effects of auditor-level cybersecurity breaches on auditor-client relationships. *Eur. Account. Rev.* ahead-of-print (2024). DOI: [10.1080/09638180.2024.2435389](https://doi.org/10.1080/09638180.2024.2435389).
- [37] Z. Rezaee, G. Zhou and L. Bu, Corporate social irresponsibility and the occurrence of data breaches: a stakeholder management perspective. *Int. J. Account. Inf. Syst.* **53** (2024) 100677.
- [38] H. Cao, H.V. Phan and S. Silveri, Data breach disclosures and stock price crash risk: evidence from data breach notification laws. *Int. Rev. Financ. Anal.* **93** (2024) 103164.
- [39] U. Soni, V. Jain and S. Kumar, Measuring supply chain resilience using a deterministic modeling approach. *Comput. Ind. Eng.* **74** (2014) 11–25.
- [40] V. Jain, S. Kumar, U. Soni and C. Chandra, Supply chain resilience: model development and empirical analysis. *Int. J. Prod. Res.* **55** (2017) 6779–6800.
- [41] S. Ambulkar, J. Blackhurst and S. Grawe, Firm’s resilience to supply chain disruptions: scale development and empirical examination. *J. Oper. Manag.* **33, 34** (2015) 111–122.
- [42] J. Gheidar-Kheljani and K. Halat, Developing a resilient supply chain in complex product systems through investment in reliability and cooperative contracts. *RAIRO-Oper. Res.* **58** (2024) 79–102.
- [43] V.S. Narwane, R.D. Raut, S.K. Mangla, M. Dora and B.E. Narkhede, Risks to big data analytics and blockchain technology adoption in supply chains. *Ann. Oper. Res.* **327** (2023) 339–374.
- [44] S. Modgil, S. Gupta, R. Stekelorum and I. Laguir, AI technologies and their impact on supply chain resilience during COVID-19. *Int. J. Phys. Distrib. Logist. Manag.* **52** (2022) 130–149.
- [45] M. Asante, G. Epiphaniou, C. Maple, H. Al-Khateeb, M. Bottarelli and K.Z. Ghafoor, Distributed ledger technologies in supply chain security management: a comprehensive survey. *IEEE Trans. Eng. Manag.* **40** (2023) 713–739.
- [46] R.K. Sadeghi, D. Ojha and A. Azadegan, Data systems in supply chain resilience: moderated moderating effects of enterprise resource planning. *Ind. Manag. Data Syst.* **125** (2025) 1437–1463.
- [47] J.-B. Kim, C. Wang and F. Wu, Privacy breaches and the effect of customer notification. *MIS Q.* **48** (2024) 1483–1502.
- [48] T. Valletti and J. Wu, Consumer profiling with data requirements: structure and policy implications. *Prod. Oper. Manag.* **29** (2020) 309–329.
- [49] S. Luo and T.-M. Choi, E-commerce supply chains with considerations of cyber-security: should governments play a role? *Prod. Oper. Manag.* **31** (2022) 2107–2126.
- [50] J.M. Song, T. Wang, J.-C. Yen and Y.-H. Chen, Does cybersecurity maturity level assurance improve cybersecurity risk management in supply chains? *Int. J. Account. Inf. Syst.* **54** (2024) 100695.
- [51] A. Adhikari, A. Bisi and B. Avittathur, Coordination mechanism, risk sharing, and risk aversion in a five-level textile supply chain under demand and supply uncertainty. *Eur. J. Oper. Res.* **282** (2020) 93–107.
- [52] C.H. Chiu, T.M. Choi and X. Li, Supply chain coordination with risk sensitive retailer under target sales rebate. *Automatica* **47** (2011) 1617–1625.
- [53] C.H. Chiu, T.M. Choi, G. Hao and X. Li, Innovative menu of contracts for coordinating a supply chain with multiple mean-variance retailers. *Eur. J. Oper. Res.* **246** (2015) 815–826.
- [54] C. Fang, X. Liao and M. Xie, A hybrid risks-informed approach for the selection of supplier portfolio. *Int. J. Prod. Res.* **54** (2016) 2019–2034.
- [55] T. Sawik, Selection of supply portfolio under disruption risks. *Omega-Int. J. Manag. Sci.* **39** (2011) 194–208.
- [56] S. Sun, S. Hua and Z. Liu, Navigating default risk in supply chain finance: guidelines based on trade credit and equity vendor financing. *Transp. Res. Pt. e-Logist. Transp. Rev.* **182** (2024) 103410.
- [57] X. Chen, S. Shum and D. Simchi-Levi, Stable and coordinating contracts for a supply chain with multiple risk-averse suppliers. *Prod. Oper. Manag.* **23** (2014) 379–392.
- [58] H. Golpira, S. Bahramara, S.A.R. Khan and Y. Zhang, Robust bi-level risk-based optimal scheduling of microgrid operation against uncertainty. *RAIRO-Oper. Res.* **54** (2020) 993–1012.
- [59] M. Zhang, L. Shen, J. Nan, J. Wang, Z. Xia and Y. Zhao, Optimal strategies for supply chain with credit guarantee using CVaR. *RAIRO-Oper. Res.* **58** (2024) 2669–2682.
- [60] H. Yang, W. Zhuo, L. Shao and S. Talluri, Mean-variance analysis of wholesale price contracts with a capital-constrained retailer: trade credit financing vs. bank credit financing. *Eur. J. Oper. Res.* **294** (2021) 525–542.
- [61] Z.-H. Wang, L. Qi, Y. Zhang and Z. Liu, A trade-credit-based incentive mechanism for a risk-averse retailer with private information. *Comput. Ind. Eng.* **154** (2021) 107101.
- [62] Q. Wu, X. Xu, R. Lin and Y. Tian, Effect of risk aversion on the performance of supply chain and carbon reducing initiatives under asymmetric information. *Manag. Decis. Econ.* **45** (2024) 1835–1867.

- [63] F. Zhou, C. Zhang, S. Tiwari, X. Huang and S. Pratap, Decision and coordination of WEEE closed-loop supply chain with risk aversion under the cap-and-trade regulation. *Int. J. Prod. Econ.* **280** (2025) 109477.
- [64] H. Song and Q. Li, Decision-making in closed-loop supply chains: effects of government subsidies and risk aversion. *Int. Rev. Financ. Anal.* **96** (2024) 103566.
- [65] Y. Wei and T.M. Choi, Mean-variance analysis of supply chains under wholesale pricing and profit sharing schemes. *Eur. J. Oper. Res.* **204** (2010) 255–262.
- [66] J. Li, T.-M. Choi and T.C.E. Cheng, Mean variance analysis of fast fashion supply chains with returns policy. *IEEE Trans. Syst. Man Cybern. -Syst.* **44** (2014) 422–434.
- [67] M. Liu, E. Cao and C.K. Salifou, Pricing strategies of a dual-channel supply chain with risk aversion. *Transp. Res. Pt. e-Logist. Transp. Rev.* **90** (2016) 108–120.
- [68] W. Zhuo, L. Shao and H. Yang, Mean-variance analysis of option contracts in a two-echelon supply chain. *Eur. J. Oper. Res.* **271** (2018) 535–547.
- [69] X. Wen and T. Siqin, How do product quality uncertainties affect the sharing economy platforms with risk considerations? A mean-variance analysis. *Int. J. Prod. Econ.* **224** (2020) 107544.
- [70] Y. Zhang and Q. Xu, Agency contracts with incentive mechanisms considering supplier risk aversion in a dynamic platform supply chain. *Ann. Oper. Res.* ahead-of-print (2024). DOI: [10.1007/s10479-024-06087-1](https://doi.org/10.1007/s10479-024-06087-1).
- [71] D. Chen, Y. Zhu, X. Lin, Q. Lin and Y.-J. Chen, Impact of suppliers' risk aversions on information sharing in a hybrid E-commerce supply chain. *Nav. Res. Logist.* **72** (2025) 187–199.
- [72] B. Xin, Y. Song, H. Tan and W. Peng, Sustainable digital fashion in a metaverse ecosystem. *J. Retail. Consum. Serv.* **82** (2025) 104099.
- [73] W. Liu, W. Wei, T.-M. Choi and X. Yan, Impacts of leadership on corporate social responsibility management in multi-tier supply chains. *Eur. J. Oper. Res.* **299** (2022) 483–496.
- [74] B. Xin, Y. Hao and L. Xie, Strategic product showcasing mode of E-commerce live streaming. *J. Retail. Consum. Serv.* **73** (2023) 103360.
- [75] P. Kowalczyk, C. Siepmann and J. Adler, Cognitive, affective, and behavioral consumer responses to augmented reality in e-commerce: a comparative study. *J. Bus. Res.* **124** (2021) 357–373.
- [76] E. Sung, S. Bae, D.-I. D. Han and O. Kwon, Consumer engagement via interactive artificial intelligence and mixed reality. *Int. J. Inf. Manag.* **60** (2021) 102382.
- [77] N. Yan, C. Liu, Y. Liu and B. Sun, Effects of risk aversion and decision preference on equilibriums in supply chain finance incorporating bank credit with credit guarantee. *Appl. Stoch. Models. Bus. Ind.* **33** (2017) 602–625.
- [78] D. Wang, W. Liu, X. Shen and W. Wei, Service order allocation under uncertain demand: risk aversion, peer competition, and relationship strength. *Transp. Res. Pt. e-Logist. Transp. Rev.* **130** (2019) 293–311.
- [79] T.P. Novak, D.L. Hoffman and Y.-F. Yung, Measuring the customer experience in online environments: a structural modeling approach. *Mark. Sci.* **19** (2000) 22–42.
- [80] D. Kim and Y.J. Ko, The impact of virtual reality (VR) technology on sport spectators' flow experience and satisfaction. *Comput. Hum. Behav.* **93** (2019) 346–356.
- [81] S.-S. Cha, C.Y. Kim and Y. Tang, Gamification in the metaverse: affordance, perceived value, flow state, and engagement. *Int. J. Tour. Res.* **26** (2024) e2635.

**Please help to maintain this journal in open access!**



This journal is currently published in open access under the Subscribe to Open model (S2O). We are thankful to our subscribers and supporters for making it possible to publish this journal in open access in the current year, free of charge for authors and readers.

Check with your library that it subscribes to the journal, or consider making a personal donation to the S2O programme by contacting [subscribers@edpsciences.org](mailto:subscribers@edpsciences.org).

More information, including a list of supporters and financial transparency reports, is available at <https://edpsciences.org/en/subscribe-to-open-s2o>.

APPENDIX A.

TABLE A.1. Specific expressions for  $F$ -value critical points.

Critical point	Specific expression
$F_1$	$\frac{2k - (2\alpha\gamma((1 + b - \alpha\gamma)\eta - c) + \alpha^2\gamma^2\eta)}{2k\gamma + \alpha^2\gamma^3\eta}$
$F_2$	$\frac{c(2k + \alpha^2\gamma^2\eta) - \eta(2k(1 + b - 2\alpha\gamma) + (1 + b)\alpha^2\gamma^2\eta)}{4\alpha\gamma^2\eta}$
$F_3$	$\frac{k(2k + \alpha\gamma(2c - (2 + 2b - 2\lambda_o\sigma - \alpha\gamma)\eta))}{\gamma(2k + \alpha^2\gamma^2\eta)}$
$F_4$	$\frac{c(2k + \alpha^2\gamma^2\eta) - \eta(\alpha^2\gamma^2\eta(1 + b - \lambda_o\sigma) + 2k(1 + b - 2\alpha\gamma - \lambda_o\sigma))}{4\alpha\gamma^2\eta}$
$F_5$	$\frac{2k + \alpha\gamma(2c - (2 + 2b - \alpha\gamma)\eta)}{4\gamma}$
$F_6$	$\frac{\alpha(c(2k + \alpha^2\gamma^2\eta) - \eta(2k(1 + b - 2\alpha\gamma) + (1 + b)\alpha^2\gamma^2\eta))}{2(2k + \alpha^2\gamma^2\eta)}$
$F_7$	$\frac{2k + \alpha\gamma(2c - (2 + 2b - \alpha\gamma - 2\lambda_o\sigma)\eta)}{4\gamma}$
$F_8$	$\frac{\alpha(c(2k + \alpha^2\gamma^2\eta) - \eta(\alpha^2\gamma^2\eta(1 + b - \lambda_o\sigma) + 2k(1 + b - 2\alpha\gamma - \lambda_o\sigma)))}{2(2k + \alpha^2\gamma^2\eta)}$
$F_9$	$\frac{2k - \alpha\gamma((1 + b)\eta - c)}{\gamma}$
$F_{10}$	$\frac{4k^2 - 2k\alpha\gamma(1 + b - c - \alpha\gamma + 2\alpha\gamma\eta) + \alpha^3\gamma^3(c - 2c\eta + (1 + b)\eta^2)}{2k\gamma + \alpha^2\gamma^3(1 - 2\eta)}$
$F_{11}$	$\frac{4k^2 - 2k\alpha\gamma(1 + b - c - \alpha\gamma + 2\alpha\gamma\eta) + \alpha^3\gamma^3(c - 2c\eta + \eta(\eta + b\eta + \lambda_o\sigma - \eta\lambda_o\sigma))}{2k\gamma + \alpha^2\gamma^3(1 - 2\eta)}$
$F_{12}$	$\frac{4k^2\lambda_r^2\sigma - 4k\alpha^2\gamma^2\eta((1 + b - \alpha\gamma)\lambda_o + \lambda_r^2\sigma) + \alpha^4\gamma^4\eta(2c\lambda_o + \eta(\lambda_o^2 + \lambda_r^2)\sigma)}{4\alpha^3\gamma^4\eta\lambda_o}$
$F_{13}$	$\frac{4k^2\lambda_r(2c + \lambda_r\sigma) + \alpha^4\gamma^4\eta(2c(1 - \eta)\lambda_o + 2c\eta\lambda_r + \eta(\lambda_o^2 + \lambda_r^2)\sigma) - 2k\alpha^2\gamma^2\eta(2(1 + b - \alpha\gamma)(1 - \eta)\lambda_o + \eta\lambda_o^2\sigma + 2\lambda_r(2c + \lambda_r\sigma))}{4\alpha^3\gamma^4(1 - \eta)\eta\lambda_o}$

TABLE A.2. Specific expressions for  $k$ -value critical points.

Critical point	Specific expression
$k$	$\frac{\alpha^2\gamma^2\eta}{2}$
$k_1$	$\frac{2\alpha\gamma((1+b-\alpha\gamma)\eta-c) + \alpha^2\gamma^2\eta}{2}$
$k_2$	$\frac{\alpha^2\gamma^2\eta((1+b)\eta-c)}{2(c-(1+b-2\alpha\gamma)\eta)}$
$k_3$	$\frac{2\alpha\gamma((1+b-\alpha\gamma-\lambda_o\sigma)\eta-c) + \alpha^2\gamma^2\eta}{2}$
$k_4$	$\frac{\alpha^2\gamma^2\eta((1+b-\lambda_o\sigma)\eta-c)}{2(c-(1+b-2\alpha\gamma-\lambda_o\sigma)\eta)}$
$k_5$	$\frac{\alpha^2\gamma^2\eta(\lambda_o + \lambda_r)}{2\lambda_r}$
$k_6$	$\frac{\alpha\gamma((1+b)\eta-c)}{2}$
$k_7$	$\frac{\alpha\gamma\left(1+b-c-\alpha\gamma+2\alpha\gamma\eta+\sqrt{(1+b-c-\alpha\gamma(1-2\eta))^2-4\alpha\gamma(c-2c\eta+(1+b)\eta^2)}\right)}{4}$
$k_8$	$\frac{\alpha\gamma\left(1+b-c-\alpha\gamma+2\alpha\gamma\eta+\sqrt{1+b^2+c^2-c(2+2\alpha\gamma(1-2\eta))+2b(1-c-\alpha\gamma(1-2(1-\eta)\eta))}\right)}{4}$
$k_9$	$\frac{\alpha^2\gamma^2\left(\eta((1+b-\alpha\gamma)\lambda_o+\lambda_r^2\sigma)+\sqrt{\eta\lambda_o((1+b-\alpha\gamma)^2\eta\lambda_o+2((1+b-\alpha\gamma)\eta-c)\lambda_r^2\sigma-\eta\lambda_o\lambda_r^2\sigma^2)}\right)}{2\lambda_r^2\sigma}$
$k_{10}$	$\frac{\alpha^2\gamma^2\eta(2c\lambda_r+\eta(\lambda_o^2+\lambda_r^2)\sigma)}{2\lambda_r(2c+\eta\lambda_r\sigma)}$
$k_{11}$	$\frac{\alpha^2\gamma^2\left(\eta(2(1+b)(1-\eta)\lambda_o+\eta\lambda_o^2\sigma+2\lambda_r(2c+\lambda_r\sigma))-2\alpha\gamma(1-\eta)\eta\lambda_o+\sqrt{\eta(\eta(2(1+b-\alpha\gamma)(1-\eta)\lambda_o+\eta\lambda_o^2\sigma+2\lambda_r(2c+\lambda_r\sigma))^2-4\lambda_r(2c+\lambda_r\sigma)(2c(\lambda_o-\eta\lambda_o+\eta\lambda_r)+\eta(\lambda_o^2+\lambda_r^2)\sigma))}\right)}{4\lambda_r(2c+\lambda_r\sigma)}$

TABLE A.3. Specific expressions for  $c$ -value critical points.

Critical point	Specific expression
$c_1$	$(1 + b - 2\alpha\gamma)\eta$
$c_2$	$(1 + b - \alpha\gamma)\eta$
$c_3$	$(1 + b - 2\alpha\gamma - \lambda_o\sigma)\eta$
$c_4$	$(1 + b - \alpha\gamma - \lambda_o\sigma)\eta$
$c_5$	$(1 + b)\eta$