Journal of
Cyber Security

Tech Science Press

Doi:10.32604/jcs.2025.065625

ARTICLE

Multi-Stage Game-Theoretical Decision Analysis of Enterprise Information Security Outsourcing Based on Moral Hazard

Qiang Xiong*, Jianlong Zhang and Qianwen Song

School of Management, Jiangsu University, Zhenjiang, 212013, China

*Corresponding Author: Qiang Xiong. Email: xiongqiang@ujs.edu.cn

Received: 18 March 2025; Accepted: 19 June 2025; Published: 14 July 2025

ABSTRACT: In the domain of information security outsourcing, the multi-stage game-theoretic decision-making process, intertwined with moral hazard and dynamic strategy adjustments, significantly impacts the long-term collaboration between the principal (outsourcing enterprise) and the contractor (Managed Security Service Provider—MSSP). This paper conducts a comprehensive analysis of these aspects within information security outsourcing partnerships. A multi-stage game model incorporating moral hazard is constructed to meticulously examine the strategic behaviors and expected revenue fluctuations of both parties across different cooperation stages. Through in-depth model derivation, the impacts of service fees, cooperation-stage progression, and long-term cooperation on expected revenues are explored, and crucial managerial recommendations are proposed. Enterprises need to flexibly adjust cooperation strategies, fully consider the influence of service fees on long-term benefits, and attach importance to long-term cooperation. Specifically, dynamic strategy adjustments can effectively address the changing risks in the outsourcing process. An appropriate increase in service fees can enhance information security defense effectiveness, while excessive fees may have the opposite effect. Long-term cooperation is beneficial for both the principal and the MSSP, promoting the stability and sustainability of the partnership. As the cooperation advances, the principal's expected revenues increase gradually, necessitating strategic adjustments based on stage-specific income changes. Simulation analyses validate the key conclusions, demonstrating the model's effectiveness and robustness in practical applications. This research provides a solid theoretical basis and practical guidance for enterprises in information security outsourcing decision-making, enabling them to better manage moral hazard and optimize the long-term value of outsourcing collaborations.

KEYWORDS: Information security outsourcing; dynamic moral hazard; multi-stage game; decision analysis

1 Introduction

1.1 Research Background

In the era of digital transformation, the exponential advancement of information technology has propelled enterprises into a profound digital revolution, intensifying the need for robust cybersecurity measures [1]. Cybersecurity has become an area of significant concern for countries around the world, following traditional security domains such as homeland security [2], supply chain security [3], and food security [4,5]. However, this transformation is fraught with escalating cybersecurity challenges, including data breaches, malicious attacks, and systemic vulnerabilities, which imperil enterprises' digital resilience and success [6]. Despite enterprises' efforts to combat these threats through in-house development and maintenance of cybersecurity infrastructures, the relentless evolution of cyber threats has rendered traditional defenses increasingly inadequate, posing significant challenges in technical capability and cost efficiency [7].

Against this backdrop, information security outsourcing has emerged as a transformative strategy, garnering substantial attention from both enterprises and Managed Security Service Providers (MSSPs) [8]. Its appeal lies in its ability to navigate the complexities of an ever-evolving cybersecurity landscape effectively [9]. Market forecasts project the global managed security services industry to grow from $30.6 billion in 2023 to $52.9 billion by 2028 [10], underscoring its pivotal role in modern enterprise risk management. This trend reflects not only enterprises' reliance on specialized security expertise but also the practical necessity of outsourcing to address technical complexity and cost constraints.

1.2 Research Gaps and Motivation

Existing research has explored information security outsourcing from perspectives such as contract design and risk sharing [11,12]. However, a critical gap remains: most studies rely on single-stage game models, overlooking the dynamic, multi-stage nature of outsourcing collaborations and the need for iterative strategic adjustments. In information security outsourcing, moral hazard is a crucial issue. Moral hazard refers to the situation where, during the execution of a contract between the principal and the agent, due to factors such as incomplete contracts, information asymmetry, and ineffective supervision, either party may act in a manner detrimental to the interests of the other party [13,14]. This issue has predominantly been analyzed in static settings. In practice, outsourcing partnerships require multi-stage negotiations and strategic iterations to build stable relationships. Single-stage models fail to capture the evolution of trust, the accumulation of collaborative experience, and the adaptive alignment of incentives over time.

Previous research mainly focused on static contract design, such as determining fixed service fees and one-time risk-sharing mechanisms. However, in real-world information security outsourcing, the security situation changes constantly, and the relationship between the principal and the MSSP evolves over time. For instance, as the threat landscape becomes more complex, the initial contract terms may no longer be sufficient to ensure the effectiveness of security services.

This study aims to bridge this gap by developing a multi-stage game model to analyze decision-making under dynamic moral hazard. By integrating the interactions of service fees, cooperation stages, and long-term payoffs, this research seeks to uncover how enterprises can design stage-specific incentive mechanisms to guide MSSPs' sustained efforts and mitigate moral hazard. This study not only provides a theoretical framework for sustainable outsourcing strategies but also responds to practical demands for stabilizing long-term partnerships and managing evolving risks in cybersecurity governance.

2 Related Work

2.1 Information Security Outsourcing and Moral Hazard: Contract Design and Risk Mitigation

Information security outsourcing is an important research direction in the field of information security [15,16]. Research on moral hazard in information security outsourcing has primarily focused on contractual mechanisms. Early works [11] laid the foundation by examining risk allocation and incentive compatibility in outsourcing contracts. Hui et al. [12] analyzed the interplay between risk interdependencies, mandatory security protocols, and contractual terms from the MSSP perspective, highlighting the need to balance multi-stakeholder interests. Zhao et al. [17] demonstrated that security externalities in multi-client scenarios could be mitigated through optimized compensation structures, enhancing security investment efficiency. Wu et al. [18,19] conducted in-depth research on optimal security investment decisions and multi-solution approaches in joint management of information security between MSSPs and enterprises.

To address moral hazard, Cezar et al. [9] compared single vs. dual MSSP outsourcing models, proposing punishment-reward contract models for the latter to deter opportunistic behavior. Lee et al. [14] investigated contract designs under security externalities, advocating multi-party contracts to resolve double moral hazard. Hui et al. [20] introduced threshold and variable responsibility contracts to align MSSPs' and enterprises' incentives, while Wu et al. [13] proposed responsibility contract mechanisms in supply chain collaborations to address moral hazard in compensation structures. Despite these contributions, these studies are rooted in single-stage frameworks, neglecting the temporal dynamics of cooperation and the need for adaptive strategies.

In contrast to previous single-stage research, this study focuses on the multi-stage nature of information security outsourcing. It takes into account how the relationship between the principal and the MSSP changes over time, such as the impact of early-stage cooperation on later-stage trust and the adjustment of incentive mechanisms based on cumulative experience.

2.2 Multi-Stage Game Models in Strategic Collaboration: From Static to Dynamic Paradigms

Multi-stage game models have shown promise in capturing dynamic interactions in strategic alliances. Elitzur and Gavious [21] applied such models to venture capitalist-entrepreneur relationships, demonstrating how staged investments alleviate information asymmetry. Roels et al. [22] introduced multi-stage contracts in service outsourcing, proving that phased incentives enhance collaborative efficiency. In IT research, Demirezen et al. [23,24] used differential games to analyze value co-creation in IT projects, emphasizing dynamic adjustments for sustained cooperation.

However, these advancements have not been systematically applied to moral hazard in information security outsourcing. Critical gaps include the failure to account for: (1) the lagged effects of security efforts on breach risks, (2) the evolving nature of threats across cooperation stages, and (3) the time-dependent efficacy of incentive mechanisms. Existing models in general outsourcing or technology alliances do not address the unique challenges of cybersecurity, such as unobservable effort quality and the asymmetric impact of moral hazard on long-term risk profiles.

2.3 Research Contributions and Novelty

Current literature exhibits two primary limitations:

Dominance of Static Perspective: Most studies assume one-shot interactions or fixed contract terms, ignoring the iterative nature of outsourcing negotiations and the changing risk landscapes across stages (e.g., increasing threat sophistication in later stages).

Inadequate Modeling of Dynamic Moral Hazard: The relationship between MSSPs' effort levels, stage-wise cost-benefit dynamics, and enterprises' adaptive fee strategies remains under-explored. For instance, the diminishing marginal returns of effort in advanced stages and the strategic value of deferring payments to incentivize long-term commitment are not systematically analyzed.

This study addresses these gaps by:

Introducing a Dynamic Framework: Developing a multi-stage game model that captures the temporal evolution of moral hazard, allowing for stage-specific strategy adjustments (e.g., front-loaded incentives for early trust-building and outcome-based fees for mature partnerships). Quantifying Long-Term Collaboration Gains: Demonstrating how multi-stage interactions enhance both parties' expected payoffs through experience accumulation and incentive alignment, providing a theoretical basis for designing "short-term flexibility-long-term stability" contract architectures.

By integrating dynamic moral hazard into a multi-stage framework, this research offers a more nuanced understanding of strategic interactions in information security outsourcing, filling a critical void in both theoretical modeling and practical decision-making.

3 Model Assumptions and Description

To formalize the multi-stage interaction between principals and MSSPs under dynamic moral hazard, this chapter establishes the theoretical framework of the game model. By defining key assumptions and describing the sequential decision-making process, a foundation is laid for analyzing strategic behaviors and payoff dynamics across cooperation stages.

3.1 Problem Description

Equifax, a globally renowned credit reporting agency, fell victim to a cyberattack due to its failure to promptly patch known vulnerabilities in the Apache Struts framework. At the time, the Apache Foundation had already released vulnerability patches, but Equifax's outsourced information security team failed to deploy them in a timely manner, exposing issues such as inadequate protection and delayed responses in outsourced services. Taking advantage of this oversight, hackers infiltrated the system and stole data from tens of millions of users, resulting in substantial financial losses for Equifax and subsequent penalties. This incident reflects deep-seated problems that have long persisted in the field of information security outsourcing.

During the long-term cooperation between enterprises and Managed Security Service Providers (MSSPs), information asymmetry and interest games are constant. As service providers, the level of effort exerted by MSSPs directly determines the security level of an enterprise's information system. However, it is difficult for enterprises to directly observe the actual work of MSSPs. Motivated by self-interest, MSSPs may reduce investment in security protection to cut costs. Such moral hazard behaviors significantly increase the probability of an enterprise's information system being attacked, severely damaging the interests of the enterprise.

Consequently, designing a reasonable contractual mechanism to incentivize MSSPs to increase their effort levels and mitigate moral hazards has become a critical issue that urgently needs to be addressed in enterprises' information security outsourcing decisions. This section will construct a multi-stage game model under unilateral moral hazard to conduct an in-depth analysis of the behavioral strategies of enterprises and MSSPs.

3.2 Model Assumptions

This section outlines the core assumptions governing the multi-stage game, focusing on rational actor behavior, information asymmetry, and the structural design of outsourcing contracts. These assumptions streamline the analysis while capturing the essential complexities of real-world information security partnerships, such as unobservable effort levels and the interdependence of stage-wise decisions.

Building upon the framework established by Ramy et al. [21], the model centers on the pivotal actors in this interaction: the principal (the outsourcing firm) and the MSSP (Managed Security Service Provider). Principal enterprises typically face numerous challenges in information security management, including a lack of in-house technical expertise, high costs associated with maintaining a comprehensive security infrastructure, and the inability to keep up with the rapid pace of technological advancements in the field of information security. On the other hand, the contractor, the Managed Security Service Provider (MSSP), is an enterprise or organization equipped with specialized information security technology, extensive industry experience, and a well-developed service system. The MSSP's technical capabilities often cover a wide range of areas, such as network security monitoring, threat detection and response, and data encryption. Its industry experience enables it to understand the unique security needs of different sectors and develop tailored solutions. Additionally, the comprehensive service system ensures that it can provide continuous support, timely updates, and effective incident management to its clients.

Both entities are assumed to be risk-neutral, implying that risk does not factor into their strategic decision-making. Given the principal's deficiency in robust network security capabilities, it delegates information security management to the MSSP, which is tasked with delivering a suite of network security management services, including but not limited to virus interception, spam filtering, intrusion detection, firewalls, and VPN (Virtual Private Network) management. The model underscores the significance of long-term outsourcing collaboration between the principal and the MSSP, encompassing multiple iterative stages of ongoing cooperation. Within each stage, both parties engage in transactions and payments related to information security and contemplate the continuation of their cooperation. The MSSP must weigh the revenue from the current period against the anticipated future benefits of sustained information security outsourcing cooperation to ascertain potential moral hazard behavior, herein termed dynamic moral hazard, in pursuit of its expected total utility. Throughout this dynamic cooperation process, the principal aims to maximize its long-term expected total utility from the outsourcing collaboration while upholding the rational and incentive constraints of the MSSP.

It is crucial to clarify that our model presupposes the MSSP has been selected by the principal, indicating that an outsourcing contract has been executed and cooperation has commenced. Consequently, the scope of our model is to dissect the game-theoretic behaviors of both parties throughout the cooperation phase and to conduct a deductive analysis aimed at deepening our understanding of moral hazard within the context of information security outsourcing.

Assumption 1: *Consider a principal that values its information assets at v. Over the course of K stages of cooperation, these assets will undergo depreciation and updates as part of the business's normal operations. Additionally, the assets require effective protection by the MSSP. The value of the principal's information assets is influenced by a multitude of factors, making it challenging to dynamically model this fluctuation with a single parameter. For the sake of simplicity, we assume that the value of the principal's information assets remains constant.*

Assumption 2: *For the sake of tractability, a zero discount rate is assumed. The outsourcing contract is structured into K stages, with each stage's duration (k) being variable across companies, potentially ranging from one month to one year. Premature termination of the contract is prohibited for both parties without just cause, unless the MSSP's defense fails. At stage k, if the defense is successful, the principal remunerates the MSSP with a service fee p_k, and the contract advances to the subsequent stage $(k+1)$. In the event of a defense failure, the principal incurs a loss of v, with the MSSP liable to compensate a proportion β_k of this loss, $\beta_k \in [0,1]$, leading to the immediate termination of the contract.*

Assumption 3: *In the natural state at stage k, when an enterprise's information asset is targeted by a hacker attack, the defense level q_k of the enterprise's information system, $q_k \in [0,1]$, which is primarily contingent on the MSSP's efforts, is denoted as qq. Let the MSSP's effort level be e_k, $e_k \geq 0$. The probability of the enterprise successfully defending against the attack at stage k is denoted as $q_k\left(e_k\right)$, $0 \leq q_k\left(e_k\right) \leq 1$, $\frac{\partial q_k(e_k)}{\partial e_k} > 0, \frac{\partial^2 q_k(e_k)}{\partial {e_k}^2} < 0$, which is positively correlated with the MSSP's effort level. This implies that as e_k increases, the probability of a successful defense also increases, albeit with diminishing marginal returns.*

Assumption 4: *The MSSP's effort cost is denoted as $C\left(e_k\right)$, and as the effort level increases, both the cost and the marginal cost of effort escalate, i.e., $C'\left(e_k\right) > 0$,$C''\left(e_k\right) > 0$. It is assumed that the MSSP's defense success* *probability q and the MSSP's effort cost C are known quantities, yet their specific values remain unknown to the principal, as they are contingent on the MSSP's effort level, which is unobservable.*

Assumption 5: *Let W_m represent the total expected payoff of the principal from k to K stages, and U_m represent the total expected payoff of the MSSP from k to K stages.*

Assumption 6: *In the natural state, the probability of a hacker attack on the enterprise's information assets is α, $\alpha \in [0,1]$.*

Assumption 7: *v and $C(e_k)$ are considered public knowledge, and both parties are assumed to be risk-neutral. That is, both parties focus on their core business objectives. In the process of cooperation, they do not actively seek risk premiums or avoid risks; instead, they concentrate on these core business goals.*

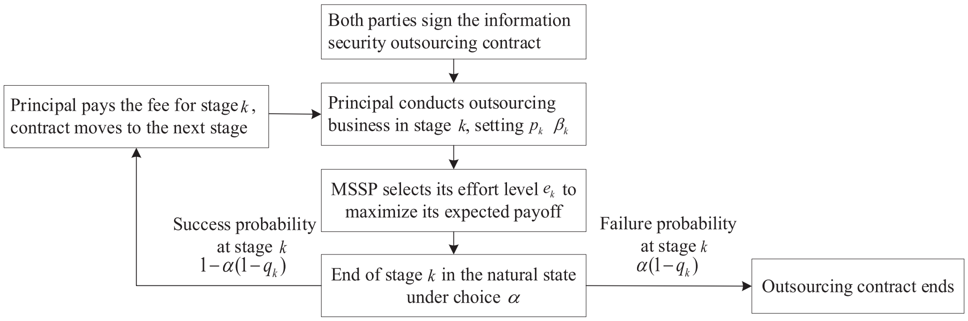
For the research model, the related variables and parameters are defined as shown in Table 1.

Table 1: Meaning of model parameters

Symbol	Meaning
v	Value of the enterprise's own information assets
p_k	Outsourcing service fee paid by the enterprise to the MSSP
β_k	Compensation ratio by the information security service provider (MSSP)
e_k	Effort level of the MSSP
$q_k(e_k)$	Probability of successful information security defense
$C(e_k)$	Effort cost of the MSSP
α	Probability of a hacker attack on the enterprise's information assets in the natural state
U_k	Expected utility of the outsourcing enterprise (MSSP)
W_k	Expected utility of the principal (outsourcing enterprise) at stage k
U_m	Total expected payoff of the MSSP from stages k to K
W_m	Total expected payoff of the principal (outsourcing enterprise) from stages k to K
Z_m	Total expected utility of both the principal and MSSP

3.3 Model Description

The game process between both parties is illustrated in Fig. 1:



Both parties sign the information security outsourcing contract
Principal pays the fee for stage k, contract moves to the next stage
Principal conducts outsourcing business in stage k, setting p_k β_k
MSSP selects its effort level e_k to maximize its expected payoff
Success probability at stage k $1-\alpha(1-q_k)$
Failure probability at stage k $\alpha(1-q_k)$
End of stage k in the natural state under choice α
Outsourcing contract ends

Figure 1: Multi-stage outsourcing cooperation game process

At the outset of their outsourcing collaboration, the principal devises the information security outsourcing contract and establishes the service fee p_k. If the MSSP successfully executes the defense at stage k, the principal is contractually obligated to remunerate the MSSP with the prearranged service fee. In accordance with the stipulations of the contract, the MSSP must determine its effort level e_k, taking into account its own capabilities and the prevailing market conditions, to ensure the quality of service and the likelihood of a successful defense. The MSSP will then execute the information security defense under the prevailing natural market environment α. Upon the conclusion of stage k, if the MSSP has successfully defended, the outsourcing cooperation will progress to the subsequent stage. Conversely, if the MSSP fails to defend at stage k, it will be responsible for compensating a proportion β_k of the incurred loss, and the outsourcing contract will be terminated. Regardless of the outcome, the MSSP will incur a cost $C(e_k)$. This entire sequence of events reflects the decision-making acumen and risk-bearing capacity of both parties and encompasses critical aspects such as risk-sharing, incentive compatibility, and profit distribution within the principal-agent relationship. These elements are essential for ensuring the long-term stability and mutual benefit of the cooperation.

Therefore, the following expressions can be derived:

The expected utility of the principal at stage k is W_k:

$$W_k = [1 - \alpha (1 - q_k)] (v - p_k + W_{k+1}) + \alpha \beta_k v (1 - q_k) \tag{1}$$

In this equation, $[1 - \alpha (1 - q_k)] (v - p_k + W_{k+1})$ represents the retention value of enterprise information assets when successfully protected, and $\alpha \beta_k v (1 - q_k)$ represents the expected compensation obtained from MSSP after being attacked.

The expected utility of the outsourcing enterprise (MSSP) is U_k:

$$U_k = [1 - \alpha (1 - q_k (e_k))] [p_k + U_{k+1}] - \alpha \beta_k v (1 - q_k) - C(e_k) \tag{2}$$

In this equation, $[1 - \alpha (1 - q_k (e_k))] [p_k + U_{k+1}]$ represents the service fee paid to MSSP for successful protection, $\alpha \beta_k v (1 - q_k)$ represents the compensation expenditure for possible protection failure, and $C(e_k)$ represents the cost of self effort.

In the above, $k = 1, \cdots K$; $U_{k+1} = 0$, $W_{k+1} = 0$

expanding (1) gives:

$$W_m = \sum_{k=m}^{K} \left\{ \prod_{j=m}^{k} \left[1 - \alpha \left(1 - q_j\right)\right] [v - p_k] \right\} \tag{3}$$

expanding (2) gives:

$$U_m = \sum_{k=m}^{K} \left\{ \prod_{j=m}^{k} \left[1 - \alpha \left(1 - q_j\right)\right] p_k \right\} - \sum_{k=m}^{K} \left\{ \prod_{j=m}^{k-1} \left[1 - \alpha \left(1 - q_j\right)\right] C(e_k) \right\} \tag{4}$$

4 Model Solution and Analysis

After establishing the model's assumptions and framework, a rigorous exploration of the model's solution and analytical results is essential. This step is crucial for uncovering the intricate game-theoretic dynamics inherent in enterprise information security outsourcing and for formulating effective strategic guidelines. Through solving the model, the intrinsic relationships among various factors can be revealed, clarifying how different decisions impact the payoffs of both parties. This, in turn, provides targeted practical advice for enterprises engaged in real-world outsourcing collaborations. Such insights not only assist enterprises in rationally planning their outsourcing strategies and mitigating moral hazard but also contribute to fostering long-term, stable, and mutually beneficial partnerships. In the subsequent sections, the key theorems derived from the model solution and their respective proofs will be elaborated, providing a solid theoretical foundation for enterprise decision-making in the realm of information security outsourcing.

Theorem 1: *The optimal effort exerted by the MSSP is positively correlated with the payment p_k made by the principal at each stage, the compensation ratio β_k in the event of an information security breach, and the MSSP's expected future payoff U_{k+1}. Enhancements in p_k or β_k, which elevate the MSSP's prospective future earnings, can serve as incentives for the MSSP to intensify its efforts and mitigate moral hazard.*

Proof: To differentiate with respect to e_k in Eq. (2), we get:

$$\frac{dU_k}{de_k} = \alpha q_k'\left(e_k\right)\left(p_k + U_{k+1}\right) + \alpha q_k'\left(e_k\right)\beta_k v - C'\left(e_k\right)$$

When $\frac{dU_k}{de_k} = 0$, the profit is maximized, i.e.,

$$\alpha q_k'\left(e_k\right)\left(p_k + \beta_k v + U_{k+1}\right) = C'\left(e_k\right) \tag{5}$$

Because:

$$q_k'\left(e_k\right) > 0, q_k''\left(e_k\right) < 0, C'\left(e_k\right) > 0, C''\left(e_k\right) > 0$$

Therefore, if and only if:

$\alpha q_k'\left(0\right)\left(p_k + \beta_k v + U_{k+1}\right) \geq C'\left(0\right)$, Eq. (5) has a solution, and we get:

$$\alpha q_k'\left(e_k\right)\left(p_k + \beta_k v + U_{k+1}\right) = C'\left(e_k\right)$$

we get:

$$e_k^* = \begin{cases} e_k^*\left[\alpha\left(p_k + \beta_k v + U_{k+1}\right)\right] & \alpha q_k'\left(0\right)\left(p_k + \beta_k v + U_{k+1}\right) \geq C'\left(0\right) \\ 0 & otherwise \end{cases} \tag{6}$$

According to Theorem 1, in the context of information security outsourcing, the MSSP's expected payoff is significantly influenced by a constellation of parameters. Primarily, the MSSP's effort level $e_k{}^*$ is a pivotal determinant, as it directly shapes the quality of service and the level of security that the MSSP is capable of delivering. Additionally, the principal's payment p_k and the compensation ratio β_k exert a substantial influence on the MSSP's expected payoff. Consequently, the principal must engage in a judicious assessment of these contractual parameters and be prepared to make adjustments throughout the life of the contract. This adaptive approach is essential to ensure that the MSSP is provided with adequate incentives to deliver high-caliber services, thereby reducing moral hazard within the outsourcing process. □

Theorem 2: *In the staged execution process of information security outsourcing, the optimal strategy should satisfy the following conditions:*

$$\alpha q_k'\left(e_k\right)\left(p_k + \beta_k v + U_{k+1}\right) = C'\left(e_k\right)$$

Proof: From the derivation process in Theorem 1, we obtain expression (5): $\alpha q_k'\left(e_k\right)\left(p_k + \beta_k v + U_{k+1}\right) = C'\left(e_k\right)$, which shows that the MSSP's optimal reward makes the marginal utility of the principal equal to the marginal cost of the MSSP's effort.

Theorem 2 elucidates that throughout the cooperation process, the optimal collaborative strategy between the principal and the MSSP should strike a balance between utility and cost. If the marginal benefit accruing to the principal from elevating the service fee surpasses the incremental cost incurred by the MSSP for heightened effort, it is advisable for the principal to contemplate an increase in the service fee. On the contrary, if the marginal benefit fails to exceed the cost, the fee should either remain static or be reduced. This equilibrium is crucial for ensuring that both parties can maximize their benefits throughout the cooperation, thereby fostering a long-term, stable cooperative relationship. In practical terms, the principal and the MSSP must employ game theory and engage in collaborative negotiations to ascertain the optimal cooperation strategy, ensuring that both parties can attain an optimal level of benefits. □

Theorem 3: *During the sequential execution of information security outsourcing tasks, the marginal impact of payments made by the outsourcing principal on the MSSP diminishes as the number of stages escalates. This implies that at different stages of task execution, the MSSP's marginal contribution per additional payment incrementally wanes.*

Proof: for every $j < k$,

$$\frac{\partial e_j^*}{\partial p_k} = \alpha \cdot e_j^{*\prime}\left[\alpha\left(p_j + \beta_j v + U_{j+1}\right)\right] \cdot \frac{\partial U_{j+1}}{\partial p_k}$$

And

$$e_j^{*\prime}\left[\alpha\left(p_j + \beta_j v + U_{j+1}\right)\right] = \left.\frac{de_j^*}{\partial x}\right|_{x=\alpha\left(p_j+\beta_j v+U_{j+1}\right)}$$

$$\frac{\partial e_j^*}{\partial p_k} = \alpha \cdot e_j^{*\prime} \cdot \frac{\partial U_{j+1}}{\partial p_k}$$

$$\begin{aligned}\frac{\partial U_m}{\partial p_k} &= \alpha q_m{}'\left(e_m\right) \cdot e_m^{*\prime} \cdot \frac{\partial U_{m+1}}{\partial p_k} \cdot \left[p_m + U_{m+1}\right] + \left[1 - \alpha\left(1 - q_m\left(e_m^*\right)\right)\right] \cdot \frac{\partial U_{m+1}}{\partial p_k} \\ &\quad + \alpha\beta_m v \cdot q_m{}'\left(e_m\right) \cdot e_m^{*\prime} \cdot \frac{\partial U_{m+1}}{\partial p_k} - C'\left(e_m^*\right) \cdot e_m^{*\prime} \cdot \frac{\partial U_{m+1}}{\partial p_k} \\ &= e_m^{*\prime} \cdot \frac{\partial U_{m+1}}{\partial p_k}\left\{\alpha q_m{}'\left(e_m\right) \cdot \left[p_m + U_{m+1} + \beta_m v\right] - C'\left(e_m^*\right)\right\} + \left[1 - \alpha\left(1 - q_m\left(e_m^*\right)\right)\right] \cdot \frac{\partial U_{m+1}}{\partial p_k}\end{aligned}$$

If $\alpha q_k'\left(0\right)\left(p_k + \beta_k v + U_{k+1}\right) < C'\left(0\right)$, then $e_m^* = 0$, $e_m^{*\prime} = 0$,
we can obtain: $\frac{\partial U_m}{\partial p_k} = \left[1 - \alpha\left(1 - q_m\left(e_m^*\right)\right)\right] \cdot \frac{\partial U_{m+1}}{\partial p_k}$,

If $\alpha q_k'\left(0\right)\left(p_k + \beta_k v + U_{k+1}\right) \geq C'\left(0\right)$, because $\alpha q_k'\left(e_k\right)\left(p_k + \beta_k v + U_{k+1}\right) = C'\left(e_k\right)$,
we can obtain: $\frac{\partial U_m}{\partial p_k} = \left[1 - \alpha\left(1 - q_m\left(e_m^*\right)\right)\right] \cdot \frac{\partial U_{m+1}}{\partial p_k}$

Thus, it can be derived that:

$$\frac{\partial U_m}{\partial p_k} = \prod_{j=m}^{k}\left[1 - \alpha\left(1 - q_j\left(e_j^*\right)\right)\right] \tag{7}$$

That is, under the optimal effort level $e_k{}^*$, U_m satisfies the following condition, Eq. (7):

$$\frac{\partial U_m}{\partial p_k} = \prod_{j=m}^{k}\left[1 - \alpha\left(1 - q_j\left(e_j^*\right)\right)\right]$$

Then, from Eq. (7), we obtain:

$$\frac{\frac{\partial U_1}{\partial p_k}}{\frac{\partial U_1}{\partial p_{k+1}}} = \frac{\prod_{j=1}^{k}\left[1-\alpha\left(1-q_j\left(e_j^*\right)\right)\right]}{\prod_{j=1}^{k+1}\left[1-\alpha\left(1-q_j\left(e_j^*\right)\right)\right]} = \frac{1}{\left[1-\alpha\left(1-q_j\left(e_j^*\right)\right)\right]} > 1\,(k = 1, \cdots, K-1) \tag{8}$$

That is:

$$\frac{\partial U_1}{\partial p_k} > \frac{\partial U_1}{\partial p_{k+1}}(k = 1, \cdots, K-1) \tag{9}$$

According to Theorem 3, Within the context of the information security outsourcing process, as the payment level increases, the marginal benefit that the MSSP can derive gradually diminishes. This indicates that the principal's augmented payments do not yield a proportional increase in benefits and may even precipitate a decrease in the marginal benefit associated with the MSSP's effort level. To mitigate the MSSP's moral hazard, the principal should consider escalating stage payments contingent upon the MSSP's performance and dynamically adjust the compensation ratio. This approach is designed to preserve the efficacy of the incentive scheme and to sustain the MSSP's motivation. Implementing such dynamic adjustments necessitates a flexible contractual framework and the establishment of mechanisms capable of accommodating fluctuations in the external environment and the MSSP's performance. □

Theorem 4: *In the phased execution process of information security outsourcing, the expected payoff that the MSSP will receive in subsequent stages confers increasing marginal utility upon the outsourcing principal. Intuitively, the principal has a preference for deferring payments to the MSSP, while the MSSP has an inclination towards receiving payments sooner. For the principal, the postponement of payments to the MSSP can be more effective in curbing moral hazard.*

Proof: The principal determines the optimal service fee p_k^* to be paid to the MSSP during the first phase of cooperation. For $k = 1, \cdots$ and $p_k^* > 0$, the expected payoff for the principal is calculated. To find the first-order derivative of the principal's expected payoff, it must satisfy the following condition:

$$\frac{\partial W_1}{\partial p_k} = \alpha^2 q_1^{*\prime} \cdot e_1^{*\prime} \cdot \frac{\partial U_2}{\partial p_k} \cdot (v - p_1 + W_2 - \beta_1 v) + [1 - \alpha(1 - q_1^*)] \cdot \frac{\partial W_2}{\partial p_k} = 0 \tag{10}$$

Since expression (5) yields: $\frac{\partial U_m}{\partial p_k} = \prod_{j=m}^{k}\left[1-\alpha\left(1-q_j\left(e_j^*\right)\right)\right]$,

then $\frac{\partial U_2}{\partial p_k} = \prod_{j=2}^{k}\left[1-\alpha\left(1-q_j\left(e_j^*\right)\right)\right]$

because $\frac{\partial W_1}{\partial p_k} = \alpha^2 q_1^{*\prime} \cdot e_1^{*\prime} \cdot \frac{\partial U_2}{\partial p_k} \cdot (v - p_1 + W_2 - \beta_1 v) + [1 - \alpha(1 - q_1^*)] \cdot \frac{\partial W_2}{\partial p_k} = 0$,

then:

$$\frac{\partial W_2}{\partial p_k} = -\frac{1}{[1 - \alpha(1 - q_1^*)]}\alpha^2 q_1' \cdot e_1^{*\prime} \cdot \prod_{j=2}^{k}\left[1-\alpha\left(1-q_j\left(e_j^*\right)\right)\right] \cdot (v - p_1 + W_2 - \beta_1 v) < 0 \tag{11}$$

then: if

$$j > k, \frac{\partial W_2}{\partial p_j} = \prod_{i=k+1}^{j}\left[1-\alpha\left(1-q_j\left(e_j^*\right)\right)\right]\frac{\partial W_2}{\partial p_k} > \frac{\partial W_2}{\partial p_k} \tag{12}$$

In the multi-stage execution of information security outsourcing, the expected payoff for the MSSP in subsequent stages confers escalating marginal utility upon the outsourcing principal. This dynamic signifies that as the project advances, the principal's reliance on the MSSP's services becomes increasingly pronounced. Consequently, it is imperative for the principal to foster and maintain a robust cooperative relationship with the MSSP. Regular performance assessments are essential to mitigate moral hazard and to ensure that the security requirements are effectively addressed and satisfied. □

Theorem 5: *Modulating the service fee exerts a salutary influence on the long-term benefits derived from information security outsourcing. Specifically, an appropriately calibrated increment in the service fee can augment the likelihood of successfully repelling cyber attacks. This enhancement not only bolsters the capacity of both the principal and the MSSP to fortify information security but also substantively contributes to the accrual of long-term benefits from their collaborative endeavor.*

Proof: From Theorem 4, it is known that for $k > 1$, we have:

$$\frac{\partial W_1}{\partial p_k} = \alpha^2 {q_1}' e_1^{*\prime} \cdot \frac{\partial U_2}{\partial p_k} \left[(1-\beta_1)\, v - p_1 + W_2\right] + \left[1-\alpha\,(1-q_1)\right] \frac{\partial W_2}{\partial p_k} \tag{13}$$

For every k and m, $k > m$, we have:

$$\frac{\partial W_m}{\partial p_k} = \alpha^2 {q_m}' e_m^{*\prime} \cdot \frac{\partial U_{m+1}}{\partial p_k} \left[(1-\beta_m)\, v - p_m + W_{m+1}\right] + \left[1-\alpha\,(1-q_m)\right] \frac{\partial W_{m+1}}{\partial p_k} \tag{14}$$

$$\frac{\partial W_k}{\partial p_k} = \alpha^2 {q_k}' e_k^{*\prime} \cdot \left[(1-\beta_k)\, v - p_k + W_{k+1}\right] - \left[1-\alpha\,(1-q_k)\right] \tag{15}$$

From Theorem 2, $\alpha q_k'\,(e_k)\,(p_k + \beta_k v + U_{k+1}) = C'\,(e_k)$, substituting the above three equations, we can derive:

$$\frac{\partial W_1}{\partial p_k} = \alpha^2 \left\{\prod_{j=1}^{k}\left[1-\alpha\left(1-q_j\right)\right]\right\} \sum_{i=1}^{k} \frac{1}{1-\alpha\,(1-q_i)} \cdot {q_i}' \cdot e_i^{*\prime} \left[(1-\beta_i)\, v - p_i + W_{i+1}\right] - \prod_{j=1}^{k}\left[1-\alpha\left(1-q_j\right)\right] \tag{16}$$

Therefore, for $k = 1, \cdots, K-1$, we have:

$$\frac{\partial W_1}{\partial p_{k+1}} = \frac{\partial W_1}{\partial p_k}\left[1-\alpha\,(1-q_{k+1})\right] + \alpha^2 \left\{\prod_{j=1}^{k}\left[1-\alpha\left(1-q_j\right)\right]\right\} \cdot {q_{k+1}}' \cdot e_{k+1}^{*\prime} \left[(1-\beta_{k+1})\, v - p_{k+1} + W_{k+2}\right] \tag{17}$$

So, modulating the service fee is crucial in the dynamics of information security outsourcing partnerships. Initially, a judicious escalation of the service fee enhances the likelihood of mounting a successful defense against cyber threats, thereby affording both the principal and the contractor the opportunity to bolster information security and, consequently, to augment the long-term benefits of their collaboration. Secondly, in light of the dynamic moral hazard parameters, the fine-tuning of service fees exerts a nuanced influence on long-term benefits, with outcomes that are contingent upon the specific values of these parameters. To navigate this intricacy, both parties must weigh the dual effects of service fee adjustments on defense efficacy and the presence of dynamic moral hazard within their decision-making processes. Given the inherently dynamic nature of information security outsourcing, decision-makers are tasked with the flexibility to calibrate their service fee strategies in response to varying circumstances. Ultimately, conducting regular assessments of the cooperation's various facets, including the probability of successful defense, the implications of moral hazard, and the service fee strategy, will facilitate the timely recalibration of cooperation tactics and the optimization of long-term benefits. This conclusion underscores the multifaceted nature of information security outsourcing decisions, which necessitate a comprehensive consideration of multiple factors to ensure the success and maximization of benefits in enduring cooperation. □

Theorem 6: *In the context of long-term information security outsourcing cooperation, the aggregate benefits for both the MSSP and the principal escalate with an increasing number of stages. This observation suggests that a sustained cooperative relationship is instrumental in enabling both parties to realize enhanced overall benefits.*

Proof: From Eqs. (3) and (4), the total benefit function for both parties can be expressed as follows:

For every k and m, $k > m$, we have:

$$\begin{aligned} Z_m &= W_m + U_m \\ &= \sum_{k=m}^{K}\left\{\prod_{j=m}^{k}\left[1-\alpha\left(1-q_j\right)\right]v\right\} - \sum_{k=m}^{K}\left\{\prod_{j=m}^{k-1}\left[1-\alpha\left(1-q_j\right)\right]C\left(e_k\right)\right\} \end{aligned} \tag{18}$$

$$\begin{aligned} Z_{m-1} &= W_{m-1} + U_{\mathrm{m}-1} \\ &= \sum_{k=m}^{K}\left\{\prod_{j=m}^{k-1}\left[1-\alpha\left(1-q_j\right)\right]v\right\} - \sum_{k=m}^{K}\left\{\prod_{j=m}^{k-2}\left[1-\alpha\left(1-q_j\right)\right]C\left(e_k\right)\right\} \end{aligned} \tag{19}$$

$$Z_m - Z_{m-1} = \prod_{j=m}^{k}\left[1-\alpha\left(1-q_j\right)\right]v - \prod_{j=m}^{k-1}\left[1-\alpha\left(1-q_j\right)\right]C\left(e_k\right) \tag{20}$$

Because

$$\frac{\prod_{j=m}^{k}\left[1-\alpha\left(1-q_j\right)\right]v}{\prod_{j=m}^{k-1}\left[1-\alpha\left(1-q_j\right)\right]C\left(e_k\right)} = \frac{\left[1-\alpha\left(1-q_j\right)\right]v}{C\left(e_k\right)} > 1 \tag{21}$$

Then, we can obtain: for very k and m,

$$k > m, Z_m > Z_{m-1} \tag{22}$$

Long-term cooperation significantly enhances the efficacy of information security outsourcing, as it nurtures the accumulation of experience and the development of trust, thereby bolstering operational efficiency. By aligning on common objectives in information security and mutual interests, the MSSP and the principal can collaboratively mitigate risks and diminish the incidence of moral hazard. It is imperative for the MSSP and the principal to forge a strategic alliance, routinely reassess and refine their cooperative dynamics, and persistently invest in technological innovation and upgrades to keep pace with the ever-evolving information security landscape. Consequently, long-term cooperation is anticipated to yield more substantial benefits, although it necessitates concerted efforts from both parties to maintain and optimize their collaborative relationship. □

5 Case Analysis

To illustrate the multi-stage cooperative game process of information security outsourcing under dynamic moral hazard, a case study is conducted using a specific MSSP (Managed Security Service Provider) service company. As a leading enterprise in the fields of network security and cloud computing in China, it has been dedicated to enterprise-level network security, cloud computing, IT infrastructure, and the

Internet of Things (IoT), offering comprehensive products and services. It is committed to supporting the fundamental aspects of digital transformation across various industries, making digitalization simpler and more secure for users. In terms of scale, the company has witnessed a steady revenue growth from 2020 to 2024. Notably, its cloud computing business has emerged as a new growth driver. Based on the company's service case, the corresponding parameter values are set as follows: $\alpha = 0.3, v = 100000, \beta = 0.2, p = 10000, K = 10$. Through numerical simulation analysis, this section specifically studies the key factors influencing the long-term information security outsourcing cooperation between both parties, as well as their marginal utility, while also verifying the rationality, feasibility, and robustness of the conclusions.

5.1 Analysis of the Factors Affecting MSSP's Effort Level

Understanding how MSSPs allocate effort across stages is critical to designing effective incentives. This section examines the relationship between effort investment, marginal utility, and external environmental conditions. Through simulation results, the impact of varying effort levels on defense success probabilities and expected payoffs is illustrated, providing empirical support for the theoretical models developed earlier.

As depicted in Fig. 2, the analysis reveals that the marginal utility varies distinctively with the MSSP's effort level, exhibiting a clear stage-wise pattern, and is profoundly influenced by the external environmental index. In the initial stage, near the left end of the horizontal axis, the marginal utility of the MSSP increases sharply with escalating effort. This rapid increase is attributed to the significant enhancement in the quality of information security services that even modest efforts can achieve when fundamental security issues are yet to be fully resolved, thereby improving customer experience and satisfaction and leading to a substantial increase in expected utility. This indicates that minimal efforts can yield relatively high utility returns.

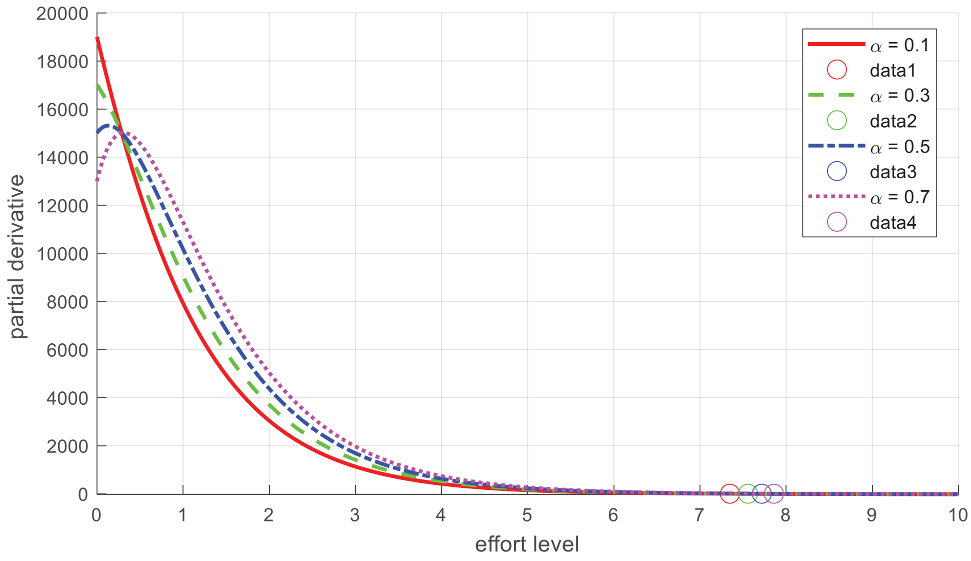


Figure 2: Factors affecting MSSP's effort level

As the effort level continues to rise, the curve gradually plateaus, and the marginal utility increment decelerates, marking the intermediate stage. During this phase, the MSSP begins to tackle more complex issues, necessitating greater resource allocation. However, given that many foundational problems have been effectively addressed, the incremental returns per unit of effort commence to diminish, signifying diminishing marginal returns.

Ultimately, when the effort level reaches a high stage, near the right end of the horizontal axis, the curve becomes nearly flat, and the marginal utility approaches zero. This suggests that most information security challenges have been effectively mitigated, and while additional efforts can still contribute to utility growth, the increase is markedly limited. It implies that at high effort levels, the MSSP must rely on advanced technological innovation and research and development investment to achieve marginal utility growth, which demands considerable resources and time.

The external environmental index (α) emerges as a pivotal variable that significantly modulates the relationship between effort level and marginal utility. The diverse curves in the figure correspond to various α values, reflecting how external environmental conditions influence the effectiveness of the MSSP's efforts. When α is low (e.g., 0.1 or 0.3), indicating a more favorable external environment such as abundant market opportunities, fewer technological barriers, or strong policy support, the MSSP's marginal utility grows rapidly at low effort levels, peaks, and then gradually decreases at a slower rate. This suggests that in a favorable environment, MSSPs can capitalize on external opportunities with higher levels of effort, prolonging the duration of utility growth and achieving a higher expected utility peak.

Conversely, as showed in Fig. 3, when α is high (e.g., 0.5 or 0.7), reflecting a relatively harsh external environment such as intensified market competition, increasing technological challenges, or rising natural risks, the marginal utility of MSSP's efforts increases more slowly at lower effort levels, with the peak appearing earlier and at a lower level. As the effort level increases, the rate of decrease in marginal utility accelerates. This trend indicates that in a competitive environment, external constraints limit the MSSP's potential for utility growth, and the returns on resource investment are lower and decrease more rapidly.

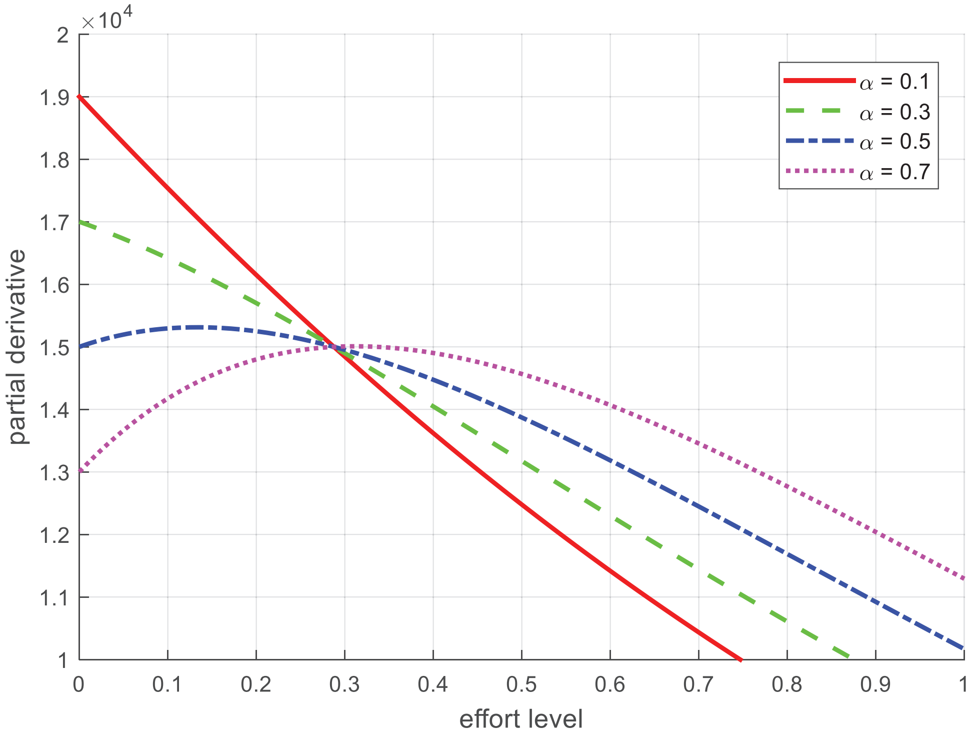


Figure 3: Local illustration of factors affecting MSSP's effort level

In summary, Fig. 4 not only reveals the stage-wise impact of the MSSP's effort level on expected marginal utility but also underscores the central role of the external environmental index in mediating the relationship between effort and utility. This implies that in information security outsourcing cooperation, MSSPs must adjust their effort strategies flexibly according to the external environment: in favorable information security environments, they can opt for higher effort levels to maximize utility returns, whereas in more challenging environments, they need to optimize resources and seek new growth opportunities through technological innovation and strategic adjustments to avoid inefficient resource consumption and premature diminishing marginal utility.

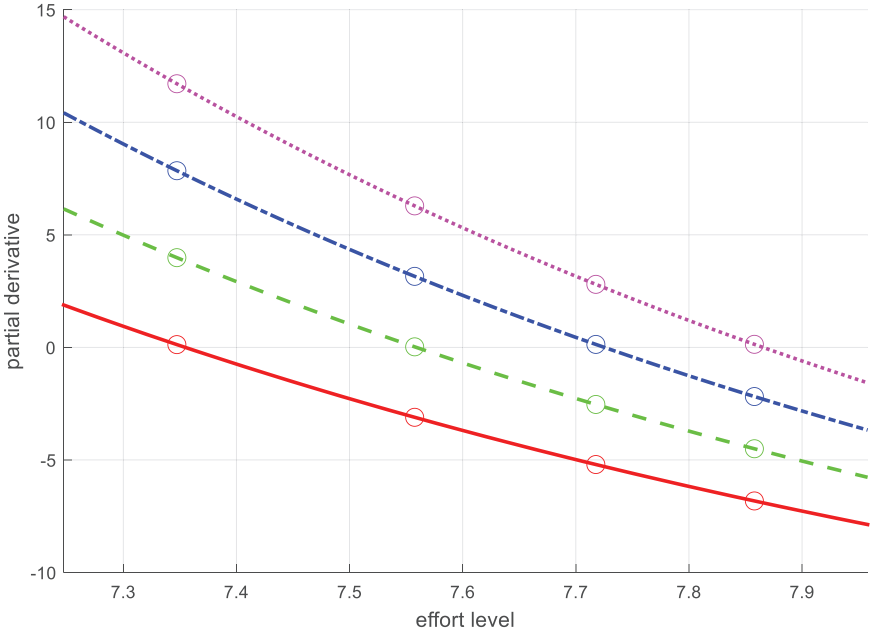


Figure 4: Local illustration of factors affecting MSSP's effort level (continued)

5.2 Analysis of the Factors Affecting the Expected Payoffs of the Principal and MSSP

Figs. 5 and 6 depict the influence of natural external conditions and compensation ratios on the expected payoffs of the principal and MSSP, illustrating how the expected utility of both parties evolves as cooperation progresses under varying natural environmental conditions and corresponding parameter settings.

Fig. 5 reveals that in a favorable environment, the principal's expected utility exhibits a smooth and steady growth trajectory. This trend suggests that under favorable external conditions, the enterprise can consistently generate profits, which gradually increases as the cooperation advances. In a moderate natural environment, the expected utility of the principal grows slightly more rapidly than in a favorable environment, yet the overall growth trend remains stable. This may be attributed to the fact that a moderate environment presents a balance of market opportunities and challenges, necessitating the enterprise to capitalize on opportunities while managing certain risks. Conversely, in a harsh natural environment, the principal's expected utility surges in the early stages but subsequently decelerates markedly, potentially even transitioning to negative growth. This indicates that while the enterprise may achieve relatively high returns in the short term, the harsh external conditions are deleterious to its long-term development, possibly culminating in declining profits or even losses.

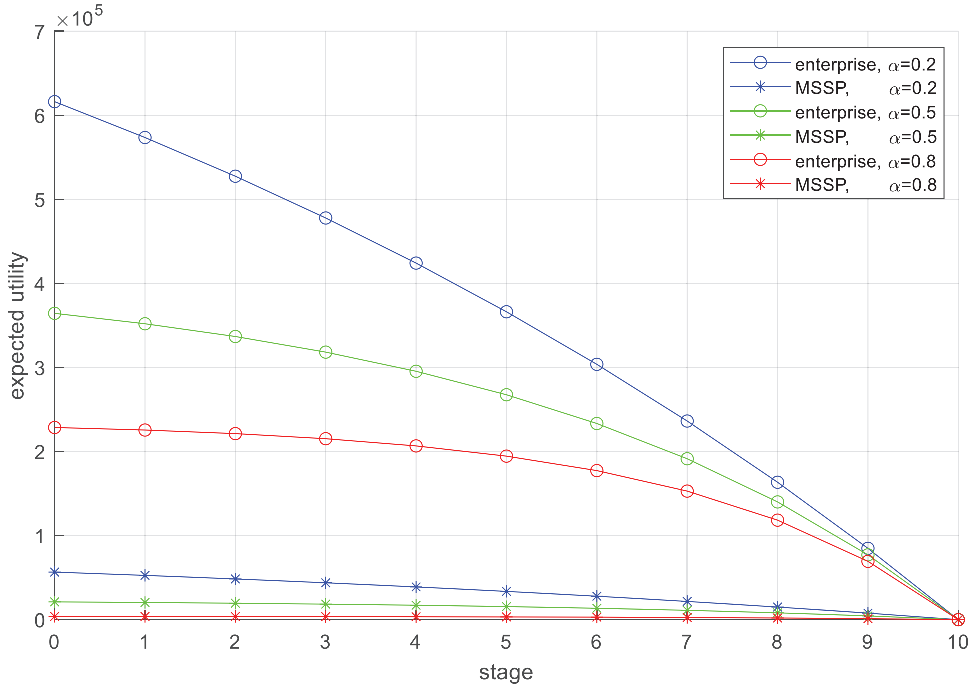


Figure 5: Comparison of expected payoffs under different natural states

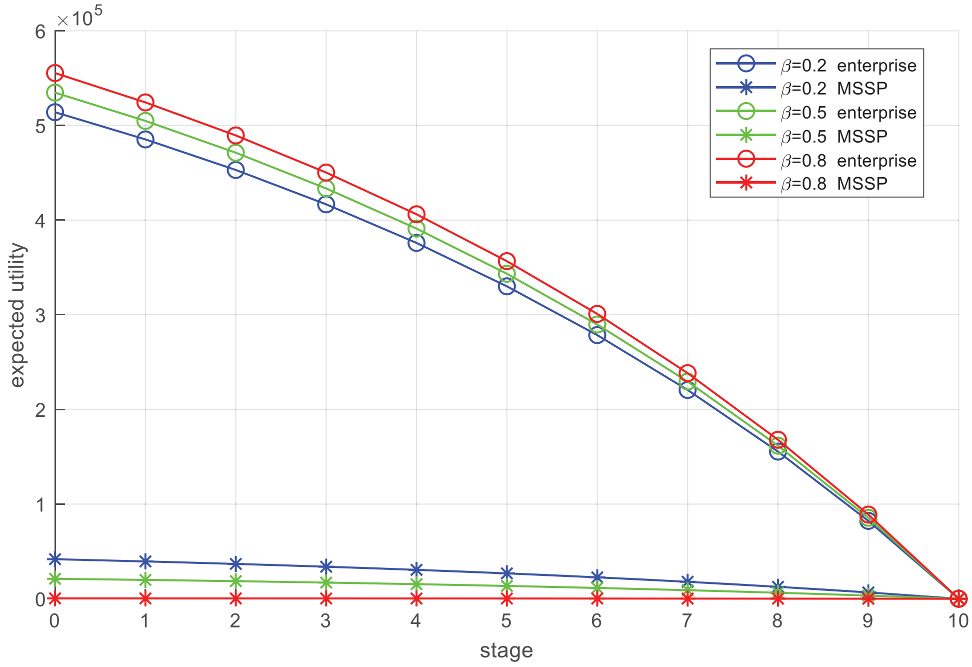


Figure 6: Comparison of expected payoffs under different compensation ratios

The MSSP's expected utility also demonstrates steady growth in a favorable environment. This indicates that under favorable external conditions, the MSSP can provide stable and efficient services, resulting in sustained growth in its expected utility. In a moderate natural environment, the MSSP's expected utility grows slightly faster than in the favorable environment, yet the growth rate remains steady. This may be because the MSSP encounters more challenges and opportunities in the moderate environment but can still achieve stable utility growth through professional services and management capabilities. In a harsh environment, the MSSP's expected utility surges initially but then experiences a sharp deceleration. This suggests that even with professional services and management capabilities, the MSSP struggles to maintain high growth in the long term under harsh external conditions. Adverse environments may severely impact the MSSP's operations and service quality, thereby reducing its expected utility.

These figures underscore how the expected utility of both the principal and MSSP fluctuates under different natural environmental conditions, highlighting the profound impact of the external environment on the operations of both parties. In favorable environments, both the enterprise and the MSSP can achieve steady and consistent profit growth. In contrast, while higher returns may be obtained in the short term in harsh environments, the long-term impact on the development of both the enterprise and MSSP is highly detrimental. Therefore, when devising long-term strategies and plans, both the enterprise and MSSP need to fully consider external environmental factors to address potential risks and challenges.

Fig. 6 delineates the variation in the expected utility of both the principal and the MSSP as their collaboration progresses under varying compensation ratios. At lower compensation ratios, the principal's expected utility curve is comparatively subdued, indicating that with a reduced compensation ratio, the principal possesses diminished safeguarding against potential risks and losses, culminating in diminished expected utility. Conversely, as the compensation ratio escalates, the principal's expected utility ascends in a steady manner. This suggests that with an enhanced compensation ratio, the principal secures greater risk mitigation, consequently bolstering their expected utility. The trajectory of the principal's expected utility may fluctuate at different stages, with utility growth in response to an increasing compensation ratio being more pronounced at certain junctures. Such variations could be attributable to specific market conditions, business demands, or risk factors prevalent at those stages.

Paralleling this trend, the MSSP also manifests lower expected utility at lower compensation ratios. This may stem from the fact that a reduced compensation ratio alleviates the risks and liabilities shouldered by the MSSP but concurrently caps their potential returns. As the compensation ratio increments, the MSSP's expected utility curve follows suit, exhibiting a gradual rise. By embracing greater compensation responsibilities, the MSSP correspondingly reaps a heightened expected utility. However, unlike the principal, the MSSP's expected utility growth may be swayed by additional considerations. With higher compensation ratios, the MSSP must allocate increased resources to ensure the delivery of superior services and to manage burgeoning risks. This allocation subsequently influences the MSSP's operational costs and profit margins, which in turn have repercussions on their expected utility.

In summary, Fig. 6 underscores the pivotal role of the compensation ratio in shaping the benefit relationship between the principal and the MSSP. As the compensation ratio mounts, the expected utility trends of both the principal and the MSSP tilt upwards, albeit with potentially varying growth rates and overall patterns between the two entities. When establishing contract terms and negotiating compensation ratios, both parties must take into account a spectrum of factors, including the market environment, business demands, and their individual risk propensities, to secure a mutually advantageous outcome.

5.3 Analysis of the Marginal Effect Trends of Payments Made by the Principal at Each Stage

The marginal effects of payments made by the principal at each stage are elucidated through simulation results presented in Fig. 7. This figure delineates how the marginal effect of the principal's payments varies at each stage of cooperation under disparate external conditions. As depicted in Fig. 7, an increment in the value of α corresponds to a steeper slope of each line, signifying that under more challenging external environments, the marginal effect of the principal's payments escalates more swiftly at each stage of cooperation. In the nascent stage of cooperation, the lines' starting points are proximate, indicating that the marginal effects of the principal's payments across different external environments are not markedly divergent at the outset of the collaboration. As cooperation unfolds, the lines diverge, demonstrating that the discrepancies in the marginal effects of the principal's payments in varying external environments amplify over time. In a favorable external environment (low α value), the principal encounters lower risks and uncertainties, resulting in a relatively stable and gradual increase in the marginal effect of payments. Conversely, in a stringent external environment (high α value), the principal must make more substantial investments to mitigate risks and uncertainties. Consequently, in the later stages of cooperation, the marginal effect of payments escalates rapidly to ensure the cooperation's smooth progression and the achievement of anticipated outcomes.

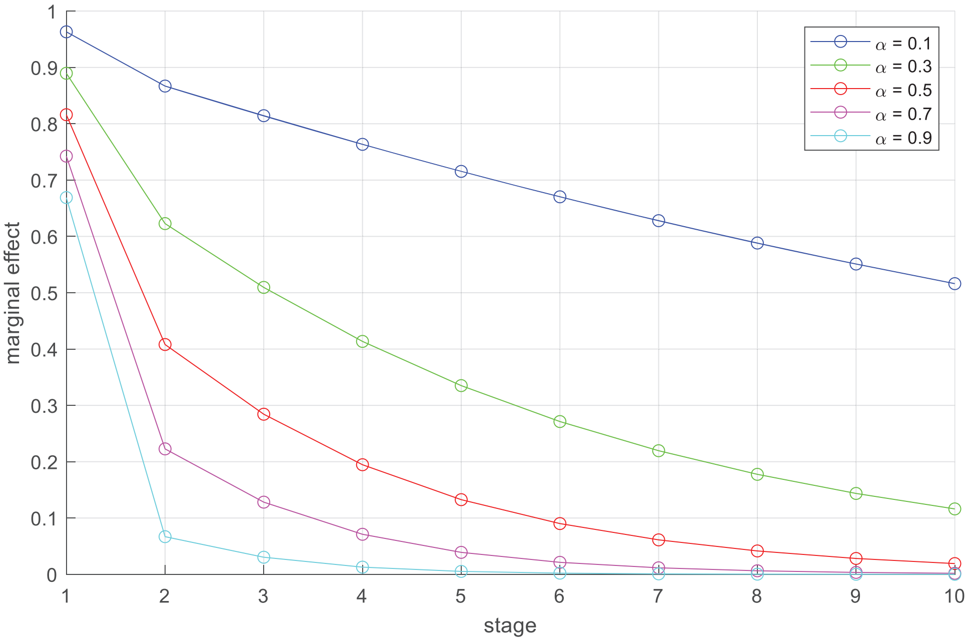


Figure 7: Trend of marginal effect of payments made by the principal at each stage

Fig. 7 furnishes the principal with a rationale for calibrating their payment strategy under fluctuating external conditions. In adverse environments, the principal must anticipate their budget to accommodate potentially elevated payment demands in the cooperation's later stages. Moreover, this underscores the importance of the principal fully evaluating a partner's capacity to manage risks and uncertainties when selecting a collaborator, thereby minimizing the prospective for exorbitant payment risks in the future. By portraying the marginal effects of payments at each stage of cooperation under various natural external conditions, Fig. 7 imparts significant decision-making insights for the principal. It unveils the external environment's influence on cooperation costs and counsels the principal to incorporate external environmental factors when devising cooperation strategies and payment plans.

5.4 Analysis of the Trend of Comprehensive Benefits of MSSP and the Principal over Time

Fig. 8 presents simulation results that track the comprehensive benefits of the MSSP and the principal across the course of their cooperation under three distinct natural selection conditions: α = 0.1, 0.3, and 0.5. To illustrate the evolution of benefits over time, the cooperation phases are extended while holding other parameters constant. The findings reveal that, across various external environmental indices, the collaboration between the MSSP and the information security outsourcing principal follows a characteristic trajectory of profit growth. The total expected profit of the MSSP from stage k to stage K (denoted as U_m), the total expected profit of the principal from stage k to stage K (denoted as W_m), and the total expected utility for both parties (denoted as Z_m) all increment gradually as the cooperation advances. This pattern suggests a positive correlation between long-term information security outsourcing cooperation and the aggregate benefits for both the MSSP and the principal.

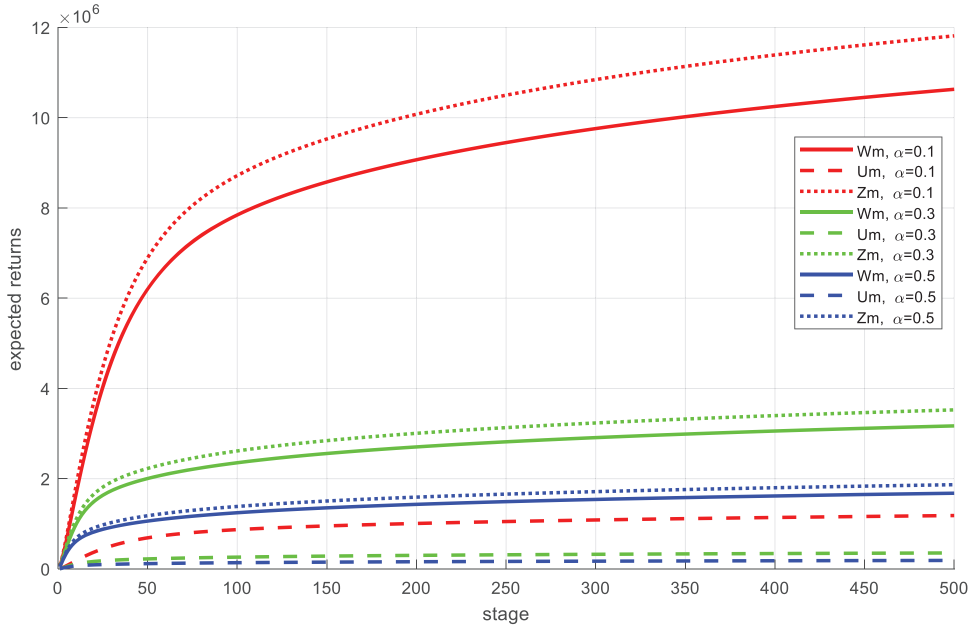


Figure 8: Trend of comprehensive benefits of MSSP and the principal

In the early stages of cooperation, factors such as initial resource integration, early market expansion benefits, and swift technological innovation adoption result in rapid growth of *Um*, *Wm*, and *Zm*. During this phase, both parties achieve significant profit expansion through concerted efforts, underscoring the salutary effects of cooperation. As cooperation intensifies, the initial benefits wane, and diminishing marginal returns start to become apparent. Concurrently, issues like communication barriers and profit distribution challenges arise, which can decelerate profit growth. Thus, in the mid-to-late stages of cooperation, the growth rate of *Um*, *Wm*, and *Zm* gradually slows. When both parties reach a stable state of cooperation, profit levels stabilize as well. At this juncture, both parties have established a sophisticated cooperation mechanism and profit distribution scheme, enabling them to sustain relatively stable profits while continuously generating value for one another.

It is also crucial to highlight that the external environment significantly influences *Um*, *Wm*, and *Zm*. In a favorable environment characterized by robust market demand, substantial policy support, and moderate competition, both parties can capitalize on more business opportunities and policy incentives, facilitating profit growth. In contrast, in markets with sluggish demand, inadequate policy support, or fierce competition, both parties must exert additional effort and resources to surmount challenges and attain stable profit growth.

In conclusion, the cooperation process between the MSSP and the information security outsourcing principal is intricate and dynamic, subject to a multitude of influencing factors. In practical applications, both parties must vigilantly monitor shifts in the external environment, strengthen communication and collaboration, and continuously refine the cooperation mechanism and profit distribution plan to achieve enduring profit growth and mutually advantageous development.

6 Conclusion

In the realm of information security outsourcing, both the principal and the contractor attach great importance to the continuity of long-term contracts. They must also account for the dynamic nature of moral hazard throughout the outsourcing process. Against this backdrop, this study constructs a multi-stage game model incorporating moral hazard. By analyzing this model, the strategic behaviors of both parties over time are derived, and several significant inferences are drawn. Through simulation analysis, the cooperative relationship between the contractor and the principal is elucidated, leading to the following conclusions from the perspective of information security management:

(1) Information security outsourcing enables enterprises to transfer information security responsibilities to specialized service providers, thereby reducing information security risks. However, during this process, enterprises need to strike a balance between service quality and costs to maximize expected payoffs. As outsourcing service fees increase, expected outcomes may decline. Thus, enterprises should strive to achieve an equilibrium between enhancing service quality and controlling costs. This balance is crucial for both parties involved, and cooperation strategies should be adjusted flexibly in response to changing risk and benefit conditions. For example, enterprises can regularly assess the MSSP's service quality through key performance indicators (KPIs) such as the number of security incidents detected and resolved in a timely manner, and then adjust the service fees based on the assessment results.

(2) Long-term outsourcing generates positive effects for both the principal and the Managed Security Service Provider (MSSP). The principal's steadily increasing expected payoffs during the cooperation can strengthen the stability and sustainability of the partnership. Meanwhile, it also helps the MSSP secure more business and profits. Therefore, both enterprises and MSSPs should value the long-term nature of their cooperation. They should enhance communication and coordination to ensure stable and long-term development. For instance, they can hold regular joint meetings to discuss security threats, service improvements, and future cooperation plans.

(3) Information security outsourcing is a multi-stage process. As cooperation progresses, the principal's expected payoffs may increase incrementally. However, the principal's payoffs may fluctuate at different stages of the collaboration. Thus, it is necessary to make adjustments and optimizations based on stage-specific payoff changes. When formulating cooperation strategies, the principal should carefully consider the impact of service fee adjustments on long-term benefits and conduct comprehensive assessments to achieve optimal cooperation. For example, in the early stages of cooperation, the principal can offer a relatively lower base service fee with performance-based bonuses. As the cooperation matures and the MSSP's performance is proven, the principal can gradually increase the base fee while still maintaining a certain proportion of performance-related incentives.

The research conclusions offer the following managerial insights for both parties in information security outsourcing cooperation:

(1) Long-term planning and continuous cooperation: To ensure the sustainability of information security outsourcing collaboration, the principal should focus on long-term planning and continuous cooperation. In terms of contract design, it should explicitly include long-term cooperation clauses. For instance, setting the contract term to at least 3–5 years with renewal options based on performance provides a stable framework for both parties to plan resources and investments. When it comes to incentive mechanism development, a multi-dimensional approach is needed. Besides financial incentives like performance-based bonuses, non-financial incentives such as public recognition in industry reports or preferential treatment in future business expansions should be offered. For example, publicly praising the MSSP in the principal's annual security report when it reaches a certain security performance level can enhance the MSSP's market reputation. Regarding risk-sharing and monitoring, the contract should clearly define the scope of responsibilities and risk-sharing ratios. For example, in the case of a minor security incident, the MSSP could be made responsible for 70% of the loss-mitigation costs, and for major incidents, the ratio can be adjusted according to the cause. A real-time monitoring system should be established to track the MSSP's activities, including the frequency of security audits, response time to security alerts, and the effectiveness of security patches. This data can then be used to evaluate the MSSP's performance and ensure compliance with the contract terms.

(2) Building reputation and credibility: For the MSSP, establishing and maintaining a strong reputation and credibility is essential. To ensure high-quality service, the MSSP should invest in continuous employee training. This can be achieved by organizing regular internal training sessions focused on the latest security technologies and threats and by encouraging employees to obtain relevant industry certifications. In terms of incident response, the MSSP needs to develop a comprehensive plan. In the event of a security incident, it must respond within a predefined time frame, like within 1 h for high-priority incidents. The plan should cover incident containment, investigation, and recovery steps, and the MSSP should maintain timely and transparent communication with the principal throughout the process. Additionally, to adhere to ethical standards, the MSSP should establish an internal ethics committee to review and monitor its operations. This committee can set strict ethical guidelines for handling client data, such as implementing strict data-access controls and encryption requirements. Regular audits of the MSSP's compliance with these guidelines are necessary to safeguard its reputation.

(3) Continuous learning and adaptation: To stay competitive and effectively manage information security outsourcing, the MSSP must prioritize continuous learning and adaptation. This involves allocating a certain proportion of its revenue to research and development, which can be utilized to explore novel security technologies like artificial intelligence-based threat detection systems and enhance existing services. Simultaneously, the MSSP should establish a market intelligence team tasked with monitoring industry trends, competitor activities, and emerging threats. The team can gather information from diverse sources such as industry reports, security conferences, and online forums. Leveraging this data, the MSSP can proactively adjust its service offerings and strategies. Moreover, internal moral hazard management is crucial. The MSSP should implement a system of internal checks and balances, for example, separating the security operation and auditing functions. Regular reviews of employee performance and behavior are necessary to identify any signs of moral hazard, including unauthorized access to client data or negligence in security operations.

These managerial insights aid both the principal and contractor in better managing the information security outsourcing relationship, enhancing the effectiveness and sustainability of cooperation while ensuring adequate protection of information assets. In the dynamic information security landscape, adhering to these insights ensures effective cooperation and a productive outcome for both parties.

It is essential to acknowledge the limitations of this study's model. Firstly, the model assumes a rather simplistic relationship between the MSSP's effort level and the probability of successful security defense. In reality, this relationship can be influenced by numerous complex factors, such as the interaction among different security technologies, the evolving nature of cyber threats, and the synergy within the MSSP's teams. Secondly, the model presumes that both the principal and the MSSP have complete knowledge of the market environment and each other's capabilities at the onset of cooperation. In practice, significant information asymmetry often exists, which may lead to sub-optimal decision-making. Thirdly, the model does not fully account for the impact of external factors like regulatory changes, technological disruptions, and economic fluctuations on the outsourcing relationship. For example, new data protection regulations may require the MSSP to make substantial changes to its service offerings, which can disrupt the cost-benefit balance of the cooperation.

In practical applications, determining the specific values of various parameters still requires further research and exploration. Moreover, this study assumes that both the MSSP and the enterprise are rational game participants, without considering the moral hazard behaviors of other participants. Future research can incorporate the moral hazard behaviors of other participants into the game model for further refinement. Future research could also take into account the differences in bargaining power and reputation between Managed Security Service Providers (MSSPs) and enterprises, further enhancing the game model. Additionally, scenario simulations and real-world data analyses could be conducted to analyze and discuss the parameter values under different scenarios. Finally, the design of more effective incentive mechanisms for MSSPs, aimed at boosting their motivation, could be explored to further promote the development of information security outsourcing cooperation.

Acknowledgement: The authors gratefully acknowledge the insightful reviews and constructive comments provided by the reviewers of the Journal of Cybersecurity.

Funding Statement: Qiang Xiong and Jianlong Zhang were supported by National Social Science Fund of China (No. 24BGL279).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Qiang Xiong, Jianlong Zhang; data collection: Qianwen Song; analysis and interpretation of results: Jianlong Zhang; draft manuscript preparation: Jianlong Zhang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors confirm that the data supporting the findings of this study are available within the article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Yao YC, Li JC. Digital transformation and technological innovation in state-owned enterprises: a new perspective based on environmental uncertainty and relational embeddedness. China Soft Sci. 2024;(7):122–36. (In Chinese).
2. Bourque P, Smith A. Autonomy for homeland security. Sea Technol. 2021;62(3):24–7.
3. Tong X, Lai K, Lo CKY, Cheng TCE. Supply chain security certification and operational performance: the role of upstream complexity. Int J Prod Econ. 2022;247(3):108433. doi:10.1016/j.ijpe.2022.108433.
4. Alhussam MI, Ren J, Yao H, Abu Risha O. Food trade network and food security: from the perspective of Belt and Road Initiative. Agriculture. 2023;13(8):1571. doi:10.3390/agriculture13081571.

5. Ali Lakhiar I, Yan H, Zhang J, Wang G, Deng S, Bao R, et al. Plastic pollution in agriculture as a threat to food security, the ecosystem, and the environment: an overview. Agronomy. 2024;14(3):548. doi:10.3390/agronomy14030548.
6. Dong K, Xie Z, Zhen J. Optimal decision analysis of information security investment and cyber insurance under mandatory constraints. Chin J Manag Sci. 2021;29(6):70–81. (In Chinese).
7. Sun C. Research on countermeasures for network security governance. Netinfo Secur. 2023;6:104–10.
8. Cezar A, Cavusoglu H, Raghunathan S. Outsourcing information security: contracting issues and security implications. Manag Sci. 2013;60(3):638–57. doi:10.1287/mnsc.2013.1763.
9. Cezar A, Cavusoglu H, Raghunathan S. Sourcing information security operations: the role of risk interdependency and competitive externality in outsourcing decisions. Prod Oper Manag. 2017;26(5):860–79. doi:10.1111/poms.12681.
10. Wu Y, Wang LP, Feng GZ. Incentive contracts research of information security outsourcing for complementary firms in supply chain under double moral hazard. Syst Eng Theory Pract. 2022;42:2916–26. (In Chinese).
11. Dey D, Fan M, Zhang C. Design and analysis of contracts for software outsourcing. Inf Syst Res. 2009;21(1):93–114. doi:10.1287/isre.1080.0223.
12. Hui KL, Hui W, Yue WT. Information security outsourcing with system interdependency and mandatory security requirement. J Manag Inf Syst. 2012;29(3):117–56. doi:10.2753/MIS0742-1222290304.
13. Wu Y, Xu M, Feng G. Contract design in information security outsourcing under cost information asymmetry. J Ind Eng Eng Manag. 2024;38(4):196–208. (In Chinese).
14. Lee CH, Geng X, Raghunathan S. Contracting information security in the presence of double moral hazard. Inf Syst Res. 2012;24(2):295–311. doi:10.1287/isre.1120.0447.
15. Alzubi OA. Quantum readout and gradient deep learning model for secure and sustainable data access in IWSN. PeerJ Comput Sci. 2022;8(1):e983. doi:10.7717/peerj-cs.983.
16. Alzubi OA. BotNet attack detection using MALO-based XGBoost model in IoT environment. In: Proceedings of Third International Conference on Computing and Communication Networks; 2023 Nov 17–18; Manchester, UK.
17. Zhao X, Xue L, Whinston AB. Managing interdependent information security risks: cyberinsurance, managed security services, and risk pooling arrangements. J Manag Inf Syst. 2013;30(1):123–52. doi:10.2753/MIS0742-1222300104.
18. Wu X, Zhao R, Tang W. Uncertain agency models with multi-dimensional incomplete information based on confidence level. Fuzzy Optim Decis Mak. 2014;13(2):231–58. doi:10.1007/s10700-013-9174-9.
19. Wu Y, Tayi GK, Feng G, Fung RYK. Managing information security outsourcing in a dynamic cooperation environment. J Assoc Inf Syst. 2021;22(3):827–50. doi:10.17705/1jais.00681.
20. Hui KL, Ke PF, Yao Y, Yue WT. Bilateral liability-based contracts in information security outsourcing. Inf Syst Res. 2019;30(2):411–29. doi:10.1287/isre.2018.0806.
21. Elitzur R, Gavious A. A multi-period game theoretic model of venture capitalists and entrepreneurs. Eur J Oper Res. 2003;144(2):440–53. doi:10.1016/S0377-2217(02)00144-3.
22. Roels G, Karmarkar US, Carr S. Contracting for collaborative services. Manag Sci. 2010;56(5):849–63. doi:10.1287/mnsc.1100.1146.
23. Demirezen EM, Kumar S, Shetty B. Managing co-creation in information technology projects: a differential games approach. Inf Syst Res. 2016;27(3):517–37. doi:10.1287/isre.2016.0636.
24. Demirezen EM, Kumar S, Shetty B. Two is better than one: a dynamic analysis of value co-creation. Prod Oper Manag. 2020;29(9):2057–76. doi:10.1111/poms.12862.