AIMS Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 11(7): 22354–22379.
DOI: 10.3934/math.2026904
Received: 26 May 2026
Revised: 05 July 2026
Accepted: 14 July 2026
Published: 27 July 2026

Research article

Modeling and pricing cybersecurity insurance with information asymmetry

Rong Hu[1], **Na Ren**[2] **and Xin Zhang**[1,*]

[1] School of Mathematics, Southeast University, Nanjing 211189, China
[2] School of Science, Lanzhou University of Technology, Lanzhou 730050, China

* **Correspondence:** Email: xzhangseu@seu.edu.cn.

Abstract: Firms typically invest in security measures to reduce potential losses from cyber incidents. Since such measures cannot fully eliminate cyber risks, cyber insurance plays an important role in hedging residual losses. This paper studies contract design in a monopolistic cyber insurance market where policyholders differ in their underlying risk levels and choose unobservable security effort. We consider both risk-neutral and risk-averse agents and develop a theoretical framework to derive optimal insurance contracts and security investments. These contracts are designed to alleviate moral hazard and adverse selection under three information scenarios. The theoretical results reveal three main incentive effects: premium discounts promote security effort, more generous coverage weakens the incentive to protect, and protection generated by neighboring firms creates a substitution effect that weakens individual effort. Numerical experiments compare the optimal premium discount, coverage rate, security effort, and the insurer's expected payoff across the three information scenarios.

Keywords: cyber risks; security investment; information asymmetry; optimal insurance contracts
Mathematics Subject Classification: 91B41, 91B43

1. Introduction

With the widespread use of the internet and the rapid development of information technology, cyber risk has become a major challenge for both individuals and enterprises. Cyber incidents are characterized by substantial uncertainty in both their occurrence and loss severity. Sun et al. [27] and Xu et al. [31] show that such incidents may lead to serious consequences, including direct financial losses, business interruption, regulatory penalties, and reputational damage. Although firms and individuals can invest in security measures to mitigate potential losses, such measures cannot fully eliminate cyber risk. Against this background, cyber insurance has emerged as an important mechanism for transferring residual losses and providing compensation for losses caused by malicious attacks, ransomware, hacker intrusions, and other cyber events; see, for example, Vojnovic and Ganesh [29], Sun et al. [27], and Xu et al. [31]. Awiszus et al. [3] classified cyber risks into three categories, idiosyncratic, systematic, and systemic risks, and discussed different analytical approaches for these distinct risk types. Cyber insurance has attracted increasing attention in recent years because of its growing theoretical and practical importance. Hofmann [13], Schwartz and Sastry [26], and Romanosky et al. [24] investigated cyber insurance and related risk-sharing mechanisms from different perspectives. Nevertheless, substantial challenges remain in both market development and theoretical analysis, as discussed by Hillairet et al. [12] and Schatz and Bashroush [25].

This paper studies security investment and premium pricing in an interdependent network. As discussed by Lelarge and Bolot [18], agents may invest in security measures to reduce the probability of infection and improve cybersecurity. Anderson [2] further pointed out that such measures may include upgrading technical systems, improving access control and monitoring, providing staff training, and strengthening information security practices. Self-protection investment has attracted considerable attention in the cybersecurity literature; see, for example, Varian [28], Bravard et al. [4], and Bolot and Lelarge [17]. Yang and Lui [33] provided a basic understanding of how network externalities and node heterogeneity affect security adoption. Pal and Golubchik [22] contended that cybersecurity investment is affected by both full and partial coverage models of cyber insurance. Cavusoglu et al. [7] proposed a game-theoretic approach to determine the level of IT security investment and compared the game-theoretic solution with the decision-theoretic solution in terms of investment level, vulnerability, and return on investment. Cavusoglu et al. [6] addressed the shortage of historical data and propose a comprehensive model for analyzing IT security investment. Schatz and Bashroush [25] extracted information from several databases to study key methods for measuring the value of information security investments. However, due to the interconnected nature of networks, an agent's security investment not only protects its own system, but also lowers the likelihood of indirect attacks on its neighbors. In other words, improving one's own security creates positive externalities for connected users. As a result, many agents tend to free-ride on others' security efforts to reduce their own investment costs, leading to underinvestment in security and a decline in the overall security level.

On the other hand, cyber insurance pricing is much more challenging than traditional insurance pricing. Khalili et al. [15] and Xie et al. [30] discussed such difficulties from the perspectives of contract design and cyber insurance market performance. One important reason is that traditional insurance pricing typically relies on actuarial tables constructed from abundant historical records. However, in cyber insurance, firms are often reluctant to disclose breach information owing to concerns about reputational damage. As a result, cyber insurance suffers from a lack of standardized rating systems and sufficient actuarial data. Because cyber risks are inherently interdependent, properly characterizing their dependence structure and loss model is essential for cyber insurance pricing. Existing studies have examined the dependence structure from several perspectives. Pal [23] studied cyber insurance premium design in a setting where an agent's loss depends not only on its own effort, but also on the investments of its neighbors. Copula functions have also been used to capture nonlinear dependence among cyber risks, with common choices including the Gaussian copula, the t-copula, and Archimedean copulas; see, for example, Herath and Herath [11], Liu et al. [20], and Carannante et al. [5]. Related studies have also adopted game-theoretic frameworks to analyze interdependent security and investment incentives, such as Kunreuther and Heal [16] and Naghizadeh and Liu [21]. With regard to the loss model, Xu and Hua [32] characterized cyber losses by the number of agents attacked in the system and the duration of downtime. Khalili et al. [15] discussed which losses should be covered or excluded in cyber insurance contracts for first- and third-party losses, as well as how insurers price cyber insurance products. Gordon et al. [10] proposed a comprehensive four-step cyber insurance decision framework based on the overall risk management process, in which insurance is used as a tool for managing information security risk.

Accurate premium customization requires detailed information about insured firms, including their organizational structure, employees' security awareness, and investment in protection systems. However, such information is often not fully observable to insurers, making information asymmetry a key issue in cyber insurance pricing. Chiappori and Salanié [8] discussed information asymmetry in insurance markets, where the parties to a transaction may possess different levels of information, leading to adverse selection or moral hazard. Akerlof [1] showed that quality uncertainty may undermine market sustainability when buyers cannot distinguish between different quality levels. In the context of cyber insurance, this implies that if insurers cannot distinguish users with different security levels and offer differentiated premiums, their profitability may be unsustainable. Similarly, Hofmann [13] studies an insurance market with loss externalities and shows that a monopolistic insurer can achieve social optimality through premium discrimination in a model with heterogeneity and incomplete information.

In this paper, we mainly consider two forms of information asymmetry: moral hazard and adverse selection. Moral hazard arises because insurers cannot perfectly monitor policyholders' security actions after a contract is signed. Adverse selection occurs when high-risk agents have a stronger demand for insurance, while insurers cannot fully observe their actual risk exposure. The related literature shows that Ligon and Thistle [19] studied a single-period monopoly insurance market with adverse selection and moral hazard, and showed that when the distortions caused by moral hazard are sufficiently mild, insurers can use price-quantity contracts to address the two information asymmetries simultaneously. Pal [23] extended this line of research to cyber insurance and developed the model formulated for internet and distributed network environments.

To reflect real-world cybersecurity insurance practices, we consider three information scenarios: (i) Both sides do not know the risk type: For firms in emerging industries, historical incident data may be limited, or some firms may be unwilling to incur the substantial cost of third-party assessments; in either case, even the firms themselves may not have accurate knowledge of their true cyber risk type. (ii) The policyholder learns the risk type after signing: The risk type is unclear at the contracting stage, but becomes known later through security audits, vulnerability scans, or incident signals. This timing affects the subsequent self-protection decision and makes moral hazard more important. (iii) The policyholder knows the risk type before signing: Firms may learn their own risk type from third-party assessments, while the insurer cannot observe this information at the time of contracting, which creates adverse selection. Awiszus et al. [3] pointed out that the loss assumptions in most existing game-theoretic models are overly simplistic, since losses are typically treated as constant quantities. To address this limitation, we model cyber losses as random variables rather than fixed values. Based on this framework, we derive the optimal pricing and self-protection strategies for both risk-neutral and risk-averse agents.

This paper studies cyber insurance contract design under asymmetric information. The main contributions are summarized as follows. First, in contrast to Ligon and Thistle [19], who assume a binary setting with a fixed loss amount, we model cyber loss severity as a random variable. This formulation better captures the uncertainty and heterogeneity of cyber losses. Second, we incorporate network externalities into the cyber insurance framework. Each agent's effective protection level depends not only on its own security effort but also on the efforts transmitted from neighboring agents. Our theoretical results show that a higher level of external protection reduces the agent's own optimal effort, reflecting a substitution effect and a possible free-riding incentive. Third, we examine three information scenarios according to whether and when the policyholder learns its risk type, thereby providing a way to alleviate information asymmetry in insurance contract design. Under these scenarios, we characterize the optimal contracts, optimal effort levels, and the insurer's expected profit. By comparing risk-neutral and risk-averse policyholders, we further show that risk aversion is crucial in driving insurance demand. The numerical analysis reports the corresponding optimal premium discounts, coverage rates, and security efforts.

The remainder of this paper is organized as follows. Section 2 describes the utility functions of risk-neutral and risk-averse agents. Section 3 establishes the optimal contracts for mitigating information asymmetry under three cases. Section 4 presents numerical simulations to examine the effects of parameters and illustrate the optimal solutions. Finally, Section 5 concludes the paper.

2. Model

This section is organized into three parts. In the first part, we introduce the basic concepts of networks and present the network structure of agents studied in this paper. The second part presents the utility function and its properties. The third part develops the information structure, which lays the foundation for alleviating information asymmetry in the next section. The symbols used in this article are summarized in Table 1.

Table 1. Meaning of key variables.

Variable	Meaning
P	Base premium
α_i	Premium discount factor of agent i
β_i	Coverage rate of agent i
e_i	Security effort of agent i
a	Risk aversion coefficient
W_i	Wealth level of agent i
S_i	Observable underwriting score of agent i
m_i	External protection level from neighboring agents
s_i	Effective protection level of agent i
a_{ij}	Adjacency indicator between agents i and j
x_{ij}	Security spillover factor from agent j to agent i
L_i	Cyber loss amount of agent i
$C(\cdot)$	Cost of self-protection investment
θ_i	Risk type of agent i
$\mu_k(\cdot)$	Mean parameter of log-loss for type k
$\lambda_k(\cdot)$	Variance parameter of log-loss for type k

2.1. *Network structure*

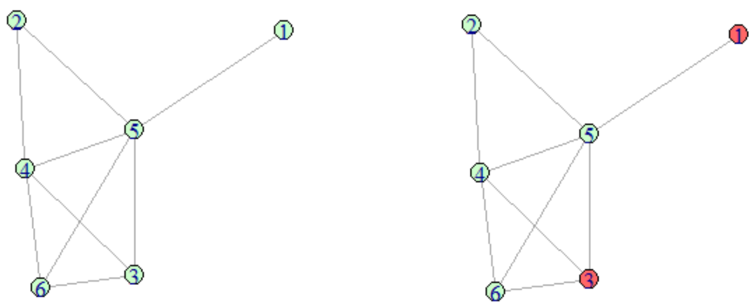
Assume the relationship of internet agents is described as an undirected graph $\Gamma = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the node set, and $\mathcal{E}$ is the edge set. Γ represents the network structure, where $(u, v) \in \mathcal{E}$ means the two agents u and v can influence each other. If any $u \in \mathcal{V}$ can affect any $v \in \mathcal{V}$, we call it a complete graph. In a complete graph, all agents can influence each other. Denoting $A = (a_{uv})$ as the adjacency matrix of Γ,

$$a_{uv} = \begin{cases} 1 & \text{if } (u, v) \in \mathcal{E}, \\ 0 & \text{otherwise.} \end{cases}$$

It is worth noting that the problem setting naturally implies $a_{vv} = 0$. In addition, we let $N(i) = \{j \in \mathcal{V} \mid a_{ij} = 1\}$ be the set of the one-hop neighbors of i, and neighboring nodes can affect each other. We represent the degree of a node i by d_i, where d_i equals $|N_i(v)|$. For illustrative purposes, we consider two network states, denoted by

$$(I_1^0, I_2^0, \ldots, I_N^0) \quad \text{and} \quad (I_1^1, I_2^1, \ldots, I_N^1),$$

representing the network before and after a possible cyber incident, respectively, where $I_v^b = 1$ indicates that node v has been attacked in state b, while $I_v^b = 0$ indicates that node v remains secure, $b = 0, 1$.



(a) Network state before a cyber incident. (b) Network state after a cyber incident.

Figure 1. Network diagrams of six companies before and after possible cyber incidents. Red nodes indicate companies affected by cyber incidents and suffering corresponding losses.

As shown in Figure 1 (a), all companies in the network are secure before cyber incidents occur. Company 1 is a one-hop neighbor of company 5 and therefore affects only the security of company 5. In other words, a higher security investment by company 1 not only improves its own security, but also reduces the probability of security incidents for company 5. Figure 1 (b) illustrates the network after possible cyber incidents occur. In this state, company 1 is affected by a cybersecurity incident and suffers a loss. Due to the direct connection between companies 1 and 5, the incident involving company 1 may also increase the risk exposure of company 5. Similarly, company 3 is compromised and may affect its directly connected neighbors, namely companies 4, 5, and 6.

2.2. *Properties of the utility function*

We model the utility function U_i as a function of agent i's wealth, its security effort level, and the effort levels of its neighbors. Mathematically, the utility function is given by

$$U_i = U_i(W_i, e_i, \vec{e}_i),$$

where $e_i \in [0,1]$ is the self-security effort of agent i, $\vec{e}_i \in [0,1]^{d_i}$ is the vector of effort levels of agent i's one-hop neighbors, and W_i is the wealth of agent i. Security effort generates a positive externality: When the neighbors of agent i invest in security and improve their own protection levels, the utility of agent i also increases. This effect can be expressed mathematically as follows: For any $\vec{e}_i \geq \vec{e'}_i$*.

$$U_i(W_i, e_i, \vec{e}_i) \geq U_i(W_i, e_i, \vec{e'}_i).$$

The positive externality of neighbors' security effort also implies a substitution effect. In particular, a higher level of neighbors' security effort reduces the marginal benefit of the agent's own security effort. This can be expressed mathematically as follows: For any $\vec{e}_i \geq \vec{e'}_i$,

$$U_i(W_i, e_i, \vec{e'}_i) - U_i(W_i, e_i', \vec{e'}_i) \geq U_i(W_i, e_i, \vec{e}_i) - U_i(W_i, e_i', \vec{e}_i).$$

This condition reflects that neighbors' effort creates a positive externality, thereby weakening agent i's incentive to invest in self-protection.

2.3. *Information structure*

We consider three information scenarios: (i) Neither the insurer nor the policyholder knows the policyholder's risk type throughout the contract horizon. (ii) The insurer still cannot observe the policyholder's risk type, whereas the policyholder learns its type only after signing the contract but before choosing the self-protection effort level. (iii) The insurer cannot observe the policyholder's risk type, whereas the policyholder learns its own type before signing the contract.

In all three scenarios, we assume that agents can be classified into two risk types: high-risk (H) and low-risk (L). Depending on the information scenario, an agent's risk type may be unknown or may become known to the agent at different stages of the contracting process, whereas the insurer cannot directly observe this information. When the policyholder learns its risk type before contracting, but the insurer does not, adverse selection arises. After entering the insurance contract, agent i chooses a self-protection effort level e_i. Since the insurer cannot observe the agent's actual effort choice, moral hazard may arise. We assume that the insured's network structure is publicly known, whereas agents' types and effort choices are unobservable to the insurer.

Let $\mathbf{e} = (e_1, e_2, \cdots, e_N)$ denote the effort profile of all agents, where each agent chooses its effort individually and incurs a cost $C(e_i)$. The cost function $C(\cdot)$ is twice continuously differentiable, strictly increasing, and convex, that is, $C'(e) > 0$ and $C''(e) \geqslant 0$. For each agent i, define the effective protection level by

$$s_i := e_i + \sum_{j=1}^{N} a_{ij} x_{ij} e_j,$$

where $A = (a_{ij})$ is the adjacency matrix of the network, x_{ij}† is the impact factor from agent j to agent i, and e_j is the effort level of agent j. Thus, the protection level of agent i depends not only on its own effort, but also on the efforts transmitted from its neighboring agents.

*$\vec{e}_i \geq \vec{e'}_i$ means that the sum of the components of $\vec{e}_i$ is greater than or equal to that of $\vec{e'}_i$.

†$x_{ij} \in [0,1]$ measures the strength of the security spillover transmitted from agent j to agent i. It captures the extent to which agent j's security effort contributes to the effective protection of agent i, conditional on their network connection. This coefficient may reflect the intensity of their cyber dependence, connection strength, technological compatibility, or other pair-specific characteristics.

For an agent with risk type $\theta_i \in \{H, L\}$, we assume that the cyber loss L_i is conditionally lognormally distributed. This specification is appropriate for cyber losses because such losses are non-negative, right-skewed, and may occasionally exhibit extreme realizations. Moreover, log-normal distributions have been commonly used in cyber risk modeling. For example, Awiszus et al. [3] reviewed their application in cyber insurance modeling, and Chong et al. [9] compared several candidate severity distributions for cyber incidents, including log-normal, exponential, gamma, and Weibull distributions, and show that the log-normal distribution provides a good fit for conditional cyber loss severity. Precisely,

$$\ln L_i \,\Big|\, \{\theta_i = k\} \sim \mathcal{N}(\mu_k(s_i), \lambda_k(s_i)), \qquad k \in \{H, L\}, \tag{2.1}$$

where $\mu_k(s_i)$ and $\lambda_k(s_i)$ are the conditional mean and variance parameters of $\ln L_i$, respectively.

Assumption 2.1. *We impose the following assumptions:*

- $\mu_L(s_i) < \mu_H(s_i)$ *for all* $s_i \geq 0$*, that is, at the same security level, high-risk agents have a larger mean log-loss than low-risk agents.*
- *For each* $k \in \{H, L\}$*,* $\mu_k(\cdot)$ *is twice continuously differentiable, strictly decreasing, and strictly convex. Moreover,* $\mu'_H(s_i) < \mu'_L(s_i) < 0$*,* $\mu''_k(s_i) > 0$*. Thus, increasing security effort is more effective for high-risk agents, while the marginal reduction effect diminishes as* s_i *increases.*
- *For each* $k \in \{H, L\}$*,* $\lambda_k(\cdot)$ *is twice continuously differentiable, strictly decreasing, and convex, namely,* $\lambda'_k(s_i) < 0$*,* $\lambda''_k(s_i) \geq 0$*.*

Remark 2.2. *Assumption 2.1 describes the nature of heterogeneity risks and effective protection level. The high-risk type is associated with a larger expected loss exposure, and therefore imposes a higher expected claim on the insurer. In addition, the protection level decreases both the conditional mean and variance parameters of log-loss, indicating that cybersecurity investment can mitigate the expected severity and uncertainty of cyber losses. The convexity assumptions capture the diminishing marginal effectiveness of security effort. Economically, this means that when the protection level is low, additional security investment can substantially reduce exposed vulnerabilities and improve the agent's risk profile. However, as the protection level increases, the remaining risks become more difficult to eliminate, because they may arise from more sophisticated attacks or residual system vulnerabilities. Thus, security investment continues to enhance protection, but the improvement gradually weakens.*

We assume that the insurer offers a cyber insurance contract with base premium P. Before the contract is signed, the insurer observes a set of verifiable underwriting characteristics of agent i, including an observable financial capacity indicator W_i and other verifiable underwriting information H_i. The latter may include externally verifiable indicators such as past claims records, incident reports, or audit-based assessments available at the underwriting stage. Based on these observable characteristics, we define the underwriting score as $S_i = W_i + H_i$. The insurer then determines a premium discount factor $\alpha_i \in [0, 1]$ and a coverage rate $\beta_i \in [0, 1]$. Accordingly, the premium paid by agent i is $P - \alpha_i S_i$, and the insurer provides coverage equal to $\beta_i L_i$. Importantly, S_i is constructed from observable and verifiable pre-contract information and does not reveal the agent's current hidden security effort e_i. Since both the agents' expected utilities and the insurer's expected profit depend on the moments of L_i implied by the log-normal distribution in (2.1), we first state the following lemma.

Lemma 2.3 (Log-normal moments)**.** *Under* (2.1)*, for any* $r > 0$*,*

$$\mathbb{E}[L_i^r \mid \theta_i = k] = \exp\left\{r\,\mu_k(s_i) + \frac{1}{2}r^2\,\lambda_k(s_i)\right\}. \tag{2.2}$$

In particular, we obtain $\mathbb{E}[L_i \mid \theta_i = k] = \exp\left\{\mu_k(s_i) + \frac{1}{2}\lambda_k(s_i)\right\}$ *when* $r = 1$.

Proof. Let $Y_i := \ln L_i$. Then, (2.1) can be rewritten as

$$Y_i \mid \{\theta_i = k\} \sim \mathcal{N}(\mu_k(s_i), \lambda_k(s_i)).$$

Since $L_i^r = e^{rY_i}$, it follows that

$$\mathbb{E}[L_i^r \mid \theta_i = k] = \mathbb{E}[e^{rY_i} \mid \theta_i = k] = \exp\left\{r\mu_k(s_i) + \frac{1}{2}r^2\lambda_k(s_i)\right\},$$

which is the moment generating formula of a normal random variable. □

Corollary 2.4. *The conditional expected loss* (2.2) *is convex in* s_i*.*

Proof. Since $\mu_k(\cdot)$ is strictly convex and $\lambda_k(\cdot)$ is convex by Assumption 2.1, it follows that $\mu_k(s_i)+\frac{1}{2}\lambda_k(s_i)$ is convex in s_i. Therefore, $\mathbb{E}[L_i \mid \theta_i = k]$ is convex in s_i. □

2.3.1. Insurer

Under the above assumptions and by Lemma 2.3, if agent i purchases an insurance contract with premium $P - \alpha_i S_i$ and coverage rate β_i, then the insurer's expected payoff conditional on $\theta_i = k$ is

$$\begin{aligned} U_1(\alpha_i, \beta_i, \mathbf{e} \mid \theta_i = k) &= P - \alpha_i S_i - \beta_i \mathbb{E}(L_i \mid \theta_i = k) \\ &= P - \alpha_i S_i - \beta_i \exp\left\{\mu_k\left(e_i + \sum_{j=1}^{N} a_{ij}x_{ij}e_j\right) + \frac{1}{2}\lambda_k\left(e_i + \sum_{j=1}^{N} a_{ij}x_{ij}e_j\right)\right\}. \end{aligned} \tag{2.3}$$

2.3.2. Risk-neutral insured

We distinguish between two cases for agent i: The agent does not purchase insurance, and the agent purchases insurance. First, let e_i^0 denote agent i's effort level in the absence of insurance, and define

$$s_i^0 := e_i^0 + \sum_{j=1}^{N} a_{ij}x_{ij}e_j.$$

Then, conditional on $\theta_i = k$, the expected utility of agent i without insurance is

$$U_{2i}^0(e_i^0, \vec{e}_i \mid \theta_i = k) = \mathbb{E}(-L_i - C(e_i^0) \mid \theta_i = k) = -\exp\left\{\mu_k(s_i^0) + \frac{1}{2}\lambda_k(s_i^0)\right\} - C(e_i^0). \tag{2.4}$$

Next, suppose that agent i purchases an insurance contract characterized by the premium $P - \alpha_i S_i$ and coverage rate β_i, and define

$$s_i^1 := e_i^1 + \sum_{j=1}^{N} a_{ij}x_{ij}e_j,$$

where e_i^1 denotes the effort chosen by agent i after purchasing insurance. Then, the terminal wealth of agent i is $-P + \alpha_i S_i - L_i + \beta_i L_i - C(e_i^1)$. Hence, conditional on $\theta_i = k$, the expected utility is

$$\begin{aligned} U_{2i}(\alpha_i, \beta_i, e_i^1, \vec{e}_i \mid \theta_i = k) &= \mathbb{E}(-P + \alpha_i S_i - L_i + \beta_i L_i - C(e_i^1) \mid \theta_i = k) \\ &= -P + \alpha_i S_i + (\beta_i - 1) \exp\left\{\mu_k(s_i^1) + \frac{1}{2}\lambda_k(s_i^1)\right\} - C(e_i^1). \end{aligned} \tag{2.5}$$

Proposition 2.5. *Let $\hat{e}_i^1 = \hat{e}_i^1(\alpha_i, \beta_i, \vec{e}_i \mid \theta_i = k)$ denote the optimal effort under insurance. Then, $\hat{e}_i^1$ is decreasing in the coverage rate β_i, that is, $\frac{\partial \hat{e}_i^1}{\partial \beta_i} \leq 0$.*

Proof. For a risk-neutral agent, the expected utility under insurance is given by (2.5). By Corollary 2.4 and the strict convexity of $C(\cdot)$, we have that $U_{2i}(\cdot)$ is strictly concave in e_i^1. Since $e_i^1 \in [0, 1]$ and $U_{2i}(\cdot)$ is continuous, the optimal effort $\hat{e}_i^1$ exists, and strict concavity implies its uniqueness.

Then, the first-order condition

$$\begin{aligned} F(e_i^1; \beta_i) &:= \frac{\partial U_{2i}(\alpha_i, \beta_i, e_i^1, \vec{e}_i \mid \theta_i = k)}{\partial e_i^1} \\ &= (\beta_i - 1) \exp\left\{\mu_k(s_i^1) + \frac{1}{2}\lambda_k(s_i^1)\right\}\left(\mu_k'(s_i^1) + \frac{1}{2}\lambda_k'(s_i^1)\right) - C'(e_i^1), \end{aligned} \tag{2.6}$$

and the second-order condition can be expressed as

$$F_e(\hat{e}_i^1; \beta_i) = \frac{\partial^2 U_{2i}(\alpha_i, \beta_i, e_i^1, \vec{e}_i \mid \theta_i = k)}{\partial (e_i^1)^2}\Big|_{e_i^1 = \hat{e}_i^1} < 0. \tag{2.7}$$

Therefore, the implicit function theorem applies to $F(\hat{e}_i^1(\beta_i); \beta_i) = 0$, and $\hat{e}_i^1$ is locally differentiable with respect to β_i. Differentiating the above identity with respect to β_i, we obtain $F_e \frac{\partial \hat{e}_i^1}{\partial \beta_i} + F_\beta = 0$. Then,

$$\frac{\partial \hat{e}_i^1}{\partial \beta_i} = -\frac{F_\beta}{F_e},$$

where $F_\beta = \exp\left\{\mu_k(s_i^1) + \frac{1}{2}\lambda_k(s_i^1)\right\}\left(\mu_k'(s_i^1) + \frac{1}{2}\lambda_k'(s_i^1)\right) < 0$ through Assumption(2.1). Hence, $\frac{\partial \hat{e}_i^1}{\partial \beta_i} \leq 0$. □

Remark 2.6. *Proposition 2.5 considers the agent's effort response under a given insurance contract. It shows that a higher coverage rate β_i reduces the agent's uncovered loss, $(1 - \beta_i)L_i$, thereby weakening the incentive to exert effort.*

Cyber risk is inherently interdependent, and neighbors' security efforts generate positive externalities through the network. As the external protection level $m_i := \sum_{j=1}^N a_{ij} x_{ij} e_j$ increases, the agent's own optimal effort under insurance decreases, which reflects a substitution effect and gives rise to a free-riding incentive. This is formalized in the following proposition.

Proposition 2.7. *The local optimal effort under insurance $\hat{e}_i^1$ satisfies $\frac{\partial \hat{e}_i^1}{\partial m_i} \leq 0$.*

Proof. According to (2.5) and $s_i^1 := e_i^1 + m_i$, the expected utility can be written as

$$U_{2i}(\alpha_i, \beta_i, e_i^1, m_i \mid \theta_i = k) = -P + \alpha_i S_i + (\beta_i - 1)\exp\left\{\mu_k(e_i^1 + m_i) + \frac{1}{2}\lambda_k(e_i^1 + m_i)\right\} - C(e_i^1).$$

Hence, for fixed m_i, the first-order condition for a local optimum with respect to e_i^1 is

$$\begin{aligned} G(e_i^1; m_i) &:= \frac{\partial U_{2i}(\alpha_i, \beta_i, e_i^1, m_i \mid \theta_i = k)}{\partial e_i^1} \\ &= (\beta_i - 1)\exp\left\{\mu_k(e_i^1 + m_i) + \frac{1}{2}\lambda_k(e_i^1 + m_i)\right\}\left(\mu_k'(e_i^1 + m_i) + \frac{1}{2}\lambda_k'(e_i^1 + m_i)\right) - C'(e_i^1). \end{aligned} \tag{2.8}$$

Let $\hat{e}_i^1$ be a local optimal effort corresponding to the parameter value m_i. Then, $\hat{e}_i^1$ satisfies the first-order condition $G(\hat{e}_i^1; m_i) = 0$. Moreover, by (2.7),

$$G_e(\hat{e}_i^1; m_i) = \frac{\partial^2 U_{2i}(\alpha_i, \beta_i, e_i^1, m_i \mid \theta_i = k)}{\partial (e_i^1)^2}\Big|_{e_i^1 = \hat{e}_i^1} < 0. \tag{2.9}$$

Differentiating the first-order condition with respect to m_i, the chain rule gives

$$G_e(\hat{e}_i^1(m_i); m_i)\frac{\partial \hat{e}_i^1}{\partial m_i} + G_m(\hat{e}_i^1(m_i); m_i) = 0,$$

and hence

$$\frac{\partial \hat{e}_i^1}{\partial m_i} = -\frac{G_m(\hat{e}_i^1(m_i); m_i)}{G_e(\hat{e}_i^1(m_i); m_i)}.$$

Next, since m_i enters the utility only through $s_i^1 = e_i^1 + m_i$, and (2.8) can be rewritten as

$$G(e_i^1; m_i) = (\beta_i - 1)\frac{\mathrm{d}}{\mathrm{d}s_i^1}\mathbb{E}[L_i \mid \theta_i = k] - C'(e_i^1),$$

then,

$$G_m(\hat{e}_i^1; m_i) = (\beta_i - 1)\frac{\mathrm{d}^2}{\mathrm{d}(s_i^1)^2}\mathbb{E}[L_i \mid \theta_i = k].$$

Because $\beta_i \in [0, 1]$, we have $\beta_i - 1 \le 0$. On the other hand, by Corollary 2.4, $\mathbb{E}[L_i \mid \theta_i = k]$ is convex in s_i^1, thus $\frac{\mathrm{d}^2}{\mathrm{d}(s_i^1)^2}\mathbb{E}[L_i \mid \theta_i = k] \ge 0$. Therefore, $G_m(\hat{e}_i^1; m_i) \le 0$. Combining this with (2.9), $G_e(\hat{e}_i^1; m_i) < 0$, we conclude that $\frac{\partial \hat{e}_i^1}{\partial m_i} = -\frac{G_m}{G_e} \le 0$. □

2.3.3. Risk-averse agent

For analytical tractability, we adopt the quadratic utility function $U(W) = W - \frac{1}{2}aW^2$[‡] to model risk-averse agents. Similar to a risk-neutral agent, the expected utility function of a risk-averse agent

[‡]The parameter $a > 0$ measures the curvature of the utility function and reflects the degree of risk aversion. Since $U'(W) = 1 - aW$ and $U''(W) = -a < 0$, a larger value of a implies stronger concavity and hence stronger risk aversion within the economically relevant range $W < 1/a$. In this range, the utility function is increasing and concave, so it can capture risk-averse preferences. However, when $W \ge 1/a$, the marginal utility $U'(W)$ becomes nonpositive, which is economically unreasonable for a global utility function. Therefore, the quadratic utility should be interpreted as a tractable local approximation to risk-averse preferences. Our analysis focuses on the economically relevant range where $U'(W) = 1 - aW > 0$.

without insurance is given by:

$$
\begin{aligned}
U_{3i}^{0}(e_i^0, \vec{e}_i \mid \theta_i = k) &= \mathbb{E}\left[(-L_i - C(e_i^0)) - \frac{1}{2}a(-L_i - C(e_i^0))^2 \middle| \theta_i = k\right] \\
&= -\exp\left\{\mu_k(s_i^0) + \frac{1}{2}\lambda_k(s_i^0)\right\} - C(e_i^0) \\
&\quad - \frac{1}{2}a\Big\{\exp\left(2\mu_k(s_i^0) + 2\lambda_k(s_i^0)\right) \\
&\quad\quad + 2C(e_i^0)\exp\left(\mu_k(s_i^0) + \frac{1}{2}\lambda_k(s_i^0)\right) + C^2(e_i^0)\Big\}.
\end{aligned} \tag{2.10}
$$

where a is the degree of risk aversion, and higher a implies greater risk aversion.

Using a similar argument to the risk-neutral case, we characterize the optimal effort choice of a risk-averse agent under insurance. If agent i accepts the contract, then the terminal wealth is $-P + \alpha_i S_i - L_i + \beta_i L_i - C(e_i^1)$. Define

$$
B_i(\alpha_i, \beta_i, e_i^1) := -P + \alpha_i S_i - C(e_i^1) + (\beta_i - 1)\exp\left\{\mu_k(s_i^1) + \frac{1}{2}\lambda_k(s_i^1)\right\}.
$$

Then, conditional on $\theta_i = k$, the expected utility of agent i under insurance $U_{3i}(\alpha_i, \beta_i, e_i^1, \vec{e}_i \mid \theta_i = k) := U_{3i}$ is

$$
\begin{aligned}
U_{3i} &= \mathbb{E}\left[\Big(-P + \alpha_i S_i - C(e_i^1) + (\beta_i - 1)L_i\Big) - \frac{1}{2}a\Big(-P + \alpha_i S_i - C(e_i^1) + (\beta_i - 1)L_i\Big)^2 \;\Big|\; \theta_i = k\right] \\
&= B_i(\alpha_i, \beta_i, e_i^1) - \frac{1}{2}a\Big\{B_i^2(\alpha_i, \beta_i, e_i^1) + (\beta_i - 1)^2\Big[\exp\left\{2\mu_k(s_i^1) + 2\lambda_k(s_i^1)\right\} \\
&\quad - \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\Big]\Big\}.
\end{aligned} \tag{2.11}
$$

Proposition 2.8. *Assume that*

$$
\frac{\partial^2}{\partial (e_i^1)^2}\left[\exp\left\{2\mu_k(s_i^1) + 2\lambda_k(s_i^1)\right\} - \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\right] \geq 0, \tag{2.12}
$$

where $s_i^1 := e_i^1 + \sum_{j=1}^{N} a_{ij} x_{ij} e_j$, *and*

$$
1 - aB_i(\alpha_i, \beta_i, \hat{e}_i^1) > 0. \tag{2.13}
$$

Then, the optimal effort $\hat{e}_i^1$ *of the risk-averse agent satisfies*

$$
\frac{\partial \hat{e}_i^1}{\partial \alpha_i} > 0. \tag{2.14}
$$

Proof. Using (2.11), then

$$
M(e_i^1; \alpha_i, \beta_i) := \frac{\partial U_{3i}(\alpha_i, \beta_i, e_i^1, \vec{e}_i \mid \theta_i = k)}{\partial e_i^1}
$$

$$
\begin{aligned}
&= (1 - aB_i(\alpha_i,\beta_i, e_i^1))\frac{\partial B_i(\alpha_i,\beta_i, e_i^1)}{\partial e_i^1} \\
&\quad - \frac{1}{2}a(\beta_i - 1)^2\frac{\partial}{\partial e_i^1}\Big[\exp\Big\{2\mu_k(s_i^1) + 2\lambda_k(s_i^1)\Big\} - \exp\Big\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\Big\}\Big].
\end{aligned}
$$

Since $\hat{e}_i^1$ is an interior local optimum, it satisfies $M(\hat{e}_i^1;\alpha_i,\beta_i) = 0$. Moreover, by (2.12) and (2.13), the second-order satisfies

$$
M_e(\hat{e}_i^1;\alpha_i,\beta_i) = \frac{\partial^2 U_{3i}(\alpha_i,\beta_i, e_i^1,\vec{e}_i \mid \theta_i = k)}{\partial (e_i^1)^2}\Big|_{e_i^1=\hat{e}_i^1} < 0. \tag{2.15}
$$

Hence, the implicit function theorem applies to the identity $M(\hat{e}_i^1(\alpha_i);\alpha_i,\beta_i) = 0$. Differentiating the identity with respect to α_i, we obtain $M_e\frac{\partial \hat{e}_i^1}{\partial \alpha_i} + M_\alpha = 0$. Then,

$$
\frac{\partial \hat{e}_i^1}{\partial \alpha_i} = -\frac{M_\alpha}{M_e}. \tag{2.16}
$$

Next, since $\frac{\partial B_i(\alpha_i,\beta_i,e_i^1)}{\partial \alpha_i} = S_i$, $\frac{\partial^2 B_i(\alpha_i,\beta_i,e_i^1)}{\partial \alpha_i\, \partial e_i^1} = 0$, we have

$$
\begin{aligned}
M_\alpha(\hat{e}_i^1;\alpha_i,\beta_i) &= -a\frac{\partial B_i(\alpha_i,\beta_i,\hat{e}_i^1)}{\partial \alpha_i}\frac{\partial B_i(\alpha_i,\beta_i,\hat{e}_i^1)}{\partial e_i^1} + (1 - aB_i(\alpha_i,\beta_i,\hat{e}_i^1))\frac{\partial^2 B_i(\alpha_i,\beta_i, e_i^{1,*})}{\partial e_i^1 \partial \alpha_i} \\
&= -aS_i\frac{\partial B_i(\alpha_i,\beta_i,\hat{e}_i^1)}{\partial e_i^1}.
\end{aligned}
$$

On the other hand, since $M(\hat{e}_i^1;\alpha_i,\beta_i) = 0$, it follows that

$$
\begin{aligned}
&(1 - aB_i(\alpha_i,\beta_i,\hat{e}_i^1))\frac{\partial B_i(\alpha_i,\beta_i,\hat{e}_i^1)}{\partial e_i^1} \\
&\quad = \frac{1}{2}a(\beta_i - 1)^2\frac{\partial}{\partial e_i^1}\left[\exp\left\{2\mu_k(s_i^1) + 2\lambda_k(s_i^1)\right\} - \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\right].
\end{aligned}
$$

Moreover, by Assumption 2.1, we have $\mu_k'(s_i^1) < 0$, $\lambda_k'(s_i^1) < 0$, $\lambda_k(s_i^1) > 0$. Then,

$$
\begin{aligned}
&\frac{\partial}{\partial e_i^1}\left[\exp\left\{2\mu_k(s_i^1) + 2\lambda_k(s_i^1)\right\} - \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\right] \\
&\quad = \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\left[2\mu_k'(s_i^1)(e^{\lambda_k(s_i^1)} - 1) + \lambda_k'(s_i^1)(2e^{\lambda_k(s_i^1)} - 1)\right] < 0.
\end{aligned}
$$

By (2.13), we have $\frac{\partial B_i(\alpha_i,\beta_i,\hat{e}_i^1)}{\partial e_i^1} < 0$. Hence, for $S_i > 0$,

$$
M_\alpha(\hat{e}_i^1;\alpha_i,\beta_i) = -aS_i\frac{\partial B_i(\alpha_i,\beta_i,\hat{e}_i^1)}{\partial e_i^1} > 0.
$$

Combining this with (2.15) and (2.16), we conclude that (2.14). □

Proposition 2.9. *Assume that* (2.12)*,* (2.13)*, and*

$$a(1-\beta_i)\exp\left\{\mu_k(s_i^1)+\frac{1}{2}\lambda_k(s_i^1)\right\}\le 2\Big(1-aB_i(\alpha_i,\beta_i,\hat{e}_i^1)\Big), \tag{2.17}$$

where $s_i^1 := e_i^1 + \sum_{j=1}^N a_{ij}x_{ij}e_j$*. Then, the optimal effort* $\hat{e}_i^1$ *satisfies*

$$\frac{\partial \hat{e}_i^1}{\partial \beta_i} < 0. \tag{2.18}$$

Proof. The derivation with respect to β_i follows the same implicit function argument as in Proposition 2.8. Specifically, differentiating the identity

$$N(\hat{e}_i^1(\beta_i);\alpha_i,\beta_i)=0$$

with respect to β_i, we obtain

$$N_e\frac{\partial \hat{e}_i^1}{\partial \beta_i}+N_\beta=0,$$

hence

$$\frac{\partial \hat{e}_i^1}{\partial \beta_i}=-\frac{N_\beta}{N_e}.$$

Differentiating $N(e_i^1;\alpha_i,\beta_i)$ with respect to β_i, we obtain

$$\begin{aligned}N_\beta=&-a\frac{\partial B_i(\alpha_i,\beta_i,e_i^1)}{\partial \beta_i}\frac{\partial B_i(\alpha_i,\beta_i,e_i^1)}{\partial e_i^1}+(1-aB_i(\alpha_i,\beta_i,e_i^1))\frac{\partial^2 B_i(\alpha_i,\beta_i,e_i^1)}{\partial e_i^1\partial\beta_i}\\&-a(\beta_i-1)\frac{\partial}{\partial e_i^1}\Big[\exp\Big\{2\mu_k(s_i^1)+2\lambda_k(s_i^1)\Big\}-\exp\Big\{2\mu_k(s_i^1)+\lambda_k(s_i^1)\Big\}\Big].\end{aligned}$$

Since

$$\frac{\partial B_i(\alpha_i,\beta_i,e_i^1)}{\partial \beta_i}=\exp\left\{\mu_k(s_i^1)+\frac{1}{2}\lambda_k(s_i^1)\right\},$$

and

$$\frac{\partial^2 B_i(\alpha_i,\beta_i,e_i^1)}{\partial e_i^1\partial\beta_i}=\exp\left\{\mu_k(s_i^1)+\frac{1}{2}\lambda_k(s_i^1)\right\}\left(\mu_k'(s_i^1)+\frac{1}{2}\lambda_k'(s_i^1)\right)<0,$$

we further have

$$\begin{aligned}N_\beta=&(1-aB_i(\alpha_i,\beta_i,e_i^1))\exp\left\{\mu_k(s_i^1)+\frac{1}{2}\lambda_k(s_i^1)\right\}\left(\mu_k'(s_i^1)+\frac{1}{2}\lambda_k'(s_i^1)\right)\\&-a(\beta_i-1)\frac{\partial}{\partial e_i^1}\Big[\exp\Big\{2\mu_k(s_i^1)+2\lambda_k(s_i^1)\Big\}-\exp\Big\{2\mu_k(s_i^1)+\lambda_k(s_i^1)\Big\}\Big]\\&-a\exp\left\{\mu_k(s_i^1)+\frac{1}{2}\lambda_k(s_i^1)\right\}\frac{\partial B_i(\alpha_i,\beta_i,e_i^1)}{\partial e_i^1}.\end{aligned}$$

By the first-order condition $N(e_i^{1,*};\alpha_i,\beta_i)=0$, we have

$$\frac{\partial B_i(\alpha_i,\beta_i,e_i^1)}{\partial e_i^1}=\frac{a(\beta_i-1)^2}{2(1-aB_i(\alpha_i,\beta_i,e_i^1))}\frac{\partial}{\partial e_i^1}\Big[\exp\Big\{2\mu_k(s_i^1)+2\lambda_k(s_i^1)\Big\}-\exp\Big\{2\mu_k(s_i^1)+\lambda_k(s_i^1)\Big\}\Big].$$

Substituting this into the above expression yields

$$
\begin{aligned}
N_\beta = {} & (1 - aB_i(\alpha_i, \beta_i, e_i^1)) \exp\left\{\mu_k(s_i^1) + \frac{1}{2}\lambda_k(s_i^1)\right\}\left(\mu_k'(s_i^1) + \frac{1}{2}\lambda_k'(s_i^1)\right) \\
& + a(1-\beta_i)\frac{\partial}{\partial e_i^1}\Big[\exp\left\{2\mu_k(s_i^1) + 2\lambda_k(s_i^1)\right\} - \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\Big] \\
& \times\left[1 - \frac{a(1-\beta_i)\exp\left\{\mu_k(s_i^1) + \frac{1}{2}\lambda_k(s_i^1)\right\}}{2(1 - aB_i(\alpha_i, \beta_i, e_i^1))}\right].
\end{aligned}
$$

Moreover,

$$
\begin{aligned}
& \frac{\partial}{\partial e_i^1}\Big[\exp\left\{2\mu_k(s_i^1) + 2\lambda_k(s_i^1)\right\} - \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\Big] \\
& \quad = \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\Big[2\mu_k'(s_i^1)(e^{\lambda_k(s_i^1)} - 1) + \lambda_k'(s_i^1)(2e^{\lambda_k(s_i^1)} - 1)\Big] < 0.
\end{aligned}
$$

Since (2.13) and (2.17), combining with

$$
\frac{\partial}{\partial e_i^1}\Big[\exp\left\{2\mu_k(s_i^1) + 2\lambda_k(s_i^1)\right\} - \exp\left\{2\mu_k(s_i^1) + \lambda_k(s_i^1)\right\}\Big] < 0,
$$

we conclude $N_\beta < 0$. Since $N_e < 0$, it follows that (2.18). □

Remark 2.10. *For a given insurance contract, these comparative statics describe the agent's effort response to the contract terms. Unlike the risk-neutral case, a risk-averse agent cares not only about the expected level of terminal wealth but also about its volatility. Under suitable conditions, a larger premium discount factor α_i improves the insured's payoff and strengthens the incentive to exert self-protection effort. By contrast, a higher coverage rate β_i reduces the agent's uninsured loss exposure and shifts more risk to the insurer, thereby weakening the incentive to invest in self-protection.*

3. Mechanisms for alleviating information asymmetry

Premiums and coverage rates chosen by the insurer affect the insured's incentive to invest in self-protection. Conversely, the insured's effort affects the distribution of cyber losses, which in turn influences the insurer's expected payoff and optimal contract design. Therefore, the insurer must anticipate the insured's effort response when setting premiums and coverage rates. Such strategic interaction naturally leads to an insurance game with information asymmetry. In this section, we consider three information structures and investigate how discriminatory premium design can alleviate the distortions generated by asymmetric information.

3.1. Neither the insurer nor the insured knows the risk type

In this case, neither the insurer nor the policyholder can observe whether agent i is low-risk (L) or high-risk (H). Since the agent does not know thier own type either, adverse selection does not arise at the contracting stage. The main informational friction is moral hazard, because the insurer cannot observe or verify the realized effort after the contract is signed. We assume that both parties share the same prior belief about the agent's type.

Let $\eta_1 \in [0, 1]$ denote the prior probability that agent i is of type L. Define $\phi_k(s) := \mu_k(s) + \frac{1}{2}\lambda_k(s)$, $k \in \{L, H\}$. Then, the weighted expected loss is

$$L_i^Y(s_i) := \eta_1 \exp\{\phi_L(s_i)\} + (1 - \eta_1) \exp\{\phi_H(s_i)\},$$

where the superscript Y denotes the present situation with no information. We study the problem from the insurer's perspective. The insurer chooses the contract terms (α_i^Y, β_i^Y) to maximize expected profit (2.3). After reviewing the contract, the agent decides whether to purchase insurance and selects a level of self-protection effort. Because the insurer cannot observe the actual effort exerted, the contract must be designed by anticipating the agent's optimal response effort. This leads to the following constrained optimization problem:

$$\max_{0 \le \alpha_i^Y \le 1,\, 0 \le \beta_i^Y \le 1} \qquad P - \alpha_i^Y S_i^Y - \beta_i^Y L_i^Y(s_i^Y),$$

where $s_i^Y := e_i^Y + \sum_{j=1}^N a_{ij} x_{ij} e_j^Y$. The problem is subject to the participation constraint

$$U_{2i}^Y(\alpha_i^Y, \beta_i^Y, \hat{\mathbf{e}}^Y) \ge U_{2i}^{Y0}(\hat{\mathbf{e}}^{Y0}), \tag{3.1}$$

and the best-response conditions

$$\frac{\partial U_{2i}^Y(\alpha_i^Y, \beta_i^Y, \mathbf{e}^Y)}{\partial e_i^Y}\Big|_{\mathbf{e}^Y = \hat{\mathbf{e}}^Y} = 0, \qquad i = 1, \ldots, N, \tag{3.2}$$

$$\frac{\partial U_{2i}^{Y0}(\mathbf{e}^{Y0})}{\partial e_i^{Y0}}\Big|_{\mathbf{e}^{Y0} = \hat{\mathbf{e}}^{Y0}} = 0, \qquad i = 1, \ldots, N. \tag{3.3}$$

Here, α_i^Y and β_i^Y denote the premium discount factor and the coverage rate under the no-information case Y, $\hat{\mathbf{e}}^Y = (\hat{e}_1^Y, \hat{e}_2^Y, \ldots, \hat{e}_N^Y)$ denotes the equilibrium effort profile when insurance is purchased, and $\hat{\mathbf{e}}^{Y0} = (\hat{e}_1^{Y0}, \hat{e}_2^{Y0}, \ldots, \hat{e}_N^{Y0})$ denotes the equilibrium effort profile.

Constraint (3.1) is the participation constraint. It requires that agent i obtain at least as much expected utility from purchasing insurance as from remaining uninsured; otherwise, the agent will not purchase insurance. Constraints (3.2) and (3.3) characterize the agent's optimal effort choices under insurance and without insurance, respectively. In particular, (3.2) captures the moral-hazard feature of the model. Constraint (3.3) defines the benchmark equilibrium effort when no insurance is purchased. To solve the insurer's problem, we formulate the associated Lagrangian by introducing multipliers ξ_1, ξ_2, and ξ_3 corresponding to constraints (3.1)–(3.3), respectively.

For risk-averse agents, the insurer faces an analogous contracting problem. The insurer chooses (α_i^Y, β_i^Y) to maximize expected profit while anticipating the agent's effort response. Specifically, the insurer solves

$$\max_{0 \le \alpha_i^Y \le 1,\, 0 \le \beta_i^Y \le 1} \qquad P - \alpha_i^Y S_i^Y - \beta_i^Y L_i^Y(s_i^Y).$$

This problem is subject to

$$U_{3i}^Y(\alpha_i^Y, \beta_i^Y, \hat{\mathbf{e}}^Y) \ge U_{3i}^{Y0}(\hat{\mathbf{e}}^{Y0}), \tag{3.4}$$

$$\frac{\partial U_{3i}^{Y}(\alpha_i^Y,\beta_i^Y,\mathbf{e}^Y)}{\partial e_i^Y}\Big|_{\mathbf{e}^Y=\hat{\mathbf{e}}^Y} = 0, \qquad i = 1,\ldots,N, \tag{3.5}$$

$$\frac{\partial U_{3i}^{Y0}(\mathbf{e}^{Y0})}{\partial e_i^{Y0}}\Big|_{\mathbf{e}^{Y0}=\hat{\mathbf{e}}^{Y0}} = 0, \qquad i = 1,\ldots,N. \tag{3.6}$$

We formulate the corresponding Lagrangian by introducing multipliers ξ_4, ξ_5, and ξ_6 associated with constraints (3.4)–(3.6), respectively. Constraint (3.4) is the participation constraint for a risk-averse agent. Constraints (3.5) and (3.6) characterize the agent's optimal effort choices with and without insurance.

3.2. The insured learns the risk type after signing the contract

We now consider a situation in which the agent does not know their risk type at the contracting stage, but may learn it from a third-party audit after signing the contract and before choosing the security investment. We assume that the insurer cannot observe either the agent's information status or their realized risk type. Hence, although the cyber insurer moves first and offers the contract, it must anticipate that the agent may later acquire information and adjust their effort accordingly. Let the signed contract be denoted by

$$Z_i^d := (P - \alpha_i^d S_i, \beta_i^d),$$

where the premium and coverage terms are fixed once the contract is signed.

First, we investigate the value of information. If the agent does not learn their type, they select effort based on prior beliefs, resulting in an optimal effort profile denoted as $\hat{\mathbf{e}}^Y$ and an expected utility of $U_i^Y(Z_i, \hat{\mathbf{e}}^Y)$. Conversely, if the agent learns their type, they choose effort according to that realized type. We denote the optimal effort profiles for types L and H as $\hat{\mathbf{e}}^L$ and $\hat{\mathbf{e}}^H$, with corresponding expected utilities of $U_i^L(Z_i, \hat{\mathbf{e}}^L)$ and $U_i^H(Z_i, \hat{\mathbf{e}}^H)$, respectively. Assuming that the probability of being type L is η_1 and being type H is $(1-\eta_1)$, we define the value of information for agent i under contract Z_i as follows:

$$VI_i^1 = \eta_1 U_i^L(Z_i, \hat{\mathbf{e}}^L) + (1-\eta_1)U_i^H(Z_i, \hat{\mathbf{e}}^H) - \left[\eta_1 U_i^L(Z_i, \hat{\mathbf{e}}^Y) + (1-\eta_1)U_i^H(Z_i, \hat{\mathbf{e}}^Y)\right]. \tag{3.7}$$

In summary, VI_i represents the difference between expected utility when learning one's type and choosing optimal efforts versus remaining uninformed and selecting a single effort level for both types.

Since the information is acquired only after the contract is signed, the contract terms are fixed, and only the investment decision can be adjusted. It is immediate that if there is only one type of agent, that is, $\theta_1 = 0$ or $\theta_1 = 1$, then $VI_i = 0$. Moreover, under full insurance, the agent has no incentive to acquire type information, and thus the value of information is also zero. In general, under a fixed contract Z_i, one has $VI_i \geq 0$. This is because, after learning the realized type, the agent can always choose the same effort as in the uninformed case, so learning cannot reduce the agent's expected utility. Moreover, $VI_i > 0$ whenever type information induces a strict utility improvement for at least one realized type.

Next, we formulate the insurer's contracting problem under this post-contract information structure. The insurer chooses the contract (α_i^d, β_i^d) at signing, while the agent chooses effort afterward.

In the risk-neutral case, the insurer chooses the contract terms (α_i^d, β_i^d) to maximize expected profit, taking into account the agent's optimal adjustment to effort after the realized type is observed. Then, the insurer's problem is

$$\max_{0\leq\alpha_i^d\leq 1,\ 0\leq\beta_i^d\leq 1} \eta_1\Big(P-\alpha_i^d S_i-\beta_i^d\exp\{\phi_L(s_i^L)\}\Big)+(1-\eta_1)\Big(P-\alpha_i^d S_i-\beta_i^d\exp\{\phi_H(s_i^H)\}\Big), \tag{3.8}$$

where $s_i^k := e_i^k + \sum_{j=1}^N a_{ij}x_{ij}e_j^k$.

The contract must satisfy the participation constraint at the signing stage:

$$\eta_1 U_{2i}^L(\alpha_i^d,\beta_i^d,\hat{\mathbf{e}}^L)+(1-\eta_1)U_{2i}^H(\alpha_i^d,\beta_i^d,\hat{\mathbf{e}}^H)\geq \eta_1 U_{2i}^{L0}(\hat{\mathbf{e}}^{L0})+(1-\eta_1)U_{2i}^{H0}(\hat{\mathbf{e}}^{H0}), \tag{3.9}$$

where $\hat{\mathbf{e}}^{L0}$ and $\hat{\mathbf{e}}^{H0}$ denote the corresponding optimal effort profiles without insurance when the type is L and H, respectively. Moreover, after the contract is signed, the agent optimally chooses effort. Then, the effort profiles $\hat{\mathbf{e}}^k$ satisfy

$$\left.\frac{\partial U_{2i}^k(\alpha_i^d,\beta_i^d,\mathbf{e})}{\partial e_i}\right|_{\mathbf{e}=\hat{\mathbf{e}}^k}=0,\qquad i=1,\dots,N,,\qquad k\in\{L,H\}. \tag{3.10}$$

The benchmark equilibrium effort when no insurance is purchased satisfies

$$\left.\frac{\partial U_{2i}^{k0}(\mathbf{e})}{\partial e_i}\right|_{\mathbf{e}=\hat{\mathbf{e}}^{k0}}=0,\qquad i=1,\dots,N,,\qquad k\in\{L,H\}. \tag{3.11}$$

Constraint (3.9) requires that, before knowing the realized type, the agent is willing to sign the contract; otherwise, the agent will not purchase insurance. Conditions (3.10) and (3.11) ensure that the effort profiles entering (3.8) are the agent's own optimal responses after the contract is signed. To solve the insurer's problem, we formulate the associated Lagrangian by introducing multipliers ξ_7, ξ_8, and ξ_9 corresponding to constraints (3.9)–(3.11), respectively. Solving the resulting first-order conditions yields the optimal contract $Z_i^{d*}=(P-\alpha_i^{d*}S_i,\beta_i^{d*})$.

For a risk-averse agent, the insurer faces an analogous contracting problem. The insurer still chooses (α_i^d,β_i^d) to maximize expected profit, but the agent's effort responses are determined by the risk-averse utility. Accordingly, the insurer solves

$$\max_{0\leq\alpha_i^d\leq 1,\ 0\leq\beta_i^d\leq 1} \eta_1\Big(P-\alpha_i^d S_i-\beta_i^d\exp\{\phi_L(s_i^L)\}\Big)+(1-\eta_1)\Big(P-\alpha_i^d S_i-\beta_i^d\exp\{\phi_H(s_i^H)\}\Big),$$

subject to the participation constraint

$$\eta_1 U_{3i}^L(\alpha_i^d,\beta_i^d,\hat{\mathbf{e}}^L)+(1-\eta_1)U_{3i}^H(\alpha_i^d,\beta_i^d,\hat{\mathbf{e}}^H)\geq \eta_1 U_{3i}^{L0}(\hat{\mathbf{e}}^{L0})+(1-\eta_1)U_{3i}^{H0}(\hat{\mathbf{e}}^{H0}), \tag{3.12}$$

and the optimal effort conditions

$$\left.\frac{\partial U_{3i}^k(\alpha_i^d,\beta_i^d,\mathbf{e})}{\partial e_i}\right|_{\mathbf{e}=\hat{\mathbf{e}}^k}=0,,\qquad i=1,\dots,N,\qquad k\in\{L,H\}, \tag{3.13}$$

together with the no-insurance benchmark conditions

$$\left.\frac{\partial U_{3i}^{k0}(\mathbf{e})}{\partial e_i}\right|_{\mathbf{e}=\hat{\mathbf{e}}^{k0}}=0,,\qquad i=1,\dots,N,\qquad k\in\{L,H\}. \tag{3.14}$$

Similarly, we solve this problem by the Lagrange multiplier method. Let ξ_{10}, ξ_{11}, and ξ_{12} be the multipliers associated with constraints (3.12)–(3.14), respectively. Solving the resulting first-order conditions yields the optimal contract for risk-averse agents $Z_i^{d*}=(P-\alpha_i^{d*}S_i,\beta_i^{d*})$.

3.3. The insured obtains information before signing the contract

In this case, the agent may acquire information about their risk type before signing the contract. To quantify the benefit of such information, we compare the agent's expected utility when they know the realized type before choosing a contract with that when they remain uninformed and chooses a contract according to the prior belief.

Suppose that the insurer offers a menu of contracts $\{Z_i^H, Z_i^L\}$, where $Z_i^k := (P - \alpha_i^k S_i, \beta_i^k)$, $k \in \{H, L\}$. Let $\hat{\mathbf{e}}^{kr}$ denote the equilibrium effort profile when a type-k agent chooses contract Z_i^r, $r \in \{H, L\}$. The menu is required to satisfy the self-selection conditions

$$U_i^H(Z_i^H, \hat{\mathbf{e}}^{HH}) \geq U_i^H(Z_i^L, \hat{\mathbf{e}}^{HL}), \qquad U_i^L(Z_i^L, \hat{\mathbf{e}}^{LL}) \geq U_i^L(Z_i^H, \hat{\mathbf{e}}^{LH}).$$

First, we explore the value of information. If the agent obtains information before signing the contract, then a type-L agent chooses Z_i^L, whereas a type-H agent chooses Z_i^H. If the agent remains uninformed, then they choose one contract Z_i^Y from $\{Z_i^H, Z_i^L\}$ according to the prior belief. Assume that the agent is of type L with probability η_1 and of type H with probability $1 - \eta_1$. Then, the value of information for agent i is defined by

$$VI_i^2 = \eta_1 U_i^L(Z_i^L, \hat{\mathbf{e}}^{LL}) + (1 - \eta_1) U_i^H(Z_i^H, \hat{\mathbf{e}}^{HH}) - \Big[\eta_1 U_i^L(Z_i^Y, \hat{\mathbf{e}}^{LY}) + (1 - \eta) U_i^H(Z_i^Y, \hat{\mathbf{e}}^{HY})\Big].$$

Equivalently,

$$VI_i^2 = \eta_1\Big(U_i^L(Z_i^L, \hat{\mathbf{e}}^{LL}) - U_i^L(Z_i^Y, \hat{\mathbf{e}}^{LY})\Big) + (1 - \eta_1)\Big(U_i^H(Z_i^H, \hat{\mathbf{e}}^{HH}) - U_i^H(Z_i^Y, \hat{\mathbf{e}}^{HY})\Big). \tag{3.15}$$

Obviously, $VI_i \geq 0$. Thus, information is valuable, and it allows the agent to select a more suitable contract and adjust effort according to the true type. In particular, if $\theta_1 = 0$ or $\theta_1 = 1$, then $VI_i = 0$.

Remark 3.1. *We briefly analyze the key factors influencing the value of information and differentiate between VI_i^1 (defined in* (3.7)*) and VI_i^2 (defined in* (3.15)*). Both values represent the expected utility gain from acquiring this type of information. The distinction lies in their computation: VI_i^1 is based on a fixed contract Z_i, meaning that type information only impacts effort choices. In contrast, VI_i^2 allows for type information to be utilized prior to contract determination, enabling agents to choose between type-dependent contracts Z_i^L or Z_i^H, rather than just the benchmark contract Z_i^Y. Consequently, VI_i^2 encompasses both effort adjustment and contract selection benefits.*

Both values are influenced by several common factors. First, they depend on the heterogeneity between low-risk and high-risk agents; greater differences in loss distributions and optimal effort levels increase the value of type information. Second, they rely on the prior probability η_1; if $\eta_1 = 0$ or $\eta_1 = 1$, there is no uncertainty regarding types, rendering the value of information negligible. Third, coverage rate also plays a role: under full insurance, type information has limited impact on effort decisions since agents face minimal residual loss risk. However, with partial insurance, it becomes more valuable as it helps agents adjust security investments according to actual risk types; additionally, for VI_i^2, it facilitates selecting a more appropriate contract.

Next, we formulate the insurer's problem conditional on the case where the agent has obtained type information before signing the contract:

$$\max_{0 \leq \alpha_i^H, \alpha_i^L, \beta_i^H, \beta_i^L \leq 1} \quad \eta_1\Big(P - \alpha_i^L S_i - \beta_i^L \exp\{\phi_L(\hat{s}_i^{LL})\}\Big) + (1 - \eta_1)\Big(P - \alpha_i^H S_i - \beta_i^H \exp\{\phi_H(\hat{s}_i^{HH})\}\Big), \tag{3.16}$$

where $\hat{s}_i^{kr} := \hat{e}_i^{kr} + \sum_{j=1}^N a_{ij}x_{ij}\hat{e}_j^{kr}$. The problem is subject to the participation constraints

$$U_{2i}^L(\alpha_i^L,\beta_i^L,\hat{\mathbf{e}}^{LL}) \geq U_{2i}^{L0}(\hat{\mathbf{e}}^{L0}), \qquad U_{2i}^H(\alpha_i^H,\beta_i^H,\hat{\mathbf{e}}^{HH}) \geq U_{2i}^{H0}(\hat{\mathbf{e}}^{H0}), \tag{3.17}$$

and the incentive constraints

$$U_{2i}^L(\alpha_i^L,\beta_i^L,\hat{\mathbf{e}}^{LL}) \geq U_{2i}^L(\alpha_i^H,\beta_i^H,\hat{\mathbf{e}}^{LH}), \qquad U_{2i}^H(\alpha_i^H,\beta_i^H,\hat{\mathbf{e}}^{HH}) \geq U_{2i}^H(\alpha_i^L,\beta_i^L,\hat{\mathbf{e}}^{HL}). \tag{3.18}$$

The optimal effort profiles are characterized by the first-order conditions

$$\left.\frac{\partial U_{2i}^k(\alpha_i^r,\beta_i^r,\mathbf{e})}{\partial e_i}\right|_{\mathbf{e}=\hat{\mathbf{e}}^{kr}} = 0, \qquad i=1,\ldots,N, \quad k,r\in\{H,L\}, \tag{3.19}$$

and without insurance,

$$\left.\frac{\partial U_{2i}^{k0}(\mathbf{e})}{\partial e_i}\right|_{\mathbf{e}=\hat{\mathbf{e}}^{k0}} = 0, \qquad i=1,\ldots,N, \quad k\in\{H,L\}. \tag{3.20}$$

We solve (3.16)–(3.20) by the Lagrange multiplier method and introduce multipliers for the constraints (3.17), the constraints (3.18), and the effort first-order conditions (3.19)–(3.20). Then, we derive the first-order conditions of the Lagrangian and obtain the optimal menu $\{Z_i^{H*}, Z_i^{L*}\}$.

For risk-averse agents, the insurer's objective keeps the same form as in (3.16). Thus, the insurer solves

$$\max_{0\leq\alpha_i^H,\alpha_i^L,\beta_i^H,\beta_i^L\leq 1} \quad \eta_1\Big(P-\alpha_i^L S_i-\beta_i^L\exp\{\phi_L(\hat{s}_i^{LL})\}\Big)+(1-\eta_1)\Big(P-\alpha_i^H S_i-\beta_i^H\exp\{\phi_H(\hat{s}_i^{HH})\}\Big),$$

subject to the participation constraints

$$U_{3i}^L(\alpha_i^L,\beta_i^L,\hat{\mathbf{e}}^{LL}) \geq U_{3i}^{L0}(\hat{\mathbf{e}}^{L0}), \qquad U_{3i}^H(\alpha_i^H,\beta_i^H,\hat{\mathbf{e}}^{HH}) \geq U_{3i}^{H0}(\hat{\mathbf{e}}^{H0}), \tag{3.21}$$

the incentive compatibility constraints

$$U_{3i}^L(\alpha_i^L,\beta_i^L,\hat{\mathbf{e}}^{LL}) \geq U_{3i}^L(\alpha_i^H,\beta_i^H,\hat{\mathbf{e}}^{LH}), \qquad U_{3i}^H(\alpha_i^H,\beta_i^H,\hat{\mathbf{e}}^{HH}) \geq U_{3i}^H(\alpha_i^L,\beta_i^L,\hat{\mathbf{e}}^{HL}), \tag{3.22}$$

and the effort first-order conditions

$$\left.\frac{\partial U_{3i}^k(\alpha_i^r,\beta_i^r,\mathbf{e})}{\partial e_i}\right|_{\mathbf{e}=\hat{\mathbf{e}}^{kr}} = 0, \qquad i=1,\ldots,N, \quad k,r\in\{H,L\}, \tag{3.23}$$

together with the no-insurance effort conditions

$$\left.\frac{\partial U_{3i}^{k0}(\mathbf{e})}{\partial e_i}\right|_{\mathbf{e}=\hat{\mathbf{e}}^{k0}} = 0, \qquad i=1,\ldots,N, \quad k\in\{H,L\}. \tag{3.24}$$

We again use the Lagrange multiplier method. We add multipliers for (3.21)–(3.24), write the Lagrangian, and solve the corresponding first-order conditions. This gives the optimal menu $\{Z_i^{H*}, Z_i^{L*}\}$ for risk-averse agents.

From an economic perspective, the three cases represent a gradual increase in the degree of information asymmetry. In Case A, the policyholder does not learn the risk type during the contract horizon. Hence, neither party has private information about the realized type, and the insurer designs a contract based on the prior distribution of risk types. The main distortion in this case comes from the unobservable self-protection effort, which corresponds to moral hazard.

In Case B, the policyholder learns the risk type only after signing the contract but before choosing the self-protection effort. Since the risk type remains unknown at the contracting stage, the insurer offers a single contract, as in Case I. However, the insurer must anticipate that the policyholder's subsequent effort decision will depend on the realized type. Therefore, compared with Case I, information asymmetry is stronger because private-type information affects post-contract effort choice.

In Case C, the policyholder knows the risk type before signing the contract, whereas the insurer cannot observe it. This is the strongest form of information asymmetry among the three cases because adverse selection arises at the contract selection stage in addition to moral hazard in the effort decision. Consequently, the insurer can no longer rely on a single pooling contract and instead designs a type-specific contract menu to induce different risk types to choose their intended contracts. This comparison shows that as the policyholder's private information becomes available earlier, the insurer must use more refined contract mechanisms to alleviate the distortions caused by information asymmetry.

4. Numerical results

Section III addresses the contract design problem under three information settings involving moral hazard and adverse selection. It also provides the method for deriving the optimal contract Z_i^{opt} and the optimal security investment level e_i^*. In the numerical analysis, we use the empirical evidence in Chong et al. [9] to distinguish the low-risk and high-risk types. Since data breach (DB) incidents have higher mean and median losses than privacy violation (PV) incidents, we use PV to represent the low-risk type and DB to represent the high-risk type. Based on the relative frequencies of the low-risk and high-risk incidents reported in Table 4, we use the approximate benchmark prior probability $\eta_1 = 0.8$. Following [14], we use the functions

$$\mu_k(s_i) = \frac{\bar{\mu}_k}{1+s_i}, \qquad \lambda_k(s_i) = \frac{\bar{\lambda}_k}{(1+s_i)^2}, \qquad k \in \{H, L\},$$

where $s_i = e_i + \sum_{j=1}^{N} a_{ij}x_{ij}e_j$ is the effective protection level faced by agent i. In the numerical benchmark, we set $x_{ij} = 1$ for all existing links. In addition, based on the empirical log-normal severity calibration in Table 7 of Chong et al. [9], we set $\bar{\mu}_L = -2.5996$, $\bar{\lambda}_L = 10.7571$, $\bar{\mu}_H = -0.7916$, and $\bar{\lambda}_H = 9.6858$. The security investment cost is specified as $C(e_i) = ce_i^2/2$, which is increasing and convex for $e_i \geq 0$.

Next, we calibrate the base premium P. By (2.1), the conditional expected loss of type k is

$$\mathbb{E}[L_i \mid \theta_i = k] = \exp\left\{\mu_k(s_i) + \frac{1}{2}\lambda_k(s_i)\right\}, \qquad k \in \{L, H\}.$$

Using the expected value premium principle, we define the base premium as

$$P = (1+\vartheta)\left[\eta_1 \exp\left\{\mu_L(0) + \frac{1}{2}\lambda_L(0)\right\} + (1-\eta_1)\exp\left\{\mu_H(0) + \frac{1}{2}\lambda_H(0)\right\}\right].$$

The benchmark risk loading is set as $\vartheta = 0.2$, motivated by the loading parameter used in Xu and Hua [32]. Substituting $\eta_1 = 0.8$, $\vartheta = 0.2$, $(\bar{\mu}_L, \bar{\lambda}_L) = (-2.5996, 10.7571)$, and $(\bar{\mu}_H, \bar{\lambda}_H) = (-0.7916, 9.6858)$, we have $P = 29.25$. The observable underwriting score is specified as $S_i = H_i + W_i$, where W_i denotes an observable financial-capacity indicator and H_i represents other verifiable underwriting information. In the numerical analysis, we use the revenue variable in Table 2 of Chong et al. [9] to proxy the observable financial component of the score. Since the revenue variable is highly right-skewed, we follow the treatment of its log-transformation and set $S_i = 4.2$ as the benchmark observable underwriting score. Moreover, for the risk-averse case, we set $a = 0.03$ in the benchmark case. This choice ensures that the quadratic utility increases over the main payoff range considered in the numerical analysis.

We examine the optimal contracts and effort levels of node 3 in Figure 1. Tables 2 and 3 report the optimal contract parameters, effort choices, and insurer's expected payoff under Scenarios A–C for risk-neutral and risk-averse agents, respectively. The results show the following. In Scenario A (the insured never learns the risk type) and Scenario B (the insured learns the risk type only after signing), the insurer offers a single contract α^*, β^*, since these two situations mainly involve moral hazard. In Scenario C (the insured knows the risk type before signing), the insurer must separate high-risk and low-risk participants and offer two type-specific contracts, α_L^*, β_L^* and α_H^*, β_H^*. This contractual menu is designed to simultaneously alleviate moral hazard and adverse selection.

The numerical results for risk-neutral agents are reported in Table 2. Under the benchmark premium setting, no feasible insurance contract can satisfy the participation constraint in any of the three information scenarios. This result is consistent with the economic interpretation of risk neutrality. A risk-neutral agent evaluates an insurance contract only through its expected payoff and has no strict willingness to pay for transferring loss uncertainty. Therefore, when the loaded premium exceeds the expected benefit from insurance, the agent has no incentive to purchase the contract. At the same time, the insurer cannot reduce the premium below the actuarially required level without sacrificing its own expected payoff. Consequently, no mutually acceptable contract exists in the risk-neutral case under the benchmark loaded premium. From the insurer's perspective, the optimal decision is not to underwrite the risk, so the realized premium and the insurer's payoff are both zero. The effort levels reported in Table 2 are the no-insurance benchmark efforts obtained from the agent's self-protection problem.

Table 2. Risk-neutral agents: Optimal contracts under the benchmark premium setting.

Scenario	α^*	β^*	α_L^*	β_L^*	α_H^*	β_H^*	e^{0*}	e_L^{0*}	e_H^{0*}	Π^*	U_1^*	Feasible
I	–	–	–	–	–	–	0.183	–	–	0.000	0.000	No
II	–	–	–	–	–	–	–	0.152	0.254	0.000	0.000	No
III	–	–	–	–	–	–	–	0.152	0.254	0.000	0.000	No

In contrast to the risk-neutral benchmark, the risk-averse case yields insurance contracts with positive coverage rates, actual premiums, and insurer payoffs. This difference highlights the economic role of risk aversion in driving demand for cyber insurance. A risk-averse agent not only considers the expected payoff, but also values the reduction in loss uncertainty. Therefore, the agent is willing to pay for risk transfer, which allows the insurer to provide positive coverage while still obtaining a positive expected payoff. Table 3 reports the numerical results for risk-averse agents. Under the benchmark premium setting, feasible insurance contracts exist in all three information scenarios. Compared with the risk-neutral benchmark in Table 2, these results show that risk aversion is an important factor supporting positive insurance coverage under a loaded premium.

Table 3. Risk-averse agents: Optimal contracts under the benchmark premium setting.

Scenario	α^*	β^*	α_L^*	β_L^*	α_H^*	β_H^*	e^*	e_L^*	e_H^*	U_1^*	Feasible
I	0.160	0.966	–	–	–	–	0.166	–	–	20.780	Yes
II	0.325	0.968	–	–	–	–	–	0.145	0.193	20.052	Yes
III	–	–	0.928	0.967	0.926	0.968	–	0.148	0.196	17.634	Yes

The preceding analysis shows that risk aversion is a key factor generating insurance demand. Therefore, we further examine how the risk aversion parameter a affects the contract parameters α_i and β_i. Figure 2 shows that a higher value of a leads to a larger coverage rate β_i and a smaller premium discount factor α_i. This result is consistent with the economic trade-off between insurance demand and insurer profitability. More risk-averse agents have a greater demand for risk transfer and are willing to pay for higher coverage. At the same time, higher coverage raises the insurer's expected indemnity cost, so the insurer charges a higher premium. Hence, stronger risk aversion increases the demand for coverage, while the insurer adjusts the premium discount downward to preserve profitability.

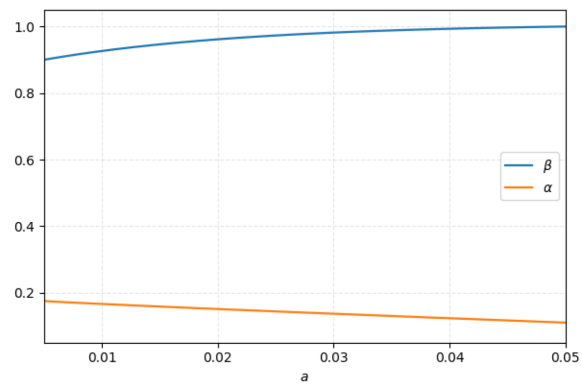


Figure 2. The effect of risk aversion level a on premium factor α and compensation factor β.

Moreover, these numerical results have clear economic interpretations. First, the comparison between risk-neutral and risk-averse agents shows that risk aversion is the fundamental driver of cyber-insurance demand. Thus, positive insurance demand arises only when agents value risk reduction. Second, the results show that stronger risk aversion leads to higher optimal coverage. This reflects the adjustment of contract terms to heterogeneous risk preferences and suggests that a uniform insurance contract may not be appropriate for policyholders with differing risk attitudes.

5. Conclusions

This paper studies the design of cyber insurance contracts under information asymmetry in a monopolistic insurance market. We consider both risk-neutral and risk-averse agents and develop a theoretical framework to characterize the optimal insurance contract and security investment under three information scenarios. For a given insurance contract, our theoretical results provide clear incentive implications: A larger premium discount factor α_i encourages the agent to exert more self-protection effort, whereas a larger coverage rate β_i will weaken this incentive. In addition, because cyber risk is interdependent, greater external protection from neighbors reduces the agent's own optimal effort, thereby creating a substitution effect and a free-riding incentive.

Then, we use numerical simulations to compute the optimal contracts, optimal effort levels, and insurer's expected payoffs under the three information scenarios. The results show that for risk-neutral agents, the optimal contract degenerates into a zero-premium, zero-coverage contract, indicating that they have no strict demand for insurance protection. In contrast, for risk-averse agents, positive coverage and positive insurer payoffs can arise, confirming that risk aversion is a key factor in generating non-degenerate insurance demand. We further conduct a sensitivity analysis to examine how the degree of risk aversion affects the optimal contract parameters. The results show that greater risk aversion increases the insured's demand for loss protection, leading to a higher coverage rate and adjustments to the premium discount and the actual premium.

The results provide several practical implications for cyber insurance design. First, insurers should take the insured's risk preference into account when designing cyber insurance products. Second, security effort and network connectedness should be incorporated into underwriting and pricing. Third, when the agent's risk type cannot be fully observed by the insurance company, the contract menus should be carefully designed to address adverse selection.

In this paper, the numerical analysis is conducted under a benchmark setting with a stylized small network and a single monopolistic insurer. Within this tractable framework, we demonstrate how the optimal insurance contracts and security efforts can be derived under different information scenarios designed to mitigate information asymmetry. We also compare different scenarios and show that the timing of information acquisition influences the optimal premium discount, coverage rate, effort choice, and the value of information. However, this simplified network setup does not fully capture the complexity of large-scale enterprise networks. In real applications, enterprise networks may consist of a large number of firms with complex topologies, multi-layer links, and dynamic structures. The current equilibrium formulation may not be applicable to this type of network. To adapt the proposed model to large, complex enterprise networks, we consider several methodological directions. First, if the enterprise network is sparse, one may exploit the local neighborhood structure of each firm and approximate its effective protection level by using only the most relevant neighboring firms. This method can reduce the dimension of the equilibrium system while preserving the main network spillover effects. Second, for networks with clear community or sectoral structures, the whole network may be decomposed into several sub-networks. The intra-community spillovers and inter-community spillovers can then be analyzed separately, which may make the equilibrium problem more tractable. Third, for very large networks, aggregate-state approximations may be used to replace individual-level interactions with representative network statistics, such as the average degree, average exposure intensity, average security effort, or community-level risk indicators.

Another limitation is that the present paper considers a static model with a single monopolistic insurer. In realistic cyber insurance markets, firms may face competition among multiple insurance providers, compare contracts offered by different insurers, purchase coverage from different insurers, or retain part of the risk through self-insurance. Therefore, a possible future direction is to extend the current framework to a competitive insurance market. It would also be meaningful to develop a dynamic version of the model to study the co-evolution of network topology, information acquisition, security investment, and insurance contracts over time. These extensions would require new game-theoretic and computational tools, and we leave them for future research.

Author contributions

R. Hu: Conceptualization, methodology, formal analysis, writing – original draft, writing– review and editing; N. Ren: Conceptualization, formal analysis, Writing – review and editing; X. Zhang: Methodology, validation, writing– review and editing. All authors have read and agreed to the published version of the manuscript.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant Nos. 12171086, 12371472) and Fundamental Research Funds for the Central Universities (Grant no. 2242024K40018). The authors are grateful to the editors and referees for their helpful comments and suggestions.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. G. A. Akerlof, The market for “lemons”: Quality uncertainty and the market mechanism, *Quart. J. Econ.*, **84** (1970), 488–500. http://doi.org/10.2307/1879431
2. R. Anderson, Why information security is hard: An economic perspective, In: *Seventeenth Annual Computer Security Applications Conference*, 2001, 358–365. http://doi.org/10.1109/ACSAC.2001.991552
3. K. Awiszus, T. Knispel, I. Penner, G. Svindland, A. Voß, S. Weber, Modeling and pricing cyber insurance, *Eur. Actuar. J.*, **13** (2023), 1–53. http://doi.org/10.1007/s13385-023-00341-9
4. C. Bravard, L. Charroin, C. Touati, Optimal design and defense of networks under link attacks, *J. Math. Econ.*, **68** (2017), 62–79. http://doi.org/10.1016/j.jmateco.2016.11.006

5. M. Carannante, V. D'Amato, P. Fersini, S. Forte, G. Melisi, Vine copula modeling dependence among cyber risks: A dangerous regulatory paradox, *Appl. Stoch. Model. Bus.*, **39** (2023), 549–566. http://doi.org/10.1002/asmb.2767

6. H. Cavusoglu, B. Mishra, S. Raghunathan, A model for evaluating IT security investments, *Commun. ACM*, **47** (2004), 87–92. http://doi.org/10.1145/1005817.1005828

7. H. Cavusoglu, S. Raghunathan, W. T. Yue, Decision-theoretic and game-theoretic approaches to IT security investment, *J. Manage. Inform. Syst.*, **25** (2008), 281–304. http://doi.org/10.2753/MIS0742-1222250211

8. P. A. Chiappori, B. Salanié, Testing for asymmetric information in insurance markets, *J. Polit. Econ.*, **108** (2000), 56–78. http://doi.org/10.1086/262111

9. W. F. Chong, D. Linders, Z. Quan, L. Zhang, Incident-specific cyber insurance, *ASTIN Bulletin.*, **55** (2025), 395–425. http://doi.org/10.1017/asb.2025.9

10. L. A. Gordon, M. P. Loeb, T. Sohail, A framework for using insurance for cyber-risk management, *Commun. ACM*, **46** (2003), 81–85. http://doi.org/10.1145/636772.636774

11. H. S. B. Herath, T. C. Herath, Copula-based actuarial model for pricing cyber-insurance policies, *Insur. Mark. Companies: Anal. Actuar. Comput.*, **2** (2011), 7–20.

12. C. Hillairet, O. Lopez, L. d'Oultremont, B. Spoorenberg, Cyber-contagion model with network structure applied to insurance, *Insur.: Math. Econ.*, **107** (2022), 88–101. http://doi.org/10.1016/j.insmatheco.2022.08.002

13. A. Hofmann, Internalizing externalities of loss prevention through insurance monopoly: An analysis of interdependent risks, *Geneva Risk Insur. Rev.*, **32** (2007), 91–111. http://doi.org/10.1007/s10713-007-0004-2

14. M. M. Khalili, P. Naghizadeh, M. Liu, Embracing risk dependency in designing cyber-insurance contracts, In: *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2017, 926–933. http://doi.org/10.1109/ALLERTON.2017.8262837

15. M. M. Khalili, P. Naghizadeh, M. Liu, Designing cyber insurance policies: The role of pre-screening and security interdependence, In: *IEEE Transactions on Information Forensics and Security*, **13** (2018), 2226–2239. http://doi.org/10.1109/TIFS.2018.2812205

16. H. Kunreuther, G. Heal, Interdependent security, *J. Risk Uncertainty*, **26** (2003), 231–249. http://doi.org/10.1023/A:1024119208153

17. J. Bolot, M. Lelarge, Cyber insurance as an incentive for internet security, In:*Managing information risk and the economics of security*, Boston, MA: Springer, 2009, 269–290. http://doi.org/10.1007/978-0-387-09762-6_13

18. M. Lelarge, J. Bolot, Economic incentives to increase security in the internet: The case for insurance, *IEEE INFOCOM*, 2009, 1494–1502. http://doi.org/10.1109/INFCOM.2009.5062066

19. J. A. Ligon, P. D. Thistle, Information asymmetries and informational incentives in monopolistic insurance markets, *J. Risk Insur.*, **63** (1996), 434–459. https://doi.org/10.2307/253620

20. J. Liu, J. Li, K. Daly, Bayesian vine copulas for modelling dependence in data breach losses, *Ann. Actuar. Sci.*, **16** (2022), 401–424. http://doi.org/10.1017/S174849952200001X

21. P. Naghizadeh, M. Liu, Voluntary participation in cyber-insurance markets, In: *The 13th Workshop on the Economics of Information Security (WEIS)*, 2014.

22. R. Pal, L. Golubchik, Analyzing self-defense investments in internet security under cyber-insurance coverage, In: *2010 IEEE 30th International Conference on Distributed Computing Systems*, 2010, 339–347. http://doi.org/10.1109/ICDCS.2010.79

23. R. Pal, Cyber-insurance in internet security: A dig into the information asymmetry problem, 2012, arXiv: 1202.0884. http://doi.org/10.48550/arXiv.1202.0884

24. S. Romanosky, L. Ablon, A. Kuehn, T. Jones, Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk? *J. Cybersecurity*, **5** (2019), tyz002. http://doi.org/10.1093/cybsec/tyz002

25. D. Schatz, R. Bashroush, Economic valuation for information security investment: A systematic literature review, *Inform. Syst. Front.*, **19** (2017), 1205–1228. http://doi.org/10.1007/s10796-016-9648-8

26. G. Schwartz, S. Sastry, Cyber-insurance framework for large scale interdependent networks, In: *HiCoNS '14: Proceedings of the 3rd international conference on High confidence networked systems*, 2014, 145–154. http://doi.org/10.1145/2566468.2566481

27. H. Sun, M. Xu, P. Zhao, Modeling malicious hacking data breach risks, *N. Am. Actuar. J.*, **25** (2021), 484–502. http://doi.org/10.1080/10920277.2020.1752255

28. H. Varian, System reliability and free riding, In: *Economics of information security*, Boston, MA: Springer, **12** (2004), 1–15. http://doi.org/10.1007/1-4020-8090-5_1

29. M. Vojnovic, A. J. Ganesh, On the race of worms, alerts, and patches, In: *EEE/ACM Transactions on Networking*, **16** (2008), 1066–1079. http://doi.org/10.1109/TNET.2007.909678

30. X. Xie, C. Lee, M. Eling, Cyber insurance offering and performance: An analysis of the U.S. cyber insurance market, *Geneva Pap. Risk Insur. Issues Pract.*, **45** (2020), 690–736. http://doi.org/10.1057/s41288-020-00176-5

31. M. Xu, K. M. Schweitzer, R. M. Bateman, S. Xu, Modeling and predicting cyber hacking breaches, *IEEE T. Inf. Foren. Sec.*, **13** (2018), 2856–2871. http://doi.org/10.1109/TIFS.2018.2834227

32. M. Xu, L. Hua, Cybersecurity insurance: Modeling and pricing, *N. Am. Actuar. J.*, **23** (2019), 220–249. http://doi.org/10.1080/10920277.2019.1566076

33. Z. Yang, J. C. S. Lui, Security adoption and influence of cyber-insurance markets in heterogeneous networks, *Perform. Evaluation*, **74** (2014), 1–17. http://doi.org/10.1016/j.peva.2013.10.003