systems

MDPI

Article

Economics of Cybersecurity Investment and Information Sharing: Firm Decision Making under Policy Constraints

Liurong Zhao *, Xinshuo Wu, Jiao Li and Huagang Tong

School of Economics and Management, Nanjing Tech University, Nanjing 211816, China; xinshuo1998@njtech.edu.cn (X.W.); lijiao66_happy@163.com (J.L.); thg_ms@njtech.edu.cn (H.T.)
* Correspondence: zhaoliurong@njtech.edu.cn

Abstract: With an increasing number of firms in cybersecurity information-sharing platforms, the potential cyber risks become a critical challenge during the exchanging of information. How to balance economic benefits and security requirements is an important topic for both firms and the government. By developing a game-theoretic model, the firms' optimal strategies are discussed considering their absorptive capacity for security information under different policy constrains. The results show that the value of security information, intrusion loss, the level of cybersecurity vulnerability, the negative impact coefficient of platform security information disclosure, and the absorptive capacity for security information are key factors impacting firms' decisions. The value of security information and intrusion loss are constrained by the marginal utility of cybersecurity investment and security information sharing. Firms prefer to increase their security investment or security information sharing only if the value of security information and intrusion loss are positively related to the marginal utility of cybersecurity investment or cybersecurity information sharing. Specifically, in the case without policy constrains, the optimal strategies of n firms are discussed, and it is found that they are consistent with those of two firms and that the utility of any firm in the platform decreases as the number of firms increases.

Keywords: cybersecurity information sharing; cybersecurity investment; the value of security information; intrusion loss

check for updates

Received: 9 December 2024
Revised: 18 January 2025
Accepted: 25 January 2025
Published: 29 January 2025

Citation: Zhao, L.; Wu, X.; Li, J.; Tong, H. Economics of Cybersecurity Investment and Information Sharing: Firm Decision Making under Policy Constraints. *Systems* **2025**, *13*, 83. https://doi.org/10.3390/systems13020083

1. Introduction

In recent years, despite the increasing frequency and sophistication of cyber-attacks, firms' cybersecurity practices have not demonstrated substantial improvements. Governments have advocated for the concept of "collaboration, participation, and common interests", encouraging firms to take social responsibility by rapidly identifying and responding to similar attack risks through cybersecurity information sharing [1], facilitating the flow of cybersecurity information from government to firms and from firms to firms. Cybersecurity information sharing refers to the process by which entities exchange vulnerability information and threat intelligence related to cybersecurity. The goal is to enhance capabilities for comprehensive threat identification and response, thereby strengthening defense and response mechanisms in cybersecurity. For instance, the U.S. government enacted the "Cybersecurity Information Sharing Act" to enhance cybersecurity through improved information sharing and collaboration while also offering legal protection for participating entities. In 2023, the European Commission introduced the "EU Directive on High Standards of Cybersecurity Measures (NIS 2 Regulation)" [2], which delineates firms' responsibilities, planning structures, and cybersecurity information resources in response to large-scale cybersecurity incidents. Similarly, China released the "Information Security Technology: Guidelines for Cybersecurity Information Sharing", aimed at strengthening national and organizational cybersecurity defenses. This initiative promotes information sharing and collaboration by establishing unified guiding principles and standards to address the increasingly complex nature of cybersecurity threats.

Cybersecurity information sharing can enhance a firm's cybersecurity capabilities. In the absence of effective cybersecurity information management policies, the value of security information sharing may still contribute to improved overall management. However, some firms continue to adopt a wait-and-see approach. On one hand, assessing the economic value of security information sharing is challenging, as is quantifying the relationship between cybersecurity investment and the benefits accrued from cybersecurity information sharing. These cybersecurity threats, such as Denial of Service (DoS), Distributed Denial of Service (DDoS) attacks, or Man-in-the-Middle (MITM) attacks, often reduce firms' motivation to engage in such activities [3]. On the other hand, joining a cybersecurity information-sharing platform may increase the risk of security information leakage. In practice, firms join these platforms with similar cybersecurity information systems. If one firm is attacked by hackers, the vulnerabilities of related firms may be exposed, resulting in risk interdependence. This scenario can cause firms to be reluctant to share their cybersecurity information [4].

In addition, when faced with cybersecurity challenges, firms also consider social responsibility to be fulfilled on behalf of the State, which influences their decision to engage in sharing actions. First, a firm's organizational structure significantly influences the efficiency of security information transmission and processing. Different structures result in varying levels of security information creation value and absorptive capacity for security information [5]. Moreover, a firm's cybersecurity risk response capabilities are constrained by its available security technologies and employee expertise. The diversity in security operations arises from the varying risk response capabilities among firms [6]. Insufficient cybersecurity capabilities can increase risks such as hacking and revenue loss [7].

However, despite the importance of a firm's own cybersecurity capabilities in the decision-making process regarding participation in a cybersecurity information-sharing platform, the current research landscape reveals certain gaps that need to be addressed. A review of existing research reveals that most studies on cybersecurity information sharing focus on a single perspective, such as economics, risk, or capability. Few studies have explored the influence of policy constraints on firm decision making. Furthermore, firms consider national policies regarding social responsibility when facing cybersecurity challenges, which subsequently affects their decisions to engage in information-sharing activities. These problems urgently need to be solved to help firms to make the right choice, aiming to leverage the strengths of policy and safeguard the economic and security interests of firms. This paper aims to explore the impact of a firm's value of security information, cybersecurity capability, platform security information disclosure, and the hacking probability by constructing a game-theoretic model that addresses firms' decisions related to cybersecurity investment and information sharing. Based on differential game theory and policy constraints, this study analyzes the optimal level of cybersecurity investment and information sharing in two scenarios: with and without policy constraints. This approach offers a novel framework for understanding firms' behaviors during the decision-making processes associated with cybersecurity investment and information sharing.

The key findings of this research are as follows: First, this study advances the understanding of the complex relationship between the value of security information and sharing benefits. By analyzing the impact mechanisms of these factors, it provides a more accurate foundation for firms to make decisions in different contexts. Second, this research study comprehensively examines how firms adjust their decisions in two scenarios: "without policy constraints" and "with policy constraints". This study introduces innovative adaptive strategies for firms responding to policy constraints. Finally, previous studies rarely provide a theoretical basis for government policy making from the perspective of firms' responses to policy changes. This study fills this gap by analyzing how firms adjust cybersecurity investment and information-sharing decisions based on factors such as the value of security information and intrusion loss when facing policy constraints.

The structure of this paper is as follows: Section 2 presents a literature review, Section 3 outlines the model description, and Section 4 provides the model analysis. Section 5 details the experimental results, Section 6 the Discussion, and Section 7 a model extension. Finally, Section 8 concludes the paper and suggests directions for future research.

2. Literature Review

This paper focuses on how the value of security information and firms' cybersecurity capabilities impact their decisions regarding cybersecurity information sharing under varying policy constraints. We providing an overview of the existing research in these three areas.

Some scholars have studied the role of cybersecurity information sharing, highlighting how firms benefit from this practice. Gal and Ghose argued that information sharing becomes more valuable as product sustainability increases, enabling firms within information-sharing alliances to obtain greater competitive advantages within their respective industries [8]. Additionally, a classification system for a firm's cybersecurity information sharing can help identify and mitigate operational risks, thereby enhancing overall security levels [9]. He et al. and Gordon et al. summarized that cybersecurity information sharing reduces defense costs and decreases the likelihood of cybersecurity incidents [10,11]. Despite these potential benefits, some studies found that firms are often unwilling to participate in sharing activities when engaged in single-shot games. Repeated interactions are necessary to determine whether they will engage in future information-sharing activities [12]. Moreover, several studies have explored the factors influencing cybersecurity information sharing. Hausken argued that cybersecurity information sharing depends on inter-firm interdependence, the attributes of the shared information, and the unit costs of cybersecurity investments [13]. Building on this, Liu found that the nature of information assets—whether sustainable or complementary—is a key determinant of firms' cybersecurity information-sharing decisions [14]. The optimal strategies regarding cybersecurity investment and information sharing have also been studied [15].

Cybersecurity capability is a crucial determinant of a firm's sharing decisions, encompassing absorptive capacity for security information, cybersecurity information exchange, and risk management. Regarding absorptive capacity for security information, Goodwin et al. suggested that firms can prevent cybersecurity incidents by effectively absorbing valuable cybersecurity information [16]. With their knowledge, expertise, and ability to analyze threat information during sharing activities, firms can better anticipate and understand potential cybersecurity risks in advance [17]. In terms of cybersecurity information exchange, Choraś defined the concept of cybersecurity information sharing and proposed both online and offline mechanisms to enhance security operational capabilities [18]. Fransen et al. also found that various methods for exchanging threat information are essential to addressing the growing cybersecurity threats [19]. Thanh and Hung demonstrated that combining deep learning with differential privacy can achieve a balance between data privacy protection and the usability of information exchange [20]. To enhance cybersecurity information exchange capabilities and improve cybersecurity defense levels, Jones et al.

and Sujatha et al. found that multiple encryption algorithms can be utilized to process data, ensuring the security of information sharing [21,22]. Additionally, other scholars have established a hierarchical model to evaluate existing cybersecurity information-sharing resources [23]. Regarding cybersecurity risk management, research on avoiding free riding, preventing privacy breaches, and designing incentive mechanisms has gained attention. This is supported by studies showing that integrating cybersecurity information sharing with insurance can improve management effectiveness [24].

Another focus of our research is cybersecurity information sharing under policy constraints. In policy development, the United States has implemented risk-based policies to enhance cybersecurity information sharing by collaborating with critical infrastructure owners and operators. Harwood and Dahl proposed that future policy making should eliminate ambiguity, provide robust safeguards for information sharers, and foster public–private partnerships to improve cybersecurity information sharing [25]. By integrating economics with cybersecurity information-sharing policies, non-cooperation and free-rider behaviors can be mitigated [26]. Regarding policy content, Prieto emphasized the importance of establishing mechanisms, rules, and measures to facilitate information sharing between the government and firms [27]. Zheng and Lewis suggested that legislation should establish a standardized process for cooperation between firms and governments in the context of cybersecurity information sharing [28]. Concerning the effects of policy enforcement, Tosh et al. clarified that appropriate incentive measures could encourage firms to share cybersecurity information, thereby increasing returns through effective countermeasures in cybersecurity investment [29]. Amini and Bozorgasl demonstrated that effective policy promotes information sharing and enhances cloud computing security [30]. However, some scholars argued that voluntary sharing policies may not be effective and that policy constraints are necessary to increase incentives for cybersecurity information sharing [31].

Despite the abundant research in the field of cybersecurity information sharing, particularly concerning cybersecurity information-sharing platforms, there remains a notable scarcity of studies focusing on how to make informed cybersecurity investment decisions and effectively share varying values of security information within the constraints imposed by policy. Specifically, there is a lack of research on the impact of cybersecurity capability and the value of security information on firms' cybersecurity investment and information-sharing decisions. In light of this gap, our research contributes in the following ways: First, we study optimization based on the relationship between the value of security information and sharing benefits. Second, from an adaptive strategy perspective, we consider firms' decisions under policy constraints. Third, in practical application, our research provides theoretical support for government policy making.

This study has two main limitations: Firstly, in terms of entity types in game theory, it mainly focuses on the interactions among social planners, cybersecurity information platforms, and firms, while individual security awareness, habits, and feedback, which can affect firms' information-sharing strategies, are not covered by the current game model. Secondly, from the research perspective, when analyzing the hacking probability, the study refers to the Gordon–Loeb model but does not consider the influence of different attack types on firms' cybersecurity information-sharing strategies. Future research could explore the specific impacts of various attack types on such strategies.

3. Model Description

The game model of cybersecurity information sharing consists of firms on the platform, with each aiming to maximize their utilities. To facilitate differentiation and discussion, in the subsequent model construction and equilibrium analysis, parameters related to firm i are denoted with the subscript i, while parameters associated with other member firms of the platform are denoted with the subscript j. It is assumed that the two firms are homogeneous, with both serving as cybersecurity service providers on the cybersecurity information-sharing platform. The model considers cybersecurity information sharing from firm j to firm i, where s_j represents the cybersecurity information shared by firm j with the platform, as this paper only considers a scenario with two firms on the platform participating in the game [32,33].

To assess the impact of differentiated values of cybersecurity information, it is essential to measure the variation in value provided by firms. Compared with low-value cybersecurity information, high-value cybersecurity information has a more significant impact on enhancing a firm's self-security investment and generates greater economic benefits. In this paper, $q_j(0 < q_j < 1)$ represents the value of security information sharing from firm j to firm i , $q_j s_j$ denotes that firm j shares the value of security information with firm i.

Firms possess varying levels of cybersecurity capabilities, necessitating a thorough assessment of their vulnerabilities prior to any potential attacks. On one hand, differences in firms' absorptive capacities for security information lead to varying benefits from information sharing. According to the law of diminishing marginal utility, as a firm's absorptive capacity increases, the additional benefits it gains from shared cybersecurity information decrease. Thus, α_j represents firm i's absorptive capacity for security information. On the other hand, once firms identify vulnerabilities, they must install repair patches within a set time frame. However, they may face operational challenges, such as high patching costs, which could lead to abandoning the repairs. Additionally, after disclosing vulnerability information on the platform, firms may face adverse consequences, such as being targeted by hackers or incurring reputational damage during the patching process. We define ϕ_i $(\phi_i > 0)$ as the coefficient that represents the negative impact of platform security information disclosure on firm i. The level of firm i's cybersecurity can be defined as $T_i = t_i + q_j s_j$ [34]. The formula suggests that the total cybersecurity capability of firm i (denoted by T_i) is the sum of two components: the firm's own cybersecurity investment t_i, which directly impacts its defensive capabilities, and $q_j s_j$, which represents the security information provided by firm j to firm i. This external information serves as an enhancement to firm i's cybersecurity efforts, increasing its overall ability to prevent, detect, and respond to security threats.

Given the uncertainty of intrusion loss, it is crucial to evaluate the impact of hacker intrusions based on different behavioral decisions made by firms. When hackers initially invade firm i without cybersecurity investment or information sharing, the probability is v_i. In order to accurately calculate the hacking probability in the process of cybersecurity investment and information sharing, the probability formula is

$$p_i(T) = v_i^{\lambda T_i + 1} = v_i^{\lambda(t_i + q_j s_j) + 1}.$$

Above, λ is a constant, and we have $(\lambda > 0)$, satisfying the condition $(0 < p_i(T) < \frac{1}{2})$ [6,35]. $p_i(T)$ represents firm i's probability of being hacked after implementing cybersecurity investment and cybersecurity information sharing. λ denotes that the probability of firm i being hacked is a non-negative constant between 0 and $\frac{1}{2}$. v represents the initial intrusion probability (level of cybersecurity vulnerability) of firm i. T_i is the total cybersecurity capability of firm i. The intrusion loss incurred by firm i is L_i. It is assumed that L_i is sufficiently large to ensure that firms have the motivation for cybersecurity investment and information sharing.

For a detailed explanation of the parameter meanings, refer to Table 1.

Table 1. Parameter description.

Parameter	Description
q_j	The value of security information shared by firm *j* with firm *i* $(0 < q < 1)$
α_i	The absorptive capacity for security information for firm *i*
ϕ_i	The negative impact coefficient of platform security information disclosure on firm *i* $(\phi > 0)$
t_i	The cybersecurity investment of firm *i*
T_i	The overall cybersecurity level of firm *i*
$p_i(T)$	The hacking probability of firm *i* after implementing cybersecurity decisions $(0 < p_i(T) < \frac{1}{2})$
v_i	The initial probability of intrusion for firm *i* $(0 < v < \frac{1}{2})$
L_i	The intrusion loss of firm *i*
s_j	The amount of cybersecurity information shared by firm *j* with firm *i* on the platform
λ	The limitation on firm *i*'s hacking probability, which lies between 0 and $\frac{1}{2}(0 < \lambda < \frac{1}{2})$

3.1. Model Construction from Perspective of Firms' Benefit Maximization

Firm *i* receives cybersecurity information from firm *j* on the cybersecurity information-sharing platform. The benefits obtained from cybersecurity information sharing are $f_i = (2\alpha_i - \alpha_i^2)q_js_j$. The costs incurred by firm *i*, denoted by c_i, include three aspects: cybersecurity investment t_i, direct loss p_iL_i caused by hacker intrusions, and intrusion loss arising from sharing cybersecurity information with *j* and the platform. We define the loss of information resulting from sharing cybersecurity information as $q_i(1 - p_i)p_jL_i$. On the other hand, intrusion loss can stem from platform information disclosure behaviors. If firms fail to complete patching during the vulnerability protection period, cybersecurity information may be exposed to hackers, potentially leading to significant intrusion loss. We define the security information leakage loss by the platform as $\Phi_i(q_is_i)^2$. The utility function of firm *j* is

$$\begin{aligned}\pi_i &= f_i - c_i\\ &= \left(2\alpha_i - \alpha_i^2\right)\left(q_js_j\right) - \left[t_i + p_iL_i + q_i(1-p_i)p_jL_i + \phi(q_is_i)^2\right]\\ &= \left(2\alpha_i - \alpha_i^2\right)\left(q_js_j\right) - \left[t_i + v_i^{\lambda\left(t_i+q_js_j\right)+1}L_i + q_i\left(1 - v_i^{\lambda\left(t_i+q_js_j\right)+1}\right)v_j^{\lambda\left(t_j+q_is_i\right)+1}L_i + \phi(q_is_i)^2\right].\end{aligned} \quad (1)$$

Similarly, the utility function of firm *j* is

$$\begin{aligned}\pi_j &= f_j - c_j\\ &= \left(2\alpha_j - \alpha_j^2\right)\left(q_is_i\right) - \left[t_j + p_jL_j + q_j\left(1-p_j\right)p_iL_j + \phi\left(q_js_j\right)^2\right]\\ &= \left(2\alpha_j - \alpha_j^2\right)\left(q_is_i\right) - \left[t_j + v_j^{\lambda\left(t_j+q_is_i\right)+1}L_j + q_j\left(1 - v_j^{\lambda\left(t_j+q_is_i\right)+1}\right)v_i^{\lambda\left(t_i+q_js_j\right)+1}L_j + \phi\left(q_js_j\right)^2\right].\end{aligned} \quad (2)$$

3.2. Model Construction from Perspective of Social Welfare Maximization

Against the background of increasingly severe cybersecurity threats, policy constraints are placed on firms' cybersecurity investment and information sharing to maximize overall societal cybersecurity benefits. We consider three policy constraints for the two firms:

cybersecurity investment only, cybersecurity information sharing only, or both of them. Therefore, the overall utility function of firm *j* and firm *j* is given by

$$\begin{aligned}
\pi_s &= f_i - c_i + f_j - c_j \\
&= \left(2\alpha_i - \alpha_i^2\right)\left(q_j s_j\right) - \left[t_i + p_i L_i + q_i(1-p_i)p_j L_i + \phi(q_i s_i)^2\right] \\
&+ \left(2\alpha_j - \alpha_j^2\right)(q_i s_i) - \left[t_j + p_j L_j + q_j(1-p_j)p_i L_j + \phi\left(q_j s_j\right)^2\right] \\
&= \left(2\alpha_i - \alpha_i^2\right)\left(q_j s_j\right) - \left[t_i + v_i^{\lambda\left(t_i + q_j s_j\right)+1} L_i + q_i\left(1 - v_i^{\lambda\left(t_i + q_j s_j\right)+1}\right) v_j^{\lambda\left(t_j + q_i s_i\right)+1} L_i + \phi(q_i s_i)^2\right] \\
&+ \left(2\alpha_j - \alpha_j^2\right)(q_i s_i) - \left[t_j + v_j^{\lambda\left(t_j + q_i s_i\right)+1} L_j + q_j\left(1 - v_j^{\lambda\left(t_j + q_i s_i\right)+1}\right) v_j^{\lambda\left(t_i + q_j s_j\right)+1} L_j + \phi\left(q_j s_j\right)^2\right].
\end{aligned} \tag{3}$$

4. Model Analysis

In this section, we analyze firms' decision-making processes regarding cybersecurity investment and information sharing, both with or without policy constraints. First, we examine the optimal strategies for cybersecurity investment and information sharing from the perspective of firms' individual interests, assuming no policy constraints. Second, we evaluate the optimal strategies from a social welfare perspective, considering the outcomes under three different policy scenarios.

4.1. Model Analysis of a Firm's Profit Maximization Perspective

Without policy constraints, the expected utility function of cybersecurity information sharing for firm *i* is as follows:

$$\begin{aligned}
Max\pi_i &= \left(2\alpha_i - \alpha_i^2\right)\left(q_j s_j\right) - \left[t_i + p_i L_i + q_i(1-p_i)p_j L_i + \phi(q_i s_i)^2\right] \\
&= \left(2\alpha_i - \alpha_i^2\right)\left(q_j s_j\right) - \left[t_i + v_i^{\lambda\left(t_i + q_j s_j\right)+1} L_i + q_i\left(1 - v_i^{\lambda\left(t_i + q_j s_j\right)+1}\right) v_j^{\lambda\left(t_j + q_i s_i\right)+1} L_i + \phi(q_i s_i)^2\right]
\end{aligned} \tag{4}$$

Equations (5) and (6) can be obtained from Equation (4):

$$\frac{\partial \pi_i}{\partial t_i} = -1 - \lambda \ln(v_i) L_i v_i^{\lambda\left(t_i + q_j s_j\right)+1} + q_i L_i \lambda \ln(v_i) v_j^{\lambda\left(t_j + q_i s_i\right)+1} v_i^{\lambda\left(t_i + q_j s_j\right)+1} \tag{5}$$

$$\frac{\partial \pi_i}{\partial s_i} = -L_i \lambda {q_i}^2 \,\mathrm{In}\left(v_j\right)\left(1 - \boldsymbol{v}_i^{\lambda\left(t_i + q_j s_j\right)+1}\right) v_j^{\lambda\left(t_j + q_i s_i\right)+1} - 2\phi {q_i}^2 s_i \tag{6}$$

We assume that firms are homogeneous and focus on the symmetric case, so there are $t_i = t_j = t_N, s_i = s_j = s_N, p_i = p_j = p_N, L_i = L_j = L_N, q_i = q_j = q_N, v_i = v_j = v_N$.

The equilibrium dynamic equations for two firms are

$$-1 - \lambda \ln(v_N) L_N p_N + q_N L_N \lambda \ln(v_N) {p_N}^2 = 0 \tag{7}$$

$$-L_N \lambda {q_N}^2 \ln(v_N)(1 - p_N) p_N - 2\phi {q_N}^2 s_N = 0 \tag{8}$$

Thus, the dynamic replication equations of firms are

$$\frac{dt_N}{dq_N} = \frac{2\phi p_N + L_N \lambda^2 \ln^2(v_N) {p_N}^2 q_N (1 - 2p_N) - 2\lambda \ln(v_N) \phi s_N (1 - 2p_N q_N)}{2\lambda \ln(v_N) \phi (1 - 2p_N q_N)} \tag{9}$$

$$\frac{ds_N}{dq_N} = \frac{\lambda L_N {p_N}^2 \ln(v_N)(1 - 2p_N)}{2\phi(2p_N q_N - 1)} \tag{10}$$

$$\frac{dt_N}{dL_N} = \frac{2\phi(1 - p_N q_N) - \lambda \ln(v_N) L_N p_N q_N (1 - q_N)}{2\phi\lambda \ln(v_N) L_N (2p_N q_N - 1)} \tag{11}$$

$$\frac{ds_N}{dL_N} = \frac{p_N(q_N - 1)}{2\phi(1 - 2p_N q_N)} \tag{12}$$

From this, Proposition 1 can be obtained.

Proposition 1. *(1) When the value of security information rises, firms tend to decrease their optimal cybersecurity investment and increase cybersecurity information sharing:* $\frac{\partial t}{\partial q} < 0, \frac{\partial s}{\partial q} > 0.$

(2) With the increase in intrusion loss, firms' optimal cybersecurity investment tends to increase, while cybersecurity information sharing tends to decrease: $\frac{\partial t}{\partial L} > 0, \frac{\partial s}{\partial L} < 0.$

Proposition 1 demonstrates that as the value of security information increases, firms tend to reduce their cybersecurity investment. A high value of security information significantly enhances firms' cybersecurity capabilities, enabling them to meet cybersecurity requirements more effectively while simultaneously lowering their need for substantial cybersecurity investment. Moreover, the value of security information is positively correlated with cybersecurity information sharing. Consequently, firms with a high value of security information should increase their information-sharing practices to strengthen overall cybersecurity and optimize their investment in cybersecurity measures.

Moreover, as intrusion loss increases, firms should increase their cybersecurity investment. The escalating negative impact of cybersecurity incidents prompts firms to prioritize cybersecurity measures over information sharing. Consequently, firms increase their cybersecurity investment to achieve the desired security level. Additionally, there is a negative correlation between intrusion loss and cybersecurity information sharing. In such scenarios, firms tend to reduce their information-sharing activities to mitigate potential indirect losses that may arise from other firms on the platform. This analysis aligns with the findings of Qian [36].

4.2. Model Analysis of the Model from the Perspective of Social Welfare Maximization

First, we examine the case where there are policy constraints on cybersecurity investment. The expected utility function for firm *i* with cybersecurity information sharing can be derived from Equation (3). The policy constraints on a firm's cybersecurity investment aim to maximize the total utility functions for both firm *i* and firm *j*, as expressed in the following equation:

$$\begin{aligned} M\alpha x \pi_s = {} & \left(2\alpha_i - \alpha_i^2\right)(q_j s_j) - \Big[t_i + v_i^{\left(\lambda\left(t_i + q_j s_j\right) + 1\right)} L_i \\ & + q_i \left(1 - v_i^{\left(\lambda\left(t_i + q_j s_j\right) + 1\right)}\right) v_j^{\lambda\left(t_j + q_i s_i\right) + 1} L_i + \phi(q_i s_i)^2\Big] \\ & + \left(2\alpha_j - \alpha_j^2\right)(q_i s_i) - \Big[t_j + v_j^{\left(\lambda\left(t_j + q_i s_i\right) + 1\right)} L_j \\ & + q_j \left(1 - v_j^{\left(\lambda\left(t_j + q_i s_i\right) + 1\right)}\right) v_i^{\lambda\left(t_i + q_j s_j\right) + 1} L_j + \phi\left(q_j s_j\right)^2\Big] \end{aligned} \tag{13}$$

Equation (14) can be obtained based on Equation (13):

$$\begin{aligned} \frac{\partial \pi_s}{\partial t_i} = {} & -1 - \lambda \ln(v_i) L_i v_i^{\lambda\left(t_i + q_j s_j\right) + 1} + q_i L_i \lambda \ln(v_i) v_j^{\lambda\left(t_j + q_i s_i\right) + 1} v_i^{\lambda\left(t_i + q_j s_j\right) + 1} \\ & - q_j L_j \lambda \ln(v_i) \left(1 - v_j^{\lambda\left(t_j + q_i s_i\right) + 1}\right) v_i^{\lambda\left(t_i + q_j s_j\right) + 1} \end{aligned} \tag{14}$$

We assume that firms are homogeneous and focus on the symmetric case, so there are $t_i = t_j = t_I, s_i = s_j = s_I, p_i = p_j = p_I, L_i = L_j = L_I, q_i = q_j = q_I, v_i = v_j = v_I$.

The equilibrium dynamic equations for two firms are listed as follows:

$$-1 + \lambda \ln(v_I) L_I p_I (2p_I q_I - q_I - 1) = 0 \tag{15}$$

$$-L_I \lambda {q_I}^2 \ln(v_I)(1 - p_I) p_I - 2\phi {q_I}^2 s_I = 0 \tag{16}$$

Thus, the dynamic replication equations of firms are

$$\frac{dt_I}{dq_I} = \frac{2\phi(1 - 2p_I) + L_I \lambda^2 \ln^2(v_I) p_I q_I (1 - 2p_I)^2 - 2\lambda \ln(v_I) \phi s_I (4p_I q_I - q_I - 1)}{2\phi\lambda \ln(v_I)(4p_I q_I - q_I - 1)} \tag{17}$$

$$\frac{ds_I}{dq_I} = \frac{-\lambda L_I p_I \ln(v_I)(2p_I - 1)^2}{2\phi(4p_I q_I - q_I - 1)} \tag{18}$$

$$\frac{dt_I}{dL_I} = \frac{2\phi(1 - q_I - 2p_I q_I) - L_I \lambda^2 \ln^2(v_I) {p_I}^2 q_I (1 - q_I)}{2\phi\lambda L_I \ln(v_I)(4p_I q_I - q_I - 1)} \tag{19}$$

$$\frac{ds_I}{dL_I} = \frac{\lambda \ln(v_I) {p_I}^2 (1 - q_I)}{2\phi(4p_I q_I - q_I - 1)} \tag{20}$$

Based on the above analysis, Propositions 2 and 3 can be obtained.

Proposition 2. *The effects of the value of security information on cybersecurity investment and information sharing decisions are as follows:*

(1) When the hacking probability is $0 < p < \frac{1}{4}$ *and the negative impact coefficient of platform security information disclosure is* $0 < \phi < \frac{L\lambda \ln(v) p (1-2p)^2}{2s(4p-1)}$, *there is a critical value of security information* $q^* = \frac{-2\phi s \lambda \ln(v)}{\lambda \ln(v) p (1-2p)^2 - 2\phi s (4p-1)}$; *if* $q \in (0, q^*)$, *the optimal cybersecurity investment* ${t_I}^*$ *increases:* $\frac{\partial t}{\partial q} > 0$; *if* $q \in (q^*, 1)$, *the optimal cybersecurity investment* ${t_I}^*$ *decreases:* $\frac{\partial t}{\partial q} < 0$.

(2) The optimal cybersecurity investment ${t_I}^*$ *increases when the hacking probability is* $0 < p < \frac{1}{4}$ *and the negative impact coefficient of platform security information disclosure is* $\frac{L\lambda \ln(v) p (1-2p)^2}{2s(4p-1)} < \phi < 1$, $\frac{\partial t}{\partial q} > 0$.

(3) When the hacking probability is $\frac{1}{4} < p < \frac{1}{2}$, *there exists a critical value of security information* $q^* = \frac{-2\phi s \lambda \ln(v)}{\lambda \ln(v) p (1-2p)^2 - 2\phi s (4p-1)}$; *if* $q \in (0, q^*)$, *the optimal cybersecurity investment* ${t_I}^*$ *increases:* $\frac{\partial t}{\partial q} > 0$; *if* $q \in (q^*, 1)$, *the optimal cybersecurity investment* ${t_I}^*$ *decreases:* $\frac{\partial t}{\partial q} < 0$.

(4) Regardless of the value of security information q, the optimal cybersecurity information sharing ${s_I}^*$ *decreases:* $\frac{\partial s}{\partial q} < 0$.

Proposition 2 demonstrates that when both the hacking probability and the negative impact coefficient of platform security information disclosure are minimized, firms initially increase their cybersecurity investment as the value of security information rises. However, cybersecurity investment begins to decline after reaching an optimal level. In this scenario, firms achieve their cybersecurity objectives, with investment decisions being primarily driven by the competitive advantages gained through cybersecurity information sharing. When the value of security information is low, the improvements in cybersecurity capabilities through information sharing are insufficient to meet firms' requirements, necessitating increased cybersecurity investment. Conversely, when the value of security information is high, effective cybersecurity information sharing significantly enhances cybersecurity capabilities, allowing firms to reduce their cybersecurity investments and achieve cost savings.

Second, when the hacking probability is low but the negative impact coefficient of platform security information disclosure is high, firms should increase their cybersecurity investment as the value of security information rises. In this scenario, cybersecurity investment decisions are primarily driven by the potential intrusion losses resulting from the heightened risk of information leakage, which is directly correlated with the value of security information. As the value of security information increases, the risk of information leakage intensifies, leading to greater exposure to indirect loss and diminished efficiency in cybersecurity information sharing. As a result, firms are increasingly compelled to augment their cybersecurity investments in order to strengthen their comprehensive cybersecurity capabilities.

Third, as the hacking probability increases, cybersecurity investment initially rises with the value of security information but eventually declines. This suggests that the parameter is positively correlated with the marginal utility of cybersecurity investment at higher value of security information and negatively correlated at lower value. A higher hacking probabilityindicates signifies a more challenging security environment, necessitating enhanced cybersecurity measures. When the value of security information is low, the improvements in cybersecurity capabilities achieved through information sharing are insufficient to meet security objectives, thus requiring additional investment. Conversely, when the value of security information is high, effective information sharing significantly enhances cybersecurity capabilities, allowing firms to leverage the benefits of sharing, reduce cybersecurity investments, and achieve both stronger security and cost efficiency.

Finally, as the value of security information increases, cybersecurity information sharing decreases. In this scenario, the marginal utility of information sharing is negatively correlated with the value of security information. Sharing decisions are primarily driven by the heightened risk of security information leakage, which intensifies as the value of security information rises. Consequently, firms should reduce their cybersecurity information sharing to mitigate these risks and minimize potential loss costs.

Proposition 3. *In this case, the impacts of a firm's hacking losses on decisions for any firm intrusion loss L are as follows:*

(1) The optimal cybersecurity investment $t_I{}^*$ increases when the value of security information satisfies $0 < q < \frac{1}{1+2p}$, which means that $\frac{\partial t}{\partial L} > 0$. When the value of security information satisfies $\frac{1}{1+2p} < q < 1$, the optimal cybersecurity investment $t_I{}^*$ decreases, i.e., $\frac{\partial t}{\partial L} < 0$.

(2) The optimal cybersecurity information sharing $s_I{}^*$ increases, which means that $\frac{\partial s}{\partial L} > 0$.

Proposition 3 asserts that when the value of security information is low, firms should consider increasing their cybersecurity investment, as potential intrusion losses tend to increase. Conversely, when intrusion loss decreases, it may be prudent for firms to reduce their cybersecurity investments. The utility derived from cybersecurity investment is positively correlated with intrusion loss when the value of security information is low and negatively correlated when the value is high. Increased intrusion loss signals a greater need for cybersecurity measures, thus driving firms to invest more in cybersecurity. However, when the value of security information is sufficiently high, cybersecurity information sharing becomes more effective, enabling firms to enhance their cybersecurity capabilities. As a result, firms can reduce their cybersecurity investment and achieve cost savings.

Additionally, as intrusion loss rises, firms tend to increase their cybersecurity information sharing, as the marginal utility of information sharing is positively correlated with intrusion loss. As intrusion loss increases, the cybersecurity capabilities strengthened by information sharing are further enhanced, allowing firms to more effectively address their cybersecurity needs and achieve their cybersecurity objectives.

This analysis contrasts with the conclusion drawn by Qian [35], whose study did not account for the influence of the value of security information on cybersecurity investment decisions or the impact of cybersecurity information sharing among firms. In contrast, the present study incorporates these factors, providing a more comprehensive and realistic description of firms' economic decisions.

Second, we discuss the case that with policy constraints on cybersecurity information sharing, *i*'s goal is to maximize its own utility function by deciding cybersecurity investment as in Equation (4). Maximizing the total utility function of firm *i* and firm *j* is performed according to Equation (13).

The partial derivative of firm *i*'s ${s_i}^*$ is

$$\begin{aligned}\frac{\partial \pi_s}{\partial s_i} &= -q_i\lambda\ln\left(v_j\right)L_i v_j^{\lambda\left(t_j+q_is_i\right)+1}\left(1-v_i^{\lambda\left(t_i+q_js_j\right)+1}\right)-2\phi {q_i}^2 s_i+\left(2\alpha_j-\alpha_j^2\right)q_i \\ &\quad - L_j\lambda\ln\left(v_j\right)v_j^{\lambda\left(t_j+q_is_i\right)+1}+L_jq_j\lambda\ln\left(v_j\right)v_i^{\lambda\left(t_i+q_js_j\right)+1}v_j^{\lambda\left(t_j+q_is_i\right)+1} \\ &\quad - q_jL_j\lambda\ln(v_i)\left(1-v_j^{\lambda\left(t_j+q_is_i\right)+1}\right)v_i^{\lambda\left(t_i+q_js_j\right)+1}\end{aligned} \tag{21}$$

We assume that firms are homogeneous and focus on the symmetric case, so there are $t_i = t_j = t_S, s_i = s_j = s_S, p_i = p_j = p_S, L_i = L_j = L_S, q_i = q_j = q_S, v_i = v_j = v_S$.

The equilibrium dynamic equations for two firms are

$$-1-\lambda\ln(v_S)L_Sp_S+\lambda\ln(v_S)q_S{p_S}^2=0 \tag{22}$$

$$\lambda\ln(v_S)L_Sp_Sq_S(2p_Sq_S-q_S-1)-2\phi {q_S}^2 s_S+\left(2\alpha-\alpha^2\right)q_S=0 \tag{23}$$

Thus, the dynamic replication equations of firms are

$$\frac{dt_S}{dq_S}=\frac{2\phi p_S-L_S\lambda^2\ln^2(v_S)p_S(p_Sq_S+p_S-1)}{2\phi\lambda\ln(v_S)(1-2q_S)} \tag{24}$$

$$\frac{ds_s}{dq_s}=\frac{\lambda L_sp_s\ln(v_s)(p_sq_s+p_s-1)-2\phi s_s(1-2p_sq_s)}{2\phi q_s(1-2p_sq)} \tag{25}$$

$$\frac{dt_S}{dL_S}=\frac{2\phi(1-p_Sq_S)-L_S\lambda^2\ln^2(v_S){p_S}^2q_S(1-q_S)}{2\phi\lambda L_S\ln(v_S)(2p_Sq_S-1)} \tag{26}$$

$$\frac{ds_S}{dL_S}=\frac{\lambda\ln(v_S)p_S^2(1-p_S)}{2\phi(2p_Sq_S-1)} \tag{27}$$

Based on the above analysis, we obtain Propositions 4 and 5.

Proposition 4. *Under policy constraints on cybersecurity information sharing between two firms, the impacts of the value of security information on their decisions are as follows:*

(1) For any value of security information q, the optimal cybersecurity investment S_s^* monotonically increases, which means that $\frac{\partial t}{\partial q} < 0$;

(2) When the negative impact coefficient of platform security information disclosure on a firm is $0 < \phi < \frac{L\lambda\ln(v)p}{-4s}$, there is a critical value of security information $q^* = \frac{L\ln(v)\lambda p(1-p)+2\phi s}{p(L\lambda\ln(v)p+4\phi s)}$, and if $q \in (0, q^*)$, the optimal cybersecurity information sharing S_s^* increases, which means that $\frac{\partial s}{\partial q} > 0$; if $q \in (q^*, 1)$, the optimal cybersecurity information sharing S_s^* monotonically decreases, which means that $\frac{\partial s}{\partial q} < 0$.

(3) For any value of security information q, the optimal cybersecurity information sharing S_s^* monotonically increases; when the negative impact coefficient of platform security information disclosure on a firm is $\frac{L\lambda\ln(v)p}{-4s} < \phi < \frac{L\lambda\ln(v)p(1-p)}{-2s}$, it means $\frac{\partial s}{\partial q} > 0$.

(4) When the negative impact coefficient of platform security information disclosure on a firm is $\frac{L\lambda \ln(v)p(1-p)}{-2s} < \phi < 1$*, there exists a critical value of* $q^* = \frac{L\ln(v)\lambda p(1-p)+2\phi s}{p(L\lambda \ln(v)p+4\phi s)}$*, and if* $q \in (0, q^*)$*, the optimal cybersecurity information sharing* S_s^* *monotonically decreases, which means that* $\frac{\partial s}{\partial q} < 0$*; if* $q \in (q^*, 1)$*, the optimal cybersecurity information sharing* S_s^* *monotonically increases, which means that* $\frac{\partial s}{\partial q} > 0$.

First, by comparing Propositions 2 and 4, it becomes evident that under policy constraints on cybersecurity information sharing, the optimal cybersecurity investment for firms consistently exhibits a negative correlation with the value of security information. In contrast, under policy constraints on cybersecurity investment, firms' optimal investment decisions become more complex. If the negative impact of platform security information disclosure is negligible, the optimal cybersecurity investment follows an inverted U-shaped curve, peaking at a specific value of security information. However, if the negative impact is substantial, the optimal cybersecurity investment maintains a positive correlation with the value of security information.

Second, firms' optimal cybersecurity information sharing consistently exhibits a negative correlation with the value of security information. However, under policy constraints on cybersecurity information sharing, firms' optimal sharing decisions become more complex. When the negative impact of platform security information disclosure is minimal, the optimal information sharing follows an inverted U-shaped curve, peaking at a specific value of security information. Conversely, when the negative impact is significant, the optimal information sharing follows a U-shaped curve, reaching its minimum at a particular value of security information.

Proposition 5. *Under policy constraints on cybersecurity information sharing between two firms, the intrusion loss on their decisions are as follows:*

(1) For intrusion loss L, there exists a critical value $L^* = \frac{2\phi(1-pq)}{\lambda^2 \ln^2(v)p^2q(1-q)}$*. If* $L \in (0, L^*)$*, the optimal cybersecurity investment* t_s^* *monotonically increases, which means that* $\frac{\partial s}{\partial q} > 0$*; if* $L \in (L^*, +\infty)$*, the optimal cybersecurity investment* t_s^* *monotonically decreases, which means that* $\frac{\partial s}{\partial q} < 0$.

(2) The optimum of cybersecurity information sharing s_s^* *monotonically increases for any intrusion loss L:* $\frac{\partial s}{\partial L} > 0$*.*

The comparison of Propositions 3 and 5 reveals the following insights: First, when there are policy constraints on both cybersecurity investment and information sharing, the optimal cybersecurity information sharing by firms consistently correlates positively with intrusion loss. Moreover, the optimal cybersecurity investment invariably follows an inverted U-shaped curve in relation to the value of security information. The key difference is that under policy constraints on cybersecurity investment, firms' optimal investment decisions are influenced by the value of security information. Conversely, under policy constraints on cybersecurity information sharing, firms' optimal investment decisions are determined by the magnitude of intrusion loss.

Lastly, we discuss policy constraints on cybersecurity information sharing and cybersecurity investment to maximize the firm *i* and firm *j* aggregate utility function (Equation (13)).

We assume that firms are homogeneous and focus on the symmetric case, so there are $t_i = t_j = t_O, s_i = s_j = s_O, p_i = p_j = p_O, L_i = L_j = L_O, q_i = q_j = q_O, v_i = v_j = v_O$.

The equilibrium dynamic equations for two firms are as follows:

$$-1 + \lambda \ln(v_O)L_O p_O(2q_O p_O - q_O - 1) = 0 \tag{28}$$

$$\lambda \ln(v_O) L_O p_O q_O (2p_O q_O - q_O - 1) - 2\phi {q_O}^2 s_O + \left(2\alpha - \alpha^2\right) q_O = 0 \tag{29}$$

Thus, the dynamic replication equations of firms are

$$\frac{dt_O}{dq_O} = \frac{1 - 2p_O}{\lambda \ln(v_O)(4p_O q_O - q_O - 1)} \tag{30}$$

$$\frac{ds_O}{dq_O} = \frac{-s_O}{q_O} \tag{31}$$

$$\frac{dt_O}{dL_O} = \frac{(1 + q_O - 2p_O q_O)}{\lambda L_O \ln(v_O)(4p_O q_O - q_O - 1)} \tag{32}$$

$$\frac{ds_O}{dL_O} = 0 \tag{33}$$

From this, Proposition 6 can be obtained.

Proposition 6. *The impacts on the value of security information and intrusion loss are as follows:*

(1) For any value of security information q, the optimal cybersecurity investment t_o^* monotonically increases, and the optimal cybersecurity information sharing s_o^* monotonically decreases, which means that $\frac{\partial t}{\partial q} > 0$, $\frac{\partial s}{\partial q} < 0$.

(2) For intrusion loss L that are compromised, the optimal cybersecurity investment t_o^* monotonically increases, and the optimal cybersecurity information sharing s_o^* is constant, which means that $\frac{\partial t}{\partial L} > 0$, $\frac{\partial s}{\partial L} = 0$.

First, Proposition 6 states that an increase in the value of security information should lead firms to increase cybersecurity investment while reducing cybersecurity information sharing. In practice, regulations such as China's "Cybersecurity Law" impose constraints on cybersecurity investment, with a primary focus on ensuring that firms meet their cybersecurity objectives. Cybersecurity information sharing is generally encouraged to enhance overall defense and governance. In this context, firms balance mandated levels of cybersecurity investment and information sharing, taking into account the value of security information. As the value of security information rises, the risk of information leakage also increases, prompting firms to prioritize their own cybersecurity over the benefits of sharing. Consequently, firms will increase cybersecurity investment and reduce cybersecurity information sharing to achieve their cybersecurity defense goals.

Second, with policy constraints on both cybersecurity investment and information sharing, firms' cybersecurity investment increases with greater intrusion losses, while cybersecurity information sharing remains unaffected by intrusion loss. The rise in intrusion loss reflects a heightened demand for cybersecurity, as improvements in cybersecurity capabilities through information sharing are insufficient to mitigate these attacks. As a result, additional cybersecurity investment is required to strengthen the firm's security posture, which aligns with the findings of Qian [36]. Consequently, intrusion loss not influences firms' decisions regarding cybersecurity information sharing. In determining what cybersecurity information to share, firms prioritize economic benefits and the risks associated with information leakage over the impact on their cybersecurity investment.

Propositions 1–6 prove that whether firms make decisions or comply with policy constraints, the relationships among cybersecurity investment, cybersecurity information sharing, the value of security information, and intrusion loss are influenced by the marginal utility of both cybersecurity investment and cybersecurity information sharing.

5. Experimental Results

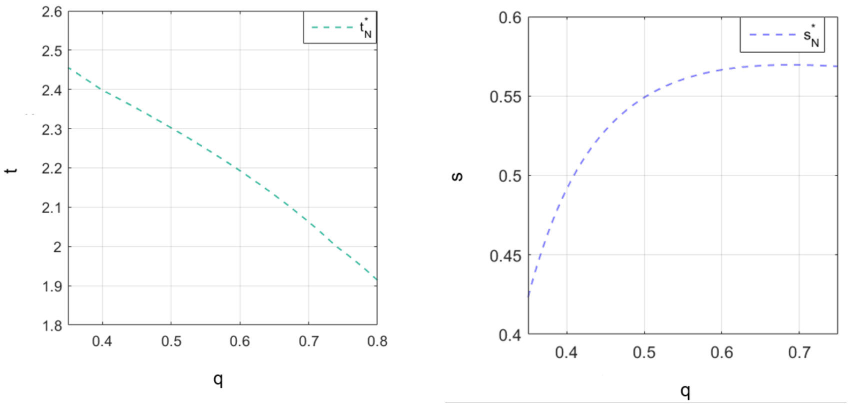
With reference to the parameter-setting method by Wu et al. [34], the parameter values in this study are mainly determined by two methods. Firstly, based on real cases and literature references, we refer to parameter values and research results from Li et al. [37], setting $v = 0.1, 0.2, 0.3, 0.015$. According to the data report from FreeBuf [38], we set $\lambda = 0.08, 0.15, 0.16, 0.2, 0.3$. Based on the policy text analysis of the "Cyber Security Law of the People's Republic of China", we set $L = 40, 100, 50$. Secondly, we take the annual data reports of firms and the equilibrium above the condition requirements, setting $q = 0.3, 0.75$, $\phi = 0.1, 0.2$, $\alpha = 0.6, 0.8$. The parameter ranges are obtained as shown in Table 2.

Table 2. Parameter scope.

Parameter	Scope
p_i	0.001–0.35
L_i	35–100
α_i	0.6–0.8
q_i	0.25–0.8
ϕ	0.01–0.25
λ	0.08–0.315

First, we use numerical simulation to analyze the perspective of firms' profit maximization.

The parameter settings are as follows: $\mathrm{v} = 0.1, \mathrm{L} = 40, \phi = 0.2$, and $\lambda = 0.3$. We analyze how firm cybersecurity investment and information sharing change under the influence of the value of security information shown in Figure 1a,b.

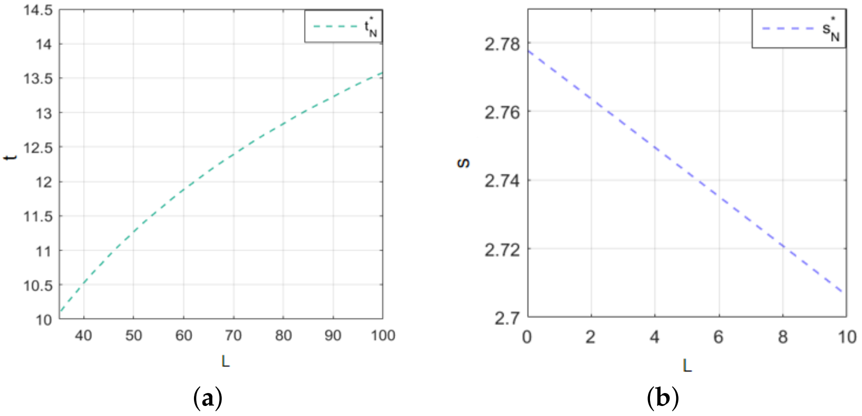


(**a**) (**b**)

Figure 1. The change trends of firm's cybersecurity investment and information sharing in relation to the value of security information are analyzed without policy constraints. (**a**) The trend of cybersecurity investment with the value of security information. (**b**) The trend of cybersecurity information sharing with the value of security information.

Figure 1 illustrates the change trends of firms' cybersecurity investment and information sharing in relation to the value of security information without policy constraints. Specifically, Figure 1a depicts the variation in cybersecurity investment as the value of security information changes, while Figure 1b shows how information sharing evolves in relation to the value of security information. As shown in Figure 1a,b, as the value of security information provided by the platform increases, firms are encouraged to leverage the positive effects of information sharing on investment effectiveness. This results in an upward trend in cybersecurity information sharing and a corresponding downward trend in cybersecurity investment. Without policy constraints, there is a negative correlation between cybersecurity investment and the value of security information, while information sharing exhibits a positive correlation with the value of security information.

When we set $v = 0.05, q = 0.6, \phi = 0.1$, and $\lambda = 0.1$, as intrusion losses change, the variations in cybersecurity investment and information sharing are as shown in Figure 2a,b.



(**a**) (**b**)

Figure 2. The change trends of firm's cybersecurity investment and information sharing in relation to intrusion loss are analyzed without policy constraints. (**a**) The trend of cybersecurity investment with intrusion losses. (**b**) The trend of cybersecurity information sharing with intrusion losses.

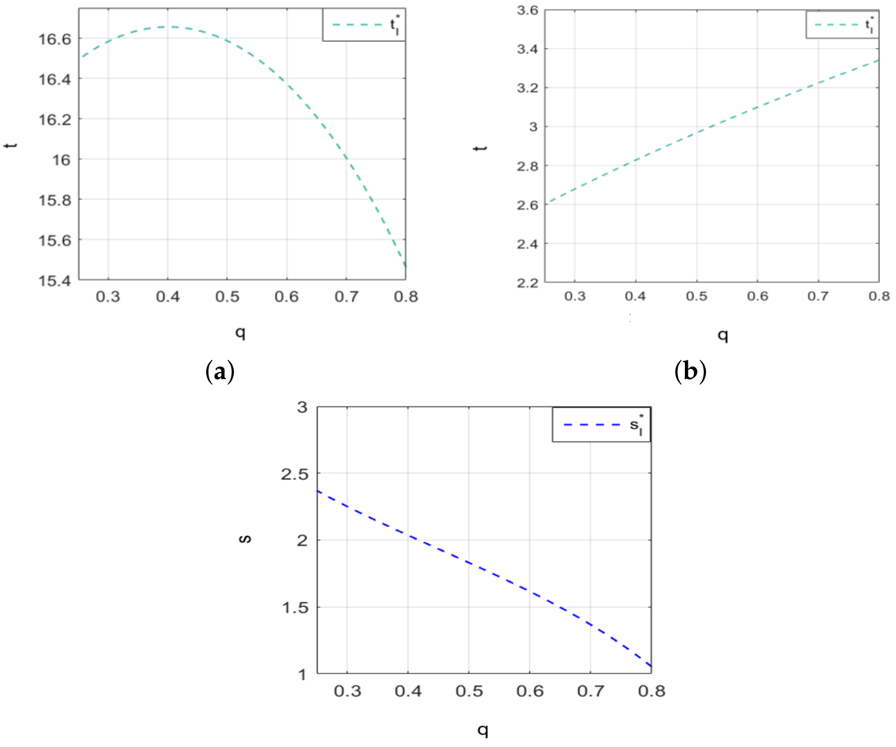
Figure 2 illustrates the changes in firms' cybersecurity investment and information sharing in response to variations in intrusion losses, without policy constraints. Specifically, Figure 2a depicts the relationship between cybersecurity investment and intrusion loss, while Figure 2b shows the correlation between information sharing and intrusion loss.

From Figure 2a,b, it is clear that as intrusion loss increases, firms can bolster their cybersecurity protection by increasing investment, which in turn reduces the hacking probability of future intrusion loss. At the same time, to mitigate the risk of significant indirect loss, firms should decrease their cybersecurity information sharing. This suggests that when facing the threat of intrusion loss, firms prioritize strengthening their own cybersecurity capabilities and carefully assessing the trade-offs of information sharing.

Second, we use numerical simulation to analyze the perspective of social welfare maximization.

Under policy constraints on cybersecurity investment and with the parameters being set to $v = 0.3$, $q = 100$, $\phi = 0.1$, and $\lambda = 0.16$, we analyze how cybersecurity investment changes with the value of security information, as shown in Figure 3a. In practice, firms routinely implement cybersecurity training programs, which not only enhance the professional competence of their employees but also effectively mitigate cybersecurity risks. Simultaneously, firms may share diverse types of cybersecurity threat information on the platform, including data on computer malware. The negative impact coefficient of platform security information disclosure on firms' cybersecurity posture and reputation can vary substantially. Therefore, we set $v = 0.008$, $L = 100$, $\phi = 0.1$, and $\lambda = 0.08$, and as parameters such as the level of cybersecurity vulnerability and the negative impact coefficient of platform disclosure behavior change, firms' cybersecurity investment varies with the value of security information, as shown in Figure 3b. Additionally, Figure 3c illustrates how firms' cybersecurity information sharing changes with the value of security information.

From Figure 3a, it is evident that for firms with a high level of cybersecurity vulnerability, when the value of security information is below 0.4, cybersecurity investment increases as the value of security information rises. However, when the value exceeds 0.4, cybersecurity investment decreases as the value of security information continues to increase. Figure 3b illustrates that for firms with a low level of cybersecurity vulnerability, where platform disclosure has a significant negative impact, cybersecurity investment should increase as the value of security information rises. Figure 3c shows that as the value of security information increases, firms tend to reduce their cybersecurity information sharing.



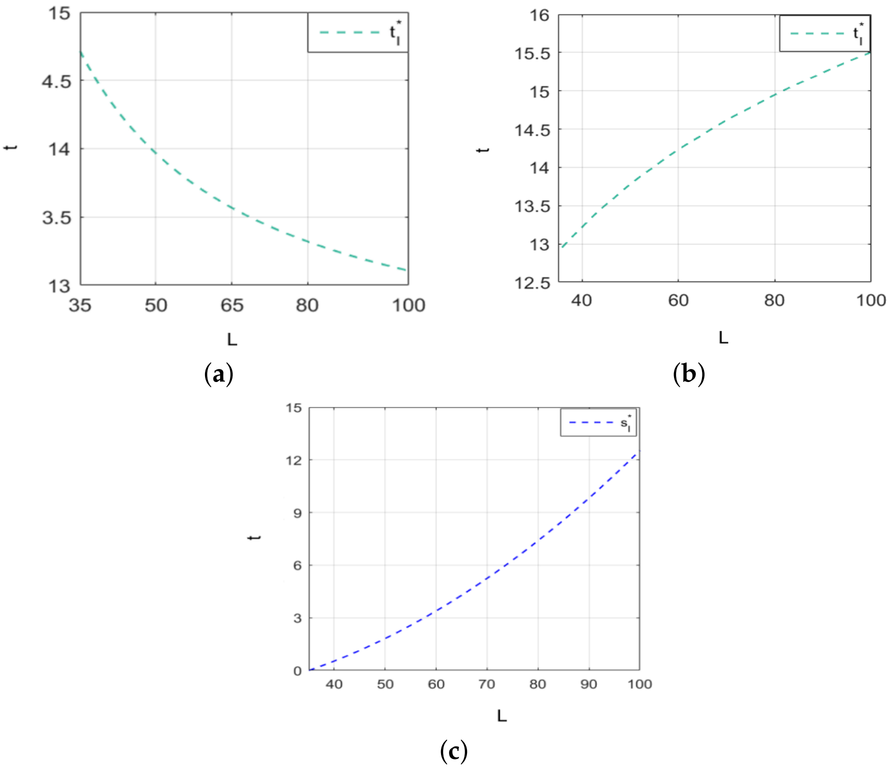
(**a**) (**b**)

(**c**)

Figure 3. Under policy constraints on cybersecurity investment, the changes in firms' cybersecurity investment and information sharing with the value of security information. (**a**) The trend of cybersecurity investment with the value of security information. (**b**) Under some factors' influence, the trend of cybersecurity investment with the value of security information. (**c**) The trend of cybersecurity information sharing with the value of security information.

We setv $= 0.1$, q $= 0.75$, $\phi = 0.1$, and $\lambda = 0.08$, and we analyze how cybersecurity investment changes with intrusion loss. Figure 4a shows the relationship between cybersecurity investment and intrusion loss when the value of security information varies. In reality, the cybersecurity environment faced by other firms on the platform is complex and changeable, and security information uploaded to the platform is constantly changing, and the value of the security information obtained by firms will also change. Therefore, we set q = 0.3. Figure 4b presents the relationship between information sharing and intrusion loss when the value of security information is 0.3, while Figure 4c shows the relationship between information sharing and intrusion loss. Figure 4a indicates that when the value of security information is high (e.g., 0.75), cybersecurity investment decreases as intrusion loss increases. Conversely, Figure 4b shows that when the value of security information is low (e.g., 0.3), cybersecurity investment increases as intrusion losse rises. Figure 4c demonstrates that cybersecurity information sharing increases with intrusion loss, which impacts firms' cybersecurity decisions differently depending on the value of security information in response to intrusion loss.

Under policy constraints on cybersecurity information sharing, we set v $= 0.015$, L $= 100$, $\alpha = 0.6$, $\phi = 0.02$, and $\lambda = 0.25$.



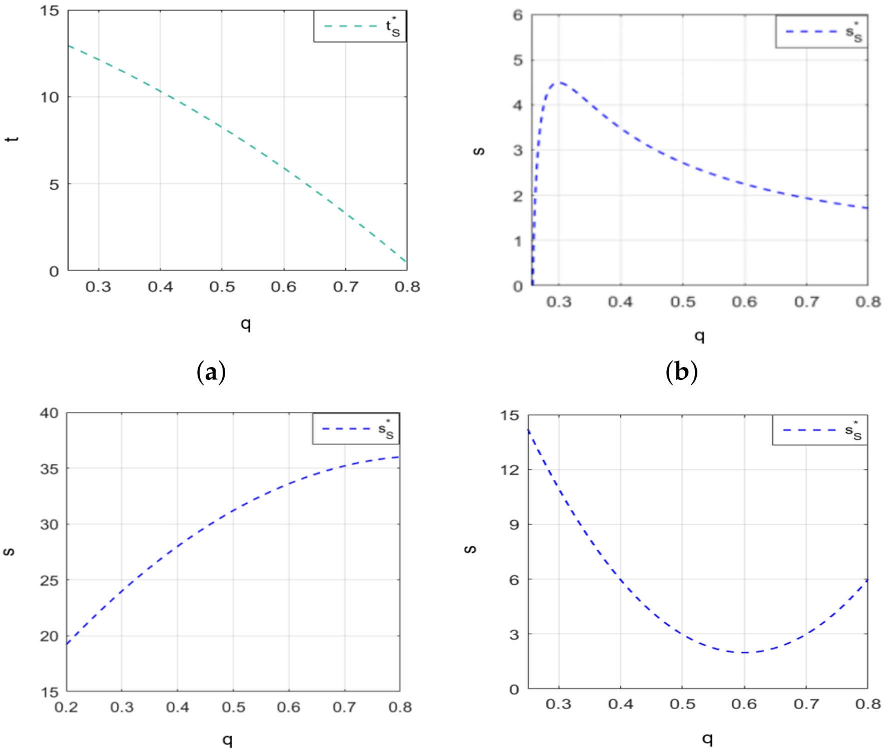
(**a**) (**b**)

(**c**)

Figure 4. Under policy constraints on cybersecurity investment, the changes in firms' cybersecurity investment and information sharing with the intrusion loss. (**a**) The value of security information affects the relationship between information sharing and intrusion loss. (**b**) The relationship between information sharing and intrusion loss when the value of security information is 0.3. (**c**) The trend of cybersecurity information sharing with intrusion loss.

When cybersecurity information sharing is subject to policy constraints, Figure 5 illustrates the dynamics of firms' cybersecurity investment and information sharing relative to the value of security information, as well as the impact of changes in the negative impact coefficients of platform disclosure on information sharing. Figure 5a depicts the relationship between cybersecurity investment and the value of security information. Figure 5b focuses on scenarios where the negative impact coefficient of platform disclosure on firms is relatively small. In practice, when firms upload various types of cybersecurity threat information to a platform, the negative impact coefficient of platform security information disclosure can differ. Therefore, by keeping factors such as cybersecurity vulnerability, intrusion loss, and the absorptive capability for security information within a limited range and setting $\phi = 0.1$ and $\phi = 0.02$, we analyze the variation in the negative impact coefficient of platform disclosure behaviors, as well as the differences in firms' cybersecurity information sharing with various values of security information, as shown in Figure 5c,d.

From Figure 5a, it can be observed that cybersecurity investment decreases as the value of security information increases. Figure 5b–d reveal that when the negative impact coefficient of platform disclosure is small (e.g., 0.02), cybersecurity information sharing follows an inverted U-shaped curve, with the highest inflection point at the value security information is 0.3. When the negative impact coefficient is moderate (e.g., 0.1), firms tend to increase cybersecurity information sharing. When the negative impact coefficient is large (e.g., 0.2), cybersecurity information sharing follows a U-shaped curve, with the lowest inflection point at the value of security information is 0.6.



(**a**) (**b**)

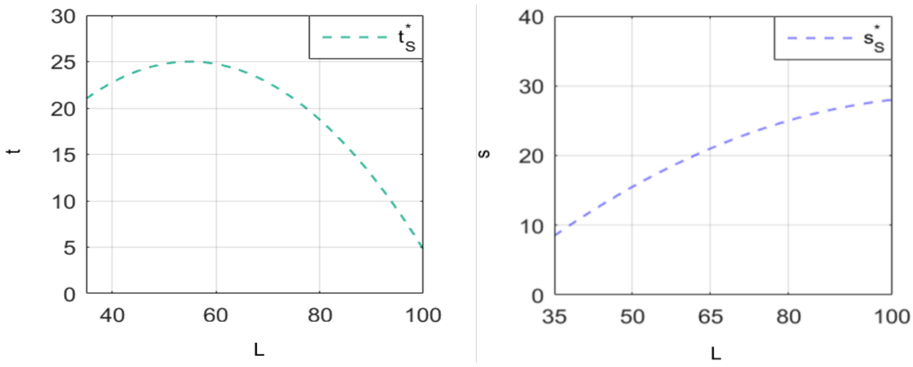
(**c**) (**d**)

Figure 5. The changes in firms' cybersecurity investment and information sharing with the value of security infotamtion under policy constrains on cybersecurity information sharing. (**a**) The trend in firms' cybersecurity investment with the value of security information increases. (**b**–**d**) The trend of cybersecurity information sharing with the value of security information under different changes in the negative impact coefficients of platform disclosure.

When we set $v = 0.1, q = 0.4, \phi = 0.1, \lambda = 0.2$, and $\alpha = 0.8$, Figure 6 illustrates the changes in firms' cybersecurity investment and information sharing in response to intrusion loss, when policy constraints are applied to cybersecurity information sharing. Figure 6a depicts the relationship between cybersecurity investment and intrusion loss, while Figure 6b shows the relationship between information sharing and intrusion loss. From Figure 6a, it is clear that firms increase cybersecurity investment when intrusion losses are below 52. However, when intrusion losses exceed 52, firms may reassess their investment strategies, taking into account factors such as cost-effectiveness. Figure 6b demonstrates that as intrusion loss increases, firms are more likely to increase cybersecurity information sharing.

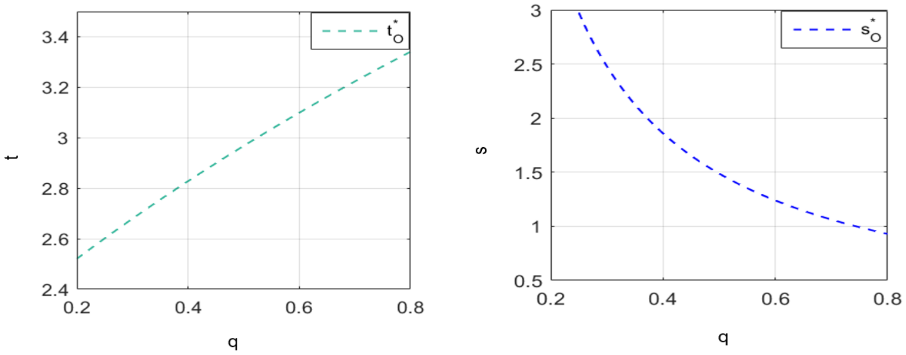
Finally, under dual policy constraints, we set $v = 0.2$, $L = 50$, $\phi = 0.2$, $\lambda = 0.3$, and $\alpha = 0.6$. The policy constraints on cybersecurity investment and information sharing lead to changes in firms' cybersecurity investment and information sharing as a function of the value of security information, as shown in Figure 7. Figure 7a illustrates the relationship between cybersecurity investment and the value of security information, while Figure 7b shows the relationship between cybersecurity information sharing and the value of security information.

From Figure 7a,b, it is evident that as the value of security information increases, firms tend to increase their cybersecurity investment while decreasing their cybersecurity information sharing. This behavior reflects the trade-off between securing valuable information and the risks associated with sharing it. A higher value of security information signals greater potential losses if compromised, prompting firms to allocate more investment to safeguard it. As a result, firms become more cautious and decrease the amount of information they share in order to mitigate these risks.



(**a**) (**b**)

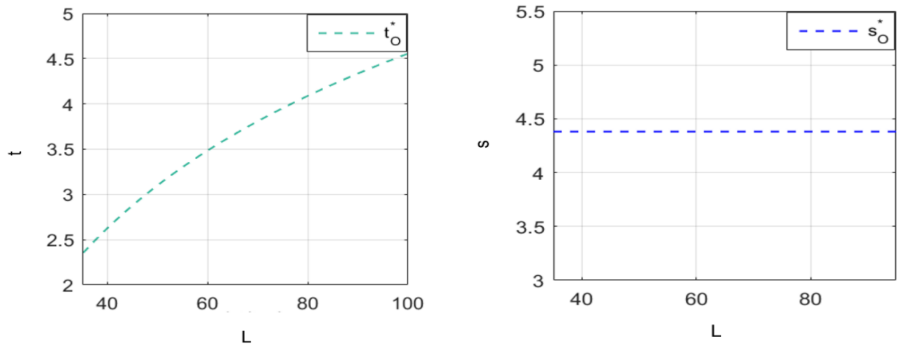
Figure 6. The changes in firms' cybersecurity investment and information sharing with intrusion loss under policy constrains on cybersecurity information sharing. (**a**) The trend of cybersecurity investment with intrusion loss. (**b**) The trend of cybersecurity information sharing with intrusion loss.



(**a**) (**b**)

Figure 7. The changes in firms' cybersecurity investment and information sharing with the value of security information under dual policy constraints. (**a**) The trend of cybersecurity investment with the value of security information. (**b**) The trend of cybersecurity information sharing with the value of security information.

When we set $v = 0.2, q = 0.7, \phi = 0.25, \lambda = 0.3$, and $\alpha = 0.6$, the changes in cybersecurity investment and information sharing can be observed under policy constraints as intrusion losses vary. These variations are illustrated in Figure 8.



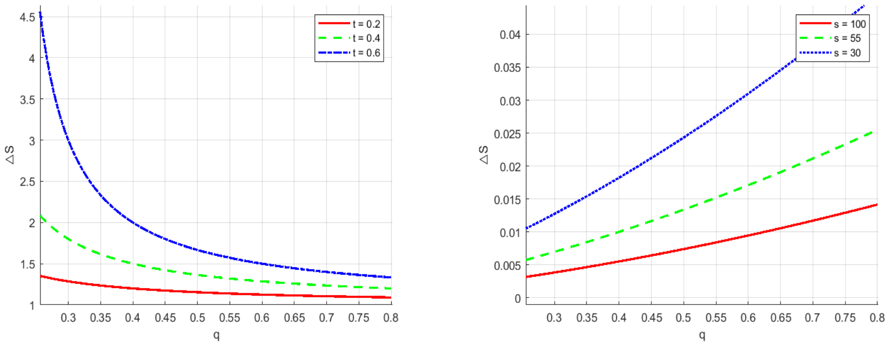
(**a**) (**b**)

Figure 8. The changes in cybersecurity investment and information sharing with intrusion losses under dual policy constraints. (**a**) The trend of cybersecurity investment with intrusion losses. (**b**) The trend of cybersecurity information sharing with intrusion losses.

Under dual policy constraints, the changes in firms' cybersecurity investment and cybersecurity information sharing in response to intrusion loss are shown in Figure 8. From Figure 8a, it is evident that as intrusion loss increases, firms are prompted to increase their cybersecurity investment. As the magnitude of intrusion loss rises, firms recognize the escalating risks and respond by proactively enhancing their cybersecurity measures. Figure 8b reveals that cybersecurity information sharing by firms remains unaffected by intrusion loss. Despite fluctuations in intrusion loss, the extent of information sharing remains relatively stable, suggesting that firms' decisions to share information are not directly influenced by the level of intrusion loss.

Sensitivity is denoted by $S = \frac{\Delta Y}{\Delta X}$. Here, S represents sensitivity, ΔY indicates the change in the dependent variable Y, and ΔX represents the change in the independent variable X.

Based on the theoretical analysis presented above, we analyze the impact of two key factors, the value of security information and intrusion losses, on firms' decision-making behavior regarding cybersecurity investment and information sharing from the perspective of firm benefit maximization. First, our sensitivity analysis studied the trend characteristics of ΔS with the increase in q under different values of t and s. The corresponding results are presented in Figure 9.

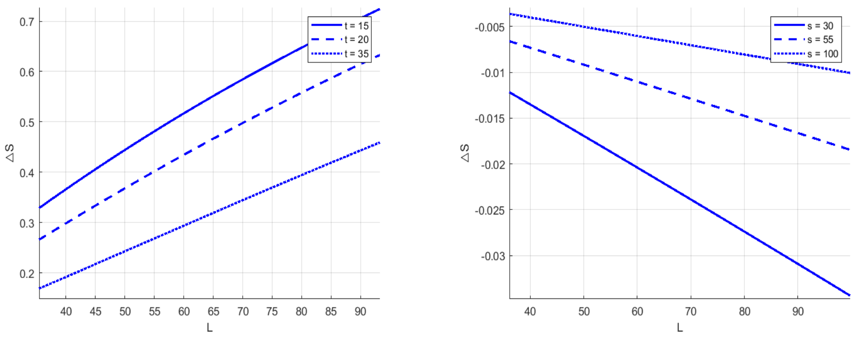


(**a**) (**b**)

Figure 9. The sensitivity analysis of the value of security information q. (**a**) The changes in cybersecurity investment t as the value of security information increases. (**b**)The changes in cybersecurity information sharing s as the value of security information increases.

As the value of security information increases, cybersecurity investment exhibits a downward trend, indicating a negative relationship between the two: as cybersecurity investment increases, the rate of decline accelerates. This can be explained by the fact that when the value of security information is high, firms are able to leverage this information more effectively to prevent and response to cybersecurity threats, thus reducing the need for additional cybersecurity investment. Conversely, there is a positive correlation between the value of security information and cybersecurity information sharing. As cybersecurity information sharing increases, the upward trend becomes slower. Specifically, as the value of security information increases, firms are more inclined to share it. This is because firms recognize the higher value of information and are more willing to share it. On one hand, cybersecurity information sharing helps firms enhance their cybersecurity capabilities, contributing to a stronger overall cybersecurity environment and, indirectly, mitigating the cybersecurity risks they face. On the other hand, firms may also benefit from receiving complementary information shared by other firms, which further increases their own value of security information.

Then, our sensitivity analysis studied the trend characteristics of ΔS with the increase in L under different values of t and s, as shown in Figure 10.



(**a**) (**b**)

Figure 10. Intrusion loss L sensitivity analysis. (**a**) The changes in cybersecurity investment t with the increase in intrusion loss. (**b**) The changes in cybersecurity information sharing s with the increase in intrusion loss.

Figure 10 clearly illustrates the significant impact of rising intrusion loss on firms' cybersecurity investment and information-sharing decisions. As intrusion loss increases, cybersecurity investment exhibits an upward trend, indicating a positive correlation between the two, and this upward trend slows down after rising. This is because when firms face a higher risk of intrusion losses, they have to invest more in cybersecurity to reduce these potentially huge loss. In contrast, the relationship between intrusion loss and cybersecurity information sharing shows a downward trend, reflecting a negative correlation, and the trend drops more rapidly. When faced with substantial intrusion loss, firms tend to reduce their information sharing, prioritizing enhanced cybersecurity investment to address emerging threats more effectively.

In conclusion, the impact of an increase in the value of security information and intrusion loss on firms' cybersecurity investment and information sharing aligns with the theoretical analysis presented. Therefore, when formulating cybersecurity strategies, firms should account for fluctuations in the value of security information and intrusion losses. By doing so, they can make informed adjustments to their cybersecurity investment and information-sharing decisions, thereby effectively managing varying levels of cybersecurity risks and maximizing the overall benefits of their cybersecurity initiatives.

6. Discussion

6.1. Discussion for Firms

Based on the above analysis, the following recommendations can be made to optimize firms' cybersecurity information sharing and investment decisions.

First, without policy constraints, as the value of security information increases, firms should consider reducing cybersecurity investment and increasing cybersecurity information sharing. Conversely, when intrusion loss rises, firms should prioritize increasing their cybersecurity investment while decreasing cybersecurity information sharing.

Second, under policy constraints on cybersecurity investment, if the value of security information increases, $L_I\lambda\ln(v_I)p_I(1-2p_I)^2$ and $2\phi s_I(4p_I-1)$ need to be compared. If L_I $\lambda\ln(v_I)p_I(1-2p_I)^2 < 2\phi s_I(4p_I-1)$, the value of $\mathrm{q}^* = \frac{-2\phi\mathrm{s_I}\lambda\ln(\mathrm{v_I})}{\left(\lambda\ln(\mathrm{v_I})\left(\mathrm{L_I}\lambda\ln(\mathrm{v_I})\mathrm{p_I}(1-2\mathrm{p_I})^2-2\phi\mathrm{s_I}(4\mathrm{p_I}-1)\right)\right)}$ needs to be calculated. If the value of security information q^* decreases, firms should reduce cybersecurity investment, and if the value of security information q^* increases, firms should increase cybersecurity investment. If $\mathrm{L_I}\lambda\ln(\mathrm{v_I})\mathrm{p_I}(1-2\mathrm{p_I})^2 > 2\phi\mathrm{s_I}(4\mathrm{p_I}-1)$, cybersecurity investment should be reduced. When the value of security information increases, firms should reduce cybersecurity information sharing. If intrusion loss increases, $q < \frac{1}{1+2p}$ needs to be determined. If it is valid, firms should increase their cybersecurity investment;

if it is not valid, firms should reduce their cybersecurity investment. When intrusion loss increases, firms should reduce cybersecurity information sharing.

Third, under policy constraints on cybersecurity information sharing, when the value of security information increases, firms should increase their cybersecurity investment; when the value of security information increases, $q^* = \frac{L_S \lambda \ln(v_S) p_S (1-p_S) + 2\phi s_S}{p_S (L_S \lambda \ln(v_S) p_S + 4\phi s_S)}$ needs to be calculated. Then, if $\frac{-2\phi s}{L\lambda \ln(v)(1-p)} < p < \frac{1}{2}$, firms should increase cybersecurity information sharing and decrease it when it is more than q^*. If $\mathrm{p} < \frac{-2\phi \mathrm{s}}{\mathrm{L}\lambda \ln(\mathrm{v})(1-\mathrm{p})}$, cybersecurity information sharing should be reduced if the value of security information is less than q^* and increased if it is greater than q^*. If $\frac{-2\phi s}{L\lambda \ln(v)(1-p)} < p < \frac{-4\phi s}{L\lambda \ln(v)}$, firms should increase cybersecurity information sharing. When intrusion loss increases, $L^* = \frac{2\phi(1-p_S q_S)}{\lambda^2 \ln^2(v_S) p_S^2 q_S (1-q_S)}$ needs to be calculated. When the intrusion loss is less than L^*, firms should increase cybersecurity investment; when intrusion loss is greater than L^*, cybersecurity investment should be reduced. When intrusion loss increases, firms should reduce cybersecurity information sharing.

Finally, with policy constraints on cybersecurity investment and information sharing, an increase in the value of security information should prompt firms to enhance their cybersecurity investment while simultaneously reducing their engagement in information sharing. Conversely, when intrusion loss rises, firms should increase their cybersecurity investment; however, the decision regarding the sharing of cybersecurity information should remain unaffected by these changes in intrusion loss.

6.2. Discussion for Social Planners

First, under policy constraints on cybersecurity information sharing only, as firms adjust their information-sharing strategy in accordance with the changes in the value of cybersecurity information, data islands may be a critical problem when the government builds a cybersecurity information-sharing platform; thus, the policy constraint on cybersecurity information sharing tends to be ineffective. The government incentivizes private entities to participate in cybersecurity information sharing by providing them with exemptions from liability. For instance, the "Cybersecurity Information Sharing Act (CISA)" of the United States points out that when firms share cybersecurity information in compliance with mandatory legal standards and the required compliance, they may be partially or wholly exempted from legal liabilities arising from sharing behaviors.

Second, under policy constraints on cybersecurity investment only, due to hacker attacks, vulnerabilities, and other network threats, firms are willing to increase their cybersecurity investment to avoid loss. Therefore, multiple options, such as cybersecurity insurance and information security technology, are part of what the government needs to offer when guiding firms' cybersecurity investment. Additionally, some countries, like China, make it mandatory for firms to meet cybersecurity risk assessment standards identifiable through third-party organizations, which constrain firms to a certain level of cybersecurity investment to ensure investment effectiveness.

Third, under policy constraints on both cybersecurity investment and information sharing, when firms are confronted with multiple factors, such as the value of security information, intrusion loss, the information disclosure problems of information-sharing platforms, and the absorptive capacity for security information, their strategies of cybersecurity investment and information sharing become more cautious. To ease the burden of firms' concern, tax measures, White List, or honored businesses can be utilized as a regulatory tool to encourage compliance by firms, so that cybersecurity investments and information-sharing policies can be effectively enacted.

7. Extension

In this section, the model is extended from two firms to any finite number, n ($n > 2$), of firms. In practice, there are multiple firms on the cybersecurity information-sharing platform to fulfill their responsibility. Hence, we try to answer two questions: (1) Will the optimal strategies of n firms change when the other conditions remain unchanged? (2) If the firm number is enlarged, will firm utility also change? The assumptions in Section 3 are introduced here. Therefore, the total utility function of n homogenous firms is

$$\begin{aligned}\text{Max}\pi_{i'} &= \sum_{i=1}^{n}\left[\left(2\alpha_i - \alpha_i^2\right)(q_j s_j) - \left(t_i + p_i L_i + q_i(1-p_i)p_j L_i + \phi(q_i s_i)^2\right)\right] \\ &= \sum_{i=1}^{n}\left[\left(2\alpha_i - \alpha_i^2\right)(q_j s_j)\left(t_i + v_i^{\lambda(t_i+q_j s_j)+1} L_i + q_i(1 - v_i^{\lambda(t_i+q_j s_j)+1})\right.\right. \\ &\quad \left.\left. v_j^{\lambda(t_j+q_i s_i)+1} L_i + \phi(q_i s_i)^2\right)\right] \\ &= n[(2\alpha_N - \alpha_N^2)(q_N s_N) - (t_N + v_N^{\lambda(t_N+q_N s_N)+1} L_N \\ &\quad + q_N(1 - v_N^{\lambda(t_N+q_N s_N)+1})v_N^{\lambda(t_N+q_N s_N)+1} L_N + \phi(q_N s_N)^2)]\end{aligned} \tag{34}$$

Hereafter, in comparing n firms with two firms, the case without policy constraints is taken as an example to illustrate the above two questions. The proof process of question (1) is similar to that of two firms. From Equation (34), we can obtain

$$\frac{dt_N}{dq_N} = \sum_{i=1}^{n} \frac{2\phi p_N + L_N \lambda^2 \ln^2(v_N) {p_N}^2 q_N (1 - 2p_N) - 2\lambda \ln(v_N) \phi s_N (1 - 2p_N q_N)}{2\lambda \ln(v_N) \phi (1 - 2p_N q_N)} \tag{35}$$

$$\frac{ds_N}{dq_N} = \sum_{i=1}^{n} \frac{\lambda L_N {p_N}^2 \ln(v_N)(1 - 2p_N)}{2\phi(2p_N q_N - 1)} \tag{36}$$

$$\frac{dt_N}{dL_N} = \sum_{i=1}^{n} \frac{2\phi(1 - p_N q_N) - L_N \lambda \ln(v_N) p_N q_N (1 - q_N)}{2\lambda \ln(v_N) L_N \phi (2p_N q_N - 1)} \tag{37}$$

$$\frac{ds_N}{dL_N} = \sum_{i=1}^{n} \frac{p_N(q_N - 1)}{2\phi(1 - 2p_N q_N)} \tag{38}$$

Then, the optimal “investment-sharing” strategies of n firms is shown in Proposition 7.

Proposition 7. *Without policy constraints, the optimal "investment-sharing" strategies for any finite number n ($n > 2$) of firms follows the same trend as that of two firms.*

By Proposition 7, the optimal strategies of n firms are consistent with those of two firms in the case of no policy constraint. By computing the derivative of q_N with respect to t_N and s_N, as well as the derivative of L_N with respect to t_N and s_N, the partial derivative expressions of n firms are the same as those of two firms.

In addition, by judging the condition $\frac{d_\pi}{d_n}$, $\frac{d_\pi}{d_n} < 0$ is derived. The utility of firm i with trends in n is shown in Proposition 8.

Proposition 8. *Without policy constraints, for any firm i, its utility decreases as n increases.*

By Proposition 8, cybersecurity information sharing does not yield a scale effect in the case of no policy constraint, which seems to go against common sense. The reason is that if there is no constrain on the investment or sharing threshold, some firms may reduce their cybersecurity investments as a result of over-reliance on cybersecurity information sharing. This “free-riding” behavior would damage those firms that actively engage in sharing actives, even causing the result of blame shifting. As a result, more and more firms choose to avoid sharing especially when the firm number increases, as the benefit of the firm that shares its cybersecurity information would be shared by the others and subsequently lose strength.

8. Conclusions

This paper constructs a game theory model to analyze firms' decision making regarding cybersecurity investment and information sharing. This study examines scenarios both with and without policy constraints, exploring the interactions among key factors such as the value of security information, intrusion loss, and the negative impact coefficient of platform security information disclosure. Through this model, the influencing factors and interrelationships of the cybersecurity information-sharing strategy are elucidated. Subsequently, a cybersecurity information-sharing strategy model for firms is developed, followed by equilibrium analysis. Empirical analysis is conducted on firms, and targeted recommendations are proposed.

Our key findings are as follows: First, firms should balance the interconnected effects of cybersecurity information sharing, investment, economic benefits, and intrusion loss to maximize their utility. Second, cybersecurity investment and information sharing are influenced by changes in the value of security information and intrusion loss and are constrained by their respective marginal utilities. The increase in the value of security information will make firms pay more attention to cybersecurity, thus increasing their willingness to invest and share information. However, as the value of security information continues to increase, its marginal utility may gradually decrease. Third, firms will only increase their cybersecurity investment or information sharing if the marginal utility of security information is positively correlated with these factors. This means that firms will have an incentive to increase cybersecurity investment or share more information only if the additional benefits from acquiring more security information outweigh its costs. Fourth, firms will increase their cybersecurity investments or information sharing if the marginal utility of intrusion loss is positively correlated with these factors. When the marginal utility of intrusion loss is positive, it means that each additional unit of intrusion loss will prompt firms to pay more attention to cybersecurity and increase investment or information sharing.

In examining intrusion loss, our research builds on the classical Gordon–Loeb model from the field of cybersecurity economics. However, the analysis does not consider the impact of different types of hacker attacks on firms' decisions regarding cybersecurity information sharing. Future research could delve into how various attack types, such as random and targeted attacks, influence these decisions, particularly given their differing effects on intrusion probabilities.

Author Contributions: Conceptualization, L.Z. and J.L.; methodology, L.Z. and X.W.; software, L.Z. and X.W.; validation, L.Z., X.W. and H.T.; formal analysis, L.Z. and J.L.; investigation, L.Z. and J.L.; resources, L.Z. and H.T.; data curation, L.Z. and J.L.; writing—original draft preparation, L.Z., X.W. and J.L.; writing—review and editing, L.Z., X.W. and H.T.; visualization, L.Z. and X.W.; supervision, L.Z.; project administration, L.Z.; funding acquisition, L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by Humanities and Social Science Foundation of the Ministry of Education of China, 22YJC630214; and National Natural Science Foundation of China, 71801125; and Jiangsu Social Science Foundation, 23GLLC015.

Data Availability Statement: All data, models, and codes generated or used during this study appear in the submitted article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. *NIST Technical Note 2111*; An Empirical Study on Flow-Based Botnet Attacks Prediction. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020; pp. 1–18. https://doi.org/10.6028/nist.tn.2111.
2. European Union (EU). The NIS2 Directive A High Common Level of Cybersecurity in the EU: EU Legislation in Progress. 2023. Available online: https://cn.overleaf.com/project/679849c8c118b5046c722ba3 (accessed on 8 February 2023).
3. Rashid, Z.; Noor, U.; Altmann, J. Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Future Gener. Comput. Syst.* **2021**, *124*, 436–466. https://doi.org/10.1016/j.future.2021.05.033.
4. Gao, X.; Gong, S.; Wang, Y.; Zhang, Y. Information sharing and security investment for substitutable firms: A game-theoretic analysis. *J. Oper. Res. Soc.* **2024**, *75*, 799–820. https://doi.org/10.1080/01605682.2023.2210594.
5. Hall, J.H.; Sarkani, S.; Mazzuchi, T.A. Impacts of organizational capabilities in information security. *Inf. Manag. Comput. Secur.* **2011**, *19*, 155–176. https://doi.org/10.1108/09685221111153546.
6. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *J. Account. Public Policy* **2003**, *22*, 461–485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001.
7. Stine, K.; Quinn, S.; Witte, G.; Gardner, R. *NIST IR 8286*; Integrating Cybersecurity and Firm Risk Management (erm). National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020; p. 10. https://doi.org/10.6028/nist.ir.8286.
8. Gal-Or, E.; Ghose, A. The economic incentives for sharing security information. *Inf. Syst. Res.* **2005**, *16*, 186–208. https://doi.org/10.2139/ssrn.629282.
9. Lewis, R.; Louvieris, P.; Abbott, P.; Clewley, N.; Jones, K. Cybersecurity information sharing: A framework for sustainable information. In Proceedings of the Twenty Second European Conference on Information Systems, Tel Aviv, Israel, 9–11 June 2014.
10. He, M.; Devine, L.; Zhuang, J. Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Anal.* **2018**, *38*, 215–225. https://doi.org/10.1111/risa.12878.
11. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *J. Account. Public Policy* **2015**, *34*, 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001.
12. Naghizadeh, P.; Liu, M. Inter-temporal incentives in security information sharing agreements. In Proceedings of the 2016 Information Theory and Applications Workshop (ITA), La Jolla, CA, USA, 31 January–5 February 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–8. https://doi.org/10.1109/ITA.2016.7888179.
13. Hausken, K. Information sharing among firms and cyber attacks. *J. Account. Public Policy* **2007**, *26*, 639–688. https://doi.org/10.1016/j.jaccpubpol.2007.10.001.
14. Liu, D.; Ji, Y.; Mookerjee, V. Knowledge sharing and investment decisions in information security. *Decis. Support.* **2011**, *52*, 95–107. https://doi.org/10.1016/j.dss.2011.05.007.
15. Gao, X.; Zhong, W.; Mei, S. Security investment and information sharing under an alternative security breach probability function. *Inf. Syst. Front.* **2015**, *17*, 423–438. https://doi.org/10.1007/s10796-013-9411-3.
16. Goodwin, C.; Nicholas, J.P.; Bryant, J.; McKay, A.; Ciglic, K.; McKitrick, P.; Kleiner, A.; Neutze, J.; Kutterer, C.; Storch, T.; et al. *A Framework for Cybersecurity Information Sharing and Risk Reduction*; Microsoft: Redmond, WA, USA, 2015.
17. Johnson, C.; Badger, L.; Waltermire, D.; Snyder, J.; Skorupka, C. *NIST Special Publication 800-150*; Guide to Cyber Threat Information Sharing; NIST: Gaithersburg, MD, USA, 2016; p. 35. https://doi.org/10.6028/nist.sp.800-150.
18. Chora's, M. Comprehensive approach to information sharing for increased network security and survivability. *Cybern. Syst.* **2013**, *44*, 550–568. https://doi.org/10.1080/01969722.2013.818433.
19. Fransen, F.; Smulders, A.; Kerkdijk, R. Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *Elektrotech. Informationstechnik* **2015**, *132*, 106–112. https://doi.org/10.1007/s00502-015-0289-2.
20. Phan, T.C.; Tran, H.C. Consideration of Data Security and Privacy Using Machine Learning Techniques. *Int. J. Data Inform. Intell. Comput.* **2023**, *2*, 20–32. https://doi.org/10.59461/ijdiic.v2i4.90.
21. Jones, K.I.; Suchithra, R. Information Security: A Coordinated Strategy to Guarantee Data Security in Cloud Computing. *Int. J. Data Inform. Intell. Comput.* **2023**, *2*, 11–31. https://doi.org/10.59461/ijdiic.v2i1.34.
22. Krishna, S.; Paryati. Advancing Cyber Resilience for Autonomous Systems with Novel AI-based Intrusion Prevention Model. *Int. J. Data Inform. Intell. Comput.* **2024**, *3*, 1–7. https://doi.org/10.59461/ijdiic.v3i3.121.
23. Rantos, K.; Spyros, A.; Papanikolaou, A.; Kritsas, A.; Ilioudis, C.; Katos, V. Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers* **2020**, *9*, 18. https://doi.org/10.3390/computers9010018.
24. Tosh, D.K.; Shetty, S.; Sengupta, S.; Kesan, J.P.; Kamhoua, C.A. Risk management using cyber-threat information sharing and cyber-insurance. In *Game Theory for Networks, Proceedings of the 7th International EAI Conference, GameNets 2017, Knoxville, TN, USA, 9 May 2017*; Springer: Cham, Switzerland, 2017; pp. 154–164. https://doi.org/10.2139/ssrn.3475640.

25. Harwood, D.I.; Dahl, E. Barriers to Cyber Information Sharing. Master's Thesis, Naval Postgraduate School, Monterey, CA, USA, 2014. Available online: https://core.ac.uk/download/pdf/36736706.pdf (accessed on 1 December 2014).
26. Kollars, N.A.; Sellers, A. Trust and information sharing: Isacs and us policy. *J. Cyber Policy* **2016**, *1*, 265–277. https://doi.org/10.1080/23738871.2016.1229804.
27. Prieto, D.B. Information sharing with the private sector. History, challenges, innovation, and prospects. In *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*; Cambridge University Press: London, UK, 2016; pp. 404–428. https://doi.org/10.1017/CBO9780511509735.025.
28. Zheng, D.E.; Lewis, J.A. *Cyber Threat Information Sharing: Recommendations for Congress and the Administration*; Center for Strategic and International Studies: Washington, DC, USA; 2015.
29. Tosh, D.K.; Sengupta, S.; Mukhopadhyay, S.; Kamhoua, C.A.; Kwiat, K.A. Game theoretic modeling to enforce security information sharing among firms. In Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 3–5 November 2015; pp. 7–12. https://doi.org/10.1109/cscloud.2015.81.
30. Amini, M.; Bozorgasl, Z. A game theory method to cyber-threat information sharing in cloud computing technology. *Int. J. Inf. Syst. Manag. Syst.* **2023**, *11*, 45–60.
31. Gyenes, R. A voluntary cybersecurity framework is unworkable-government must crack the whip. *Pittsburgh J. Technol. Law Policy* **2013**, *14*, 293. https://doi.org/10.5195/tlp.2014.146.
32. Wu, Y.; Fung, R.Y.K.; Feng, G.; Wang, N. Decisions making in information security outsourcing: Impact of complementary and substitutable firms. *Comput. Ind. Eng.* **2017**, *110*, 1–12. https://doi.org/10.1016/j.cie.2017.05.018.
33. Qian, X.; Yang, W.; Pei, J.; Liu, X.; Pardalos, P.M. A game of information security investment considering security insurance and complementary information assets. *Int. Trans. Oper. Res.* **2021**, *29*, 1791–1824. https://doi.org/10.1111/itor.12972.
34. Wu, Y.; Feng, G.; Fung, R.Y. Comparison of information security decisions under different security and business environments. *J. Oper. Res. Soc.* **2018**, *69*, 747–761. https://doi.org/10.1057/s41274-017-0263-y.
35. Zhao, L.; Liu, J.; Zhu, X. Information security strategy choices of competing firms: autonomous defence or outsourcing. *Intell. Theory Pract.* **2003**, *42*, 94. https://doi.org/10.16353/j.cnki.1000-7490.2019.12.015.
36. Qian, X.; Liu, X.; Pei, J.; Pardalos, P.M. A new game of information sharing and security investment between two allied firms. *Int. J. Prod. Res.* **2018**, *56*, 4069–4086. https://doi.org/10.1080/00207543.2017.1400704.
37. Li, X.;Xue, Q. An economic analysis of information security investment decision making for substitutable firms. *Manag. Decis. Econ.* **2021**, *42*, 1306–1316. https://doi.org/10.1002/mde.3310.
38. Freebuf. 2024 China Data Security Enterprise Panorama. 2024. Available online: https://www.freebuf.com/consult/415083.html (accessed on 12 November 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.