mathematics

MDPI

Article

Cybersecurity Investment Allocation for a Multi-Branch Firm: Modeling and Optimization

Lu Xu [1], Yanhui Li [1,*] and Jing Fu [2]

[1] School of Information Management, Central China Normal University, Wuhan 430079, Hubei, China
[2] Institute of Agricultural Economy and Technology, Hubei Academy of Agricultural Sciences, Wuhan 430064, Hubei, China
* Correspondence: yhlee@mail.ccnu.edu.cn

Received: 6 May 2019; Accepted: 28 June 2019; Published: 1 July 2019

Abstract: Network interconnection and information sharing among firms and their departments expose them to cybersecurity breaches. Traditional cybersecurity studies have paid little attention to the reallocation of security investment within firms. This paper proposes a mathematical model for optimal allocation of cybersecurity investment among headquarters and branches with budget constraints. The differences in size of information sets and system interconnection have been taken into account. The responses of optimal allocation to internal and external factors, such as the portion of branch information set, the propagation probability, the budget constraints, and the intrinsic vulnerability, have been studied in deep both theoretically and numerically. Analysis results indicate that the group will give priority to protecting headquarters when the total budget is small and intrinsic vulnerability is high. The security investment allocated to each branch increases with budget, propagation probability and portion of information set, but never exceeds $1/(n+1)$ of total budget. Numerical simulations also verify that security information sharing among headquarters and branches can help improve the efficiency of security investment in the whole system. Furthermore, the findings of this paper will draw attention to the reallocation of cybersecurity investment within a business group and help cybersecurity managers to develop investment allocation strategies and policies.

Keywords: cybersecurity; investment allocation; budget constraints; optimization

1. Introduction

The Internet of Things and communication networks have promoted the development of the network economy. However, the network interconnections also increase indirectly the probability of cybersecurity breach. It has been estimated that the global average cost on information breaches and the loss of mega data breaches are up to $3.86 million and $350 million, respectively [1]. New legislation and regulations, such as the General Data Protection Regulation (GDPR), the National Cyber Incident Response Plan (NCIRP), and People's Republic of China Network Security Law (PRCNSL), have been issued to urge firms to take cybersecurity measures. Hence, it is significant for firms to increase cybersecurity investments to avoid unnecessary losses. As we all know, there is no completely secure network environment with increasing reliance on network interconnection and information sharing [2,3]. Therefore, the optimal investment on cybersecurity has been investigated based on decision theory and economics model to reduce potential losses and security risks by taking the environmental factors, such as the network vulnerability and hacker attack types, etc. into account [4–7].

Interdependent firms and branches interconnect their databases or share information to improve the efficiency of information exchanges [8,9], which in turn would expose the participating firms

or branches to security risks. On the one hand, participating firms or branches physically connect to each other through a mutual trust network or interface, and the other information systems will become vulnerable if any of them are compromised by hackers, which makes it easier for hackers to penetrate their systems via mutual trusted IT infrastructure, e.g., local area networks (LANs) and wide area networks (WANs), and steal sensitive data [10,11]. For example, Cainiao, the logistic arm of Alibaba, run the largest logistics database all over the world by establishing a platform integrating information resources of third-party logistics systems [12]. Cainiao's centralized data platform connects its logistics parties and E-commerce merchants to integrate trading, tracking and shipping operations, which makes it possible for hackers to invade the system immediately after breaking its third-party logistics or merchants with weak cybersecurity. On the other hand, the cooperation and mutual benefit for production innovation or value creation can be achieved by information sharing, while the shared information will also be accessed once any systems on the platform are compromised by hackers. For example, a logistics server breached by hackers result in not only direct losses of the logistics department, but also indirect leakage of the partner's order information. Obviously, the more information shared, the more information loss interdependent firms or branches suffer.

It should be noted that security breaches often occur in chain enterprises with many sub-branches and members, such as chain hotels, big banking groups and aviation groups. BBC News reported that the two hacking attacks on Hilton Hotels Corporation exposed more than 360,000 credit cards and other information to risks, and Hilton Hotels Corporation was fined $700,000 at that time, which would be $420 million under GDPR [13]. The customer data were revealed from a hotel system in UK belonging to the company, and then its brands and franchises were affected by the attack without exception. Coincidentally, there were several companies suffering similar information leakage incidents, such as HSBC Bank [14], the Canadian Imperial Bank [15], and Cathay Pacific [16], who shared customer information with all their branches. Therefore, it is necessary for both headquarters and its branches to improve the level of cybersecurity to avoid losses' expansion. Considering the bidirectional indirect information breach among headquarters of a group firm and its branches, the servers of the headquarters and its branches are usually interconnected to facilitate more efficient business operations. Once hackers or virus attack the server of one branch, the information system of headquarters might be accessed and penetrated. In addition, the information assets of all branches are actually backed up in the headquarters system, which might also be revealed if the information system of headquarters is exposed to the risks.

Previous studies mainly focused on optimizing security investment in terms of system interconnection and information sharing among homogeneous firms [5,11,17]. Considering the fact that there are limited budgets on security investment which are often at a disadvantage when competing with that on other investment projects [18], one must allocate optimally the limited budgets to all branches including headquarters to achieve the highest cybersecurity gains, which, as authors known, is rarely mentioned in previous studies. Trying to fill the research gaps, a mathematical model is developed in this paper to investigate the optimal allocation of security investment among headquarters and its n-branches with budget constraints. The indirect risks of security breaches introduced by the interconnection of information systems among headquarters and branches are taken into account. In addition, the influence of security information sharing on the allocation of security investments is also analyzed via numerical simulation. Our analysis produces the following interesting findings: When the budget is small while intrinsic vulnerability is larger relatively, the firm will give priority security investment to headquarters. The allocation on branches is positively correlated to propagation probability and almost proportional to budget, but never exceed $1/(n+1)$ of the total budget, while that decreases with intrinsic vulnerability. Security information sharing can bring positive investment gains to headquarters and branches, which is conducive to improving the security level of the whole system under the same budget.

The rest of the paper is organized as follows. Section 2 reviews the literature on the studies of the independent and interdependent security investment and allocation. In Section 3, the mathematical

model is established to describe the security investment among headquarters and its branches in a business group under the bidirectional propagation risks and budget limitation. Then, the optimal allocation of cybersecurity investment is derived and analyzed in Section 4. Section 5 extends the model to consider the impact of security information sharing. Section 6 summarizes the conclusions and provides managerial implications.

2. Related Literature

Since the 1990s, cybersecurity investment has attracted extensive research interests with the rapid development of internet and information technology [19].

2.1. Independent Cybersecurity Investment

Research on cybersecurity investment for a single organization has first aroused widespread concern in the field of cybersecurity, which can be divided into two streams. One stream focuses on security investment with the decision analysis and expected utility theory. These two methods are usually used to consider the optimal security investment by maximizing returns or minimizing costs. One needs to note that the "return" of security investment is regarded as the reduction in expected security risk by some researchers [20–22]. The "return" function can be expressed as (likelihood of breaches without investment–likelihood of breaches with investment) * (potential losses) − (costs of security investment), which originally derived from the study of Gordon and Loeb [7]. They have proposed a mathematical model to optimize cybersecurity investment by two security breach probability functions. Since then, studies on security investment have constantly emerged. For example, Hausken [6] presented four analyses towards marginal returns of security investment, and concluded that the optimal investment is no longer capped at 1/e of potential loss, which is different from the findings of the study of Gordon and Loeb [7]. Huang et al. [5] explored the relationship between information vulnerabilities and investment effectiveness for a risk-averse firm. Furthermore, the impacts of potential losses and system sensitivity on optimal security investment has also been studied from the perspective of health information exchange [23].

The other stream is based on the game-theoretic approach to analyze the decisions and reactions between rational decision-makers, such as firms and attackers. Game theory is an efficient way to study the behavioral interactions in the field of cybersecurity, in which firms try to protect their information assets and the attackers intend to access or destroy proprietary information [24–26]. However, in these studies, the utility function of attacker is hard to quantify, thus some scholars have combined game theory with algorithmic simulation to address this problem. For example, Kantzavelou and Katsikas [27] applied game theory to intrusion detection systems to cope with internal attacks by a detailed game-based detection algorithm. Based on game theory and combinatorial optimization, a mathematical model of interaction between the endogenous organization's and attackers' decisions has been proposed, and a Knapsack algorithm were adopted to derive optimal investment strategies [28]. These studies on security investment of single organization have laid the theoretical foundation for security investment optimization and provide some insights for the model of this paper.

2.2. Interdependent Cybersecurity Investment

As the network economy develops, the information interaction and transmission among firms have become the hot point of cybersecurity. The cybersecurity problem among interconnected firms could be seen as the typical interdependent security (IDS) problem, proposed firstly by Kunreuther and Heal [29], who conducted a case study of security investment behaviors among firms in airline security and found that there is a "free-riding problem" of firms' security investment, also denoted as negative externality. Later, some research committed to solving such a negative external issue [10,17,30,31]. For example, Zhao, Xue, and Whinston [9] explored the effects of three risk management methods including cyberinsurance, managed security services (MSSs), and risk pooling arrangements (RPAs)

in addressing the investment inefficiency, and the results showed that MSSs has the best effect on security risk management, followed by RPAs and cyberinsurance. Wu et al. [17] focused on the impacts of attack types and network vulnerabilities on security investments, and examined three economic incentives for solving security underinvestment among interconnected firms. A differential game model was established to study the impact of interdependence of security investments between firms and strategic attackers [32]. Previous studies on interdependent security investment were mostly carried out between firms, while security investment within a firm has rarely been discussed. Furthermore, the interdependent firms are mostly assumed as homogeneous or symmetric. However, interconnected firms are usually the firms with different businesses and even scales. For example, IKEA allows Amazon Alexa and Apple HomeKit to access its smart lighting systems [33], but they belong to different industries with different scales. The investments they spend on information system security, and the losses they will suffer are both different. Thus, we take heterogeneous interdependent departments within a firm as the research objects to consider the optimal allocation with a limited security budget.

2.3. Allocation of Security Investment

The issues on security investment allocation has not been sufficiently studied. There are only a handful of studies that focus on addressing the allocation of budgetary resources among independent firms. For example, Bodin, Gordon, and Leob [34] adopted an Analytic Hierarchy Process (AHP) to determine the optimal security allocation with budget constraints between two firms for improving the security level of information systems. An economics model of security investment was proposed by Huang and Behara [35] to study security investment allocation against simultaneous heterogeneous attacks. Schilling and Werner [36] established a combinatorial optimization model to maximize the security level of systems, by which the best combination of security controls can be derived with available budgets, and verified through case studies.

Our review of literature shows that the optimized combination for specific security strategies has been studied with fixed budgets, but the issue of reallocation within a firm is ignored. The internal allocating control with budgetary constraints is closely related to the investment efficiency of a firm. Therefore, to address the research gaps, this paper proposes a security investment model to obtain an optimal security allocation with limited budget among headquarters and branches within a business group.

3. Model Description

We consider a multi-event model for cybersecurity investment with budget constraints among a headquarters and its n branches, where $n \geq 2$. To simplify the analysis, it is assumed that the branches are homogeneous regardless of the influence of specific business on its security investment. Information systems of headquarters and branches interconnect via trusted networks or interfaces. The notations and functions of the model are summarized in Table 1.

3.1. Values of Information Set

The threat of hacking to information sets is considered based on the study of Gordon and Loeb et al. [7]. They believe that the information set exist in many forms, including customers' information, financial data, strategic plans, etc. Exposure of the essential data about the firm's operations to competitors or illegal traders could cause not only direct economic losses, but also serious consequences of damage to reputation and customers churn. In fact, in order to facilitate management, headquarters often backs up all information of branches and itself. Each branch, of course, also stores its own information. The loss of total information is represented as L, and the information proportion of each branch is accounted by α, where $\alpha < 1/(n+1)$ indicates that headquarters has more information data than its branches.

Table 1. Summary of notations.

Notation	Name	Conditions
Parameters		
n	Number of branches	$n > 2$
v	System intrinsic vulnerability	$0 < v < 1$
K	Total security budget	$K = K_a + \sum_i K_{bi}$
p	Direct breach probability	$p(v, K_i)$
μ	Effectiveness parameter of security investment	$0 \leq \mu \leq 1$
q	Propagation probability	$0 < q < 1$
L	The loss of total information	$L > 0$
α	Proportion of branch's information set	$\alpha(n+1) < 1$
β	Benefit rate of security information sharing	$0 \leq \beta \leq 1$
Decision variables		
K_a	Security investment of headquarters	$K_a \geq 0$
K_b	Security investment of each branch	$K_b \geq 0$
Function		
C	Total cost function without security information sharing	$C \geq 0$
C_s	Total cost function with security information sharing	$C_s \geq 0$

3.2. Direct Breach

As shown in Figure 1, the firms of the system are usually breached directly by hackers or implicated indirectly by interconnected ones. The direct breach is often caused by a direct attack on a branch or headquarters through spam, malware, and phishing websites, etc. The direct breach probability in this paper follows previous studies [7,17,35] and is expressed as $p(v, K_i)$, which is determined by intrinsic vulnerability and investment amount, and the attack probability is implicitly assumed and omitted in the following. The intrinsic vulnerability v expresses the success probability of an attack without security protection, which is usually a constant associated with the physical characteristics of a system and its network topology [37]. Noted that there is no invulnerable information system, and a completely vulnerable information system can be regarded as an open system, such as the price and quarter information system of listed companies in the last quarter. Thus, $0 < v < 1$. The chance of a hacker attacking any information set is assumed to be the same, regardless of his strategic behaviors.

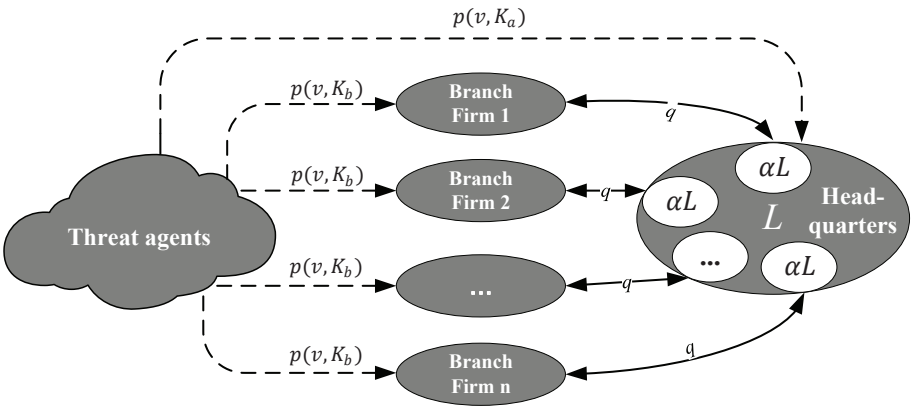

Figure 1. Conceptual model of cybersecurity.

The investment actions can be taken in many forms, such as antivirus or anti-malware software, firewalls, intrusion prevention systems, and staff training, etc. It is denoted that K_a and K_{bj} are the investment of headquarters and the j-th branch, respectively, and $K = K_a + \sum_j K_{bj}$. is the total budget

limitation for the group. The information breach probability function adopts classical exponential model [5,7,17],

$$p(v, K) = v^{\mu K+1}, \tag{1}$$

where the constant μ ($0 \leq \mu \leq 1$) measures the effectiveness of security investment. Some boundary conditions can be easily drawn from the breach probability. The increase in security investment will reduce the breach probability following the law of diminishing marginal returns ($\partial p/\partial K_i < 0, \partial^2 p/\partial {K_i}^2$, $\forall K_i$). Specifically, the application of large-scale hardware and useful software can rapidly improve the level of security when a firm begins to invest in cybersecurity. However, as security measures become increasingly complete, the impact of increasing investment on the breach probability will not be obvious at the current technical level. If the group firm does not make any security invesment, the direct breach probability will be determined by the intrinsic vulnerability, i.e., $p\,(v, 0) = v$.

3.3. Indirect Breach

A group suffers information breach caused by not only direct hacking attacks, but also indirect infection from other interconnected members. Indirect breach occurs when a branch firm is attacked successfully; the hackers might penetrate the connections and break into the headquarters information systems as shown in Figure 1. In contrast, if the headquarters system is compromised, each of the branch firms connected to it has the possibility of information breach due to the spreading. We assume that the probability of the indirect attack propragation is a constant q ($0 < q < 1$) mainly determined by the extent of mutual trust and empowerment among headquarters and branches. Each node firm can reduce its own direct breach probability, but cannot change the propagation probability.

All of the homogeneous branches invest the same amount for cybersecurity and bear the same probability of information breach. We use p_a and p_b to represent the direct breach probability of headquarters and each branch, respectively. Thus, the breach probability of the headquarters is $1-(1-p_a)(1-qp_b)^n$ including the direct hacker attacks and indirect infections from n branches. Note that, when headquarters is breached, information of all branches is leaked, resulting in a loss of $(1-(1-p_a)(1-qp_b)^n)L$. Losses of information breaches of branches should be considered when headquarters information is secure. Hence, the conditional breach probability of each branch is $p_b\,(1-q)\,(1-qp_b)^{n-1}\,(1-p_a)$. The loss of all branches and headquarters should both be taken into consideration. Therefore, the total expected cost can be expressed as

$$C = (1-(1-p_a)(1-qp_b)^n)L + np_b(1-q)(1-qp_b)^{n-1}(1-p_a)\alpha L + nK_b + K_a. \tag{2}$$

4. Optimal Allocation of Cybersecurity Investment

Since branches are assumed to be homogeneous, we have $K_{bj} = K_b$, for $i = 1, \ldots, n$. Substituting $K_a = K - nK_b$ into (1) and (2), we get

$$C\,(K_b) = (1-(1-p(K-nK_b))(1-qp\,(K_b))^n)L + np\,(K_b)\,(1-q)(1-qp\,(K_b))^{n-1}(1-p(K-nK_b))\alpha L + K. \tag{3}$$

Proposition 1. *$K \geq ln\left(\frac{\alpha(q-1)(nqv-1)-q^2v+q}{v\alpha(q-1)(n-1)-qv+1}\right)/\mu lnv$ is the necessary and sufficient condition for the existence and uniqueness of optimal allocation. Morever, when $v > (\alpha-1)/((nq-n+1)\alpha-q)$ and $K < ln\left(\frac{\alpha(q-1)(nqv-1)-q^2v+q}{v\alpha(q-1)(n-1)-qv+1}\right)/\mu lnv$, the group does not allocate the information security budget to its branch firms.*

Proof. Then, the optimal investment allocation of a branch can be obtained by minimizing the cost function of (3). The concavity and convexity of the cost function are not considered for the time being, thus the extreme point can be obtained by first-order condition as follows:

$$\frac{\partial C(K_b)}{\partial K_b} = \left(1 - qv^{K_b\mu+1}\right)^{n-2} \ln(v)\, n\mu L \left(\begin{array}{l} \left(-v^{K_b\mu+1}\alpha(q-1)(n-1) - \left(1 - qv^{K_b\mu+1}\right)\right) v^{\mu(-K_b n+K)+1} \\ + \left(\alpha(q-1)\left(v^{K_b\mu+1}nq - 1\right) + \left(1 - qv^{K_b\mu+1}\right)q\right) v^{K_b\mu+1} \end{array} \right) = 0, \quad (4)$$

where $\left(1 - qv^{K_b\mu+1}\right)^{n-2} \ln(v)\, n\mu L < 0$ during $K_b \in [0, K/n\,]$. The solution of the first-order condition is determined by the following:

$$\begin{aligned} R(K_b) = &\left(-v^{K_b\mu+1}\alpha(q-1)(n-1) - \left(1 - qv^{K_b\mu+1}\right)\right) v^{\mu(-K_b n+K)+1} \\ &+ \left(\alpha(q-1)\left(v^{K_b\mu+1}nq - 1\right) + \left(1 - qv^{K_b\mu+1}\right)q\right) v^{K_b\mu+1} = 0. \end{aligned} \quad (5)$$

To find the possible extreme point of the cost function, we derive:

$$\frac{\partial R(K_b)}{\partial K_b} = \left(\begin{array}{l} \left(((q-1)(n-1)\alpha - q)(n-1)\, v^{K_b\mu+1} + n\right) v^{\mu(-K_b n+K)+1} \\ + \left(\left(2(\alpha n(q-1) - q)\, qv^{K_b\mu+1} + (1-q)\alpha + q\right)\right) v^{K_b\mu+1} \end{array} \right) ln(v)\, \mu. \quad (6)$$

Before judging the sign of (6), we need to compare the sizes of $v^{\mu(-K_b n+K)+1}$ and $v^{K_b\mu+1}$. According to (4), we get

$$v^{\mu(-K_b n+K)+1} = \frac{v^{K_b\mu+1}\left(qn(\alpha(q-1) - q)\, v^{K_b\mu+1} + (1-q)\alpha + qn\right)}{((q-1)(n-1)\alpha - qn)\, v^{K_b\mu+1} + n} \quad (7)$$

and then

$$v^{\mu K_b^*+1}q - v^{\mu\left(-nK_b^*+K\right)+1} = \frac{-v^{\mu K_b^*+1}\alpha(q-1)\left(v^{\mu K_b^*+1}q - 1\right)}{((q-1)(n-1)\alpha - qn)\, v^{\mu K_b^*+1} + n}. \quad (8)$$

It is clear to see that the right side of the above formula is negative, and, immediately, the relationship between the breach probability of headquarters and branch is

$$v^{\mu K_b^*+1}q < v^{\mu\left(-nK_b^*+K\right)+1}. \quad (9)$$

Furthermore, substituting (9) into (6), we get

$$\begin{aligned} \frac{\partial R(K_b)}{\partial K_b} &< \left(\begin{array}{l} \left(((q-1)(n-1)\alpha - q)(n-1)\, v^{K_b\mu+1} + n\right) qv^{K_b\mu+1} \\ + \left(\left(2(\alpha n(q-1) - q)\, qv^{K_b\mu+1} + (1-q)\alpha + q\right)\right) v^{K_b\mu+1} \end{array} \right) ln(v)\, \mu \\ &= ln(v)\, \mu v^{K_b\mu+1}\left(\left(\left(n^2+1\right)(q-1)\alpha - q(n+1)\right) qv^{K_b\mu+1} + (n-\alpha+1)q + \alpha\right) < 0, \end{aligned} \quad (10)$$

which indicates that $R(K_b)$ is monotonic. If the solution of $R(K_b)$ exists, it must be unique, that is, the total cost function has at most one extreme point in $K_b \in [0, K/n\,]$. Next, we discuss whether this point is the optimal allocation in two cases respectively (existence of optimal solution).

Case 1: $\partial C(K_b)/\partial K_b \leq 0$ at $K_b = 0$. In practice, firms will never begin to protect their information systems if they suffer negative returns at the first security investment, i.e., the marginal benefit of the security investment should be greater than the marginal cost [5]. The return here can be regarded as the relative reduction of cost function when increasing investment in information security, so $\partial C(K_b)/\partial K_b \leq 0$ at $K_b = 0$ is beneficial for group's security investment decision. Then, the derivative of the cost function at the right boundary $K_b = K/n$ is given by

$$\frac{\partial C(K/n)}{\partial (K/n)} = \begin{pmatrix} \alpha v^{\mu K/n+1}(1-q)\left(v^{\mu K/n+1}nq - nv + v - 1\right) \\ +\left(1 - qv^{\mu K/n+1}\right)\left(qv^{\mu K/n+1} - v\right) \end{pmatrix} \left(1 - qv^{\mu K/n+1}\right)^{n-2} ln(v)\, n\mu L. \quad (11)$$

Obviously, $C'(K/n)$ is always greater than zero. At this time, $C'(0) < 0$ can be expressed as

$$\begin{pmatrix} (-v\alpha(q-1)(n-1) - (1-qv))\, v^{K\mu+1} \\ +(\alpha(q-1)(nqv-1) + (1-qv)q)\, v \end{pmatrix} (1-qv)^{n-2} L \ln(v)\, n\mu < 0. \quad (12)$$

The cost function decreases at the left boundary and increases at the right boundary of $K_b \in [0, K/n]$, thus there must be at least one minimum. The minimum must be unique in this domain because the cost function has at most one extreme. Therefore, the existence and uniqueness of optimal allocation to branches is proved. Furthermore, the condition can be derived from (12):

$$K > K_0 = \frac{\ln\left(\frac{\alpha(q-1)(nqv-1) - q^2v + q}{v\alpha(q-1)(n-1) - qv + 1}\right)}{\mu \ln(v)}. \quad (13)$$

When $C'(0) = 0$, the optimal security investments of headquarters and branch are exactly $K_b^* = 0$ and $K_a^* = K$, respectively.

Case 2: $\partial C(K_b)/\partial K_b > 0$ at $K_b = 0$. In contrast to Case 1, the group invests the first dollar in branches' security, and the security cost will increase. According to $C'(K/n) > 0$ given by Case 1, the total cost function increases at the left and right boundaries of $K_b \in [0, K/n]$. If the minimum cost exists, the number of optimal solutions must be no less than two, which conflicts with the uniqueness of solution. Therefore, the cost function will increase with K_b in $K_b \in [0, K/n]$, and the minimum cost will be obtained at $K_b^* = 0$ and $K_a^* = K$.

The above analysis shows that $K > K_0$ is the sufficient and necessary condition for the existence and uniqueness of the optimal allocation to branches, that is, if only $K > K_0$, $K_b > 0$. Noted that if $K_0 > 0$, i.e., $v > (\alpha - 1)/((nq - n + 1)\alpha - q)$, information security budget would be allocated to each branch only when $K > K_0$, while $K \geq 0$ is always established if $v \leq (\alpha - 1)/((nq - n + 1)\alpha - q)$. According to the above analysis, we arrive at the following proposition. If only $v > (\alpha - 1)/((nq - n + 1)\alpha - q)$ and $K < K_0$, the group will not allocate the security investment to branches. Proposition 1 is proved. □

Proposition 1 reveals that, if the intrinsic vulnerability is high enough while total security budget is relatively small ($K < K_0$), the group would give priority allocation to its headquarters. Conversely, if the intrinsic vulnerability is sufficiently low for $K_0 < 0$, $K > K_0$ always stand up and then the group will always invest in information security for all its headquarters and branches. It is clear that under extremely tight budgetary and external conditions, the most of the budget will be used for the security risk management of headquarters to minimize potential losses due to the fact that it stores all data of the whole information system. Security investment and breach probability satisfy the property of diminishing marginal benefit, and the breach risk of headquarters is low enough to be insensitive to security investment when intrinsic vulnerability is small. Therefore, the group will achieve more security returns by allocating part of the budget to branches, which, in practice, implies that intrinsic vulnerability of the system deserves attention and a sufficient security budget is also necessary if the group expects to achieve a higher level of information security because of the inevitable interaction of subsystems and the information liquidity under interconnected network.

On the basis of the boundary condition above, the optimal investment level ("*"in this paper indicates the optimal allocation of security investment with given budget.) K_b^* is subject to (4) and the proportion of it in the total budget, i.e., K_b^*/K, will be explored. The relationship between

K_b^* or K_b^*/K with related factors, such as the proportion of information assets α, the propagation probability q, the budget constraints K, and the intrinsic vulnerability v, etc., is significant in practical decision-making. Since it is difficult to give the analytical solution of K_b^* from (4) directly, the implicit function analysis method is adopted in the following study. At this point, the parameter x $(x = \mu, v, K, \alpha)$ and the optimal investment ${K_b}^*$ can be determined by the implicit function of $R\left(x, K_b^*\right) = 0$. The derivative of the K_b^* to x can be obtained [38].

4.1. The Proportion of Branch Information Set

Next, we analyze the relationship of the optimal allocation K_b^*/K with the proportion of branch information set α in the whole group. The following proposition is given first.

Proposition 2. *The optimal security investment for each branch K_b^* increases with the proportion of branch information set α.*

Proof. The relationship between $alpha$ and K_b^* can be solved from (4) as follows:

$$\alpha = \frac{n\left(v^{\mu K_b^*+1}q-1\right)\left(v^{\mu K_b^*+1}q-v^{\mu\left(-nK_b^*+K\right)+1}\right)}{(q-1)\left((1-n)\,v^{\mu\left(-nK_b^*+K\right)+1}+v^{\mu K_b^*+1}nq-1\right)v^{\mu K_b^*+1}}. \tag{14}$$

According to the above condition $v^{\mu K_b^*+1}q < v^{\mu\left(-nK_b^*+K\right)+1}$, it is obvious that the molecule on the right side of (14) is positive. Combining $\alpha > 0$ and $q < 1$, breach probability of headquarters and branch also satisfies

$$(n-1)v^{\mu\left(-nK_b^*+K\right)+1} - nqv^{\mu K_b^*+1} + 1 > 0. \tag{15}$$

Following the principle of derivation of implicit function $\frac{\mathrm{d}K_b^*}{\mathrm{d}\alpha} = -\frac{\partial R/\partial\alpha}{\partial R/\partial K_b^*}$, $\frac{\partial R}{\partial K_b^*} < 0$ given by (10), and $sign\left(\frac{\mathrm{d}\,K_b^*}{\mathrm{d}\,\alpha}\right) = sign\left(\frac{\partial R}{\partial\alpha}\right)$. The first order partial derivative of (5) with respect to α can be expressed as

$$\frac{\partial R}{\partial\alpha} = (1-q)\left((n-1)\,v^{\mu\left(-K_b^*n+K\right)+1} - v^{K_b^*\mu+1}nq+1\right)v^{K_b^*\mu+1}. \tag{16}$$

It is easy to obtain that (16) is greater than zero. Thus, $\frac{\mathrm{d}K_b^*}{\mathrm{d}\alpha} > 0$ is established, and then Proposition 2 is proved. □

To present Proposition 2 intuitively, Figure 2 shows numerically the relationship of the optimal allocation of security investment on each branch K_b^*/K with the proportion of branch information set α under $q = 0.5$, $n = 10$, $v = 0.5$, $\mu = 0.000005$, $L = \$1.5$ M, $K = 0.25L$ (As of 2018, the cost of a data breach study by Ponemon shows that the United States and the Middle East respectively spend \$1.76 million and \$1.47 million—the most on post data breach response activities [1]. We take the median of the two numbers as an example of numerical simulation, and let $L = \$1.5$ M. Gorden and Leob [7,39] suggested that the optimal cybersecurity investment will not exceed 37% of potential losses. In practice, this proportion will be less, according to a breach survey of U.K. Department for Digital, Culture, Media & Sport [40]. This paper sets the security budget as 25% of potential losses.), and $\alpha < 1/(n+1)$. Proposition 2 and the numerical result both indicate that the optimal security investment and its allocation K_b^*/K for given budget increase continuously with the proportion of its information set. The result accords with our intuition. The more valuable information stored in branch firms, the greater the potential loss it will suffer, and it is necessary to reduce the information risk by increasing the allocation of security investment to branches.

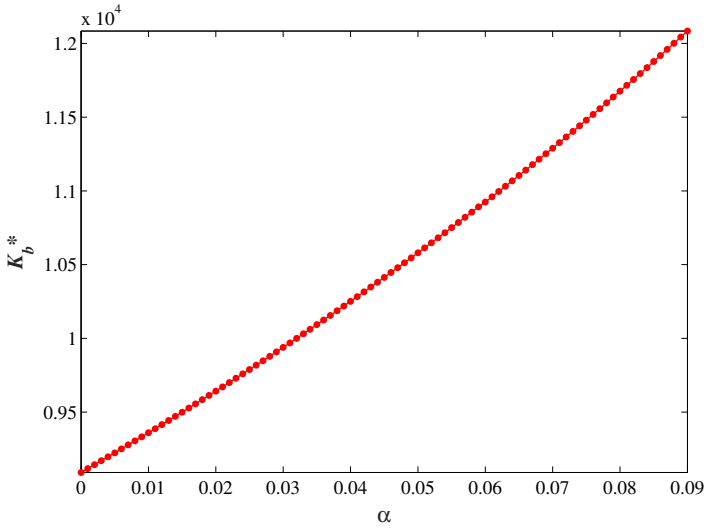

Figure 2. Optimal security investment allocation of each branch over the proportion of branch information set.

4.2. Propagation Probability

Proposition 3. *If* $q < q_0 = \frac{b+\sqrt{(-4\alpha cnv^2+4cv^2+b^2)}}{(-2\alpha n+2)v^2}$, *where* $b = (-(n-1)\alpha+1)v^{\mu K+2} + (-n\alpha v-\alpha+1)v$ *and* $c = (-1-(-n+1)\alpha v)v^{K\mu+1}+\alpha v$, *the group would not allocate cybersecurity funds to branches. The optimal cybersecurity investment of a branch* K_b^* *increases and approaches* $K/(n+1)$ *with propagation probability* q *when* $q > q_0$.

Proof. Since $-\partial R/\partial K_b^* > 0$ in (10), the sign of $\partial K_b^*/\partial q$ is determined by $\partial R/\partial q$, which is

$$\frac{\partial R}{\partial q} = v^{\mu {K_b}^*+1}\left((1+(-n+1)\alpha)v^{\mu(-{K_b}^*n+K)+1}+(\alpha(2q-1)n-2q)v^{\mu {K_b}^*+1}-\alpha+1\right). \quad (17)$$

Let $g = (1+(-n+1)\alpha)v^{\mu(-{K_b}^*n+K)+1}+(\alpha(2q-1)n-2q)v^{\mu {K_b}^*+1}-\alpha+1$ for convenience, then it is apparent that

$$sign\left(d{K_b}^*/dq\right) = sign\left(\partial R/\partial q\right) = sign\left(g\right). \quad (18)$$

As $v^{\mu K_b^*+1}q - v^{\mu\left(-nK_b^*+K\right)+1} < 0$ according to (9), we can obtain

$$g > (((n+1)q-n)\alpha-q)v^{\mu {K_b}^*+1}-\alpha+1 > (q-1)(\alpha n+\alpha-1) > 0. \quad (19)$$

Therefore, $\partial K_b^*/\partial q > 0$, i.e., the optimal allocation of cybersecurity budget to branches will increase with the propagation probability. Substituting $K_b^* = 0$ into $R(q, K_b^*) = 0$, we can obtain the lowest propagation probability that the group begins to consider for investing in the cybersecurity of branches:

$$q_0 = \frac{b+\sqrt{(-4\alpha cnv^2+4cv^2+b^2)}}{(-2\alpha n+2)v^2}, \quad (20)$$

where $b = (-(n-1)\alpha+1)v^{\mu K+2}+(-n\alpha v-\alpha+1)v$ and $c = (-1-(-n+1)\alpha v)v^{K\mu+1}+\alpha v$. Since K_b^* monotonically increases with q, the group will allocate all its budget to headquarters at $q \in [0, q_0]$, and the upper limit of security investment allocated to each branch can be calculated by substituting $q = 1$ into $R(q, K_b^*) = 0$ and simplifying it as

$$n\left(v^{K_b*\mu+1}-1\right)\left(v^{\mu(-K_b*n+K)+1}-v^{K_b*\mu+1}\right) = 0. \quad (21)$$

The upper limit of $K^*{}_{b0} = K/(n+1)$ can be easily obtained from (21). □

Figure 3 numerically analyzes the response of optimal security allocation to propagation probability considering different numbers of branch under $v = 0.5$, $\mu = 0.000005$, $L = \$1.5\,\mathrm{M}$, $K = 0.25L$, and $\alpha < 1/(n+1)$. We can see that, with the increase of propagation probability q, the cybersecurity of branches has been paid more and more attention. If $q < q_0$, the risks caused by indirect breach from branches are not enough to attract sufficient attention from the overall situation, thus the group does not invest in branches' security. The internal security risks have grown in the real network environment when the systems of headquarters and its branches are more interconnected and exposed. Then, there are more channels and ways for the intruders to launch attacks, and more investment is required accordingly. Figure 3 also illustrates that, when ${K_b}^* > 0$, ${K_b}^*$ decreases with increasing n, which simply means that the more branches there are in the group, the less security investment each branches will obtain, while the security information investment in its headquarters has been always guaranteed. We also see that, consistent with common sense, K_b^* gradually approaches $K/(n+1)$ as q increases, which indicates that the amount of security investment allocated to headquarters is always higher than that allocated to each branch, and although the investment proportion of headquarters will decrease as the number of branches increases, it is still higher than the average level of $1/(1+n)$.

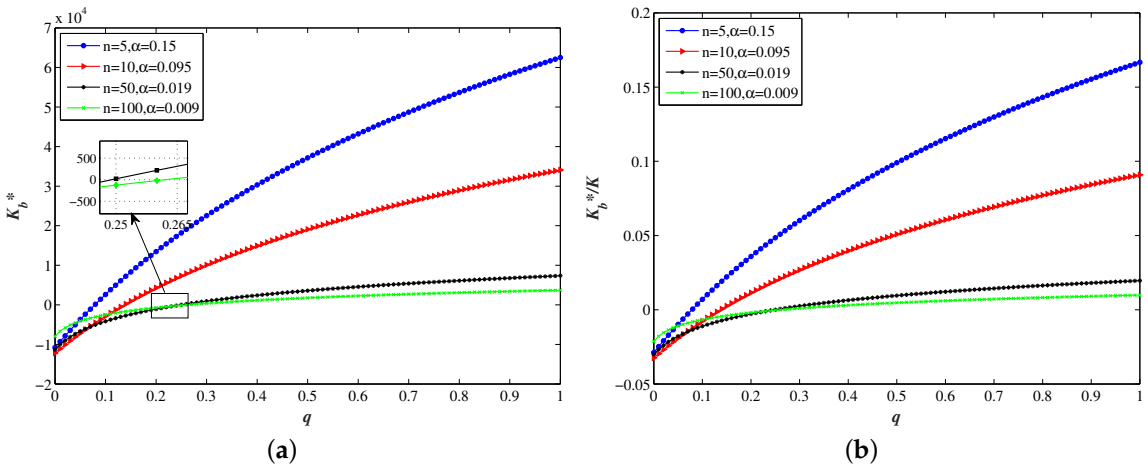

Figure 3. Optimal security investment and its allocation over propagation probability.

4.3. Total Budget Constraints

Next, the relationship between the total investment budget K and optimal security investment of each branch K_b^* will be investigated.

Proposition 4. *The cybersecurity investment of each branch K_b^* increase almost linearly with the total security budget K, and its proportion K_b^*/K approach to $1/(1+n)$ with decreasing rate.*

Proof. The first-order derivative of $R(K, K_b^*)$ to K can be solved from (7) as follows:

$$\frac{\partial R}{\partial K} = -v^{\mu(-{K_b}^* n+K)+1}\mu ln v\left(1+\left((q-1)(n-1)\alpha - q\right)v^{{K_b}^*\mu+1}\right), \tag{22}$$

which is obviously greater than zero. Similar to the proof of Proposition 3, it is clear to see that $\partial K_b^*/\partial K > 0$ according to (10), which indicates that K_b^* increases monotonously with K.

Solving the equation of $R(K, K_b^*) = 0$ about K, we obtain the relationship of K with ${K_b}^*$ as

$$K = A + K_b^*(n+1), \tag{23}$$

where $A = \frac{\ln\left(\frac{qv\,K_b^{*\mu+1}(n(q-1)\alpha-q)+(1-q)\alpha+q}{1+((q-1)(n-1)\alpha-q)v\,K_b^{*\mu+1}}\right)}{\mu \ln v}$ monotonically increases with K_b^*. It is easy to obtain that the range of A is $[\frac{\ln\left(\frac{qv(n(q-1)\alpha-q)+(1-q)\alpha+q}{1+((q-1)(n-1)\alpha-q)v}\right)}{\mu \ln v}, \frac{\ln((1-q)\alpha+q)}{\mu \ln v}]$, which is very small and can be negligible relative to K_b^* $(n+1)$. Therefore, K_b^* is approximately proportional to K with the ratio of $1/(n+1)$. With the increasing of K, A is close to the constant $\ln((1-q)\alpha+q)/\mu \ln v$, and the linear relationship between K_b^* and K is more obvious. From (23), the investment proportion of each branch can be expressed as

$$\frac{K_b^*}{K} = \frac{1}{A/K_b^* + n + 1}. \tag{24}$$

Obviously, the monotonicity of the K_b^*/K is determined by A/K_b^*. Then, we derive the derivative of A/K_b^* with respect to K_b^* as

$$\begin{aligned}\frac{\partial A/K_b^*}{\partial K_b^*} = {} & v^{K_b^*\mu+1}\alpha^2(q-1)^2 \frac{n-1}{K_b^*\left((n(q-1)\alpha-q)qv^{K_b^*\mu+1}+(1-q)\alpha+q\right)\left(1+((q-1)(n-1)\alpha-q)v^{K_b^*\mu+1}\right)} \\ & + \frac{-\ln\left((n(q-1)\alpha-q)qv^{K_b^*\mu+1}+(1-q)\alpha+q\right)+\ln\left(1+((q-1)(n-1)\alpha-q)v^{K_b^*\mu+1}\right)}{\mu K_b^{*2}\ln v},\end{aligned} \tag{25}$$

which is easy to prove to be less than zero. Therefore, with the increase of $K < K_b^*$ increases, A/K_b^* decreases, and K_b^*/K increases.

According to Proposition 1, when $K < \frac{\ln\left(\frac{\alpha(q-1)(nqv-1)-q^2v+q}{v\alpha(q-1)(n-1)-qv+1}\right)}{\mu \ln(v)}$, $K_b^*/K = 0$. As K increases, A/K_b^* is gradually close to zero, so the investment proportions of each branch and headquarters approach $1/(n+1)$ from 0 and 1, respectively, which indicates that, when the cybersecurity budget is sufficient, the headquarters and branches will divide the budget equally. □

Figure 4 numerically shows the relationship of optimal security investment with a total budget for intuitive analyses of Proportion 4 under the conditions of $v = 0.5$, $q = 0.5$, $a = 0.09$, $L = \$1.5\,\mathrm{M}$, and $\alpha < 1/(n+1)$. The result indicates that the optimal security investment of each branch and its proportion both increase with total security budget. It is clear that K_b^* is approximately proportional to K, while its proportion slows down and approaches $1/(n+1)$. In addition, the efficiency of cybersecurity investment μ will promote the group to increase the investment proportion to its branches.

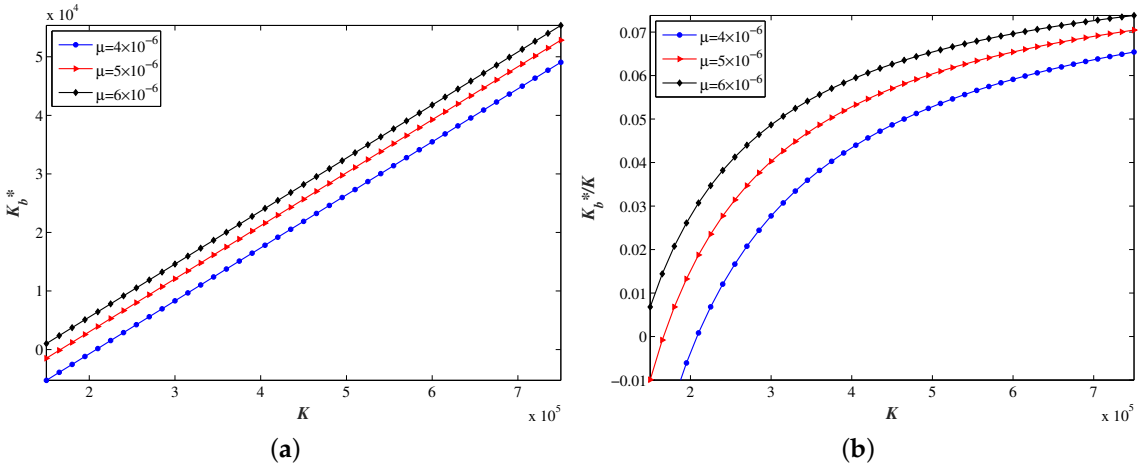

Figure 4. Optimal security investment and its allocation with a security investment budget.

The theoretical and numerical results clearly reveal that the increased budget will be approximately divided equally among all departments on the basis of the original allocation. When the

budget is small, the investment proportion of branches will be sensitive to other factors, such as propagation probability, intrinsic vulnerability, and branch information set, etc., which will be ignored with sufficient budget. At this time, the headquarters and branches will enjoy the same level of cybersecurity. The efficiency of security investment cannot significantly affect the linear relationship between the investment amount of branches and the total budget, but high efficiency will greatly promote the group to pay more attention to the cybersecurity of branches.

4.4. Intrinsic Vulnerability

The intrinsic vulnerability is determined by the internal configuration of the system. In general, the system configuration and performance of headquarters and branches are the same, and hence we assume that there is an equal internal vulnerability among them. In this section, the impact of intrinsic vulnerability on optimal cybersecurity allocation K_b^*/K will be investigated numerically.

Due to that fact that an accurate analytical solution of $\partial K_b^*/\partial v$ is impossible to obtain from the equation of $R(v, K_b^*) = 0$, and the implicit function analysis method is also incapable of drawing any interrelated results; therefore, the numerical simulation is employed to verify the relationship between K_b^*/K and v under conditions of $q = 0.5$, $a = 0.09$, $\mu = 0.000005$, $n = 10$, $L = \$1.5\,\mathrm{M}$, and $\alpha < 1/(n+1)$ as shown in Figure 5.

It is clear to see that the proportion of security investment to each branch decreases with the increase of intrinsic vulnerability under different budgets, and the decline rate is gradually increasing. The K_b^*/K varies between $[0, 1/(n+1)]$, and, when intrinsic vulnerability is very high, the most favorable decision is not to protect the branch system, which is consistent with the conclusion of Proposition 1. Such results imply that, in order to minimize potential losses, it is better for the group to focus the most or even all of budgets on protecting the cybersecurity of headquarters as the intrinsic vulnerability increases because the potential losses caused by indirect propagation from branches will be much smaller than those caused by direct breach of the headquarters system. However, it is a radical strategy to allocate all budgets to headquarters, which can be improved by increasing total budgets for cybersecurity.

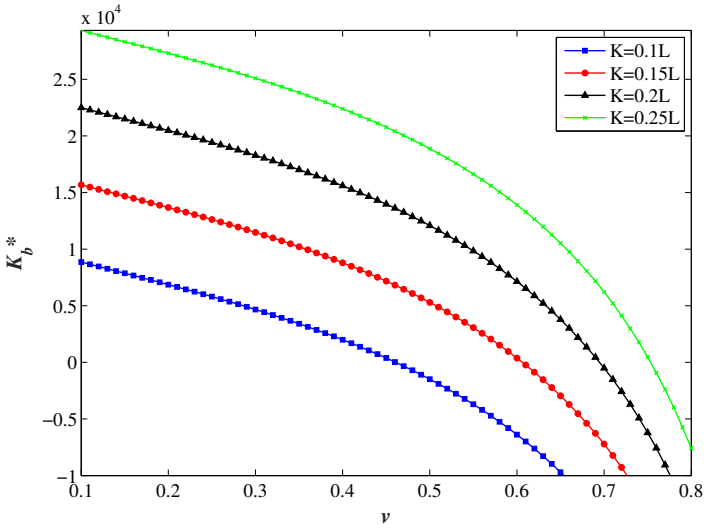

Figure 5. Optimal security investment allocation with intrinsic vulnerability.

5. Extension to Effects of Security Information Sharing

Sharing computer security vulnerabilities, breaches, intrusions, and technological solutions is an effective way to help organizations prevent, detect and correct security breaches proactively. Studies have also pointed out that security information sharing could reduce the uncertainty of network security investment to a certain extent, and thus depress the value of deferred options related to the

investment [24,25,30]. President Obama signed the Cybersecurity Information Sharing Act (CISA) in 2015 to improve the level of cybersecurity in the United States. The US Department of Homeland Security (DHS) has made security information sharing an important strategy. Some security-based sharing organizations have been established and funded to exchange cybersecurity threat information, such as the industry-based Information Sharing and Analysis Centers (ISACs) and the Computer Emergency Readiness Team (CERT). The industry and the UK government also jointly launched an initiative, named Cyber Security Information Sharing Partnership (CISP), to share threat information in order to enhance the public awareness and reduce negative influences on businesses. Thus, we plan to study the impact of security information sharing on the optimal allocation of security investment within a business group in this section.

In general, a group's internal departments and branches often share their security information, such as hacking attempts including successful and unsuccessful cases, methods to prevent vulnerabilities, and ways to minimize economic loss. If one firm shares security information, it will help other firms to prevent future breaches to reduce security breaches probability to a certain extent. The reduction in the breaches probability could be regarded as a virtual increase in security investments for other firms.

Specifically, if a branch invests K_b on cybersecurity and share security information with the headquarters, the effective investment amount of the headquarters is $K_{ae} = K_a + n\beta K_b$. On the contrary, if the headquarters shares security information with its branches, the effective expenditures each branch spends on cybersecurity could be expressed as $K_{be} = K_b + \beta K_a$. We assume that the headquarters and branch firms in the group share all their security information respectively, and sharing security information will bring the security investment benefits by βK_i to the sharing partners, where $\beta \in [0, 1]$ is denoted as the benefited rate of security information sharing. Notice that full sharing of security information does not achieve a 100% benefited rate due to the repeatability of security information and the uncertainty of external attacks. Therefore, β reflects the security sharing efficiency, and $\beta = 0$ means that sharing security information is completely invalid for reducing the system breach risk, at which time the optimal allocation is consistent with that of non-sharing security information discussed above.

Replacing K_a and K_b with K_{ae} and K_{be}, then rewrite (2) as

$$C_S = \left(1 - (1 - p\left(K_{ae}\right))\left(1 - qp\left(K_{be}\right)\right)^n\right) L + n\left(1 - q\right)\left(1 - p\left(K_{ae}\right)\right) p\left(K_{be}\right)\left(1 - qp\left(K_{be}\right)\right)^{n-1} \alpha L + K, \tag{26}$$

whose first-order derivative to K_{bS} is

$$\frac{\partial C_S}{\partial K_{bS}} = \left(1 - qp_{bS}\right)^{n-2} \left(\begin{array}{l} \mu n L \ln v \left(\left(n-1\right)\beta p_{aS}(nqp_{bS} - 1) + (\beta n - 1)(1 - nqp_{bS})\right) p_{bS}\left(q-1\right)\alpha \\ + \left(1 - qp_{bS}\right)\left(\left(\left(n-1\right)\beta p_{aS} - \beta n + 1\right) qp_{bS} + p_{aS}\left(\beta - 1\right)\right) \end{array} \right), \tag{27}$$

where $p_{bS} = v^{\mu((K - K_{bs}n)\beta + K_{bS}) + 1}$ and $p_{aS} = v^{n\mu(\beta-1)K_{bS} + K\mu + 1}$. Since the analytical solution of K^*_{bS} cannot be obtained from $\frac{\partial C_S}{\partial K_{bS}} = 0$ directly and it is also hard to find relevant results through an implicit function analysis method. Therefore, the numerical method is used to solve the first-order condition by bringing all into the cost function. We have ergodically verified whether the extreme point obtained by the numerical method is the minimum on the domain of $[0, K/n\ ]$. Figure 6 shows the changes of the optimal allocation to each branch K^*_{bS}/K with respect to the benefited rate β, where $\mu = 0.000005$, $q = 0.5$, $v = 0.5$, $n = 10$, $\alpha = 0.09$, $L = \$1.5\,\mathrm{M}$, and $K = 0.25L$.

We can see that K^*_{bS}/K decreases and approaches zero as β increases continuously. On the one hand, the increase of benefited rate means a reduced repetition rate of security information and more complete data information containing breaches and technology solutions, which is equivalent to indirectly improving the total budget of the whole system. Obviously, all branches will benefit after increasing the security investment of headquarters, and, along with the enhancement of headquarters security level, security measures and experiences can be shared with all branches, thus further improving the security level of the whole group. On the other hand, it is more efficient for the group to centralize its budget to protect cybersecurity at headquarters than to decentralize its budget

to all branches. At this time, the headquarters achieves lower security risks, and all branches indirectly improve the stability of the system through the security information shared by the headquarters. On the contrary, if the budget allocation of all branches is increased, there is a weak improvement of information system for the single branch, and the headquarters will also get less security information from branches, which is very disadvantageous to the whole system. Therefore, the group chooses to reduce actual security investments in branches under security information sharing.

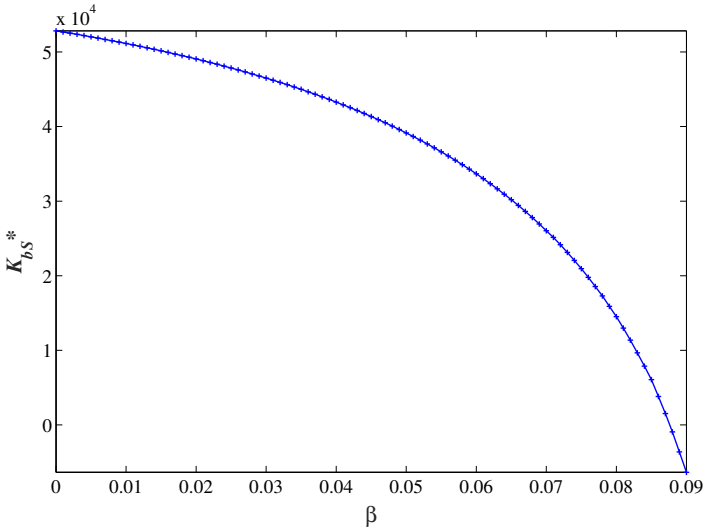

Figure 6. Optimal security investment allocation to branches over the benefited rate of security information sharing.

Next, the interesting issue is the influence of security information sharing on the relationship of optimal allocation with propagation probability. Table 2 shows the numerical analysis of the response of K_{bS}^* and K_{bS}^*/K to q by varying v of 0.1, 0.3, 0.5, 0.7 compared with that of no security information sharing ($\beta = 0$).The other constant parameters are set as $\mu = 0.000005$, $n = 10$, $\alpha = 0.09$, $\beta = 0.05$, $L = \$1.5\,\text{M}$, and $K = 0.25L$. Several indicates are obtained from Table 2. First, K_{bS}^*/K increases with q, but, with the larger v, the less the security investment K_{bS}^* and K_{bS}^*/K allocated to each branch, which are consistent with the conclusions in Sections 4.2 and 4.4. Second, the investment allocation to branches under no security information sharing is more than that under security information sharing, i.e., $K_b^*/K > K_{bS}^*/K$, which is not affected by intrinsic vulnerability. Since security information sharing brings more virtual investment from headquarters to branches than from branches to headquarters, the actual investment allocation of each branch would slowly respond to the increasing propagation probability. To reduce cost and improve security levels, the group could reduce its security investment in branches. Third, we need to pay attention to the critical value of propagation probability, expressed as q^* and q_S^* , when optimal security investment in each branch is greater than or equal to zero under the two cases. We note that both q^* and q_S^* increasing with v and $q^* \leq q_S^*$ always stands, and, when v is small, the optimal allocation to branches is always greater than zero regardless of sharing security information or not. It is also very intuitive that the optimal security investments of security information sharing are allocated to branches later than that of no information sharing with the same conditions because of the virtual investment effect. As security risks increase between interconnected systems, the group will start to invest in branches' cybersecurity at slightly higher propagation probability.

Finally, the relationship between K_{bS}^*/K and total budget at different level of $\beta = 0$, 0.02, 0.04, and 0.06 will be analyzed, where $\mu = 0.000005$, $v = 0.5$, $n = 10$, $\alpha = 0.09$, and $L = \$1.5\,\text{M}$. The curve of $\beta = 0$ in Figure 7 is actually the same as the red line in Figure 4b when there is no information sharing, and K_{bS}^*/K also increases with the total budget K, which is consistent with the non-sharing result. Under the same budget, the increase in the benefited rate β makes the group more inclined to protect the headquarters system because the security information sharing will enhance virtually the

security level of the branches, and thus the investment amount will be increased actually. Furthermore, at the zero point that the group begins to invest in branches' security, the corresponding budget K will increase with β, which is mainly because the group with a small budget expends all the funds for the security risk management of headquarters which stores all the information. Coupled with the virtual investment effect brought by security information sharing, the security investment budget will be allocated to branches only when the total security budget is larger.

Table 2. Optimal security investment and its allocation with propagation probability q and intrinsic vulnerability v.

	q	K_b^*	K_b^*/K	K_{bS}^*	K_{bS}^*/K
$v = 0.1$	$q^* = 0$	1.563	0.010		
	$q_S^* = 0$			1.549	0.04
	0.2	2.392	0.064	1.895	0.051
	0.4	2.79	0.074	2.338	0.062
	0.6	3.053	0.081	2.632	0.070
	0.8	3.251	0.087	2.855	0.076
$v = 0.3$	$q^* = 0$	0.190	0.001		
	$q_S^* = 0.118$			0	0
	0.2	1.533	0.041	0.489	0.013
	0.4	2.246	0.056	1.313	0.035
	0.6	2.735	0.073	1.887	0.050
	0.8	3.107	0.083	2.334	0.062
$v = 0.5$	$q^* = 0.151$	0	0		
	$q_S^* = 0.42$			0	0
	0.2	0.351	0.010	**	**
	0.4	1.459	0.039	**	**
	0.6	2.261	0.060	0.886	0.024
	0.8	2.89	0.077	1.7	0.045
$v = 0.7$	$q^* = 0.413$	0	0		
	$q_S^* = 0.727$			0	0
	0.2	**	**	**	**
	0.4	0.098	**	**	**
	0.6	1.273	0.034	**	**
	0.8	2.419	0.065	0.584	0.016

Note: all the security investment in Table 2 should multiply by \$10 K, and negative values are denoted by "**".

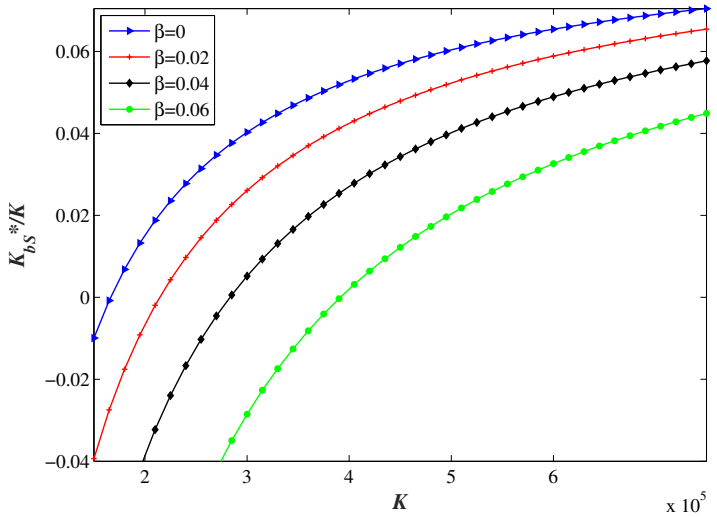

Figure 7. Optimal security investment allocation under security information sharing with budget constraints.

The numerical analysis results suggest that sharing security information can bring the virtual investment to branches. In turn, the group can reduce the investment allocation to branches for the

overall benefit when the budget is fixed, further highlighting the value of security investment in cybersecurity defense.

6. Discussion and Conclusions

In this paper, we built a mathematical model to study both theoretically and numerically the optimal allocation of security investment among the headquarters and its branches in a group under budget limitation. The relationships between various characteristics of investment environment and optimal security investment are considered, such as the proportion of branch's information set, propagation probability, budget constraints, and intrinsic vulnerability. In addition, the influence of security information sharing on optimal allocation is also investigated numerically. First, we study the reallocation of security investment within a group considering the intra-group characteristics, for example, the systems among the headquarters and its branches are interconnected, and the headquarters stores all the information of the whole group, which is different from the previous studies on the optimal security investment between interconnection organizations. Second, this paper assumes that the interconnected headquarters and branches are heterogeneous with different importance levels to cybersecurity and are invested to varying degrees, which is more realistic than homogeneous assumption proposed in previous studies for simplifying processing. Third, our study introduces the benefited rate rather than the sharing portion to investigate the influence of security information sharing on investment allocation among the headquarters and branches, which will be propitious to arrange the limited budget for a higher security level.

The following findings and some insights into managerial practices of security investment have been summarized:

(1) Proposition 1 reveals that when the intrinsic vulnerability of the system is high and the total budgets are insufficient, the group will allocate all the budgets to protect cybersecurity of the headquarters. This is reasonable since the headquarters stores all the information of the group, and the data security of headquarters becomes a priority when the system security is poor. Therefore, the assessment of intrinsic vulnerability and security budget becomes obviously significant for the security of the whole group.

(2) Security investment of branch increases with the propagation probability, but the group will not allocate the budget to its branches when the propagation probability is low. This is to be expected since the mutual trust and authorization inevitably increases the likelihood of indirect breaches; the group will allocate more security funds to their branches as the propagation probability grows. Surprisingly, groups with a large number of branch firms are more likely to increase the investment of headquarters because it is difficult for them to protect the system security of many branches under the limited budget.

(3) The proportion of security investment allocated to each branch grows with total budget and propagation probability, but never exceed the level of $1/(n+1)$. The higher the efficiency of investment, the lower the security budget of branches. This demonstrates that the security investment is efficient, and the group can transfer more security funds to headquarters, which indicates the importance of headquarters' cybersecurity again. This finding reminds the group that, in response to the deteriorating cybersecurity situation, adequate security investment budgets should be prepared, and interconnectivity and exposure between systems should be monitored timely.

(4) The allocation of security investment on each branch decreases with the increase of intrinsic vulnerability, and a higher budget will improve the underinvestment caused by higher intrinsic vulnerability. This indicates that the more vulnerable the system is, the more the group needs to allocate security funds to headquarters where more information is stored. When the total budget is large, the underinvestment of branches can be improved.

(5) The numerical analysis results in extensions show that the higher benefited rate, the less investment is allocated to branches. Under a security information sharing case, the total budget

required for branches allocated investment is greater than that without information sharing. This can be explained by the fact that security information sharing can indirectly offset part of security investment, which alleviates the group's pressure on the security budget allocation to a certain extent.

There are also some limitations in our study. In general, cybersecurity involves two issues: defenses and attacks. This paper only discusses the information breach probability caused by an attacker from the perspective of defenders. In the future research, we will take the attackers' strategies into consideration and further explores the offensive and defensive behaviors among them. In terms of the security information sharing mechanism, this paper only sets a benefit rate parameter to express. One can refer to some models of security knowledge sharing to make the research more detailed and perfect. For example, Safa et al. discussed the organizational support in the role of security knowledge sharing [41] and He et al. adopted decision theory to discuss the costs involved in information sharing and cybersecurity [42]. In addition, most studies have always followed the information breach function proposed by Gorden and Leob [7], and one can also try to explore more realistic models instead.

Author Contributions: Writing—original draft preparation, L.X.; writing—review and editing, Y.L.; supervision, J.F.

Funding: This research was funded by the National Natural Science Foundation of China under Grant No. 71471073, the Fundamental Research Funds for the Central Universities under Grant No. 2018YBZZ106 and No. CCNU19TS078, and the Hubei Center of Agricultural Science and Technology Innovation "Agricultural Economy and Information Research" team project under Grant No. 2019620016002.

Acknowledgments: The authors would like to thank the editors and the anonymous reviewers for their comments and suggestions, which were very helpful for improving the manuscript.

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

References

1. Cost of a Data Breach Study: Benchmark Research. Available online: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ (accessed on 1 March 2019).
2. Bellovin, S.M. Computer Security—An End State? *Commun. ACM* **2001**, *44*, 131–132. [CrossRef]
3. Sun, L.; Srivastava, R.P.; Mock, T.J. An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *J. Manag. Inf. Syst.* **2006**, *22*, 109–142. [CrossRef]
4. Cavusoglu, H.; Mishra, B.; Raghunathan, S. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *Int. J. Electron. Commer.* **2004**, *9*, 70–104. [CrossRef]
5. Huang, C.D.; Hu, Q.; Behara, R.S. An economic analysis of the optimal cybersecurity investment in the case of a risk-averse firm. *Int. J. Prod. Econ.* **2008**, *114*, 793–804. [CrossRef]
6. Hausken, K. Returns to cybersecurity investment: The effect of alternative cybersecurity breach functions on optimal investment and sensitivity to vulnerability. *Inf. Syst. Front.* **2006**, *8*, 338–349. [CrossRef]
7. Gordon, L.A.; Loeb, M.P. The economics of cybersecurity investment. *ACM Trans. Inf. Syst. Secur.* **2002**, *5*, 438–457. [CrossRef]
8. PwC. The Global State of Cybersecurity Survey 2013. Available online: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf (accessed on 1 March 2019).
9. Nagurney, A.; Shukla, S. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *Eur. J. Oper. Res.* **2017**, *260*, 588–600. [CrossRef]
10. Zhao, X.; Xue, L.; Whinston, A.B. Managing interdependent cybersecurity risks: Cyberinsurance, managed security services, and risk pooling arrangements. *J. Manag. Inf. Syst.* **2013**, *30*, 123–152. [CrossRef]
11. Guo, H.; Cheng, H.K.; Kelley, K. Impact of network structure on malware propagation: A growth curve perspective. *J. Manag. Inf. Syst.* **2016**, *33*, 296–325. [CrossRef]
12. Cainiao to Launch Smart Logistics Parks at Scale in China. Available online: https://www.alizila.com/cainiao-logistics-future-park-china/ (accessed on 1 March 2019).
13. Hilton to Pay $700,000 over Credit Card Data Breaches. Available online: https://www.reuters.com/article/us-hilton-wrldwide-settlement/hilton-to-pay-700000-over-credit-card-data-breaches-idUSKBN1D02L3 (accessed on 1 March 2019).

14. HSBC Bank in U.S. Suffers Data Breach. Available online: https://www.techworm.net/2018/11/hsbc-bank-suffers-data-breach.html (accessed on 1 March 2019).
15. Two Canadian bAnks Report Breaches Exposing Customer Data. Available online: https://www.eweek.com/security/two-canadian-banks-report-breaches-exposing-customer-data (accessed on 1 March 2019).
16. Cathay Pacific Faces Probe over Massive Data Breach. Available online: https://www.reuters.com/article/us-cathaypacific-cyber/cathay-pacific-faces-probe-over-massive-data-breach-idUSKCN1NB0JY (accessed on 1 March 2019).
17. Wu, Y.; Feng, G.; Wang, N.; Liang, H. Game of cybersecurity investment: Impact of attack types and network vulnerability. *Expert Syst. Appl.* **2015**, *42*, 6132–6146. [CrossRef]
18. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Int. J. Inf. Secur.* **2018**, *9*, 720–726. [CrossRef]
19. Anderson, R. Why cybersecurity is hard-an economic perspective. In Proceedings of the Seventeenth Annual Computer Security Applications Conference, New Orleans, LA, USA, 10–14 December 2001; Computer Security Applications (IEEE): New Orleans, LA, USA, 2002; pp. 358–365.
20. Yue, W.T.; Çakanyıldırım, M.; Ryu, Y.U.; Liu, D. Network externalities, layered protection and IT security risk management. *Decis. Support Syst.* **2007**, *44*, 1–16. [CrossRef]
21. Sherer, S.A.; Alter, S. Information systems risks and risk factors: are they mostly about information systems? *Commun. Assoc. Inf. Syst.* **2004**, *14*, 36. [CrossRef]
22. Laszka, A.; Felegyhazi, M.; Buttyan, L. A survey of interdependent cybersecurity games. *ACM Comput. Surv.* **2015**, *47*, 23.
23. Huang, C.D.; Behara, R.S.; Goo, J. Optimal cybersecurity investment in a Healthcare Information Exchange: An economic analysis. *Decis. Support Syst.* **2014**, *61*, 1–11. [CrossRef]
24. Cavusoglu, H.; Raghunathan, S.; Yue, W.T. Decision-theoretic and game-theoretic approaches to IT security investment. *J. Manag. Inf. Syst.* **2008**, *25*, 281–304. [CrossRef]
25. Ezhei, M.; Ladani, B.T. Information sharing vs. privacy: A game theoretic analysis. *Expert Syst. Appl.* **2017**, *88*, 327–337. [CrossRef]
26. Liu, X.; Qian, X.; Pei, J.; Pardalos, P.M. Security investment and information sharing in the market of complementary firms: Impact of complementarity degree and industry size. *J. Glob. Optim.* **2018**, *70*, 413–436. [CrossRef]
27. Kantzavelou, I.; Katsikas, S. A game-based intrusion detection mechanism to confront internal attackers. *Comput. Secur.* **2010**, *29*, 859–874. [CrossRef]
28. Fielder, A.; Panaousis, E.; Malacaria, P.; Hankin, C.; Smeraldi, F. Decision support approaches for cyber security investment. *Decis. Support Syst.* **2016**, *86*, 13–23. [CrossRef]
29. Kunreuther, H.; Heal, G. Interdependent security. *J. Risk Uncertain.* **2003**, *26*, 231–249. [CrossRef]
30. Qian, X.; Liu, X.; Pei, J.; Pardalos, P.M.; Liu, L. A game-theoretic analysis of cybersecurity investment for multiple firms in a network. *J. Oper. Res. Soc.* **2017**, *68*, 1290–1305. [CrossRef]
31. 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. [CrossRef]
32. Ezhei, M.; Tork Ladani, B. Interdependency analysis in security investment against strategic attacks. *Inf. Syst. Front.* **2018**, 1–15.%2Fs10796-018-9845-8. [CrossRef]
33. How to get Ikea Trådfri Smart Lights Set Up with Alexa. Available online: https://www.the-ambient.com/how-to/connect-ikea-tradfri-to-alexa-1419 (accessed on 1 March 2019).
34. Bodin, L.D.; Gordon, L.A.; Loeb, M.P. Evaluating cybersecurity investments using the analytic hierarchy process. *Commun. ACM* **2005**, *48*, 78–83. [CrossRef]
35. Huang, C.D.; Behara, R.S. Economics of cybersecurity investment in the case of concurrent heterogeneous attacks with budget constraints. *Int. J. Prod. Econ.* **2013**, *141*, 255–268. [CrossRef]
36. Schilling, A.; Werners, B. Optimizing cybersecurity investments with limited budget. In Proceedings of the International Conference on Operations Research (OR 2014), Aachen, Germany, 2–5 September 2014; pp. 493–499.
37. Simonsen, I.; Buzna, L.; Peters, K.; Bornholdt, S.; Helbing, D. Transient dynamics increasing network vulnerability to cascading failures. *Phys. Rev. Lett.* **2008**, *100*, 218–701. [CrossRef] [PubMed]
38. Robinson, S.M. An implicit-function theorem for a class of nonsmooth functions. *Math. Oper. Res.* **1991**, *16*, 292–309. [CrossRef]

39. Gordon, L.A.; Loeb, M.P.; Zhou, L. Investing in cybersecurity: insights from the Gordon-Loeb model. *J. Inf. Secur.* **2016**, *7*, 49. [CrossRef]
40. Cyber Security Breaches Survey 2018: Statistical Release. Available online: https://researchportal.port.ac.uk/portal/files/10339594/Cyber_Security_Breaches_Survey_2018_Main_Report.pdf (accessed on 1 March 2019).
41. Safa, N.S.; Von Solms, R. An cybersecurity knowledge sharing model in organizations. *Comput. Hum. Behav.* **2016**, *57*, 442–451. [CrossRef]
42. 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. [CrossRef] [PubMed]

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).