1-1-2014

Rethinking FS-ISAC: An IT Security Information Sharing Model for the Financial Services Sector

Charles Liu
University of Texas at San Antonio, xliu6@kennesaw.edu

Humayun Zafar
Kennesaw State University, hzafar@kennesaw.edu

Yoris A. Au
University of Texas at San Antonio

THE UNIVERSITY OF TEXAS AT SAN ANTONIO, COLLEGE OF BUSINESS

Working Paper SERIES

WP # 0023IS-673-2013

Date April 11, 2013

RETHINKING FS-ISAC: AN IT SECURITY INFORMATION SHARING MODEL FOR THE FINANCIAL SERVICES SECTOR

Charles Z. Liu
Department of Information Systems and Cyber Security
The University of Texas at San Antonio

Humayun Zafar
Department of Information Systems
Kennesaw State University

Yoris A. Au
Department of Information Systems and Cyber Security
The University of Texas at San Antonio

UTSA COLLEGE OF BUSINESS KNOWLEDGE FOR A NEW WORLD

ONE UTSA CIRCLE
SAN ANTONIO, TEXAS 78249-0631
210 458-4317 | BUSINESS.UTSA.EDU

RETHINKING FS-ISAC: AN IT SECURITY INFORMATION SHARING MODEL FOR THE FINANCIAL SERVICES SECTOR

Charles Z. Liu
Department of Information Systems and Cyber Security
The University of Texas at San Antonio
Charles.Liu@utsa.edu

Humayun Zafar
Department of Information Systems
Kennesaw State University
HZafar@kennesaw.edu

Yoris A. Au
Department of Information Systems and Cyber Security
The University of Texas at San Antonio
Yoris.Au@utsa.edu

March 31, 2013

RETHINKING FS-ISAC: AN IT SECURITY INFORMATION SHARING MODEL FOR THE FINANCIAL SERVICES SECTOR

Abstract

This study examines a critical incentive alignment issue facing FS-ISAC (the information sharing alliance in the financial services industry). Failure to encourage members to share their IT security-related information has seriously undermined the founding rationale of FS-ISAC. Our analysis shows that many information sharing alliances' membership policies are plagued with the incentive misalignment issue and may result in a "free-riding" or "no information sharing" equilibrium. To address this issue, we propose a new information sharing membership policy that incorporates an insurance option and show that the proposed policy can align members' incentives and lead to a socially optimal outcome. Moreover, when a transfer payment mechanism is implemented, all member firms will be better off joining the insurance network. These results are demonstrated in a simulation in which IT security breach losses are compared both with and without participating in the proposed information sharing insurance plan.

***Keywords*:** security, organization, information sharing, economic theory, game theory, simulation

JEL Classification Codes: C70, D53, D71, D74, G22.

I. INTRODUCTION

In January 2009, Heartland Payment Systems, the sixth largest payment processor[1] in the United States, announced that hackers had compromised its processing systems. The effects of this information technology (IT) security breach reverberated through dozens of partners that included Forcht Bank of Kentucky, Farmers & Merchants Bank of Arkansas, and Adams Bank and Trust of New England. The forensics team found that hackers were able to obtain account numbers using sniffer malware when the systems were processing payments [Claburn, 2009]. The pattern and consequences of this breach were very similar to another breach reported by the TJX Companies in 2007 that affected as many as 94 million credit card accounts.

Earlier, in 2008, the Bank of New York Mellon reported that sensitive data of over four million customers who owned shares in public companies were compromised after the data were sent to a remote storage facility. The data included names, addresses, and social security numbers. The estimated cost of this breach was $197 per customer record. In another incident in 2008, the Federal Bureau of Investigation arrested an employee of Countrywide Financial Corporation for stealing and selling private information of over two million mortgage loan applicants. The company estimated that the employee profited from $50,000 to $70,000 from the sale of these private information [Mills, 2009].

The above incidents are just a few of the many IT security breaches that have been publicly disclosed in the past few years. Today the financial services industry continues to face the prospect of an increase in regulations, while at the same time having to combat persistent cyber threats.[2] Costs associated with information security breaches have also increased significantly. A study by the Ponemon Institute indicated that the cost of data breach continues to increase [Ponemon, 2009]. The report stated that the average total per-incident cost of a security breach in 2009 was $6.75 million. The report also stated that the cost of lost business increased to 65 percent of data breach costs, up from 54 percent the year before. A report from McAfee showed that information security losses amounted to over $1 trillion globally in 2008 [Mills, 2009].

These incidents show that there is a need for increasing industry collaboration to reduce information security risks. None of them represents a novel way of attack. Each has been well-documented, and best practices for countering such threats have also been presented at length [Panko, 2003]. Yet none of the victims had been able to obtain such information before the events occurred, and the disaster recovery processes were largely unprepared.

At first glance, these cases appear to be independent. However, all these companies are members of the Financial Services Information Sharing and Analysis Center (FS-ISAC). The center was established by the financial services sector under Presidential Decision Directive/NSC-63 in 1999. The directive, which was later updated by the 2003s Homeland Security Presidential Directive 7, mandates that public and private sectors share information about the physical and security threats and vulnerabilities faced by financial services organizations. As a nonprofit organization, FS-ISAC has over 7,000 members as of June 2010. FS-ISAC is attractive to financial companies primarily because it is the only centralized official portal capable of providing services specifically tailored to financial service companies. FS-ISAC offers members benefits such as the publication of cyber threat level for the financial sector and early notification of attacks based on a tiered membership structure: Core, Standard, Premier, Gold, and Platinum. A color coded scheme is used for the type of information (white, green, yellow, and red). Each tier varies in subscription cost, which in turn is linked to a plethora of services such as access to XML data feeds, member contact directory, threat conference calls, free attendance at member meetings, and trusted email registry.

---

[1] Heartland handles 100 million transactions per month for more than 250,000 businesses.

[2] A brief list of other major financial services institutions which have suffered IT security breaches so far in 2011 includes Bank of America, JP Morgan Chase, and Pentagon Federal Credit Union (Privacy Rights Clearinghouse, “Chronology of Data Breaches 2005-present,”http://www.privacyrights.org/data-breach, current March 4, 2011).

Even though FS-ISAC's mission is to encourage cooperation between financial institutions to prevent or limit instances of cyber attacks, its members continue to commit rudimentary mistakes. Heartland Payment Systems would have been wary of similar mistakes other organizations (such as TJX) had made in the past had such information been made available [Claburn, 2009]. However, without appropriate incentives, member firms may find no particular motivation to share their IT security incident information because such sharing often has a negative impact on the firm's current and future profitability. This is especially true for the financial services industry, which is one of the most competitive industries. The fact that FS-ISAC requires its members only to voluntarily share security-related information also leads to the prevalence of "free riding," further impacting FS-ISAC's efficacy.

In this research, we focus on the role of organizations such as FS-ISAC in successfully fostering information sharing among its members. Although there have been several prior studies on the economic incentives and consequences of information sharing, most of them have examined these issues from the perspective of the firms. Organizations such as FS-ISAC have largely been viewed as free information exchange portals that take a passive role in the network. We argue that the role of these organizations has not been adequately addressed in prior research. For example, in reality FS-ISAC not only acts as an information sharing forum, but also serves a pivotal role in directing the behaviors of its member firms through its membership policies and provision of value-added services.

To better understand the dynamics in information sharing alliances such as FS-ISAC, we develop a game theory model to study the existing information sharing network membership policies and their impact on the level of information sharing and the resulting economic welfare of its member firms. We find that the membership policies of most information sharing alliances may actually either lead to a "free-riding" or a "no-information-sharing" equilibrium and yield outcomes inconsistent with their mission statements. We identify the sources of such problems and demonstrate that the incentives of member firms can be aligned to avoid the "free-riding" problems in such information sharing alliances. In particular, we propose to integrate an innovative insurance plan with a revised membership policy and create a new mechanism that not only generates incentives for members to actively engage in information sharing activities but also provides insurance coverage to members that suffer a loss from security attacks. We show that the inclusion of the insurance policy can yield an outcome consistent with the social optimal equilibrium. Moreover, by implementing a mechanism that redistributes the gains from information sharing, all firms will be better off joining the proposed insurance network.

The rest of the article is organized as follows: Section II reviews the literature pertaining to security information sharing. Section III presents a baseline model that analyzes the existing information sharing networks' membership policies. Section IV extends the baseline model to include an insurance plan and examines whether such a policy will motivate firms to actively share information. Section V discusses the implications of our findings and offers directions for future research. Section VI concludes the article.

II. LITERATURE REVIEW

Over the past few years researchers have begun to extend seminal works in information systems (IS) security such as Baskerville [1993], Dhillon and Backhouse [2001], and Siponen [2005]. Many of these studies investigate the causes and consequences of security breaches at the firm level and have focused on areas such as governance [Straub and Nance, 1990], information privacy [Greenaway and Chan, 2005], development of best practice security models [Ma and Pearson, 2005], maintaining data integrity [Ba, Stallaert, Whinston, and Zhang, 2005], preventing unauthorized user access [Zviran and Haga, 1999], developing secure applications [Tryfonas, 2007], and encouraging information security in the workplace [Whitworth and Zaic, 2003]. At the same time, researchers have begun to realize that failures in IT security mechanisms are caused not only by bad design, but also by inferior incentive mechanisms [Anderson and Moore, 2006]. This has also resulted in a growth of research that utilizes game theory and microeconomics to study firms incentives and strategies in their battles against security breaches [Campbell, Gordon, Loeb, and Zhou, 2003; Cavusoglu, Mishra, and Raghunathan, 2004; Gal-Or and Ghose, 2005; Gordon and Loeb, 2002]. This stream of research generally concludes that without proper incentive mechanisms, organizations tend to rely on technological solutions to protect their information systems.

As a result of this finding, application of incentives in an organization's security strategy has been categorized as being critical to preventing and countering security attacks [Acquisti, 2004; Gordon et al., 2003]. Varian [2000] states that, in a typical organization, security analysts should not only investigate weak points in a system, but they should also go one step further and examine the incentives of those responsible for the system. Economics theory would suggest that insurance is an approach toward the development of an effective security metric. In a typical insurance model, underwriters use expert assessors to consider a client's infrastructure and attribute an associated element of risk, following which a premium is decided. This area of economics of IS security is both underdeveloped and underutilized. According to Bohme [2005], the reason for this is the interdependence of risk, since a firm's IT infrastructure is connected to other entities, a firm's efforts to improve its IT infrastructure may be undermined by failures elsewhere. This interdependence also reduces members' incentives to invest in security technology and increases their reliance on cyber insurance [Baer and Parkinson, 2007], making cyber insurance an unattractive option for insurers. Therefore, a catalyst may be necessary to stimulate the interests of the insurers. Due to the unique role of information sharing alliances such as FS-ISAC, if properly designed, the insurance they offer can potentially be the catalyst that may finally fulfill the goals of reducing the losses from security breaches for the financial services sector. However, there is a need to consider market distortions that will result from the asymmetry of information [Cawley and Philipson, 1999] between well-informed members and poorly informed supplier of insurance, which may lead to the adverse selection problem. Bandyopadhyay, Mookerjee, and Rao [2009] state that cyber insurance has not fulfilled its initial hype due to the presence of information asymmetry between customers and providers, leading to overpricing of cyber insurance contracts.

Another area that may be subject to the incentive misalignment issue is the information sharing activities related to security breaches. Information sharing has been studied extensively in the economics literature in the context of non-security related trade associations [Gal-Or, 1985; Shapiro, 1986; Vives, 1990]. The information shared involves either an industry's demand parameter or the individual firm's cost parameter, and most of these studies focus on investigating the optimal information sharing strategies to maximize a firm's profits. Recently, due to the increasing frequency and soaring costs of security breaches, this stream of research has been extended to the IS security arena [Cavusoglu and Raghunathan, 2004; Gal-Or and Ghose, 2005; Gordon and Loeb, 2002]. Although most studies show that there are significant benefits associated with information sharing activities, pitfalls associated with sharing security information among organizations have been recognized. Researchers have found that failures in IS security systems are caused not only by the lack of channels for sharing information, but also by the lack of incentive mechanisms. Unlike information sharing in the traditional trade association context, a firm may attempt to avoid the responsibility of sharing with the hope that they can take advantage of the information provided by other firms in the network. Anderson [2001] discusses various distorted incentives that could arise in the security information sharing process due to moral hazard and adverse selection problems. Gordon, Loeb, and Lucyshyn [2003] show that information sharing might lead to situations where some firms would have an incentive to free-ride on the information security expenditures of the other firms. This finding is similar to the conclusion reached in Varian [2004], which states that free-riders will emerge when the reliability of a system depends on the total efforts contributed by all stakeholders.

Building on these findings, we seek to extend the research on incentive mechanisms in IT security information sharing alliances. A review of the literature shows that most studies assume that organizations such as FS-ISAC are passive intermediaries that offer only free information sharing services, and the information shared by these agencies alone can significantly reduce security risks facing firms. These assumptions fail to capture three important characteristics of information sharing activities within networks such as FS-ISAC: (1) To maintain its operations and leverage service quality, organizations such as FS-ISAC offer their services at a fee (most prior studies assume that these organizations do not charge a fee to its members): such a fee can have a significant impact on a member's information sharing behavior in the network; (2) Without existing security information technology infrastructure, information shared by these organizations alone cannot significantly reduce the risk of security breaches; investment in security technologies serves as an important strategic complement to information sharing activities; (3) The goal of organizations such as FS-ISAC is not to maximize its member firms' profits, but to increase the overall system reliability and reduce the total losses from security breaches.

To better capture the impact of these characteristics on the dynamics of the information sharing activities, we use game theory to model the behaviors of various players in an information sharing network. Game theory is the study of a multi-agent strategic decision-making process and is widely used in economics, computer science, political science, and many other disciplines. A central feature of game theory is the strategic interdependence of multi-agent (multi-player) interaction. Each player in the game recognizes that the payoff she receives (in utility or profits) depends not only on her own actions but also on the actions of other individuals [Mas-Colell, Whinston, and Green, 1995]. Hence, with the assumption of rationality, each player chooses the best strategy in response to the actions other players have taken or will be taking to maximize her payoffs. The term *game* highlights the importance of strategic interaction and forward looking in capturing the behaviors of players under study. Due to the rational and structured nature of the theory, mathematical models are often chosen to represent the calculation of payoffs by various players. A more thorough review of game theory can be found in Fudenberg and Tirole [1991], Myerson [1995], and Osborne and Rubinstein [1994], along with the classic references of Von Neumann and Morgenstern [1944] and Schelling [1960].

In the following section, we develop a baseline game theory model with two firms to examine how the existing information-sharing alliances membership policies affect a firm's information sharing efforts and identify reasons that lead to the "free-riding" behavior. We then generalize the baseline two-firm model to an N-firm setting and incorporate an insurance option and compare the equilbria derived in both situations.

III. A BASELINE GAME THEORY MODEL

Model Setup

As it is general in game theory modeling, we start the analysis by setting up a simplified model that has only two firms in an information sharing network. Such a simplified model allows straightforward derivation of the results without introducing too many parameters and can be easy to follow for readers who are not familiar with the game theory approach. We then show that, without loss in generality, the results derived from the two-firm setup can be extended to an N-firm setting.

Consider a market that consists of FS-ISAC and two financial services firms, indexed by i = 1, 2. Let A_i denote a firm's total assets (A_i>0). Both firms face similar security risks in their information systems (there exist some hackers who will attempt to compromise systems of both firms). To reduce such risks, both firms devote a fraction of their total assets αA_i ($0<\alpha<1$) to enhance the security of their systems.[3] Firms can split their security budget between: (1) investment in security technologies, t_i (i.e. network security components such as a firewall or antivirus software), and (2) a membership fee f_i to participate in an information sharing network (such as FS-ISAC) in exchange for security-related information which can be used to reduce the firm's system vulnerability. In order to enjoy member benefits, member firms are also required to voluntarily share information related to the security of their information systems such as attacks detected, security breaches, self-discovered system vulnerabilities and associated solutions, if any. For simplicity, we normalize the total amount of security-related information shared by firm i to a fraction s_i ($0\leq s_i\leq 1$), where $s_i = 0$ indicates that firm i does not share any information and $s_i = 1$ means firm i shares all the security-related information it possesses. After FS-ISAC receives the information contributed by the membership firms, it analyzes the information and classifies it into security warnings, virus patterns, software patches, technical solutions, disaster recovery tips, etc. and provides processed information to its member firms. We use a general function $r_i(f_i, \sum s_i)$ to represent the amount of information FS-ISAC delivers to firm i. It is worth noting that r_i is not always equal to the total amount of information member firms report to FS-ISAC, $\sum s_i$, which is essentially $s_i + s_j$ in our two-firm setup. As will

[3] In our model, α is assumed to be a constant value rather than a decision variable. The reason is that, for the majority of the organizations, the fraction of budget allocated to information security is typically determined prior to the start of the fiscal year. Hence, it is not very likely that firms will freely increase the security budget once the fiscal year begins. In this study, we are trying to capture the reality that firms have to make a strategic decision in the presence of budget constraint. Therefore, a constant upper-bound of the security budget will allow us to better model the tradeoffs firms have to make. Moreover, allowing the fraction to be different will only change the optimal level of security information sharing investment, but that will not change the results derived from the model and our conclusions. Hence, for simplicity and analytical tractability, we assume this fraction to be a constant.

be shown later, r_i also depends on FS-ISAC's membership policy and the membership level chosen by the firm (often represented by the membership fee f_i that firm i pays), and $\sum s_i$, the total amount of information available to FS-ISAC.

Firms make their decisions in a three-stage sequential game in which the outcome occurred in an earlier stage of the game becomes public information to all players involved in subsequent stages of the game. In stage 0, FS-ISAC announces the membership policy (to be discussed in more details later). In stage 1, both firms simultaneously decide on their respective levels of information sharing s_i. In stage 2, FS-ISAC sets a membership fee f_i based on its membership policy and the amount of the information it collects ($\sum s_i$), and then both firms simultaneously decide on their respective levels of security information technology investment (t_i) as well as their membership levels (at cost f_i), subject to the budget constraint: $t_i+f_i \leq \alpha A_i$. The sequential nature of the game implies that firms can determine the best way to allocate its resources after FS-ISAC announces its membership fee structure.[4]

Let $P(t_i, A_i, r_i(f_i, \sum s_i))$ be the probability of a successful defense by firm i against a security attack. Such a probability depends on three factors: (1) t_i, the level of security technology investments, (2) A_i, a firm's total assets, and (3) $r_i(f_i, \sum s_i)$, the total amount of information FS-ISAC delivers to firm i. Here we use a collective measure $\sum s_i$ to represent the value of the information even though firm i already possesses part of the collective information s_i. This is because in reality the information obtained from a particular security attack can be fragmented and carries very little useful information until it is extrapolated with other related information. Hence the collective measure can better represent the value of the information. We assume that the probability function is concave[5] and twice differentiable in both t_i and r_i, $\partial P/\partial t_i>0$, $\partial P/\partial A_i<0$, and $\partial P/\partial r_i>0$. That is, all else being equal, the more a firm invests in security protection technologies, the less likely its systems will be compromised. Conversely, all else being equal, the greater a firm's total assets (and presumably the larger the firm's information systems), the more resources it takes and the more difficult it is to protect the firm's systems from security breaches. Finally, all else being equal, the more information obtained from FS-ISAC, the more likely it is that a firm can be better prepared and reduce the vulnerability of its information systems.

In reality, security technologies alone, to some extent, can reduce the likelihood of security breaches even if a firm does not have too much information about the security attacks and its system vulnerability. On the contrary, the security information FS-ISAC delivers to its members alone cannot prevent a firm's information system from being compromised if there is no technology infrastructure in place to implement any preventive actions.[6] Therefore, we assume that security information sharing is a strategic complement to security technology investment in improving the system's reliability, but not vice versa. More specifically, when $t_i = 0$, regardless of the value of r_i, $P(t_i, A_i, r_i) = 0$, whereas when $r_i = 0$, as long as $t_i>0$, $P(t_i, A_i, r_i)>0$. Accordingly, we reconstruct the probability function to capture this complementary relationship.[7]

$$P(t_i, A_i, r_i(f_i, \sum s_i),) = P\left(\frac{t_i(1+r_i(f_i,\sum s_i))}{A_i}\right). \quad (1)$$

[4] The reason that we consider firms to set their information sharing in stage 1 and determine their level of security technology investment in stage 2 is because the amount of money firms are willing to spend on a membership fee to enjoy the benefits of security information sharing depends on the total amount of security information available to them. Also, member firms cannot determine the amount of money they will spend on security information sharing before FS-ISAC publishes the fee structure, which in turn depends on the amount of information member firms submitted.

[5] A twice differentiable concave function ensures that a solution exists for the optimization of the function. It also implies that there is decreasing return to scale for variables involved in the function.

[6] An example is that FS-ISAC shares some patterns (or source code) of certain viruses. However, if the firm does not have a firewall or antivirus software, it cannot take any actions to block these malicious codes in order to prevent its systems from being breached by these viruses.

[7] Equation (1) can be viewed as a simple form of the Cobb-Douglas production function widely used in the economics literature to measure the output of various complementary production factors [Simon and Blume, 1994]. In our context, the complementary factors are technology investments t_i, and the information provided by FS-ISAC, r_i, as an increase in one factor implies a decrease in the other factor.

A firm suffers a loss if hackers breach its information system. Let ϕA_i denote the direct losses incurred as a result of a security breach, such direct losses include but are not limited to lost business (i.e., bank customers cannot perform the routine deposit/withdraw activities due to malfunctioning information systems), data loss (i.e., the costs of retrieving lost information or replacing compromised credit cards), hardware/software costs (i.e., the costs of recovering the breached systems), etc. We measure the direct losses as a fraction (ϕ) of a firm's total assets, since, all else being equal, the direct losses of security breaches are largely a function of the cost of replacing/repairing services impacted [Whitman and Mattord, 2006], which, in turn, depends mainly on the size of the firm. Since such losses may be dependent on some unknown exogenous factors and, hence, vary from case to case, we also allow ϕ to be uniformly distributed on an interval [0, Φ], where $\alpha<\Phi<1$.[8]

At the same time, based on FS-ISAC's rules, member firms should voluntarily submit their security-related information to FS-ISAC and allow other members to share such information. However, since consumers in the financial market are extremely sensitive about system security, disclosing IT security breaches information may lead to significant indirect losses to a firm. Such losses are often intangible (e.g., decreased customer loyalty) and depend on the extent of sharing by the firm itself as well as by the other firm. In general, the losses increase with the amount of security information shared by the firm itself, but decrease with the amount of security information shared by the other firms.[9]

Based on the above assumptions, a firm's objective is to protect its information systems from suffering a security attack and to try to minimize any costs associated with such an attack (regardless of whether it is successful or not). Therefore, firm *i*'s objective function[10] is:

$$Max\ P\left(\frac{t_i(1+r_i(f_i,\sum s_i))}{A_i}\right)\phi A_i - d_{i1}s_i + d_{i2}s_j - \alpha A_i, \quad \text{s.t. } t_i+f_i \le \alpha A_i. \tag{2}$$

where ϕA_i can be regarded as the value of a secure system to firm *i*, s_j denotes the amount of information shared by the other firm *j*, d_{i1} measures the extent of indirect loss to firm *i* as a result of sharing its IT security-related information, and d_{i2} measures the extent of indirect positive impact that the other firm's information sharing has on firm *i*. As discussed above, we assume that $d_{i1}>d_{i2}$ so that the negative impact of information sharing cannot be completely offset by the same behavior by the rival firm.

Currently the membership policy varies across different information sharing alliances. We broadly classify these policies into three different categories: (i) a free membership for small firms with a limited amount of information, (ii) a hierarchical membership fee structure in which the membership fee is proportional to the member firm's total assets, and (iii) a hierarchical fee structure based on the amount of information requested by the member firm. Note that in case (i), $f_i=0$ and $r_i(f_i, \sum s_i)=r\cdot(\sum s_i)$, where the ratio r is a constant set by FS-ISAC. In case (ii) $f_i = (A_i/\bar{A})F$, where $\bar{A}$ is the highest asset level among all FS-ISAC members and F is the membership fee FS-ISAC charges its members. Unlike the role of a private agent assumed in other studies, the objective of FS-ISAC is not to maximize its own profits. Rather, it seeks to reduce the total losses to its members due to security breaches. Hence when FS-ISAC sets the fee F, it will make sure that such a fee is affordable to all members, that is, $F<\alpha\bar{A}\Leftrightarrow f_i<\alpha A_i$. In case (iii), $f_i=(r_i/R)F$, where $R=\sum s_i$, the maximum amount of information FS-ISAC can deliver to its members. In this case, firms can determine the amount of information they request from FS-ISAC and pay a proportional membership fee.

In the next section, we solve the model in the game theory framework and analyze how the current FS-ISAC membership fee policies affect member firms' information sharing behaviors.

---

[8] This assumption ensures that the maximum direct cost of a security breach is larger than a firm's security budget but does not exceed a firm's total assets, which we believe, based on the current history of cyber attacks, is a true reflection of the reality.

[9] For example, if Firm *i* shares a lot of information about a security breach in its information systems, it will have a negative impact on Firm *i*'s competitiveness in the market. However, such a negative impact can be partially reduced if the rival firm also reveals information about a similar security breach.

[10] Our results still hold if we construct a firm's objective function as a minimization problem where the firm is minimizing its expected loss and overall costs. However, for ease of interpretation, we present it as a maximization problem.

Key Results from the Baseline Model

Following the standard approach in the game theory literature, we solve the model using backward deduction.[11] We start by examining the firm's strategy regarding security technology investment in stage 2, then we substitute the optimal level of technology investment obtained from stage 2 into the firm's maximization problem in stage 1 and derive the firm's optimal information sharing strategy.

In stage 2, the firm chooses the optimal level of technology investment to maximize its objective function. Differentiating equation (2) with respect to t_i yields the following first order condition (FOC):[12]

$$P'_{t_i}\left(\frac{t_i(1+r_i(f_i,\sum s_i))}{A_i}\right)\left(1+r_i(\alpha A_i - t_i,\sum s_i)+t_i r'_{t_i}(\alpha A_i - t_i,\sum s_i)\right)E[\phi]=\frac{\partial \alpha A_i}{\partial t_i}. \quad (3)$$

Since different FS-ISAC membership policies lead to different ways to compute the membership fee f_i and, consequently, the information sharing benefits FS-ISAC delivers to its members, $r_i(f_i, \sum s_i)$, we analyze the firm's strategies case by case below.

In case (i), since the membership fee is free and the amount of information FS-ISAC delivers is a constant ratio of the total information available, we can rewrite equation (3) as:

$$P'\left(\frac{t_i(1+r(\sum s_i))}{A_i}\right)E[\phi]\left(1+r(\sum s_i)\right)=1.$$

Since the above equation was derived by differentiating the objective function with respect to t_i, the left-hand side of this equation can be interpreted as the marginal benefit of technology investment, and the right-hand side of the equation can be interpreted as the marginal cost of technology investment. Therefore, as long as the marginal benefit of technology investment is greater than the marginal cost (i.e., $P'(\frac{t_i(1+r(\sum s_i))}{A_i})E[\phi]\left(1+r(\sum s_i)\right)>1$), a firm will devote its entire security budget to technology investment until the budget constraint is met ($t_i^* = \alpha A_i$). In reality, most firms have a limited IT security budget relative to its potential loss and often exhaust their budget before the marginal return of technology diminishes; hence, we focus on the case where the budget constraint is binding[13] ($t_i^* = \alpha A_i$).

Next, going back to stage 1, the firm's objective is to maximize equation (2) given the optimal technology investment t_i^* derived from stage 2. Substituting $t_i^* = \alpha A_i$ into (2) and differentiating (2) with respect to stage 1 decision variable s_i yields the following FOC:

$$P'\left(\alpha\left(1+r(\sum s_i)\right)\right)E[\phi]A_i\alpha r = d_{i1}. \quad (4)$$

The above FOC is similar to one of the situations studied in Varian [2004] in which he analyzes users behaviors when the reliability of the system depends on the total efforts exerted by all users. Following the approach used in Varian [2004], let $G(\cdot)$ be the inverse of the derivative of the probability function $P(\cdot)$, we can simplify (4) to derive the reaction function for firm i:

$$s_i(s_j) = \frac{G(d_{i1}/E[\phi]A_i\alpha r)/\alpha - 1}{r} - s_j. \quad (5)$$

Since $0 \le s_i \le 1$, the equilibrium outcome depends on the value of the first component on the right hand side of equation (5). When $\frac{G(d_{i1}/E[\phi]A_i\alpha r)/\alpha-1}{r} > 2$, it leads to $s_i+s_j>2$ which violates the constraint that $0 \le s_i \le 1$.

---

[11] Sequential games cannot be solved using forward-deduction due to the temporal nature of the game, namely, players in an earlier stage cannot predict the strategies of other players that would occur later.

[12] In mathematics, the solution to an optimization problem is generally obtained by differentiating the objective function with respect to the variable of interest and solving the resulted equation, also known as the first order condition (FOC).

[13] Binding constraint means that the solution to the optimization problem is beyond the range of values that meet the requirement of the constraint and, hence, will result in a "corner solution" which equals a boundary value set by the constraint. We derive the same result when the budget constraint is not binding. Since the nonbinding solution involves a more complicated expression, for simplicity we present our results derived from the case where the constraint is binding.

Hence the FOC outlined in (4) cannot be met, resulting in a corner solution in which $s_i^*=s_j^*=0$, indicating that at equilibrium no firms are willing to contribute any information.[14]

When $\frac{G(d_{i1}/E[\phi]A_i\alpha r)/\alpha-1}{r} \leq 2$, an interior solution can be derived from equation (5). In our model the probability function $P(\cdot)$ is the same for both firms, and α, r, and $E[\phi]$ are all constants. Therefore, the first component on the right-hand side of equation (5) differs only in d_{i1} and A_i. In this situation, which firm will provide more information will depend on the benefit-cost ratio A_i/d_{i1}. To illustrate how the equilibrium emerges in this case, we plot the both firms' reaction functions in Figure 1 and derive the Nash equilibrium graphically.

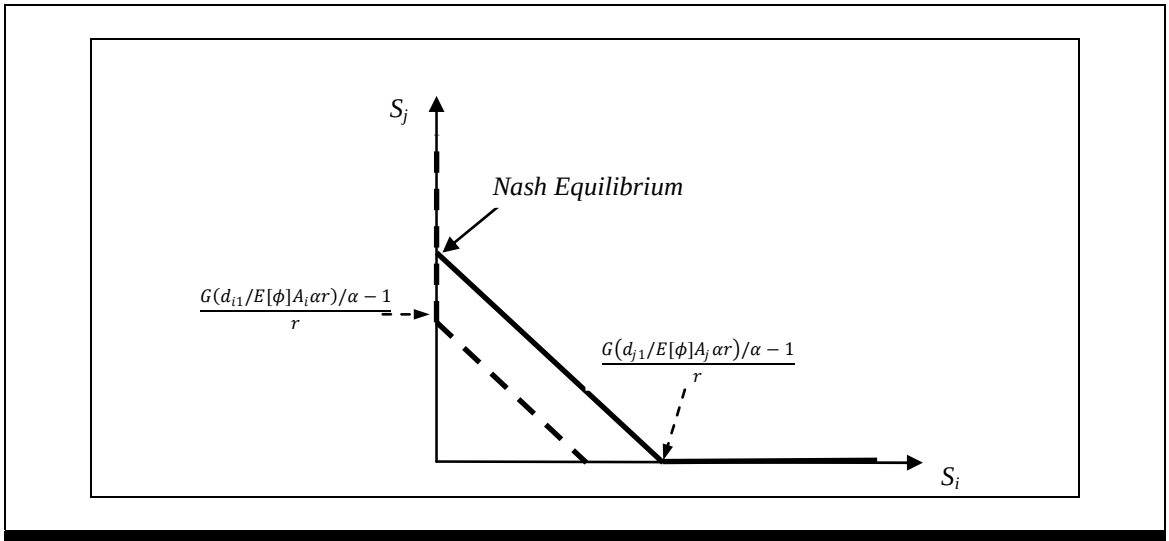

Figure 1. Nash Equilibrium in Baseline Model Case (i) (Assuming $A_j/d_{j1} > A_i/d_{i1}$)

In Figure 1, the dashed line and the solid line represent the reaction curves for s_i and s_j, respectively, and the Nash equilibrium is where the two reaction curves intersect. Figure 1 shows that, in case (i) where FS-ISAC offers a free membership and a fixed ratio of the total available information to its members, the Nash equilibrium involves firm *j* (with a higher benefit-cost ratio A_j/d_{j1}) providing all the information and firm *i* free-riding on the information provided by firm *j*. This result is very intuitive: when the amount of information FS-ISAC delivers to its members depends on some exogenous factors unrelated to information sharing, only the firm that benefits most from information sharing (i.e., either the firm with greater assets, hence, can save more from information sharing or the firm with smaller negative impact of information sharing) has incentives to contribute information and enhance the benefits of information sharing.

Next we examine if the equilibrium derived in case (i) will still emerge if FS-ISAC charges a membership fee to its members. In case (ii), FS-ISAC charges a membership fee that is proportional to a member firm's total assets ($f_i = (A_i/\bar{A})F$, where *F* is the membership fee FS-ISAC charges to the member with the highest level of assets $\bar{A}$). Accordingly, the amount of information FS-ISAC delivers to firm *i* is also proportional to the firm's total assets: $r_i(f_i, \sum s_i)=(A_i/\bar{A})(\sum s_i)$. Since the membership fee each firm pays is a fixed ratio of its security budget, similar to case (i), as long as the marginal benefit of security technology investment is greater than the marginal cost, firms will devote the remaining budget to enhancing their security technologies. In other words, t_i^* will be a fixed fraction of the firm's total assets $A_i(t_i^* = (\alpha - (F/\bar{A})A_i)$. Substituting t_i^* into (2) and differentiating with respect to s_i yields:

[14] This could happen when *r,* the extent of information sharing set by FS-ISAC, is too small or when firms have very limited security budgets (small α).

$$P'\left((\alpha-\frac{F}{\bar{A}})\left(1+\frac{A_i}{\bar{A}}(\sum s_i)\right)\right)E[\phi]A_i(\alpha-\frac{F}{\bar{A}})\frac{A_i}{\bar{A}}=d_{i1}$$

Similar to case (i), since α, $\bar{A}$, and $E[\phi]$ are all constants, the intercept of the reaction function is determined by d_{i1} and A_i. Let $\alpha'=\alpha-(F/\bar{A})$, we can rewrite firm *i*'s reaction function[15] as:

$$s_i(s_j)=\frac{G\left(\frac{d_{i1}\bar{A}}{E[\phi]{A_i}^2\alpha'}\right)/\alpha'-1}{A_i/\bar{A}}-s_j. \quad (6)$$

In this case, free-riding may still occur as long as the first component on the right hand side of equation (6) differs between the two member firms.[16] However, which firm will be willing to contribute information is unclear, due to the opposite effects a firm's total assets have on the benefits of information sharing. On the one hand, as in case (i), the firm with greater assets values the benefits of information sharing more, as their loss will be larger should a security breach indeed occur. On the other hand, due to FS-ISAC's membership policy, firms with greater assets are also entitled to more information from FS-ISAC, effectively reducing their incentives to share more information. Given these two counteracting effects, under some circumstances, it is likely that the firm with a higher benefit-cost ratio A_i/d_{i1} may choose not to share any information and free-ride the information provided by the firm with a smaller benefit-cost ratio, resulting in a further distorted equilibrium.

The analysis so far has led to the following results:

Result 1: Free-riding or no information sharing may arise as a Nash equilibrium if FS-ISAC's membership fee is free or based on the total asset level.

Result 2: In case (i) where the membership fee is free (for small firms) and free-riding is the Nash equilibrium, the firm that has a higher benefit/cost-ratio has more incentive to share information.

Result 3: In case (ii) where the membership fee depends on a firm's total assets and free-riding is the Nash equilibrium, under some circumstances even the firm that has a higher benefit/cost ratio may choose to free-ride the information provided by the firm with a lower benefit/cost ratio.

Next, we examine case (iii). When FS-ISAC sets a membership fee based on the amount of information a member firm requests, the benchmark membership fee *F* is the highest fee FS-ISAC charges to members who demand all the security-related information. For firms that choose not to request the full amount of information, the membership fee will be proportional to the amount of information it requests. That is, $f_i=(r_i/\sum s_i)F=\alpha A_i-t_i$. Accordingly, the amount of information FS-ISAC delivers to firm *i* is: $r_i=\frac{\alpha A_i-t_i}{F}(\sum s_i)$. Therefore, firm *i*'s maximization problem can be rewritten as:

$$Max \quad P\left(\frac{t_i(1+\frac{(\alpha A_i-t_i)}{F}(\sum s_i))}{A_i}\right)\phi A_i \; -d_{i1}s_i+d_{i2}s_j-\alpha A_i. \quad (7)$$

Unlike the previous two cases, firms need to strategically determine how they will split the budget between technology investment and FS-ISAC membership fee.[17] As before, we start by examining firm's strategy in stage 2. Differentiating equation (7) with respect to t_i yields the following FOC:

$$P'(\frac{t_i(1+\frac{(\alpha A_i-t_i)}{F}(\sum s_i))}{A_i})(1+\frac{(\alpha A_i-2t_i)}{F}(\sum s_i))\frac{1}{A_i}E[\phi]=0. \quad (8)$$

---

[15] A reaction function is a function that represents a player's best response to other player(s)' action(s). Jointly solving a group of reaction functions is a common method to derive the equilibrium of a game (the best outcome for all players involved in the game).

[16] As discussed in case (i), if the first component on the right hand side of equation (6) is too large, then the FOC cannot be met and a corner solution will arise in which no firms are willing to share any information.

[17] As in the previous two cases, we assume that the budget constraint is binding.

Since $P'(t_i)>0$ when $0<t_i\leq\alpha A_i$, solving equation (8) yields:

$$t_i^* = \frac{\alpha A_i}{2} + \frac{F}{2(\sum s_i)}, \tag{9}$$

$$f_i^* = \frac{\alpha A_i}{2} - \frac{F}{2(\sum s_i)}. \tag{10}$$

Not surprisingly, a higher membership fee F increases a firm's investment in security technology since the marginal benefit of information sharing decreases relative to that of technology investment. Conversely, the more information FS-ISAC collects ($\sum s_i$), the more likely a firm will prefer to allocate more of its budget to paying a information sharing membership fee.

Going backward to Stage 1, substituting (9) and (10) into (7) yields:

$$Max \quad P\left(\frac{(\frac{\alpha A_i}{2}+\frac{F}{2(\sum s_i)})(1+\frac{\left(\frac{\alpha A_i}{2}-\frac{F}{2(\sum s_i)}\right)}{F}(\sum s_i))}{A_i}\right)\phi A_i \; - d_{i1}s_i + d_{i2}s_j - \alpha A_i.$$

Since the functional form of the probability function $P(\cdot)$ is unknown, we are unable to derive an explicit expression for s_i^*. However, to gain some insights from this case, we discuss a simplified form of the model. Let $F(\sum s_i)$ be the function FS-ISAC uses to determine the benchmark (highest) membership fee. It is reasonable to expect that the fee FS-ISAC charges depends on the total amount of information it collects ($\sum s_i$) and is increasing in $\sum s_i$. We assume that $\partial F/\partial \sum s_i = m$, where m is a scalar exogenously determined by FS-ISAC. This assumption implies that the benchmark membership fee F is a linear function of the total amount of information available to FS-ISAC. In this case, we can simplify expressions (9) and (10) to:

$$t_i^* = \frac{\alpha A_i}{2} + \frac{m}{2}, \tag{11}$$

$$f_i^* = \frac{\alpha A_i}{2} - \frac{m}{2}. \tag{12}$$

(11) and (12) suggest that t_i^* and f_i^* do not depend on $\sum s_i$. Substituting them into equation (7) yields:

$$Max \quad P\left(\frac{(\frac{\alpha A_i+m}{2})(\frac{\alpha A_i+m}{2m})}{A_i}\right)\phi A_i \; - d_{i1}s_i + d_{i2}s_j - \alpha A_i.$$

Since the only component in the objective function that involves s_i is $d_{i1}s_i$, it is straight forward that both firms will not share any security-related information because doing so will only results in some detrimental effect on the firm itself without reducing its system vulnerability. Hence, a firm's optimal strategy is not to share any security-related information and to invest only on security technologies.

> *Result 4: In case (iii), when the benchmark membership fee FS-ISAC charges is a linear function of the total amount of information available to FS-ISAC, both firms will choose not to share any security-related information.*

The above results can be easily extended to a setting where there are n member firms in the network. Therefore, we conclude that the current membership policies adopted by various information-sharing alliances all have the potential to suffer the free-riding problem. Under some circumstances, the membership fee policy may even lead to an equilibrium where none of the firms is willing to share any information. These outcomes are largely because the existing membership policies fail to align the interests of the individual members with the benefits of the entire network. More specially, the membership fee charged to a given member is not associated with the amount of information it shares, which to some extent explains the puzzle we described in the introduction—although many victims of the security attacks are members of FS-ISAC, information about security breaches are not shared effectively within the network due to the lack of an appropriate mechanism to encourage sharing. To address this issue, in the next section we propose a new membership policy that incorporates an insurance option and

examine whether such a new policy can encourage member firms to share more information and reduce the potential loss from a security attack. Moreover, since several prior studies indicate that insurance companies may be reluctant to offer cyber insurance due to the possibility that they may not profit from the security market, we also investigate if such an insurance plan is feasible from the insurer's standpoint.

IV. AN EXTENDED MODEL

Our analysis in Section III shows that even if FS-ISAC customizes its membership fee based on the individual member's asset level or demand for information, the member firm may not have a strong incentive to truthfully share any security-related information with other firms in the network. Hence, the solution to this problem lies in establishing a mechanism that ties a firm's membership fee to the amount of information it contributes and demonstrating that firms will be better off paying such a membership fee to participate in an information sharing alliance, rather than fighting independently against various security vulnerabilities. However, as stated in the introduction, a major challenge of such a mechanism is the difficulty involved in measuring and monitoring how much security-related information a member firm possesses relative to how much information it discloses, which is probably one of the main reasons why the current FS-ISAC membership fee policies does not involve the amount of information shared by a member firm. Without a robust approach to measure this critical output factor, it is impossible to create an incentive compatible mechanism to resolve the free-riding issue that currently prevails in many information sharing networks.

Social Optimal Outcome

In order to derive such a mechanism, we start by exploring what the optimal outcome is from the social welfare's standpoint. Assuming that there is a social planner who coordinates the behaviors of various member firms in an information sharing network such as FS-ISAC, this social planner aims at maximizing the overall security protection (or minimizing the total losses due to security breaches) of all members within the network. In other words, when there are n firms in the network, the social planner seeks to maximize the following objective function:[18]

$$Max \quad \sum_i P\left(\frac{t_i(1+r_i(f_i,\sum s_i))}{A_i}\right)\phi A_i \; - \sum_i d_{i1}s_i + \sum_i d_{i2}Max(s_j) - \sum_i \alpha A_i. \qquad (13)$$

Since the goal of the social planner is not to maximize the profits of FS-ISAC and there is a positive relationship between the overall benefits and the information available to each member firm, namely $r_i(\sum s_i)$, it follows that providing a free membership[19] to member firms will maximize the above objective function. That is, set f_i=0 so that $r_i(\sum s_i)=\sum s_i$ and $t_i \le \alpha A_i$. Substituting f_i=0 into the above objective function and differentiating with respect to t_i yields the following FOC:

$$P'\left(\frac{t_i(1+\sum s_i)}{A_i}\right)E[\phi](1+\sum s_i) = 1.$$

Let function $G(\cdot)$ be the inverse of the derivative of the probability function $P(\cdot)$. We can rewrite the above FOC as:

$$t_i^* = G\left(\frac{1}{E[\phi](1+\sum s_i)}\right)\frac{A_i}{(1+\sum s_i)} = k(\sum s_i)A_i. \qquad (14)$$

where $k(\sum s_i)$ is a function of $\sum s_i$. Since member firms can enjoy the benefits of information sharing without paying a membership fee, as long as the marginal benefit of technology investment is greater than 1 (marginal cost), each firm will devote as much budget to maximize the technological protection until equation (14) is satisfied or when the budget limit is reached, whichever comes first. Moreover, because α, $E[\phi]$, and $\sum s_i$ are identical across firms, equation (14) also implies that the social optimal level of technology investment is a fraction of the firm's assets and this fraction is the same across firms.

---

[18] In the N-firm setting, the indirect positive effect for firm i is computed as d_{i2} multiply $Max(s_j)$, the maximum amount of information shared by other firms.

[19] For simplicity, we are assuming that the cost of running FS-ISAC is zero. Our results will still hold if there is a positive cost.

Going back to stage 1, each member firm will determine how much security-related information it will contribute given its expected technology investment derived in (14). Substituting (14) (or $t_i^* = \alpha A_i$ if the budget constraint is binding) into the objective function (13) and differentiating with respect to s_i yields:[20]

$$\begin{cases} \frac{\sum A_i}{(1+\sum s_i)} - d_{i1} = k'(\sum s_i)A_i \text{ (if the budget constraint is not binding), or} \\ \sum_i P'\big(\alpha(1+\sum s_i)\big)\alpha E[\phi]A_i = d_{i1} \text{ (if the budget constraint is binding).} \end{cases} \quad (15)$$

Since $P'\big(\alpha(1+\sum s_i)\big)\alpha E[\phi]$ is the same across firms, we can rewrite (15) as:

$$\begin{cases} (1+\sum s_i) = \frac{\sum A_i}{k\prime(\sum s_i)A_i + d_{i1}} \text{ (if the budget constraint is not binding), or} \\ (1+\sum s_i) = \frac{G\left(\frac{d_{i1}}{\alpha E[\phi]\sum A_i}\right)}{\alpha} \text{ (if the budget constraint is binding).} \end{cases} \quad (16)$$

Both expressions in (16) show that a key difference between the social planner's optimal strategy and that of the individual member firm is that the social planner takes into account all the assets that could be affected by the information sharing behavior ($\sum A_i$), whereas the individual member cares only about its own assets (A_i). Hence, as long as the negative impact factor d_{i1} is similar across member firms, all members will contribute equal amount of information and the extent of sharing increases with the total wealth within the network ($\sum A_i$).

Based on this result, we proceed to explore whether an incentive mechanism can be built into the membership policy to achieve this social optimal outcome. In a prior study on system reliability, Varian [2004] proposes that, to avoid free-riding in a system that depends on collective efforts, a fine equal to the cost of a system failure to all other users should be imposed on the user who is most likely to deviate from exerting efforts. Can we introduce a similar mechanism into information sharing networks such as FS-ISAC to eliminate the free-riding issue and achieve a higher level of information sharing?

Unfortunately, a thorough evaluation of the characteristics of the information sharing alliances shows that such a mechanism is infeasible due to a number of reasons. First, as discussed earlier, in the financial industry, the cost of a single security breach can reach as high as several million dollars, not to mention the costs of all security breaches for the entire network. Imposing such a huge fine on a single institution is practically impossible and would only discourage firms from joining the network. Second, as recognized in Varian [2004], if such a fine is used to compensate the victims of a security attack, it will change the behaviors of these victims. When the liability payment is too large, it may actually encourage members to "seek to be injured" (in our context, this is equivalent to inviting security attacks). Last, but not the least, such a mechanism might induce firms to reduce their investments in security technologies and rely solely on liability payments to cover the losses from security breaches, leading to a potential moral hazard issue that could jeopardize the existence of organizations such as FS-ISAC.

An Insurance Model

To address the aforementioned issues, based on the idea of "liability payment" introduced in Varian [2004], we propose that information sharing alliances such as FS-ISAC should revise their existing membership policies and incorporate an insurance plan that is affordable to members of information sharing alliances and yet compatible with the objectives of information sharing. The insurance plan aims at achieving three goals: (1) to encourage firms to join an information sharing alliance and truthfully disclose their security-related information, (2) to improve the overall system reliability of all members within the network, and (3) to provide compensations to firms who actively participate in the information sharing activities through insurance premium from all members. Specifically, the changes we propose are:

[20] Since $P'(\cdot)$ is a decreasing function, $G(\cdot)$ is also a decreasing function. Hence both expressions in (15) yield the same outcome.

1) FS-ISAC offers an insurance plan to its member firms. Such an insurance plan provides coverage up to a certain limit (discussed in more detail later) when a member firm suffers some losses from an IT security breach.

2) The insurance premium replaces the existing membership fee. As long as a member firm is enrolled in the insurance plan offered by FS-ISAC, the firm is entitled to full access to the information shared by all other members and does not need to pay an additional membership fee.

3) The insurance covers only loss suffered from a security breach but not from other security incidents (i.e., employees selling sensitive customer information to outsiders, loss of data during transportation process, natural disasters, etc.).[21]

4) Unlike the insurance plans offered in other markets where the insurance premium depends on the coverage level, in our extended model the insurance premium depends on the expected losses of all member firms. More specially, in an information sharing network where there are *n* member firms, the insurance premium Firm *i* pays is calculated as the average expected loss across all firms in the network:

$$(\sum_i (1 - P\left(\frac{t_i(1+\sum s_i)}{A_i}\right))\phi A_i)/n.$$

5) For firms enrolled in the insurance plan, if they suffer a loss from a security breach, FS-ISAC will compensate them based on the amount of funds available (total amount of premium collected) and the actual loss of the firm (denoted by AL_i) relative to the total losses occurred within the entire network. That is, the loss coverage provided to firm *i*, denoted by LC_i, is represented as:

$$LC_i = \frac{AL_i}{\sum_i AL_i}(\sum_i (1 - P\left(\frac{t_i(1+\sum s_i)}{A_j}\right))\phi A_i)$$

The purpose of this rule is to protect the FS-ISAC from going bankrupt in the event that the total losses is much larger than the insurance premium FS-ISAC has collected.

To analyze this new policy, we rewrite Firm *i*'s objective function as follows:

$$Max\, P\left(\frac{t_i(1+\sum s_i)}{A_i}\right)\phi A_i - \frac{\sum_i (1 - P\left(\frac{t_i(1+\sum s_i)}{A_i}\right))\phi A_i}{n} + E[\frac{AL_i}{\sum_i AL_i}](\sum_i (1 - P\left(\frac{t_i(1+\sum s_i)}{A_j}\right))\phi A_i)] - d_{i1}s_i + d_{i2}Max(s_j) - t_i.$$

Note that even though the actual loss occurred to a firm is unknown (neither is the actual loss coverage), a firm can maximize its objective function based on the expected values of the factors involved in the calculation of the loss coverage. Since $E[\sum_i AL_i] = (\sum_i (1 - P\left(\frac{t_i(1+\sum s_i)}{A_j}\right))\phi A_i)$, it follows that $E[LC_i] = E[AL_i] = (1 - P\left(\frac{t_i(1+\sum s_i)}{A_j}\right))\phi A_i$, and Firm *i*'s objective function becomes:

$$Max\ \phi A_i - \frac{\sum_i (1 - P\left(\frac{t_i(1+\sum s_i)}{A_i}\right))\phi A_i}{n} - d_{i1}s_i + d_{i2}Max(s_j) - t_i. \quad (17)$$

As before, we solve the model using backward deduction. In Stage 2, the firm's FOC with regard to t_i is:

$$P'\left(\frac{t_i(1+\sum s_i)}{A_i}\right) = \frac{n}{E[\phi](1+\sum s_i)}. \quad (18)$$

Note that in this insurance model the marginal cost of technology investment is *n* times larger than the marginal cost in the baseline model. Therefore, the budget constraint is much less likely to be binding and an interior solution is more likely to arise. Let $G(\cdot)$ be the inverse of the derivative of the probability function $P(\cdot)$. We can rewrite (18) as:

$$t_i^* = G(\frac{n}{E[\phi](1+\sum s_i)})\frac{A_i}{(1+\sum s_i)} = k(\sum s_i)A_i. \quad (19)$$

[21] This rule avoids member firms to rely on the insurance to cover losses that cannot be minimized through information sharing.

Furthermore, since n, $E[\phi]$ and $\sum s_i$ are all the same across firms, equation (19) shows that the optimal level of technology investment is a fraction of the firm's assets and this fraction is the same across firms. Substituting (19) into (17) and differentiating with respect to s_i yieds:

$$P'\left(G\left(\frac{n}{E[\phi](1+\sum s_i)}\right)\right)\frac{\sum \phi A_i}{n} - d_{i1} = k'(\sum s_i)A_i.$$

Since G is the inverse of $P'(\ )$, the two functions cancel out and we can rewrite the above FOC as:

$$(1+\sum s_i) = \frac{\sum A_i}{k'(\sum s_i)A_i + d_{i1}}, \tag{20}$$

which is the same as the optimal solution to the social planner's problem derived in (16). Hence, the insurance plan we propose enables FS-ISAC to achieve the social optimal level of information sharing.

Result 5: When firms pay an insurance premium equal to the average expected loss of all the firms within the insurance network, it will lead to the social optimal level of information sharing behavior.

From (20) we can also derive the firm i's reaction function:

$$s_i(s_j) = \frac{\sum A_i}{(k'(\sum s_i)A_i + d_{i1})} - \sum_{j(j\neq i)} s_j - 1. \tag{21}$$

Since the function form of $P(\cdot)$ is unknown, we are not able to derive a closed form solution for the Nash equilibrium. However, if $k(\sum s_i)$ is twice differentiable in s_i, and the first term on the right hand side of (21) differs across firms, the parallel reaction curves that we see in Figure 1 do not arise in equilibrium. Firms' reaction curves will intersect at a point not locating on either X- or Y-axis, leading to a Nash equilibrium that does not involve the free-riding behavior.

Result 6: Free-riding does not arise in equilibrium when firms pay an insurance premium equal to the average expected loss of all the firms within the insurance network.

Incentives to Join the Insurance Network

When the insurance option is available, an important issue is whether member firms are willing to pay the premium and enroll in the insurance plan. We compare the equilibrium solutions both in the presence and absence of the insurance option to examine whether firms will be better off joining the insurance network.

From the above analysis, we know that, if a firm chooses not to participate in the insurance plan, it invests in security technology only to maximize its objective function. This optimal solution is given by: $t_i^* = G(\frac{1}{E[\phi]})A_i$. Substituting t_i^* into a firm's objective function yields the firm's maximal benefits in the absence of insurance coverage:

$$P\left(G\left(\frac{1}{E[\phi]}\right)\right)\phi A_i - G\left(\frac{1}{E[\phi]}\right)A_i.$$

For ease of comparison, we also substitute the same $t_i^* = G(\frac{1}{E[\phi]})A_i$ into a firm's objective function[22] that includes the insurance coverage:

$$\phi A_i - \left(1 - P\left(G\left(\frac{1}{E[\phi]}\right)(1+\sum s_i)\right)\right)\frac{\sum_i \phi A_i}{n} - d_{i1}s_i + d_{i2}Max(s_j) - G\left(\frac{1}{E[\phi]}\right)A_i.$$

[22] Since this t_i^* is not the optimal level of security technology investment derived from the objective function with the insurance coverage, the resulted equilibrium payoff will be less than that of the insurance equilibrium. Hence, if, at this technology investment level, enrolling in the insurance plan leads to a better outcome than not doing so, then it follows that, at equilibrium, the insurance equilibrium will dominate the noninsurance equilibrium.

It follows that in order for a firm to enroll in the insurance plan, the premium it pays plus the net indirect effect of information sharing ($d_{i1}s_i - d_{i2}Max(s_j)$) must be less than its expected loss in the absence of insurance. That is, the following condition needs to be satisfied:

$$\left(1 - P\left(G\left(\frac{1}{E[\phi]}\right)(1+\sum s_i)\right)\right)\frac{\sum_i \phi A_i}{n} + d_{i1}s_i - d_{i2}Max(s_j) < (1 - P\left(G\left(\frac{1}{E[\phi]}\right)\right))\phi A_i. \quad (22)$$

Since the function form of the probability function $P(\cdot)$ and the parameters values of d_{i1} and d_{i2} are all unknown, we are not able to derive an explicit result. However, assuming that the net indirect impact of information sharing is small relative to expected loss of a security breach, then the option a firm prefers reduces to the comparison of the insurance premium and the expected loss of a security breach, that is: $\left(1 - P\left(G\left(\frac{1}{E[\phi]}\right)(1+\sum s_i)\right)\right)\frac{\sum_i \phi A_i}{n}$ and $(1 - P\left(G\left(\frac{1}{E[\phi]}\right)\right))\phi A_i$. A quick comparison of these two expressions shows that when a firm is enrolled in the insurance plan, the probability of successfully protecting its systems from being compromised is much higher than that in the absence of the insurance. Furthermore, as the number of firms that join the insurance plan increases, this probability further increases (due to higher $\sum s_i$). Hence, for a firm whose asset level is larger than or equal to the average asset level within the network, it will be better off enrolling in the insurance plan. However, the outcome of the comparison is undetermined if a firm's total asset level is much smaller than the average. Inequality (22) suggests that by paying an insurance premium equal to the average expected loss of all firms in the network, a small firm will have to bear some extra risks ceded from other larger firms in the network. Hence if a firm's asset level is significantly lower than the average asset level in the network, it may not benefit as much from enrolling in the insurance plan as those whose total assets are relatively high. The above discussion leads to the following conclusion:

Result 7: When firms are similar in the asset level and the net impact of information sharing is small relative to the expected loss of a security breach, firms will be better off joining an information sharing network and enrolling in the insurance plan.

To address this issue, we propose to add an additional rule to the insurance policy.

6) Firms enrolled in the insurance plan will be categorized into different groups based on their asset levels (i.e., large, medium, and small). FS-ISAC will charge firms in the large group an additional premium to compensate firms in the small group. This transfer payment is calculated as one half of the difference between the expected loss of a large and a small firm in the absence of insurance.

$$\left(1 - P\left(G\left(\frac{1}{E[\phi]}\right)\right)\right)\phi\left(\frac{A_{large} - A_{small}}{2}\right)$$

The transfer payment seeks to eliminate the incentive misalignment that results from the unproportional premium imposed on small firms. We illustrate how the transfer payment works in Figure 2.

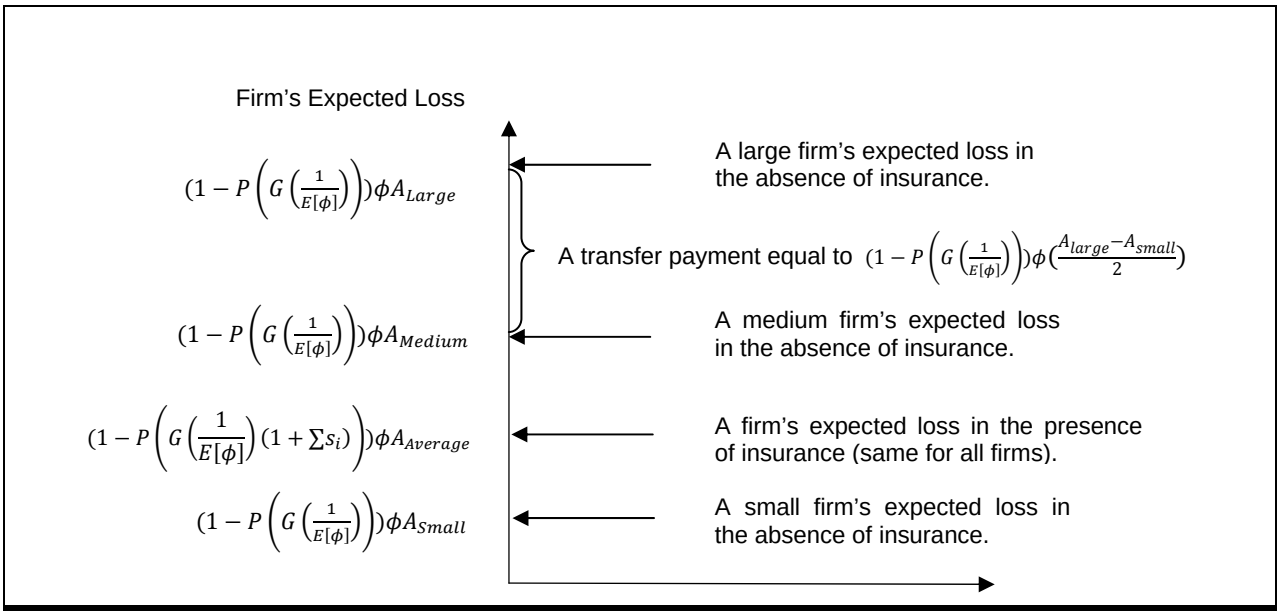

Figure 2. A Transfer Payment Scheme

Figure 2 shows the expected loss of firms of different sizes both in the presence and absence of insurance and how the transfer payment is calculated. It is obvious that larger firms benefit most from enrolling in the insurance plan, followed by medium firms. Depending on the actual size and the amount of information provided by the insurance network, small firms may or may not benefit from enrolling in the insurance network. However, if FS-ISAC charges large firms an extra fee equal to one half of the difference between the expected loss of a large and a small firm in the absence of insurance and transfers this payment to small firms, it effectively makes the expected loss of all firms within the network equal to the expected loss of an average sized firm. Since an averaged sized firm will be better off joining the insurance network, it follows that:

> *Result 8: All firms will be better off joining the insurance plan if FS-ISAC charges large firms an extra fee equal to one half of the difference between the expected loss of a large and a small firm in the absence of insurance and transfers this payment to small firms.*

This transfer payment effectively aligns the premium with the benefits derived from enrolling in the insurance plan. More importantly, the transfer payment is based on some exogenous factors and does not involve a firm's decision variables such as t_i and s_i; hence, incorporating this new rule does not change the equilibrium results derived in our extended model, and the total premium collected is still equal to the total expected loss from all firms.

V. SIMULATION

In order to demonstrate how the insurance plan proposed in our article helps to enhance the protection against cyber attacks and reduce the overall losses for companies participated in an information sharing network, we conducted a simulation to compare the total security losses of a sample of 100 firms with and without participation in an information sharing insurance plan. The two parameters that need to be randomized in this simulation are the firms that suffer a security breach in a given time period and their degree of losses from this security breach, ϕ.

Our baseline case was the loss suffered from a series of security attacks without firms participating in the insurance plan. In this baseline case, as shown in Results 1 through 4, member firms have no incentive to share any security-related information. Hence, the optimal protection strategy is to invest all of their security budgets to security protection technologies t_i. Accordingly, the direct loss to a member firm can be computed as the product of the probability of its systems being compromised $p(\ )$, its total assets A_i,

and the degree of loss from an attack ϕ. We started the simulation by randomly generating 100 firms with a mean asset level of \$100 million and a standard deviation of \$10 million.[23] This represented an information sharing network consisting of member firms of approximately the same size. These firm sizes were fixed throughout the simulation. Next, to reflect the longitudinal nature of the security breach problem, within each simulation, we repeated the randomization for the probability of security breaches and the degree of loss variables 120 times to simulate 120 months of continuous security attacks for these 100 firms. Based on equation (2), given that a firm's security budget is a function of its total assets, the probability of a member firm's information systems being compromised is the same across all member firms. We assumed such a probability is 10 percent, implying that within a given month, an average of ten out of 100 firms would suffer a loss from security breaches, and these ten victim firms were randomly generated for each month. For each firm randomly chosen as a security breach victim, we also randomly generated a value for the degree of loss that varied in the range between 0 and 10 percent of the firm's total assets.[24] Based on these randomized numbers, we computed the monthly security loss of each individual firm during the 120-month period to obtain the monthly total losses of all firms during this period. As a result, we had a series of 120 total losses data points for each simulation. The upper solid line in Figure 3 shows the monthly total losses of these 100 firms in the 120-month span for a given simulation. Since no security-related information was shared among member firms, it is not surprising to see the total losses occurred are normally and independently distributed, with an approximate average loss of \$5.5 million, and a lack of a clear trend. The dotted line is the monthly total losses of these 100 firms averaged across 20 simulations. It follows a smoother trend but shows the same pattern as demonstrated in the individual simulation.

Next, to examine what would happen if our proposed insurance plan was implemented on these 100 firms and the same security attacks were to occur again in the same 120-month period, we computed the monthly total losses of these 100 member firms that now shared their security breach information and participated in the insurance plan. As discussed in Section IV, when the insurance option is available, member firms will have strong incentives to share information related to prior security attacks in return for similar information from other member firms. Accordingly, their losses will be covered by the premium collected by the information sharing network. In the presence of insurance participation and information sharing, one important distinction is that the probability of security breaches is no longer a constant value as modeled in the baseline case but will change from month to month. To compute the probability of security breaches, we operationalized the contribution of the shared security information to the probability of security breaches based on the amount of losses suffered by a given firm. In other words, we assumed that each security attack was independent and the more losses suffered by a firm, the more information it would be able to contribute to the information sharing network; thus reducing the probability of security risks facing the entire network. Moreover, consistent with the set-up in our analytical model, and to capture the fact that new attacks constantly emerge which cannot be fully prevented through the use of past security breach information, we discounted the contribution of security breach information through a concave function and modeled it as a variable that showed decreasing return to scale.[25]

Similarly, since the insurance premium was based on the expected losses of all firms, which change as the amount of the shared security-related information increases, we also computed the premium as a dynamic variable based on the overall losses in the previous period. For the first period, we used the average losses in the absence of insurance in the baseline case to determine the premium. Because these firms were assumed to be of similar sizes, for ease of computation, the insurance premium paid by a given firm was the total expected losses divided by 100, which was the number of firms in our simulation.

---

[23] Note that changing the values of these randomization parameters does not change the results, as long as the randomized variables follow the same distribution.

[24] Changing the value of this probability does not change our results, as this probability is the same across all member firms.

[25] Because we did not assume a specific function form in the analytical analysis, for this simulation we used a backward induction approach to determine a specific functional form. Namely, we assume that there is a breakeven point in a concave probability function where the probability of security breaches is 10 percent when the firm's security budget is equal to 90 percent of its expected loss (which can be computed from the average loss simulated in the baseline case in which the probability of security breaches is exactly 10 percent). Through this approach, we are able to recover a concave probability function.

Based on these new parameters and the same random numbers for the degree of losses generated in the baseline case, we computed the total losses of these 100 firms and plotted the results from one simulation as the bold solid line in Figure 3. We then repeated the same simulation 100 times and plotted the averages total losses from the first twenty simulations and from all 100 simulations in the dotted and double lines in Figure 3. These lines show a clear downward trend over time, thus supporting the prediction of our proposed insurance model. For a given simulation, there are occasional spikes which capture unexpected increases in security losses caused by either a random disastrous security incident (i.e., security breaches of highly sensitive or valuable information) or a surge of new attacks not observed before (as represented by a random larger number of victim firms than projected). Despite these spikes, the overall security losses are clearly decreasing due to the contribution of shared security breach information. Moreover, it is interesting to note that within the first few months, the security losses from insurance participants can be higher than those who do not enroll in the insurance plan. This is largely due to the security budget constraint imposed in our model, which requires member firms to reduce their investment in security protection technology in order to pay for the insurance premium, and hence increasing the probability of security breaches in the earlier periods. However, the overall security vulnerability will begin to decrease as firms share more information, effectively reducing both the insurance premium and the probability of security breaches. Therefore, these higher security losses will become less and less likely in the subsequent periods.

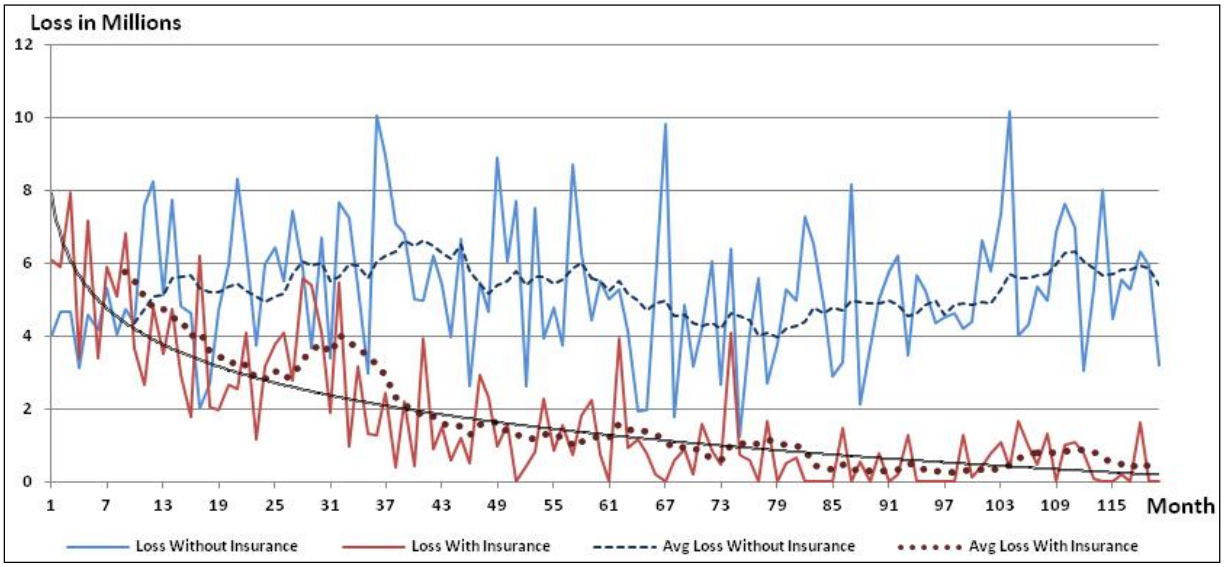

Figure 3. Comparison of Simulated Security Breach Loss (Firms of Similar Sizes)

Finally, the average plots evidently exhibit a consistent pattern as observed in the individual simulation plot, with a notable difference that occasional fluctuations in security loss essentially disappear, demonstrating the consistency of our proposed insurance method when implemented in a broader scope.

In the above simulation analysis, we show that firms of similar sizes generally benefit from participating in an information sharing insurance plan. Nevertheless, what happens if member firms vary substantially in asset level? Does the insurance option still dominate the noninsurance option? To answer this question, we performed the same simulation on a different sample of firms. This time we generated another 100 random numbers for firm size from a distribution that had the same mean value ($100 million), but with a higher standard deviation of $100 million. We computed the total losses for these 100 companies using the same method and random numbers used in the aforementioned simulation. We plotted the results in Figure 4. These plots show that the conclusions we drew in the previous simulation analysis also apply to this sample, with the only difference being that there is a higher degree of variation in overall security losses for firms that did not participate in the insurance plan, which was anticipated due to a larger

variation in firm asset level, and the probability of incurring a security breach on a much larger firm than those generated in the previous simulation. Hence, we can safely conclude that the results derived from the analytical model are supported by our simulation analysis, and regardless of asset levels, firms will enjoy significant savings by enrolling in an information sharing insurance plan.

VI. DISCUSSIONS, LIMITATIONS AND FUTURE RESEARCH

The analysis in Section IV shows that in our proposed membership policy, the insurance premium can serve as an instrument to align the incentives of member firms in sharing their security-related information. When the insurance option is absent, as shown in our baseline model, member firms have no incentive to share their security-related information due to a situation similar to the classic "*prisoner dilemma.*" Even though each member firm will be better off sharing more information, the simultaneous nature of the game and the difficulty involved in verifying and penalizing the non-cooperative behavior will lead some firms to free-ride the information shared by other firms and

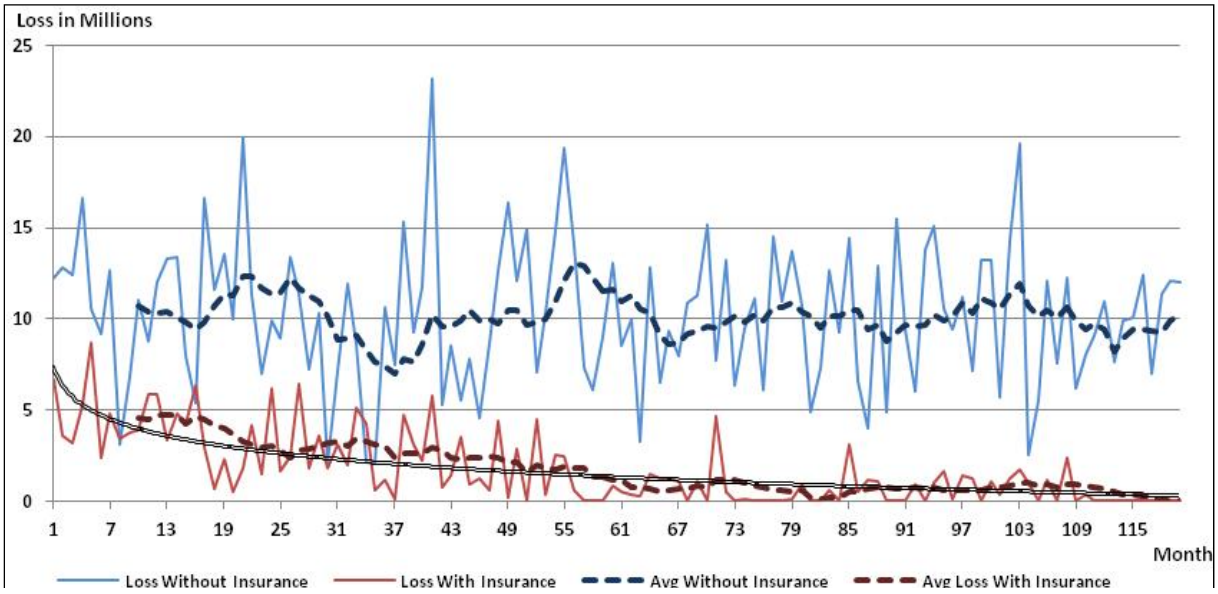

Figure 4. Comparison of Simulated Security Breach Loss (Firms of Different Sizes)

minimize the amount of information they disclose. As a result, the reliability of member firms' information systems remains unchanged after a firm joins an information sharing alliance such as FS-ISAC.

When an insurance option is incorporated into the membership policy, any potential loss from a security breach is covered by the insurance and the only significant cost factor is the insurance premium. Naturally, a member firm has a strong incentive to reduce the amount of premium it pays. Since the premium is based on the average expected loss of all member firms within the network, the only way for a firm to reduce its premium is to supply the maximum amount of information it possesses to increase the other members' system reliability. Of course, increasing the level of information sharing may also increase the indirect negative impact on the member firm itself. Nevertheless, such a negative effect will be largely offset by a similar information sharing action by the other member firms and the savings from the insurance premium will more than likely compensate the net effect. By comparing the firms' expected loss with and without the insurance option, our analysis suggests that when firms are similar in their total assets and the net negative impact of information sharing is small relative to the expected loss of a security breach, they will all be better off joining the insurance network.

However, our analysis also shows that if firms differ significantly in terms of asset levels, smaller firms may choose not to purchase insurance due to the relatively high premium it has to pay compared to its low expected loss in the event of a security breach. Consequently, the information sharing network can attract only firms with similar asset levels. This finding can be explained intuitively: The purpose of the insurance policy is to share liabilities among member firms and hold every member accountable for the other member's system reliability. Under the initial insurance policy, the identical premium implies that members will share equally the expected loss from security breaches within the entire network. Since such a loss is proportional to the other firm's assets (ϕA_i), small firms face a disadvantage as they have to undertake a larger burden of security losses than they do without enrolling in the insurance plan. Despite the coverage FS-ISAC provides and the improved system reliability, it may not compensate the extra cost of the small firms. In this case, even though enforcing the proposed insurance plan may result in the socially optimal outcome, it may come at the cost of small firms and, hence, is not incentive compatible.

To cope with this potential limitation, we revise our proposed insurance policy and implement a transfer payment from large firms to small firms. The transfer payment subsidizes small firms by reallocating the gains from fostering information sharing among various member firms, and results in the same social optimal outcome as achieved in the original insurance plan. Hence, it provides the most incentive compatible mechanism to the current information sharing alliances.

In addition to motivating firms to join the network and share information, the proposed insurance policy also ensures that any organization that provides the insurance plan will be solvent in the presence of increasing security attacks. The way insurance premium and coverage is calculated suggests that the insured has sufficient fund to cover all the claims from member firms. In the long run, we expect that such an information sharing network will attract more and more firms to participate, leading to a healthy sustainable growth cycle. Both prospects will provide important incentives for insurance companies to step into the market of cyber insurance.

Although the above analysis sheds some interesting light on existing information sharing alliances' membership policies, it is worth noting that our proposed model may be subject to a number of limitations due to its simplistic nature of the analytical model. The values of some parameters, such as the value of information and the probability of security breaches, may be difficult to determine in practice. Our simulation analysis offers a first attempt to assess security losses in the presence of an information sharing insurance plan. Other possible extensions of our study include the addition of the individual firm's security rating in the computation of insurance premium and different coverage levels for firms facing different risks. In short, we believe that our model presents an alternative approach to solve the incentive alignment issue currently confronting most information sharing networks and extensions to our proposed insurance policy will be interesting and valuable topics for both practitioners and researchers.

VII. CONCLUSION

This study examines a critical incentive alignment issue that exists in the information sharing alliance in the financial services sector and possibly other information sharing networks. Failure to encourage members to share their security-related information has seriously undermined the founding rationale of organizations such as FS-ISAC. Our analysis shows that the existing information sharing membership policies are plagued with the danger of encouraging members to free-ride the information shared by other members, leading to an outcome opposite to those proposed in these organizations' mission statements. In light of these findings, we propose to revise the existing information sharing network membership policy and incorporate an insurance option. The proposed new policy seeks to address the incentive problem from the social planner's perspective. We contend that organizations such as FS-ISAC are not merely a platform that facilitates information sharing among its member firms. They actually can play an important role in shaping the member firms' behaviors. Our results show that our proposed insurance policy can indeed align members' incentives to share their security-related information and lead to a social optimal outcome. We also demonstrate that when FS-ISAC categorize member firms based on the levels of their total assets and implement a transfer payment equal to one-half of the difference between the expected loss of a large and a small firm in the absence of insurance, all firms will be better off joining

the insurance network, and such a joint effort will lead to significant enhancement in the overall security across the network and significant savings in security breach losses.

The results of our study have important theoretical and practical implications in the security arena. The insurance model developed in this study differs substantially from any insurance policy currently offered in any markets. It is designed to address the problems presented in the field of information security. To the best of our knowledge, no such insurance model has been proposed. Hence, we believe that our novel theoretical model will challenge and shift current paradigms in research and practice. Other than the financial services industry, many other industries have also been confronted with increasing risks from cyber attacks. The method proposed in this study can be applied to those industries, too. In the short run, it may take some time for the network to accumulate a critical mass and reach the scale to leverage the power of information. Temporary loss may occur as a result of initial inefficient pricing of insurance premium, and inaccurate forecast of security risks and government subsidy may be needed for the cyber insurance market to take off. However, we expect that these issues will resolve as the network grows and policy makers have a better understanding of the dynamics in such a network.

ACKNOWLEDGEMENTS

The first author thanks the College of Business at the University of Texas at San Antonio for the financial support provided through the Summer Research Grant program.

REFERENCES

Acquisti, A. (2004) "Privacy and Security of Personal Information: Economic Incentives and Technological Solutions", in Camp, J., and R. Lewis (eds.) *The Economics of Information Security,* Kluwer. Amsterdam, Netherlands, pp-165-178.

Anderson, R. (2001) "Why Information Security Is Hard—An Economic Perspective," *Proceeding of 17th Annual Computer Security Applications Conference,* New Orleans, LA, pp. 358–365.

Anderson, R. and T. Moore (2006) "The Economics of Information Security", *Science* (314)5799, pp. 610–613.

Ba, S., J. Stallaert, A. Whinston, and H. Zhang (2005) "Choice of Transaction Channels: The Effects of Product Characteristics on Market Evolution", *Journal of Management Information Systems* (21)4, pp. 173–197.

Baer, W. and A. Parkinson (2007) "Cyberinsurance in IT Security Management", *IEEE Security & Privacy* (5)3, pp. 50–56.

Bandyopadhyay, T., V.S. Mookerjee, and R.C. Rao (2009) "Why IT Managers Don't Go for Cyber-insurance Products", *Communications of the ACM* (52)11, pp. 68–73.

Baskerville, R. (1993) "Information Systems Security Design Methods: Implications for Information Systems Development", *ACM Computing Surveys (CSUR)* (25)4, pp. 375–414.

Bohme, R. (2005) "Cyber-insurance Revisited", *Proceedings of Workshop on the Economics of Information Security, Kennedy School of Government,* Cambridge, MA, pp-31-40

Campbell, K., L.A. Gordon, MP. Loeb, and L. Zhou (2003) "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", *Journal of Computer Security* (11)3, pp. 431–448.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2004) "A Model for Evaluating IT Security Investments", *Communications of the ACM* (47)7, pp. 87–92.

Cavusoglu, H. and S. Raghunathan (2004) "Economics of IT Security Management: Four Improvements to Current Security Practices", *Communications of the Association for Information Systems* (12) Article 3, pp. 65–74.

Cawley, J. and T. Philipson (1999) "An Empirical Examination of Information Barriers to Trade in Insurance", *American Economic Review* (89)4, pp. 827–846.

Claburn, T. (2009) "Heartland Payment Systems Hit by Data Security Breach", http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212901505 (current Apr. 2, 2009).

Dhillon, G. and J. Backhouse (2001) "Current Directions in IS Security Research: Towards Socio-organizational Perspectives", *Information Systems Journal* (11)2, pp. 127–153.

Fudenberg, D. and J. Tirole (1991) *Game Theory*, Cambridge, MA: The MIT Press.

Gal-Or, E. (1985) "Information Sharing in Oligopoly", *Econometrica* (53)2, pp. 329–343.

Gal-Or, E. and A. Ghose (2005) "The Economic Incentives for Sharing Security Information", *Information Systems Research* (16)2, pp. 186–208.

Gordon, L.A. and M.P. Loeb (2002) "The Economics of Information Security Investment", *ACM Transactions on Information and System Security* (5)4, pp. 438–457.

Gordon, L.A., M.P. Loeb, and W. Lucyshyn (2003) "Sharing Information on Computer Systems Security: An Economic Analysis", *Journal of Accounting and Public Policy* (22)6, pp. 461–485.

Greenaway, K.E. and Y.E. Chan (2005) "Theoretical Explanations for Firms' Information Privacy Behaviors", *Journal of the Association for Information Systems* (6) Article 6, pp. 171–198.

Ma, Q. and J.M. Pearson (2005) "ISO 17799: 'Best Practices' in Information Security Management?", *Communications of the Association for Information Systems* (15) Article 32 , pp. 577-591.

Mas-Colell, A., M.D. Whinston, and J.R. Green (1995) *Microeconomic Theory,* New York, NY: Oxford University Press.

Mills, E. (2009) "Cybercrime Cost Firms $1 Trillion Globally", http://news.cnet.com/8301-1009_3-10152246-83.html (current Sep. 25, 2009).

Myerson, R.B. (1995) *Game Theory: Analysis of Conflict,* Cambridge, MA: Harvard University Press.

Osborne, M.J. and A. Rubinstein (1994) *A Course in Game Theory*, Cambridge, MA: The MIT Press.

Panko, R. (2003) *Corporate Computer and Network Security*, Upper Saddle River, NJ: Prentice-Hall, Inc.

Ponemon (2009) "2009 Annual Study: Cost of a Data Breach", http://www.encryptionreports.com/download/Ponemon_COB_2009_US.pdf (current Dec. 9, 2010).

Schelling, T.C. (1960) *The Strategy of Conflict*, Cambridge, MA: Harvard University Press.

Shapiro, C. (1986) "Exchange of Cost Information in Oligopoly", *The Review of Economic Studies* (53)3, pp. 433–446.

Simon, C.P. and L. Blume (1994) *Mathematics for Economists, Vol. 1,* New York, NY: Norton.

Siponen, M. (2005) "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice", *European Journal of Information Systems* (14)3, pp. 303–315.

Straub, D.W. and W.D. Nance (1990) "Discovering and Disciplining Computer Abuse in Organizations: A Field Study", *MIS Quarterly* (14)1, pp. 45–60.

Tryfonas, T. (2007) "On Security Metaphors and How They Shape the Emerging Practice of Secure Information Systems Development", *Journal of Information System Security* (3)3, pp. 21–50.

Varian, H. (2000) "Managing Online Security Risks", *New York Times* (June 1), pp. 2000–06.

Varian, H.R. (2004) "System Reliability and Free Riding", in Camp, L.J. and S. Lewis (eds.) *Economics of Information Security*, Norwell, Kluwer, Amsterdam, Netherlands p. 250.

Vives, X. (1990) "Trade Association Disclosure Rules, Incentives to Share Information, and Welfare", *The RAND Journal of Economics* (21)3, pp. 409–430.

Von Neumann, J.V., and O. Morgenstern (1944) *Theory of Games and Economic Behavior,* Princeton, NJ: Princeton University Press.

Whitworth, B., and M. Zaic (2003) "The WOSP Model: Balanced Information System Design and Evaluation", *Communications of the Association for Information Systems* (12) Article 17, pp. 258–282.

Zviran, M., and W.J. Haga (1999) "Password Security: An Empirical Study", *Journal of Management Information Systems* (15)4, pp. 161–185.