Inf Syst Front
DOI 10.1007/s10796-012-9348-y

An economic mechanism to manage operational security risks for inter-organizational information systems

Fang Fang · Manoj Parameswaran · Xia Zhao · Andrew B. Whinston

Abstract As organizations increasingly deploy Inter-organizational Information Systems (IOS), the interdependent security risk they add is a problem affecting market efficiency. Connected organizations become part of entire networks, and are subject to threats from the entire network; but members' security profile information is private, members lack incentives to minimize impact on peers and are not accountable. We model the problem as a signaling-screening game, and outline an incentive mechanism that addresses these problems. Our mechanism proposes formation of secure communities of organizations anchored by Security Compliance Consortium (SCC), with members held accountable to the community for security failures. We study the interconnection decisions with and without the mechanism, and characterize conditions where the mechanism plays roles of addressing moral hazard and hidden information issues by screening the organizations' security types and/or by providing them incentives to improve. We also discuss the welfare gains and the broad impact of the mechanism.

Keywords Inter-organizational information systems · Information security · Risk management · Economics of information systems · Economic mechanisms

1 Introduction

Today's competitive environment has significantly raised the stakes for modern organization, forcing them to explore new initiatives to improve their business efficiencies and reduce cost. To meet this particular need, the focus of information technology has shifted from the organizational level to the inter-organizational level. Hengst and Sol (2001) For example, Wal-Mart and Procter & Gamble have developed a channel partnership by leveraging their information technologies and sharing data across their mutual supply chains. The coordination of supply chain channel activities is significantly improved and the need for inventory is also reduced as a result. Grean and Shaw (2000) In addition, a rich set of literature (e.g. Ghattas and Soffer 2009; Soper et al. 2007) has reported on the organizational activities of routinely using networks to interconnect and share information with their partners, suppliers and customers. Such interconnections serve a wide variety of purposes: communication, information sharing, electronic data interchange, transaction fulfillment, business process integration, outsourcing relationships, and formation of strategic alliances. Information systems are transitioning to an era of inter-organizational information systems (IOS).

F. Fang (✉)
Department of ISOM, California State University at San Marcos, San Marcos, CA 92096, USA
e-mail: fangfang@csusm.edu

M. Parameswaran
Department of ISOM, University of Washington, Seattle, WA 98195, USA
e-mail: manojpc@uw.edu

X. Zhao
Department of ISOM, University of North Carolina at Greensboro, Greensboro, NC 27402, USA
e-mail: X_zhao3@uncg.edu

A. B. Whinston
Department of IROM, University of Texas, Austin, TX 78712, USA
e-mail: abw@uts.cc.utexas.edu

Published online: 28 March 2012

However, the above literature also points out that the further development of IOS faces many challenges, which may be related to strategy, management, policy and technology. Potential lock-in effects, network externalities, change management and organizational resistance, differing organizational cultures, variation in law and regulations across markets, differing business protocols and process definitions, data format incompatibility, consensus of choice and availability of appropriate technologies and variation in compliance requirements, are among a few on the list. Majority of the current research and industry efforts have focused on the above aspects (e.g. Fang et al. 2008; Soliman and Janz 2004). In this paper, we focus on a key challenge of IOS that has not received sufficient attention: security.

When companies connect their Information Systems with one another, the security risk accrues not only due to potential vulnerabilities of their direct partners, but also due to the vulnerability of organizations that their partners in turn connect to. Inter-organizational link to a business partner can expose an organization to network-wide risks in multiple ways: a virus at a remote member of the business network may travel multiple trusted links to eventually harm the organization's network; a hacker gaining access to a remote network can cascade intrusions through a sequence of links in the network and gain access to the organization; a zombie node in a remote organization can initiate denial-of-service attacks against the network; lack of compliance by employees in a remote organization can lead to security breaches of any of the above types; the organization may be indirectly reachable from another whose security policies fall below requirements.

The risks described above are considered to be a type of security risks caused by interconnection. To describe the idea of risks caused by interconnection, one can think of the risks that a house is caught on fire. In a community when houses are closely located, the risk is higher even though the owners themselves protect their house very carefully, such as not leaving the house with the candles lit. However, the house can still be vulnerable if the neighbors were careless. The same idea applies when organizations interconnect their information systems to improve business efficiencies. Even though one organization has invested a significant amount of money in safeguarding their own information systems and training their own employees on security risks (such as ways to prevent social engineering), their transaction data could be available through their interconnected business partners (e.g. suppliers) who do not have a good security protection and are easier for hackers to find ways to break into their systems.

Such interconnection risks significantly affect the organizations' incentives to use IOS due to the inability to foresee the vulnerability of the overall interconnection (Kumar and Sareen 2009; Kunreuther and Heal 2003). To alleviate such concerns and provide better incentives for organizations to conduct business more efficiently, we propose an incentive mechanism anchored by a Security Compliance Consortium (SCC), leading to the formation of a secure community of organizations, each member of which is accountable to every other member for security related losses caused by it.

Our proposed incentive mechanism tries to tackle the problem of self-interested organizations withholding private information (a.k.a. information asymmetry). For example, organizations may not have security infrastructure in place to protect themselves and their business partners. It could be an acceptable situation inside the organization due to the way their systems support their business. However, if such an organization creates an interconnected link with their business partners, their business partners will incur a much higher risk than expected. Our mechanism is designed to induce organizations to reveal their true types regarding their existing security profiles. Or, even better, it can provide such organizations incentives to improve the infrastructure and hence enhance their chance of establishing business connections. Revelation of types and improved investments in security by an individual organization would benefit the community as a whole. In other words, our proposed mechanism seeks to ensure that self-interested actions aggregate to advancing the community welfare as well.

The key to resolving the interdependency issue and meeting the above objective is accountability. Our proposed SCC will impose accountability among the participating organizations and force them to make their security and interconnection decisions considering not only themselves but the overall network as a whole. The secure community of organizations serves as the basis of a mechanism that reduces information asymmetry. The community is administered by a Security Compliance Consortium (SCC), and choice to join is voluntary, but comes with accountability for losses caused by the member organization to any other member of the community. The SCC administers membership in the community with the objective of ensuring outcomes that are best for the community. It may be constituted by consensus among a consortium of leading organizations. It is not required that the SCC takes specific stances on choice of technologies or specific standards of security within the community. SCC does not require member organizations to conform to a specified level of

security, given the difficulty to observe and verify the security level or investment.

To demonstrate the improvement in efficiency, we present an analytical model with two types (type 1 and type 2) of organizations, which are different in their costs of improving security from low to high probability of safety. A type 1 organization tends to maintain a high security level but a type 2 organization does not have an incentive to maintain a high security level due to various reasons. A type 2 organization finds it more expensive to improve its security level in order to ensure accountability to the whole community. Both types are self-interested in all actions, and their information about their types is private. Their investments in improving security are not publicly observable.

The most obvious reason for an organization to be of type 2 is that the company's security policy and practice may be too liberal. Organizations that consider security important may still find themselves in type 2 category for a variety of reasons. Some possible reasons are: lack of resources in small firms, lax employee practices, lack of central control, treating security as a necessary but not important requirement primarily for compliance, lack of attention due to a lack of any past history of attacks, and being located in a geographic area or internet domain which has low security profile.

Organizations in our model have three choices: to join the community or not, the type of connection used (with or without IOS) to share information with each partner, and what type of safety level to maintain for their information systems. There is no value in not being connected. We model the interdependent choices of organizations as a signaling-screening game.

When members of the community connect with others using IOS, they incur managed risk and gain value. The risk is managed because community membership implies accountability by partners. Connecting with other members without using IOS is a dominated strategy for the members. With non-members (outsiders), members of the community have two choices. The first is to connect using IOS, which implies higher security risk. The other option is to connect without IOS, implying no risk of interconnection, but less added value due to increased operational costs, delayed information acquisition, and/or sub-optimal decision making.

When the partners are not members of the community, connection using IOS also incurs additional cost of securing the interconnection. Outsiders' choices of mode of interconnection with other outsiders will also involve choosing whether to connect with IOS or not, with the former option adding risk, and the latter option reducing value. Outsiders' interconnection with members will depend on the choices made by members.

The rest of the paper is organized as follows: Section 2 reviews the existing literature on organizational security risks and interorganizational systems. We then describe the analytical model, discuss its implications, characterize the effects of introduction of the mechanism under various conditions and demonstrate welfare gains in Section 3. Section 4 concludes the paper with a discussion of managerial implications and future extensions.

2 Literature review

Information security has been a focus of Information Systems (IS) research long before security became a mainstream topic (e.g. Straub 1990; Straub et al. 2008). Many of the recent studies focus on the economic aspects of information system security (Gordon and Loeb 2006; Kannan and Telang 2005). Of particular interest is the question of how organizations decide to invest in security and at what levels. The investment question has been addressed in the general context (e.g., Gordon and Lobe 2002; Hausken 2006) and in the context of a specific class of security solutions, Intrusion Detection Systems (Cavusoglu et al. 2005). The common approach in investment research has been to treat security risks as exogenous, even when both external attacks and internal threats are investigated. In general, IS research has focused on information security in the context of intra-organizational information systems. We identify issues of interdependent risk originating from interconnections using IOS, and propose a solution to improve efficiency of investment in the presence of such risk.

Literature on economic aspects and interdependent risks of IOS is limited. Prior research has examined IOS from the economic perspective in the context of their adoption, diffusion, property rights, network externalities and switching costs (e.g. Bakos and Nault 1997; Barua and Lee 1997; Han et al. 2004; Wang and Seidmann 1995; Zhu et al. 2006). Kunreuther and Heal (2003) characterizes a class of interdependent security risks and demonstrate that firms generally under-invest in security protections when their security risks are interdependent. Varian (2004) explained the decision on security investment in such a multi-firm environment using the theory of "private provisioning of public goods," which was well-studied in economics (See Mas-Colell at al. 1995; Varian 1992; Samuelson 1954). This line of literature has been extended to a supply chain setting in Bandyopadhyay et al. (2010). Ogut et al. (2005) uses an economic model to examine firms' investments in security protections and their use of

cyber-insurance in the context of interdependent security risks. They find that security investment and the insurance coverage levels are less than the corresponding socially optimal levels when cyber-risks are interdependent. Zhao et al. (2009) considers both the positively and negatively interdependent security risks and examine two alternative risk management solutions—risk pooling arrangement (RPA) and managed security services (MSS) in addition to cyberinsurance. They find that RPA and MSS can complement cyberinsuance and help address the issues of investment inefficiency caused by risk interdependency. Interdependent risk of e-mail and Internet service providers has been examined in the context of spam, where mutual accountability among certified providers was found to reduce risk (e.g. Parameswaran et al. 2007; Zhao et al. 2008). Our paper complements this stream of research by studying solutions to inefficient investment in IOS caused by inter-dependent security risk.

3 Model setup

In this section, we first introduce an analytical model to characterize decisions by organizations when acting alone. We then extend it to the case where information systems can be interconnected. We model the interconnection environment as a signaling-screening game, characterize various outcomes, and study welfare implications.

In the absence of the mechanism, we show that moral hazard is prevalent, the low types have no incentive to improve security, and in some cases even the high types lack incentive to improve security. With the introduction of the mechanism, we show that the moral hazard problem can be addressed, high types always have an incentive to improve security, and the low types have an incentive to improve security under specific conditions.

3.1 A security model for standalone information systems

We assume a set of n modern organizations, each with its own information systems deployed within its organizational boundaries. The set of the organizations is denoted as $N := \{1, 2, \cdots, n\}$. Each organization $i \in N$ decides on the level of security investment based on a cost-benefit analysis. In order to do so, the organization needs to evaluate the following parameters: V_i—the value of implementing the information systems in organization i; $p_i \in (0, 1)$—a probability measurement of the information systems safety level; v_i—the expected loss of each security attack; and $C_i(p_i)$—the investment in security needed to maintain the security level p_i.

Note that prior literature has proposed many measurements of organizational information systems security. In this paper, we define the safety level as the probability that an organizational system stays risk free. In other words, $(1 - p_i)$ represents the probability that the organizational IS will experience a security compromise.

Without loss of generality, we assume that the safety level p_i can be maintained at two possible values: p_h and p_l, where $0 < p_l < p_h < 1$. Organization i chooses between the two values and makes corresponding investment $C_i(p_l)$ or $C_i(p_h)$. It is also straightforward to assume that $C_i(p_h) > C_i(p_l)$ because higher safety level is always harder to maintain. ΔC_i is used to denote $C_i(p_h) - C_i(p_l)$, "the cost of security improvement."

The choice is made by comparing the net value of information systems at the two specified security levels. Mathematically, the net value (denoted as U_i^{alone}) is computed as $V_i - (1 - p_i)v_i - C_i(p_i)$, the value of using the system less the expected loss due to security risk and the cost of security investment. Lemma 1[1] shows that the organization's choice of security level will be "high" if and only if the cost of security improvement is less than the benefit of improved security.

Lemma 1 *Organization i will maintain a safety level $p_i = p_h$ if the cost of security improvement ΔC_i is no higher than the expected reduction in loss from security failure $(p_h - p_i)v_i$. The resulting net value of the information systems is:*

$$U_i^{\text{alone}}(p_h) = V_i - (1 - p_h)v_i - C_i(p_h). \quad (1)$$

Otherwise, the organization will choose to maintain a low safety level p_l with a net value:

$$U_i^{\text{alone}}(p_l) = V_i - (1 - p_l)v_i - C_i(p_l). \quad (2)$$

Please note that here we assume that the value V_i is large enough so that $\max\{U_i^{\text{alone}}(p_h), U_i^{\text{alone}}(p_l)\}$ is at least positive. This condition ensures that all types of organizations will maintain a positive overall value, given their best choice of security, and stay in business.

Prior to the advent of widespread use of IOS, each organization treated its own information systems as private assets managing their own information flows and improving efficiency of business processes. Investment in security was directed at proper functioning of systems and protecting the organizational information

[1] All the proofs of the Lemmas and Propositions are provided in Appendix A.

assets from being inappropriately accessed or modified. When organizational information systems stand alone, the organizations' security investment choices are independent decisions that maximize their own net value.

In this paper, we intend to assess levels and effectiveness of investments in security across all the organizations in the set. Therefore, we use *overall welfare level*, defined as the aggregate net value generated from the information systems for the n organizations, to measure the efficiency level of security investment. When organizations independently evaluate their system security environment and make corresponding decisions on their required safety level maximizing individual net value, the welfare level of the information systems across those organizations is maximized as well. However, as we will show in the following sections, inter-connecting the information systems across organizational boundaries will change the optimality of the welfare level when organizations make their security investment decisions in a decentralized fashion.

3.2 Extending the security model to IOS

Increasingly, organizations are realizing the value of information sharing and are deploying IOS. However, linking with information systems outside the organization brings additional security concerns to existing systems. Malicious hackers may find a way to route attacks to the targeted organization through the partner. Worse, the attack may not come from the business partners the organization directly linked to but from some organization that was linked with a business partner. All the organizations that are linked together directly or indirectly form an interconnected network, whose vulnerability accumulates all the organizations' vulnerability. For example, if we denote the set of organizations in the same interconnected network with organization i as N_i, then the aggregated probability of security breaches organization i expects to suffer will be $\sum_{j\in N_i}(1-p_j)$. In the equation, j is any organization that is directly or indirectly connected to organization i. Organization i's expected loss in each attack is v_i and hence the expected loss can be calculated as $\sum_{j\in N_i}(1-p_j)v_i$. For that reason, to evaluate the risk of interconnection, organization i needs to estimate all the other organizations' safety level p_j for $\forall j \in N_i$. However, p_j is usually information private to organization j. No organization will voluntarily admit its safety level is low and push potential business partners away. This *hidden information* problem introduces a particular challenge for organizations in identifying secure business partners to interconnect with.

For each organization, we assume that interconnecting its relevant information systems with those of their partners provides the most efficient business processes and competitive advantages. That is, if a pair of companies decide to form a strategic partnership and link their systems together using IOS, both of them will enjoy an added net value of V^A, which can be considered the overall value less the investment and operating cost.[2] Alternatively, if either decides that using IOS is not in its best interest, it can choose to perform the process that uses shared information asynchronously. For example, instead of allowing the salesperson from organization b to query its inventory level directly, organization a can request that the salesperson submit a request form and organization a will assign dedicated personnel to review the request and generate such an inventory report for organization b. Such an asynchronously processed procedure may delay information acquisition and lose critical decision time, sacrificing process efficiency. Therefore, we assume that the added value from a partnership without IOS can only partially realize all the potential benefits of an information system linkage, denoted as δV^A. $\delta \in [0, 1)$ is a discount factor indicating the proportion of the value that can be realized from the asynchronously linked inter-organizational processes.

In order to study the different connection decisions, we assume that there are two types of organizations, namely type 1 and type 2 organizations. Each incurs different costs in improving its safety level. That is, ΔC_i takes two possible values: Δ_1 and Δ_2. Type 1(2) organizations incur cost Δ_1 (Δ_2) to improve their safety levels from p_l to p_h. Without loss of generality, we assume that $\Delta_1 < \Delta_2$. Each organization knows its own type, but it cannot identify whether other organizations are of type 1 or type 2. That is, both the cost of security improvement and the safety level of an organization are private information which is neither observable nor verifiable by outsiders of the organization. All organizations share the common belief that the total number of type 1 organizations is n_1 and the total number of type 2 organizations is $n_2 = n - n_1$. We also assume that $v_i = v$ for all organizations and focus on heterogeneous cost of security investment only.

[2]Please note here we do not single out each itemized benefit and cost. Rather, we keep the term in general. Our focus of this paper is on the benefit and cost from a security breach perspective. Therefore, we consider V^A as the net value when there is no security issue at all. When there is potential security concern, we need to discount the value by including the cost of security investment and expected loss of security breach.

An organization expects to establish partnerships with only a proportion of the other $n-1$ organizations. We use a parameter λ to denote this proportion. In order to avoid trivial cases and maintain tractability of our model, we consider situations when the following conditions hold.

[Condition 1] $\Delta_2 > (p_h - p_l)v$.
[Condition 2] $\Delta_1 < n_1(p_h - p_l)v$.
[Condition 3] $\lambda(1-\delta)V^A < n_1(1-p_l)v$.

Condition 1 focuses on the case where type 2 organizations do not have incentive to improve their safety level from p_l to p_h if their systems are standalone. Condition 2 restricts that the cost of security improvement is not too high for type 1 organizations so that they may invest in high safety level p_h if they were concerned about the overall risk that they may impose on other type 1 organizations. Condition 3 requires that the added value of connecting with IOS to all the type 1 organizations, $\lambda(n_1-1)(1-\delta)V^A$, is lower than the overall added risks that all the type 1 organizations may incur by connecting to each other but they all maintain low safety levels, $n_1(n_1-1)(1-p_l)v$. Note that the term (n_1-1) appear on both sides of condition 3 and were hence cancelled out. Therefore, it is more desirable to induce type 1 organizations to maintain a high security level from a welfare point of view.

An organization needs to evaluate whether it is worthwhile to connect with its partner firms using IOS by trading off the added business value derived from the connection and the expected security risk that the connection entails. Let U_i^{conn} denote the expected net value for company i to interconnect its information systems with its business partners', which can be computed using the following formula:

$$U_i^{\text{conn}} = V_i + \lambda(n-1)V^A - (1-p_i)v - \sum_{j\in N_i}(1-p_j)v - C_i(p_i). \quad (3)$$

When the value of λ is large, it indicates an abundance of business opportunities with partnerships, and it is very likely that an organization will connect with all other organizations using IOS. Organization i will have to evaluate the risk using the worst case scenario where N_i converges to the whole set N. Comparing the value of U_i^{conn} to U_i^{alone}, the company gains added value $\lambda(n-1)V^A$ from interconnection, but expects to suffer losses $\sum_{j\in N_i}(1-p_j)v$ due to compromises originating from other organizations. Alternatively, organization i can decide to connect asynchronously, without IOS, gaining a net value U_i^{asy}. We can derive the value

$$U_i^{\text{asy}} = V_i + \lambda(n-1)\delta V^A - (1-p_i)v - C_i(p_i). \quad (4)$$

Lemma 2 *Type* 2 *organizations choose to maintain a low safety level* p_l *no matter whether they decide to connect with or without IOS. Type* 1 *organizations will maintain a low safety level* p_l *if* $\Delta_1 > (p_h - p_l)v$, *otherwise, they will improve their safety levels to* p_h.

Lemma 2 shows that when an organization decides to connect using IOS, it only considers its own cost of investment in security and the losses the externally sourced security risk may cause at its own systems. Other organizations' inter-connection decisions or security investment decisions will not affect its security investment decision. Therefore, the decisions about security investment levels are made in a decentralized fashion. Then, in order to decide whether to connect its system to the systems of other organizations, organization i will need to estimate the overall network security status and the expected risk based on other organizations' investment decisions utilizing the result from Lemma 2.

Proposition 1

(1) *When* $\Delta_1 \le (p_h - p_l)v$, *an organization will connect to all its business partners with IOS only if* $\lambda(1-\delta)V^A \ge \left[1 - \frac{1}{n}(n_1 p_h + n_2 p_l)\, p_l\right] v$. *It will connect to its business partners without IOS if* $\lambda(1-\delta)V^A < \left[1 - \frac{1}{n}(n_1 p_h + n_2 p_l)\, p_l\right] v$.
(2) *When* $\Delta_1 > (p_h - p_l)v$, *an organization will connect to all its business partners with IOS only if* $\lambda(1-\delta)V^A \ge (1-p_l)v$. *It will connect to its business partners without IOS if* $\lambda(1-\delta)V^A < (1-p_l)v$.

Proposition 1 provides the threshold conditions on when an organization will adopt connecting with IOS strategies compared to connecting without IOS strategies. It is worth noting that in our assumption, the value of connection is always positive so that an organization is always better off when connecting without IOS than not connecting at all. Combining with the security level decisions, we are able to identify four possible scenarios, as shown in Fig. 1a–d. Table 1 summarizes the firms' connection decisions.

In Fig. 1a and b (corresponding to Proposition 1(1), type 1 organizations will invest in a high safety level and type 2 organization will invest in a low safety level, due to the cost of improving security is too high for type 2. However, in Fig. 1a, all the organizations will

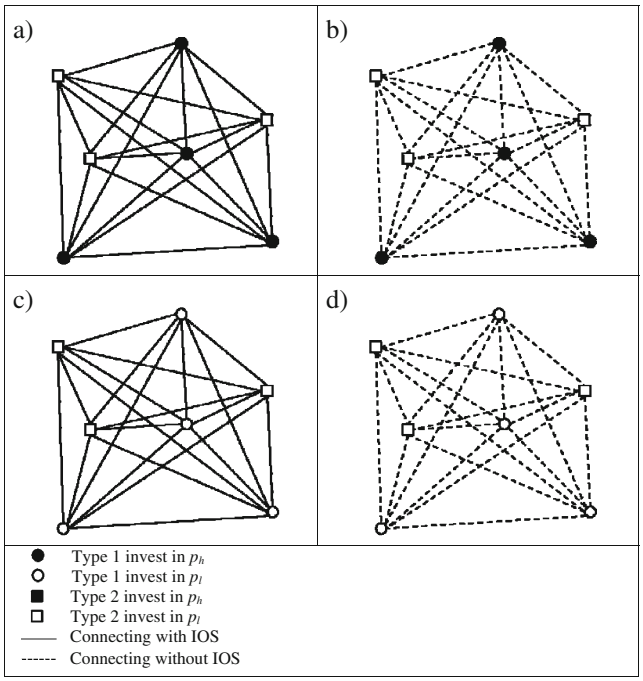

Fig. 1 Four outcomes without incentive mechanism

connect with each other with IOS, regardless of their safety levels, because the high benefit of connecting overcomes the expected loss. In Fig. 1b, the organizations will interconnect without IOS, due to the fact that the added value is not worth the cost of increased security vulnerability.

In Fig. 1c and d (corresponding to Proposition 1(2), both type 1 and type 2 organizations will invest in a low security level because the cost of improving security is too high for both types. However, in Fig. 1c, all the organizations will still connect with each other with IOS even though none of the organizations has a satisfactory safety level. This case can only occur when the added benefit of connecting is really high and the expected security loss is relatively affordable. In Fig. 1d, the organizations will interconnect without IOS, due to the fact that none of the organizations has provided a satisfactory security protection and hence the security risk of interconnection becomes really severe. This scenario is the worst situation that can occur since none of the organizations is well protected and neither can they do business efficiently with IOS due to their security concerns.

In Section 3.4, we are able to calculate the welfare level in each scenario and compare the welfare improvement when our proposed mechanism is in place.

3.3 Implementation of mechanism with SCC

In this section, we consider the case where each organization has the choice of whether to participate in SCC and comply with the accountability constraints.

The implementation of SCC works as follows. The SCC certifies all the organizations that decide to join the consortium. All the network traffics and activities send among the SCC organizations will be monitored. The certification technologies must be used to guarantee authentication and non-repudiation. That is, SCC organizations are confident of identifying the source of the security attacks due to authentication technologies. A SCC organization cannot deny the security attacks that originated from its network. Meanwhile, it cannot claim that it has suffered security attacks originated from other SCC organizations when it does not have. Candidate technologies which fulfill these characteristics of certification are Public/Private Key Infrastructure, such as digital signatures.

The implementation of the SCC mechanism may generate extra overhead to identify the organizations' certification status. We ignored such an impact in our model by assuming that the size of overhead is negligible compared to the regular traffic. In situations that the assumption does not hold, we suggest that the SCC adjust the subscription fee to accommodate the overhead cost. Although the overhead will create a deadweight loss which reduces the value of the SCC mechanism, the loss is inevitable as no security mechanism is free. Given the rising concerns on interdependent security risks, the overhead should not diminish the incentive of organizations adopting the SCC mechanism.

Since we assume that organizations will enjoy the benefit of added business efficiency if they connect

Table 1 Summary of outcomes without SCC mechanism

	$\Delta_1 \leq (p_h - p_l)v$	$\Delta_1 > (p_h - p_l)v$
$\lambda(1-\delta)V^A \geq (1-p_l)v$	Fig. 1a: type 1 high security and type 2 low. All connecting with IOS	Fig. 1c: type 1 high and type 2 low. All connecting without IOS
$E(1-p)v \leq \lambda(1-\delta)V^A < (1-p_l)v$	Fig. 1a: type 1 high security and type 2 low. All connecting with IOS	Fig. 1d: both type 1 and type 2 low security. All connecting with IOS
$\lambda(1-\delta)V^A < E(1-p)v$	Fig. 1d: both type 1 and type 2 low security. All connecting without IOS	Fig. 1d: both type 1 and type 2 low security. All connecting with IOS

with IOS, they will always want to do so if there is enough security protection. By joining the community, the organization assumes responsibility for maintaining the security of the overall community. Specifically, if an organization connects with other organizations using IOS, it is responsible for all the losses due to security failures routing via its own systems. Meanwhile, it collects compensation if it suffers from security failure originating from other participating organizations. As a result, the overall protection towards the interdependent risks inside the SCC is always better than that outside of the SCC. This fact provides organizations willing to connect with IOS an added incentive to join the SCC. However, if an organization decides not to connect with SCC, then it really does not have any incentive to join SCC since it cannot hold other organizations responsible when security attacks occur, which must be from their own network. So we ignore the possibility that an organization joins the SCC but decides not to connect with IOS.

After deciding to join the community, each organization then decides on its safety level and strategies for connecting with other members of SCC or non-members. Define N_{in} as the set of all the organizations that participate in SCC, we first introduce the following Lemma 3.

Lemma 3 *If organization i has already participated in SCC, it will maintain a high safety level if* $\Delta C_i \leq \sum_{j\in N_{\text{in}}}(p_h - p_l)v$.

Comparing the result of Lemma 3 to Lemma 1, we observe a higher threshold of security improvement cost for organizations to stay in low safety level. Therefore, the organizations are more likely to improve their safety levels when the mechanism is in place. Without the mechanism, an organization is only concerned about its own loss due to security attacks, which is $(p_h - p_l)v$. If its cost of security improvement is higher than that level, it decides to stay at a low safety level even when such a decision may cause more damage to the other interconnected organizations. When it decides to participate in SCC, it will evaluate not only its own security loss but also the expected compensation that it has to make to other organizations due to its poorly maintained safety level. Therefore, it will increase its security level to high when the cost to do so is lower than the overall expected compensation paid towards the participating organizations, $\sum_{j\in N_{\text{in}}}(p_h - p_l)v$. We can hence claim that our mechanism provides stronger incentives for security improvement.

Each organization, in order to decide whether to participate in SCC, needs to evaluate how many other organizations will participate and what their connection and security decisions are. Such a signaling-screening game may lead to multiple equilibria and requires the SCC to coordinate so as to obtain the most efficient equilibrium outcome. In this paper, we focus on examining two major types of equilibria: a pooling equilibrium where all the organizations participate in SCC and a separating outcome where only type 1 organizations participate. Each equilibrium may require different existing conditions. In the following sections, we will derive these conditions and analyze the organizations' corresponding safety levels and connecting decisions.

3.3.1 Pooling outcome: Both types participate

When both types participate, the size of the overall community is n and $N_{\text{in}} = N$. Use super-script "comm-p" to denote the case when a *pooling* outcome is obtained and the organizations join the *community*. We obtain the net value for an organization i:

$$U_i^{\text{comm}-p}(p_i) = V_i + \lambda(n-1)V^A - (1-p_i)v - \sum_{j\in N: j\neq i}(1-p_j)v - C_i(p_i) \quad (5)$$

According to Lemma 3 and Condition 2, we can conclude that type 1 organizations will always maintain a high safety level if they join the community. Type 2 organizations may maintain a high safety level if $\Delta_2 \leq n(1-p_l)v$. Otherwise, they will maintain a low safety level. Figure 2a and b summarize the two pooling outcomes. Figure 2a describes the scenario that all the organizations join SCC and maintain a high security level. Figure 2b shows the case when they all join SCC but only type 1 organizations maintain a high security level and type 2s do not. The following Proposition 2 shows the condition when each of the the pooling outcomes may hold.

Proposition 2 *When* $\Delta_2 \leq n(p_h - p_l)v - (n-1)\cdot\max\{0, (1-p_l)v - \lambda(1-\delta)V^A\}$, *both types of organizations will participate in the SCC community and choose to implement the high safety level. When* $\lambda(1-\delta)V^A \geq (1-p_l)v$ *and* $\Delta_2 > n(p_h - p_l)v$, *both types of organizations will participate in the SCC community, but type* 2 *organizations will decide to maintain the low safety level. Under other conditions, the pooling outcomes cannot be supported since type* 2 *organizations will find it better to stay outside of SCC.*

The result of Proposition 2 provides insight on when each type will participate in SCC. Table 2 summarizes

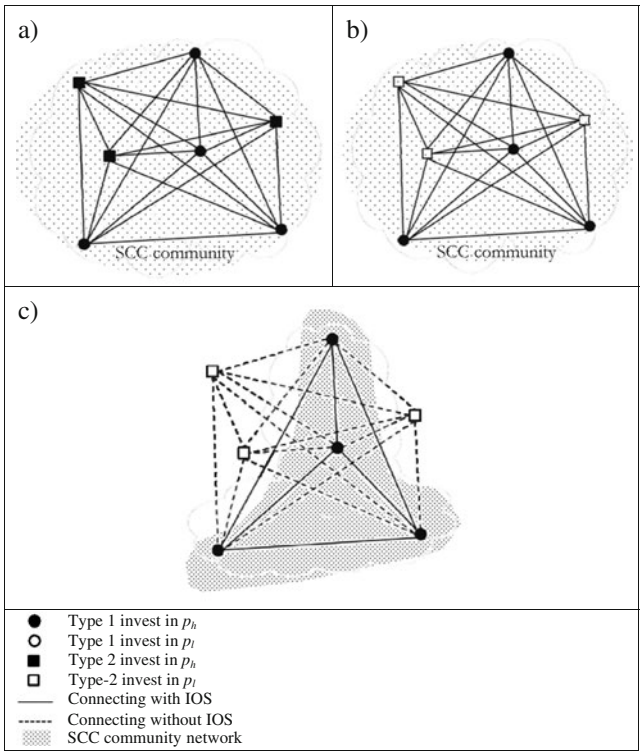

Fig. 2 Outcomes with incentive mechanism

the firms' connection and investment decisions in presence of SCC.

Generally speaking, type 2 organizations are more reluctant to improve their safety levels due to the higher security costs they incur. In order to keep them in the SCC community and to hold them accountable for security loss caused by them, one of the two conditions need to hold: (a) the cost of security level must be lower than a specific threshold so that they will improve their safety levels to p_h in order to reduce the expected compensation payout; or, (b) the added value of connection with IOS compared to connection without IOS, $\lambda(1-\delta)V^A$ must be high enough so that they would find it worth staying inside connected network and compensating their partners for the losses caused by their low safety levels.

3.3.2 Separating outcome: Only type 1 organizations participate

When the conditions to support pooling outcomes described in above Proposition 2 do not hold, type 2 organizations may start to leave the community because it is too costly for them to maintain high safety level (i.e. Δ_2 is too high) and the accountability has imposed too high a burden if they decide to just stay at the low safety level. In such a case, a type 2 organization may not be considered as a good candidate for type 1 organizations to deploy IOS with. If that is true, the SCC will attempt to maintain a smaller interconnected network with only type 1 organizations. In this case, the total number staying in the SCC community is n_1.

When type 2 organizations decide to stay outside of the SCC community, type 1 organizations need to decide whether maintaining IOS connections with them is valuable. If a type 1 organization decides to maintain such a connection, the type 2 organizations' low safety levels may cause trouble to not only its own systems but also to all the other systems in the SCC network, which the type 1 organization will be held accountable for.

Lemma 4 *A type* 1 *organization, if it decides to stay in SCC community comprised of all other type* 1 *organizations, will maintain a high safety level, and choose to connect with type* 2 *organizations without IOS.*

Type 2 organizations, if they decide to stay outside of the community, will be "cut off" from type 1 organizations as stated in Lemma 4. They can also have a choice in whether to connect using IOS with other

Table 2 Summary of the outcomes with the SCC mechanism

$\lambda(1-\delta)V^A \geq (1-p_l)v$	When $\Delta_2 \leq n(p_h - p_l)v$, Fig. 2a: All join SCC and connect with IOS All high security level When $\Delta_2 > n(p_h - p_l)v$, Fig. 2b: All join SCC and connect with IOS Only type 1 high security level
$(1-p_h)v \leq \lambda(1-\delta)V^A < (1-p_l)v$	When $\Delta_2 \leq (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Fig. 2a: All join SCC and connect with IOS. All high security level When $\Delta_2 > (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Fig. 2c: Only type 1 join SCC, connect other SCC members with IOS, and maintain high security level. Type 2 stay out SCC, connect to all other organizations without IOS, and maintain low security level
$\lambda(1-\delta)V^A < (1-p_l)v$	No one will join SCC due to the low value V^A. The mechanism will not work

type 2 organizations. However, they also do not have an incentive to do so in this case since they will also be concerned about the security risk brought by the other type 2 organizations as demonstrated in the following Lemma.

Lemma 5 *In the separating outcome, a type* 2 *organization will maintain a low safety level, and choose not to connect with other type* 2 *organizations with IOS.*

Together, Lemmas 4 and 5 describe the only possible separating outcome where only type 1 organizations will join SCC and maintain high security level. Type 2 organizations will stay outside SCC, connected to each other without IOS, and invest in low security levels. Figure 2c demonstrates such an outcome.

Proposition 3 *A separating outcome described in Fig.* 2c *is supported when* $\lambda(1-\delta)V^A \in \left[(1-p_h)v, (1-p_l)v\right]$ *and* $\frac{\Delta_1-(p_h-p_l)v}{n_1-1} \leq \lambda(1-\delta)V^A-(1-p_h)v < \frac{\Delta_2-(p_h-p_l)v}{n-1}$.

When the separating equilibrium holds, the type 1 organizations together form an interconnected network among them. Within the interconnected network, they enjoy efficient connections with IOS and the full added value of such connection. Their security risk is limited since all will maintain high safety level. The non-members will stay outside such a community and connect with either members or other non-members without using IOS. They choose to do so because they do not want to join the network by maintaining high safety levels or by compensating the members once their systems are compromised and in turn affect other members. Meanwhile, they will not connect their IOS with other non-members since they know those other non-members are also maintaining low safety levels and connecting with them will introduce too many security problems to their own systems. The separating equilibrium holds when the value of connecting $\lambda(1-\delta)V^A$ is neither too high to attract type 2 organizations into the community nor too low to become unattractive to other type 1 organizations. In addition, the cost of security improvement for type 2 must be high enough such that they would not want to improve and the cost improvement for type 1 must be low enough such that they have incentive to improve their safety levels and stay in the network.

3.4 Outcomes and Efficiency Comparison

Now we have introduced all the seven outcomes, including four outcomes when there is no incentive mechanism and three outcomes when the mechanism is introduced. We next compare the outcomes with SCC and without SCC and evaluate the efficiency change. The analysis helps examine the value of our mechanism as an incentive mechanism (to improve security) or as a signaling tool or as both. We can also identify when and why our mechanism generates higher welfare levels.

Comparing the conditions that support each outcome, we identified nine scenarios with different possible changes of outcomes from the network without mechanism to the network with mechanism. In each of them, our mechanism may play a different role. We discuss those nine possible changes one by one, by first introducing the conditions and then discussing the changes in decisions by both types of organizations. We will also quantify the welfare improvement for each case. Table 3 summarizes the following scenarios in terms of the conditions they hold, and the change of cases when there is no SCC to when SCC is implemented.

Table 3 Summary of the changes from no SCC to SCC

	$\Delta_1 \leq (p_h - p_l)v$	$\Delta_1 > (p_h - p_l)v$
$\lambda(1-\delta)V^A \geq (1-p_l)v$	When $\Delta_2 \leq n(p_h - p_l)v$, Scenario 1 (Fig. 1a → Fig. 2a) When $\Delta_2 > n(p_h - p_l)v$, Scenario 2 (Fig. 1a → Fig. 2b)	When $\Delta_2 \leq n(p_h - p_l)v$, Scenario 6 (Fig. 1c → Fig. 2a) When $\Delta_2 > n(p_h - p_l)v$, Scenario 7 (Fig. 1c → Fig. 2b)
$E(1-p)v \leq \lambda(1-\delta)V^A < (1-p_l)v$	When $\Delta_2 \leq (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Scenario 1 (Fig. 1a → Fig. 2a) When $\Delta_2 > (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Scenario 3 (Fig. 1a → Fig. 2c)	When $\Delta_2 \leq (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Scenario 8 (Fig. 1d → Fig. 2a) When $\Delta_2 > (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Scenario 9 (Fig. 1d → Fig. 2c)
$(1-p_h)v \leq \lambda(1-\delta)V^A < E(1-p)v$	When $\Delta_2 \leq (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Scenario 4 (Fig. 1b → Fig. 2a) When $\Delta_2 > (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Scenario 5 (Fig. 1b → Fig. 2c)	When $\Delta_2 \leq (p_h - p_l)v + (n-1)$ $-(1-p_h)v]$, Scenario 8 (Fig. 1d → Fig. 2a) When $\Delta_2 > (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, Scenario 9 (Fig. 1d → Fig. 2c)
$\lambda(1-\delta)V^A < (1-p_l)v$	No one will join SCC due to the low value V^A. The mechanism will not work	

Scenario 1 When $\lambda(1-\delta)V^A \geq E(1-p)v$,[3] $\Delta_1 \leq (p_h - p_l)v$, and $\Delta_2 \leq n(p_h - p_l)v - (n-1)\cdot\max\{0, (1-p_l)v - \lambda(1-\delta)V^A\}$:

- *Without the mechanism:* these conditions will lead type 1 organizations to choosing a high safety level but type 2 to choosing a low safety level. Since organizations cannot identify which of the others are of type 1, they have to make their connection decisions based on the expected safety level. When $\lambda(1-\delta)V^A \geq E(1-p)v$, they connect to all other organizations using IOS even knowing some have a low safety level. (The outcome is described in Fig. 1a)
- *With the SCC mechanism:* type 2 will find it worthwhile to improve its safety level and participate in the SCC. This is because the mechanism does not allow them to "free ride" the type 1 organizations. They need to be accountable for their own losses. In fact, type 2 also benefit from this outcome since the SCC provides a safe environment to them as well. (The outcome is described in Fig. 2a)
- *Improvement of welfare* $= n_2 n(p_h - p_l)v - n_2\Delta_2$, which is composed of the total reduced security loss of the network less the total cost for type 2 organizations to improve security. The improvement is strictly positive.

Scenario 2 When $\lambda(1-\delta)V^A \geq (1-p_l)v$, and $\Delta_1 \leq (p_h - p_l)v$:

- *Without the mechanism:* same outcome as described in the first case. (Fig. 1a)
- *With the SCC mechanism:* type 2 still finds improving its safety level is too costly and hence stays at a low safety level. However, since the value of connecting with IOS is high, they will still join the SCC community. (Fig. 2b)
- *Improvement of welfare* $= 0$. There is no change in connection and security decisions for both types of organizations. This is because the decisions are already efficient under the parameters. However, one notable issue without the mechanism was that type 1 will suffer from the low safety level maintained by type 2 organizations. With the SCC in place, type 2 will compensate type 1's losses for connecting with them. Such a re-allocation of net values introduces fairness as type 2 organizations take responsibility for the losses caused by their own decisions to stay at a low safety level.

[3]Here, we define $E(1-p)v$ as the expected loss when the type p is not know. Therefore, $E(1-p) = [n_1(1-p_h) + n_2(1-p_l)]/n$.

Scenario 3 When $\lambda(1-\delta)V^A \in \left[E(1-p)v, (1-p_l)v\right)$, $\Delta_1 \leq (p_h - p_l)v$, and $\Delta_2 > (p_h - p_l)v + (n-1)\left[\lambda(1-\delta)V^A - (1-p_h)v\right]$:

- *Without the mechanism:* same outcome as described in the first case. (Fig. 1a)
- *With the SCC mechanism:* type 2 still finds improving its safety level costly and hence stays at a low safety level. In addition, since the value of connecting with other organizations with IOS is lower than the above case 2, type 2 organizations will also find that it is not worth paying the compensation and staying in the SCC community. Therefore, they will stay out. Meanwhile, type 1 will stay in the SCC community, invest in a high safety level, and connect with other type 1 organizations with IOS, connect with those non-members (i.e.type 2 organizations) without IOS (Fig. 2c)
- *Improvement of welfare* $= n_2\left[n_1(1-p_h) + (n-1)(1-p_l)\right]v - n_2(n_1+n-1)\cdot\lambda(1-\delta)V^A$. The first term is the expected reduction of security loss and the second term is the loss due to disconnecting the type 2 organizations from the IOS. The change of welfare will be positive if the number of type 1 organizations (i.e. the size of SCC community) is large enough: $\frac{n_1}{n-1} < \frac{(1-p_l)v - \lambda(1-\delta)V^A}{\lambda(1-\delta)V^A - (1-p_h)v}$.The value of the SCC under this condition is to help separate the low safety ones to ensure secure connections (avoid unsafe connections).

Scenario 4 When $\lambda(1-\delta)V^A \in \left[(1-p_h)v, E(1-p)v\right)$, $\Delta_1 \leq (p_h - p_l)v$, and $\Delta_2 \leq (p_h - p_l)v + (n-1)\left[\lambda(1-\delta)V^A - (1-p_h)v\right]$:

- *Without the mechanism:* type 1 organizations will choose a high safety level but type 2 will choose low. Since the organizations cannot identify which of the others are of type 1, they make connection decisions based on the expected safety levels and now they decide not to connect with IOS since the expected value of connecting is too low to cover the security loss. (Fig. 1b)
- *With the SCC mechanism:* type 2s will find it worthwhile to improve their safety levels and participate in the SCC so the expected network risk is lower and both types will participate in the SCC community. (Fig. 2a)
- *Improvement of welfare* $= n(n-1)\left[\lambda(1-\delta)V^A - (1-p_h)v\right] + n_2\left[(p_h - p_l)v - \Delta_2\right]$. The first term represents the total improved net value of more efficient connections less the added risks when they are interconnected. The second term is for type 2 organizations to improve their safety levels. Our mechanism, under this condition, efficiently

provides type 2 organizations with incentives to improve security, alleviates the security concerns, and induces efficient connections.

Scenario 5 When $\lambda(1-\delta)V^A \in [(1-p_h)v, E(1-p)v)$, $\Delta_1 \leq (p_h - p_l)v$, and $\Delta_2 > (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$:

- *Without the mechanism:* this case is the same as the above case 4, where the network is not connected using IOS. (Fig. 1b)
- *With the SCC mechanism:*type 2 will stay outside due to their high cost of security improvement. Type 1 is then able to identify the other high type partners and form more efficient connections with them. (See Fig. 2c)
- *Improvement of welfare* $= n_1(n_1-1)[\lambda(1-\delta)V^A - (1-p_h)v]$, representing the improved connections among the n_1 type 1 organizations.

Scenario 6 When $\lambda(1-\delta)V^A \geq (1-p_l)v$, $\Delta_1 > (p_h - p_l)v$, and $\Delta_2 \leq n(p_h - p_l)v$:

- *Without the mechanism:* both types will choose a low safety level due to their cost concerns. However, they are still connected via IOS since the value of connection is high. This is the case where organizations expect the largest security loss from the network. (See Fig. 1c)
- *With the SCC mechanism:* both types find it worthwhile to improve their safety levels to high and participate in the SCC. The mechanism provides incentive for both to improve security. (The outcome is described in Fig. 2a)
- *Improvement of welfare* $= n^2(p_h - p_l)v - n_1\Delta_1 - n_2\Delta_2$, which is composed of the total reduced security loss less the costs for both types of organizations.

Scenario 7 When $\lambda(1-\delta)V^A \geq (1-p_l)v$, $\Delta_1 > (p_h - p_l)v$, and $\Delta_2 > n(p_h - p_l)v - (n-1)\cdot\max\{0, (1-p_l)v - \lambda(1-\delta)V^A\}$:

- *Without the mechanism:* same outcome as described in the first case. (Fig. 1c)
- *With the SCC mechanism:* type 1 organizations find it worthwhile to improve their safety level to high and participate in the SCC while type 2 will also participate but remain at low safety levels due to their high costs of improving security. The mechanism provides incentives only for type 1 to improve security. (Fig. 2b)
- *Improvement of welfare* $= n_1[n(p_h - p_l)v - \Delta_1]$, representing the improved security of type 1 organizations.

Scenario 8 When $\lambda(1-\delta)V^A \in [(1-p_h)v, (1-p_l)v)$, $\Delta_1 > (p_h - p_l)v$, and $\Delta_2 \leq (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$:

- *Without the mechanism:* both types will choose a low safety level due to their cost concerns. In addition, they will not connect their IOS since the value gained is not worth the expected loss of security. (Fig. 1d)
- *With the SCC mechanism:* both types find it worthwhile to improve their safety levels to high and participate in the SCC (Fig. 2a)
- *Improvement of welfare* $= n(n-1)[\lambda(1-\delta)V^A - (1-p_l)v] + n^2(p_h - p_l)v - n_1\Delta_1 - n_2\Delta_2$, since both types have improved their security and connection decisions.

Scenario 9 When $\lambda(1-\delta)V^A \in [(1-p_h)v, (1-p_l)v)$, $(p_h - p_l)v < \Delta_1 \leq (p_h - p_l)v + (n_1 - 1)[\lambda(1-\delta)V^A - (1-p_h)v]$, and $\Delta_2 \leq (p_h - p_l)v + (n-1)[\lambda(1-\delta)V^A - (1-p_h)v]$:

- *Without the mechanism:* both types will choose low safety levels due to their cost concerns. In addition, they will not connect their IOS since the value gained is not worth the expected loss of security. (Fig. 1d)
- *With the SCC mechanism:* type 1 will participate and invest in improving safety level but type 2 will not. (Fig. 2c)
- *Improvement of welfare* $= n_1(n_1 - 1)[\lambda(1-\delta)V^A - (1-p_h)v] + n_1[(p_h - p_l)v - \Delta_1]$, representing type 1's improved connection efficiency with other type 1 organizations and their improved security.

4 Concluding remarks

Organizations are increasingly using IOS to realize increased value from more efficient collaborations. For example, personnel from one organization can have access to the information systems of a business partner to query its inventory level or transaction history. Sales executives from one organization can query its business partner's customer information via their CRM data portal. Linking information systems across organizational boundaries has enabled efficient business process integration, such as in supply chain management in vertical industries, B2B transactions, outsourcing relationships, and in strategic alliances.

As the importance of fostering business eco-systems is increasingly recognized, information system interconnections are identified as the substrate to build such systems on. In particular, many such eco-systems rely

on the network effects generated by linking information systems based on a common platform, to compete against other networks. The advent of new paradigms in information systems such as web services, software-as-service (SaaS) models, service oriented architectures (SOA), loosely coupled systems and cloud computing all lead to the spread of information systems outside organizational boundaries, where they link with other information systems. Trends toward modular, interoperable architectures and increasing use of the Internet and web as the channel and interface for linking information systems promote the extent of interconnections. An abundance of bandwidth and increase in the potential channels that provide connectivity accelerate these trends. The increasingly global nature of business necessitates more use of IOS as well.

Use of IOS aggravates the security problems faced by organizations, which traditionally focus on protecting their systems from external intrusions and compromise of confidential information. With IOS, they are faced with security threats across an entire network of organizations they may be directly or indirectly connected to. The IOS network is affected by problems of lack of accountability by individual members toward other members, lack of incentives to invest in minimizing damage to other members, related moral hazard problems, hidden information about the security profile of peer organizations in the network and all of these lead to market inefficiencies in IOS investments. We have outlined an incentive mechanism that forms a community of organizations anchored by an SCC that emphasizes member accountability to the community to address these problems. We have demonstrated how the mechanism can address moral hazard, provide accountability, and furnish incentives under specified conditions. The introduction of the mechanism under various specified conditions was shown to lead to welfare gains. The mechanism can help separate the organizations with inferior security profile under certain conditions.

The proposed mechanism will primarily reduce the complexity of the interconnection decision. This is accomplished by giving better information about the potential partner, and the corresponding risk. The mechanism expands focus of corporate security efforts from internal protection to cover impact on external partners as well. The concept of inter-organizational accountability is new and can have far reaching impact on security in particular and collaborations in general. The tradeoff between benefits of collaboration with community members and the potential cost from accountability will motivate organizations that seek to join to make optimal investments in security so as to minimize accountability effects. Thus the mechanism creates a powerful incentive for organizations to tie together technologies, policies and standards towards the combined objectives of protecting internal assets and minimizing negative impact on outside partners. Investments in security are expected to improve in efficiency as a result.

As a community of organizations grows in size, it can develop network effects which will increase incentives for non-members to join the community and consequently, to secure their networks and connections as a precursor to joining the community. Those that have inherently low security levels, smaller organizations, and organizations that may gain minimal value from inter-organizational links may stay out. As the groups of members and non-members consolidate, the membership status will be more valuable in signaling information about the organizations.

Information security contributes to operational risk incurred by an organization. Engaging in use of IOS introduces interdependency, and compounds this risk. In this paper, we have outlined a calculus to study interdependent operational risk. On a broader level, the mechanism forms the basis for managing interdependent risk under a general class of collaborations. It can be applicable to other domains characterized by interdependence, such as financial networks and supply chains.

The mechanism can act as an encompassing framework for collaborations across national boundaries or across multiple standards where the simple focus on community membership and accountability can hide details of dealing with the disparity in laws or compliance requirements.

The mechanism we propose does not seek to impose any technological constraints. Rather, it outlines the incentive framework at a broad level, allowing each organization to make its own choices of technologies, standards and policies to ensure meeting with the accountability requirements of the mechanism. This facilitates sustainability of the mechanism as technologies and threats change. A main source of security risk that organizations guard against today is the Internet. Organizations in our model will face the risk of exposure to the Internet. While it is not explicitly stated, the model does account for exposure to the Internet, in holding members accountable for any security related loss, regardless of the manner of origin. That implies member organizations have to secure their systems from Internet based risk, as well as ensure that they do not propagate Internet based malware to peer members.

Some small organizations may rely on Internet Service Providers(ISP) and outsourcing to support their

systems and connectivity. This may exclude them from the scope of the stated model. (Such small businesses may be ruled out by inability to bear the burden of accountability as well.) The community model can be expanded to cover ISPs where we expand the notion of organizations to that of an Administrative Domain, and use domain names to represent individual entities. Each domain that is a member of the community is accountable to the entire community for losses caused by it; which in turn can motivate individual domains to secure its outgoing information flows. In such a scenario, small businesses may add another criterion to decide which ISP to get service from: checking community membership status.

In future research, the model may be applied to other forms of interdependent risk using the same calculus. The notion of an SCC may be extended to allow for the possibility of multiple communities, for example, one community supported by each industry consortium where IOS is important. It is also of interest to study communities competing against each other within the same industry. Formation of communities can lead to network effects, which are not modeled in this paper. The impact of network effects on evolution and competition of communities can be an interesting topic. The model can be extended to address changes in membership status across periods. The size of communities can have significant impact on membership decisions, and experimental investigations can study the formation and evolution of communities with a view to studying threshold and optimal sizes for communities. The role of the SCC may be compared in a consensus consortium role versus an SCC run by a dominant (keystone) player in an eco-system.

Appendix A: Proofs of Lemmas and Propositions

Proof of Lemma 1 If organization i invests $C_i(p_h)$ in information security, the net value of its information systems is $U_i^{\text{alone}}(p_h) = V_i - (1-p_h)v_i - C_i(p_h)$.

If it invests $C_i(p_l)$ in information security, the net value changes to $U_i^{\text{alone}} = V_i - (1-p_l)v_i - C_i(p_l)$. That is, when $\Delta C_i = C_i(p_h) - C_i(p_l) \le (p_h - p_l)v_i$, we have $U_i^{\text{alone}}(p_h) \ge U_i^{\text{alone}}(p_l)$ and organization i is better off when choosing high safety level p_h. When $\Delta C_i > (p_h - p_l)v_i$, $U_i^{\text{alone}}(p_l) > U_i^{\text{alone}}(p_h)$, organization i chooses p_l. □

Proof of Lemma 2 As shown in Eq. 3, the net value for organization i is $U_i^{\text{conn}}(p_i) = V_i + \lambda(n-1)V^A - (1-p_i)v - \sum_{j\in N_i}(1-p_j)v - C_i(p_i)$ when it connects with its business partners via IOS.

The difference between the net value of IOS when the organization invests high and that when it invests low can be calculated by $U_i^{\text{conn}}(p_h) - U_i^{\text{conn}}(p_l) = (p_h - p_l)v - \Delta_i$. Condition 1 imposes that $\Delta_2 > (p_h - p_l)v$, indicating that $U_i^{\text{conn}}(p_h) < U_i^{\text{conn}}(p_l)$ for type 2 organizations. Therefore, they always maintain a low safety level p_l. Type 1 organizations will maintain a high safety level p_h if $(p_h - p_l)v - \Delta_1 \ge 0$ and maintain a low safety level when $(p_h - p_l)v - \Delta_1 < 0$.

When organization i connects with its business partners without IOS, the net value for organization i changes to

$$U_i^{\text{asy}}(p_i) = V_i + \lambda(n-1)\delta V^A - (1-p_i)v - C_i(p_i). \quad (6)$$

We use the superscript "asy" to represent the case that the connection is asynchronously processed (i.e. connecting without IOS strategy). The difference in net value when organization i invests high and low is $U_i^{\text{asy}}(p_h) - U_i^{\text{asy}}(p_l) = (p_h - p_l)v - \Delta_i$, which is the same as the case when it connects with IOS. Therefore, we obtain the same results. □

Proof of Proposition 1 From Lemma 2, if $\Delta_1 > (p_h - p_l)v$, all organizations maintain low safety levels. If organization i connects with its business partners with IOS, it enjoys an expected net value of

$$U_i^{\text{conn}}(p_l) = V_i + \lambda(n-1)V^A - n(1-p_l)v - C_i(p_l). \quad (7)$$

If it connects without IOS, the expected net value is

$$U_i^{\text{asy}}(p_l) = V_i + \lambda(n-1)\delta V^A - (1-p_l)v - C_i(p_l). \quad (8)$$

Comparing Eqs. 7 and 8, we have $U_i^{\text{conn}} \ge U_i^{\text{asy}}$ if and only if $\lambda(1-\delta)V^A \ge (1-p_l)v$, which is when organization i chooses to connect with IOS. Otherwise, $U_i^{\text{conn}} < U_i^{\text{asy}}$, and organization i chooses to connect without IOS.

If $\Delta_1 \le (p_h - p_l)v$, type 1 organizations maintain high safety level and type 2 organizations maintain low safety level. The expected net value for organization i to connect with its business partners with IOS is

$$U_i^{\text{conn}} = V_i + \lambda(n-1)V^A - [n_1(1-p_h) + n_2(1-p_l)]v - C_i(p_i). \quad (9)$$

Comparing Eqs. 9 to 8, we have

$$\frac{1}{n-1}\left[U_i^{\text{conn}} - U_i^{\text{asy}}\right] \approx \lambda(1-\delta)V^A - \frac{1}{n}[n_1(1-p_h) + n_2(1-p_l)]v. \tag{10}$$

Therefore, an organization will connect to all its business partners with IOS when $\lambda(1-\delta)V^A \geq [1 - \frac{1}{n}(n_1 p_h + n_2 p_l)]v$. Otherwise, it will connect with its business partners without IOS. □

Proof of Lemma 3 If organization i joins SCC and choose to connect with the outsiders with IOS, we denote its net value as $U_i^{\text{comm-conn}}$. The net value is composed of the overall value of connection $V_i + \lambda(n-1)V^A$ less the expected cost of security breaches and the cost of its own security investment $C_i(p_i)$. The expected cost of security breaches is composed of two parts: the expected compensation made to other SCC members when organization i is the source of security breach: $\sum_{j\in N_{\text{in}}}(1-p_i)v$ and the expected compensation caused by those organizations outside the SCC but interconnected with organization i. Note that organizations i will be held accountable for those losses to other SCC members even though itself is not the source of attack. Its "careless" decision of connecting outside bad members shall be punished. For any organization k who is not an SCC member, the probability that it is the source of attack is $1-p_k$, and the expected loss to all the organizations inside SCC can be calculated as $\sum_{j\in N_{\text{in}}}(1-p_k)v$. And hence the overall expected loss caused by non SCC members ($\forall k \notin N_{\text{in}}$) is summed up to $\sum_{k\notin N_{\text{in}}}\sum_{j\in N_{\text{in}}}(1-p_k)v$. Therefore, the net value of IOS can be formally written as:

$$U_i^{\text{comm-conn}}(p_i) = V_i + \lambda(n-1)V^A - \sum_{j\in N_{\text{in}}}(1-p_i)v - \sum_{k\notin N_{\text{in}}}\sum_{j\in N_{\text{in}}}(1-p_k)v - C_i(p_i). \tag{11}$$

Now we calculate the case that members participating in the community do not connect with non-members through IOS. We use superscript "comm-asy" to denote this case. If organization i joins SCC and choose to connect with the outsiders without IOS, organization i will not become a mid-node to pass along security breaches generated from non-SCC members, hence the fourth term in Eq. 11 will not appear in the calculation. In addition, the second term in Eq. 11 will be split into two parts since organization i cannot enjoy the full benefit of interconnection with non-SCC members. With SCC members, organization i enjoys the full benefit and hence gain added value of $\sum_{j\in N_{\text{in}}}\lambda V^A$. With non-SCC members, the benefit is discounted by δ and hence $\sum_{j\notin N_{\text{in}}}\lambda\delta V^A$. The total net value $U_i^{\text{comm-asy}}$ can be written as:

$$U_i^{\text{comm-asy}}(p_i) = V_i + \sum_{j\in N_{\text{in}}}\left(\lambda V^A - (1-p_i)v\right) + \sum_{j\notin N_{\text{in}}}\lambda\delta V^A - C_i(p_i). \tag{12}$$

In both cases, organization i will maintain a high security level if $\Delta C_i \leq \sum_{j\in N_{\text{in}}}(p_h - p_l)v$. □

Proof of Proposition 2 If all the organizations participate in the SCC, organization i enjoys a net value $U_i^{\text{comm}}(p_i) = V_i + \lambda(n-1)V^A - n(1-p_i)v - C_i(p_i)$. From Condition 2, we can conclude that type 1 organization will always maintain a high safety level. For type 2, it will maintain a high safety level if $\Delta_2 \leq n(p_h - p_l)v$ and stays at p_l if $\Delta_2 > n(p_h - p_l)v$.

Suppose that all organizations except one (say, j) join SCC. The net value for an SCC organization, say i, who connect the outsider with IOS can be represented by

$$U_i^{\text{comm-conn}}(p_i) = V_i + \lambda(n-1)V^A - (n-1)(1-p_i)v - (n-1)(1-p_j)v - C_i(p_i). \tag{13}$$

The net value for organization i who connect the outsider without IOS can be represented by

$$U_i^{\text{comm-asy}}(p_i) = V_i + \lambda(n-2)V^A - (n-1)(1-p_i)v - \lambda\delta V^A - C_i(p_i). \tag{14}$$

Comparing Eqs. 13 to 14, we can conclude that organization i will connect with outsiders without IOS if $\lambda(1-\delta)V^A < (n-1)(1-p_j)v$. Since it is more costly for a type 2 organization to join SCC, we consider the outsider as a type 2 organization. From Lemma 2, the type 2 organization maintains a low safety level. From Condition 3, $\lambda(1-\delta)V^A < n_1(1-p_l)v < (n-1)(1-p_l)v$. Therefore, organizations will connect with the outsider without IOS.

Given the members' connection decisions, we now examine the payoff one gets by leaving the community. First we focus on the case that $\Delta_2 \leq n(p_h - p_l)v$:

We assume a type-2 organization, say k, deviates and does not join SCC. Then it will always maintain a low

safety level according to Lemma 1 and Condition 1. Its net value is

$$\hat{U}_k^{\text{asy}}(p_l) = V_k + \lambda(n-1)\delta V^A - (1-p_l)v - C_k(p_l). \tag{15}$$

If this organization joins SCC, it will maintain a high safety level and the net value is

$$U_k^{\text{comm}}(p_h) = V_k + \lambda(n-1)V^A - n(1-p_h)v - C_k(p_h). \tag{16}$$

In order to ensure the equilibrium holds, $U_k^{\text{comm}}(p_h) \geq \hat{U}_k^{\text{asy}}(p_l)$ must hold. Comparing Eqs. 15 to 16, we conclude that$\Delta_2 \leq n(p_h - p_l)v - (n-1)((1-p_l)v - \lambda(1-\delta)V^A)$ must hold. That is, both types of organizations will participate in SCC community and choose to implement high safety level if:

$$\Delta_2 \leq n(p_h - p_l)v - (n-1)\cdot\max\{0, (1-p_l)v - \lambda(1-\delta)V^A\}. \tag{17}$$

Next we examine on the other case that $\Delta_2 > n(p_h - p_l)v$:

Still we consider a type 2 organization, say k, deviates. If organization k does not join SCC, it will maintain a low safety level and the net value is described in Eq. 15.

If organization k joins SCC, it will still maintain a low safety level and the net value is

$$U_i^{\text{comm}}(p_l) = V_i + \lambda V^A - n(1-p_l)v - C_i(p_l). \tag{18}$$

Comparing Eqs. 18 to 15, we conclude that type 2 will join SCC in this case when $\lambda(1-\delta)V^A \geq (1-p_l)v$. So both types of organizations will participate in SCC community and type 2 organizations maintain a low safety level if $\lambda(1-\delta)V^A \geq (1-p_l)v$ and $\Delta_2 > n(p_h - p_l)v$. Violation of the above conditions will lead type 2 organizations to stay outside of SCC so that the pooling outcomes cannot hold. □

Proof of Lemma 4 In the separating outcome, organizations believe that type 1 organizations will join SCC and type 2 organizations will stay out. Similar to the proof of Lemma 3, type 1 organizations will maintain high security level if $\Delta_1 \leq n_1(p_h - p_l)v$, which holds according to Condition 2. The net value for a type 1 organization, say i, who connects the outsiders with IOS is

$$U_i^{\text{comm-conn}}(p_h) = V_i + \lambda(n-1)V^A - n_1(1-p_h)v - n_2 n_1(1-p_j)v - C_i(p_h). \tag{19}$$

The net value for organization i who connects the outsider without IOS is

$$U_i^{\text{comm-asy}}(p_h) = V_i + \lambda n_1 V^A + \lambda n_2 \delta V^A - n_1(1-p_h)v - C_i(p_h). \tag{20}$$

Comparing Eqs. 20 to 19, we have that member organizations will connect with outsiders with IOS if $n_2(\lambda(1-\delta)V^A - n_1(1-p_j)v) - \lambda V^A \geq 0$. From Lemma 2, the type 2 organizations who stay outside maintain a low safety level. And applying Condition 3, we can prove that $(n_2-1)\lambda(1-\delta)V^A - n_2 n_1(1-p_l) < 0$. Therefore, members will connect with outsiders without IOS. □

Proof of Lemma 5 From Lemma 2, type 2 organizations maintain a low safety level. If a type 2 organization chooses to connect with other type 2 organizations with IOS, the net value is

$$U_i^{\text{conn}}(p_l) = V_i + \lambda n_1 V^A + \lambda(n_2-1)V^A - n_2(1-p_l)v - C_i(p_l). \tag{21}$$

If it connects with other type 2 organizations without IOS, the net value is

$$U_i^{\text{asy}}(p_l) = V_i + \lambda(n-1)\delta V^A - (1-p_l)v - C_i(p_l). \tag{22}$$

Subtracting Eq. 22) from Eq. 21, we find that the condition $\lambda(1-\delta)V^A \geq (1-p_l)v$ should hold to keep type 2 connected with other organizations with IOS. □

Proof of Proposition 3 Suppose that all the organizations believe that only type 1 organizations will join SCC. A type 1 organization's net value is

$$U_i^{\text{conn}}(p_h) = V_i + \lambda(n_1-1)V^A + \lambda n_2 \delta V^A - n_1(1-p_h)v - C_i(p_h). \tag{23}$$

If is stays outside, its net value depends on the cost of security investment Δ_1:

$$\hat{U}_i^{\text{asy}} = \begin{cases} V_i + \lambda(n-1)\delta V^A - (1-p_h)v - C_i(p_h) \text{ if} \Delta_1 \\ \quad \geq (p_h - p_l)v \\ V_i + \lambda(n-1)\delta V^A - (1-p_l)v - C_i(p_l) \text{ if} \Delta_1 \\ \quad < (p_h - p_l)v. \end{cases} \tag{24}$$

Comparing Eqs. 23 to 24, we can conclude that type 1 organizations will not deviate if either both $\Delta_1 \le (p_h - p_l)v$ and $\lambda(1-\delta)V^A \ge (1-p_h)v$ hold, or both $\Delta_1 > (p_h - p_l)v$ and $(n_1 - 1)\left[\lambda(1-\delta)V^A - (1-p_h)v\right] + (p_h - p_l)v \ge \Delta_1$ hold.

In such a separating equilibrium, a type 2 organization's net value is

$$U_i^{\text{asy}}(p_l) = V_i + \lambda(n-1)\delta V^A - (1-p_l)v - C_i(p_l). \tag{25}$$

If type 2 deviates, its net value is

$$\hat{U}_i^{\text{comm}} = \begin{cases} V_i + \lambda n_1 V^A + \lambda(n_2-1)\delta V^A - (n_1+1)(1-p_h)v \\ \quad - C_i(p_h) \ \textbf{if} \Delta_2 \le (n_1+1)(p_h - p_l)v \\ V_i + \lambda n_1 V^A + \lambda(n_2-1)\delta V^A - (n_1+1)(1-p_l)v \\ \quad - C_i(p_l) \ \textbf{if} \Delta_2 > (n_1+1)(p_h - p_l)v. \end{cases} \tag{26}$$

Comparing Eqs. 26 to 25, we can conclude that a type 2 organization will not deviate if either $n_1[\lambda(1-\delta)V^A - (1-p_h)v] + (p_h - p_l)v < \Delta_2 \le (n_1+1)(p_h - p_l)v$, or both $\Delta_2 > (n_1+1)(p_h - p_l)v$ and $\lambda(1-\delta)V^A - (1-p_l)v < 0$ hold.

Overall, we can conclude that the condition to support a separating outcome when pooling outcome is not supported is

$$\frac{\Delta_1 - (p_h - p_l)v}{n_1 - 1} \le \lambda(1-\delta)V^A - (1-p_h)v < \frac{\Delta_2 - (p_h - p_l)v}{n-1}. \tag{27}$$

□

Appendix B: Table for summarizing the nine scenarios in Section 3.4

References

Bakos, Y., & Nault, B. R. (1997). Ownership and investment in electronic networks. *Information Systems Research, 8*(4), 321–341.

Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: Impact of network vulnerability and supply chain integration on incentives to invest. *Information Technology Management, 11*, 7–23.

Barua, A., & Lee, B. (1997). An economic analysis of the introduction of an electronic data interchange system. *Information Systems Research, 8*(4), 398–422.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28–56.

Fang, F., Guo, Z., & Whinston, A. B. (2008). Collective Outsourcing to Market (COM): A market-based framework for information supply chain outsourding. *Journal of Association for Information Systems, 9*(3/4), 98–118.

Ghattas J., & Soffer, P. (2009). Evaluation of inter-organizational business process solutions: A conceptual model-based approach. *Information Systems Frontiers, 11*(3), 273–291.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457.

Gordon, L. A., & Loeb, M. P. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers, 8*(5), 335–337.

Grean, M., & Shaw, M. J. (2000). *Supply-chain integration through information sharing: Channel partnership between Wal-Mart and Procter & Gamble* (21 pp.). Center for IT and e-Business Management, University of Illinois at Urbana-Champaign. http://citebm.business.illinois.edu/IT_cases/Graen-Shaw-PG.pdf. Accessed 30 Sept 2002.

Han, K., Kauffman, R. J., & Nault, B. R. (2004). Relative importance, specificity of investments and ownership in interorganizational systems. In *Proceedings of the workshop on information systems and economics*. University of Maryland, College Park, Maryland.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers, 8*(5), 338–349.

Hengst, M., & Sol, H. G. (2001). The impact of information and communication technology on interorganizational coordination. In *Proceedings of the 34 Hawaii international conference on systems sciences*. Hawaii, USA.

Kannan, K., & Telang, R. (2005). Market for software vulnerabilities? Think again. *Management Science, 51*(5), 726–741.

Kumar, M., & Sareen, M. (2009). Trust and technology in interorganizational business relations. *International Journal of Information Communication Technologies and Human Development, 1*(4), 40–57.

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty, 26*(2/3), 231–249.

Mas-Colell, A., Whinston, M. D., & Green, J. R., (1995). *Microeconomic theory*. USA: Oxford University Press.

Ogut, H., Menon, N., & Raghunathan, S. (2005). *Cyber insurance and IT security investment: Impact of interdependent risk*. Working paper, University of Texas at Dallas.

Parameswaran, M., Zhao, X., Whinston, A. B., & Fang, F. (2007). Reengineering the Internet for Better Security. *IEEE Computer, 40*(1), 40–44.

Soliman, K. S., & Janz, B. D. (2004). *Interorganizational information systems: Exploring an internet-based approach. issues in supply chain managment* (Vol. 1(1), 7 pp.). FedEx Center for Supply Chain Management, The University of Memphis.

Soper, D. S., Demirkan, H., & Goul, M. (2007). An interorganizational knowledge-sharing security model with breach propagation detection. *Information Systems Frontiers, 9*(5), 469–479.

Samuelson, P. (1954). The pure theory of public expenditure. *Review of Economics and Statistics, 36*(4), 387–389.

Straub, D. W. (1990). Effective is security: An empirical study. *Information Systems Research, 1*(3), 255–276.

Straub, D., Goodman, S., & Baskerville, R. (2008). Framing of information security policies and practices. In D. Straub, S. Goodman, & R. Baskerville (Eds.), *Information security policies, processes, and practices.* Armonk, NY: M. E. Sharpe.

Varian, H. (1992). *Microeconomic analysis* (3rd ed.). W. W. Norton & Company.

Varian, H. (2004). *System reliability and free riding* (pp. 1–15). Economics of Information Security, Kluwer.

Wang, E. T. G. & Seidmann, A. (1995). Electronic data interchange: Competitive externalities and strategic implementation policies. *Management Science, 41*(3), 401–418.

Zhao, X., Fang, F., & Whinston, A. B. (2008). An economic mechanism for better internet security. *Decision Support Systems, 45*(4), 811–821.

Zhao, X., Xue, L. & Whinston, A. B. (2009). Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling. In *Proceedings of the International Conference on Information Systems (ICIS)*. Arizona: Phoenix.

Zhu, K., Kraemer, K., Gurbaxani, V., & Xu, S. (2006). *Migration to open-standard interorganizational systems: Network effects, switching costs, and path dependency* (pp. 515–539). MIS Quarterly, (30), Special Issue on Standards.

Fang Fang is an associate professor in the College of Business at California State University, San Marcos. Her research interests include the economics issues of information systems design, information security management, mechanism design, supply chain information coordination, and prediction markets. She has published her papers in the Journal of Mathematical Economics, Production and Operations Management, Decision Support Systems, IEEE computer, etc. Dr. Fang Received her degree from the University of Texas at Austin.

Manoj Parameswaran is a Senior Lecturer in Information Systems at the Foster School of Business at the University of Washington, Seattle. He holds a Ph.D. in Management Science and Information Systems from the McCombs School of Business at the University of Texas at Austin. His research interests include social computing, cloud computing, emerging network architectures, and platforms. Contact him at manojpc@uw.edu.

Xia Zhao is an assistant professor of Information Systems at the Bryan School of Business and Economics, the University of North Carolina at Greensboro. Before she joined the faculty at UNCG, she was a research fellow at the Tuck's Center for Digital Strategies, Dartmouth College. She received her Ph.D. degree in Management Science and Information Systems from the McCombs School of Business at the University of Texas at Austin. Her research interests include online advertising, information security, supply chain management and IT governance. She has published papers in *Decision Support Systems, IEEE Computer, International Journal of Electronic Commerce* and many conference proceedings.

Andrew B. Whinston is the Hugh Roy Cullen Centennial Chair in Business Administration, Professor of Information Systems, Computer Science and Economics, and Director of the Center for Research in Electronic Commerce at The University of Texas at Austin. He is editor of the journal Decision Support Systems and is affiliated with most major Information Systems journals. He is the co-author or co-editor of 23 books and over 300 articles. Recent research interest is in the area of electronic commerce, economics issues in social networking, informational economics with applications to auditing.