Sharing Information on Computer Systems Security: An Economic Analysis

Lawrence A. Gordon
Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance
The Robert H. Smith School of Business, University of Maryland, College Park, MD 20742-1815

Martin P. Loeb
Professor of Accounting and Information Assurance and Deloitte & Touche Faculty Fellow
The Robert H. Smith School of Business, University of Maryland, College Park, MD 20742-1815

William Lucyshyn
Research Director, Defense Advanced Research Projects
Agency (DARPA) and Senior Research Scholar,
School of Public Affairs, University of Maryland, College Park, MD 20742-1815

Forthcoming , *Journal of Accounting and Public Policy* 22 (6), 2003

Abstract

The U.S. federal government has fostered a movement toward sharing information concerning computer security, with particular emphasis on protecting critical infrastructure assets that are largely owned by the private sector. As information security is paramount to accurate financial reporting and the provision of timely and relevant managerial accounting reports for decision-making, the issue of sharing information on computer systems security has direct relevance to accounting, as well as to public policy. This paper presents a model to examine the welfare economic implications of this movement. In the absence of information sharing, each firm independently sets its information security expenditures at a level where the marginal benefits equal the marginal costs. It is shown that when information is shared, each firm reduces the amount spent on information security activities. Nevertheless, information sharing can lead to an increased level of information security. The paper provides necessary and sufficient conditions for information sharing to lead to an increased (decreased) level of information security. The level of information security that would be optimal for a firm in the absence of information sharing can be attained by the firm at a lesser cost when computer security information is shared. Hence, sharing provides benefits to each firm and total welfare also increases. However, in the absence of appropriate incentive mechanisms, each firm will attempt to free ride on the security expenditures of other firms (i.e., renege from the sharing agreement and refuse to share information). This latter situation results in the underinvestment of information security. Thus, appropriate incentive mechanisms are necessary for increases in both firm-level profits and social welfare to be realized from information sharing arrangements.

Key words: information sharing, cyber security, information security economics, homeland security

1 Introduction

The Internet revolution has dramatically changed the way individuals, firms, and the government communicate and conduct business. For example, the telecommunications, banking and finance, energy, and transportation industries, as well as the military and other essential government services, all depend on the Internet and networked computer systems to conduct most of their day-to-day operations. However, this widespread interconnectivity has increased the vulnerability of computer systems – and more importantly, of the critical infrastructures they support – to information security breaches. According to the Report of the President's Commission on Critical Infrastructure (1997, p. ix), "This interconnectivity has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk."

In response to this new vulnerability, organizations have created an arsenal of technical weapons to combat computer security breaches. This arsenal includes firewalls, encryption techniques, access control mechanisms, and intrusion detection systems. The federal government has responded with a major reorganization (forming the Department of Homeland Security, which is responsible for cyber security and infrastructure protection), and is developing a National Strategy to Secure Cyber Space. Unfortunately, to date these measures have met with only limited success. This limited success is highlighted by Richardson (2003, p.21) in the Executive Overview of the 2003 survey conducted by the Computer Security In-

stitute and Federal Bureau of Investigation, "the most important conclusion one must draw form the survey remains that the risk of cyber attacks continues to be high. Even organizations that have deployed a wide range of security technologies can fall victim to significant losses."

Campbell et al. (2003) found empirical evidence that some security breaches result in statistically significant decreases in the market value of firms. Further evidence of the continuing problems associated with computer security breaches is provided by the fact that Representative Stephen Horn, in his third annual report card on computer security, found little improvement within the federal government and gave the federal agencies an overall average grade of F (Matthews, 2002). The United States General Accounting Office (GAO) has also been critical of the computer security activities of federal agencies (GAO/AIMD-98-68; GAO/AIMD-00-33).

It is generally presumed that one desirable way of supplementing the technical solutions to security problems is for organizations to share information related to computer security breaches, as well as to unsuccessful breach attempts. The sharing of information related to methods for preventing, detecting and correcting security breaches is also presumed desirable because it helps to prevent organizations from falling prey to security breaches experienced or stopped by other organizations. Additionally, such information helps organizations respond more quickly with focused remedies should an actual breach occur. As a consequence of the presumed benefits of information sharing, the federal government has been at the center of a movement toward developing security-based information sharing organizations (SB/ISOs)

such as the CERT Coordination Center (CERT/CC), INFRAGARD, Information Sharing Analysis Centers (ISACs), Secret Service Electron Crimes Task Force, and Chief Security Officers Round Tables (CSORTs).[1] By encouraging the sharing of information among organizations, the government could facilitate warnings of homeland security threats or attacks even before such threats or attacks are seen by a government agency. The Homeland Security Act of 2002 (which established the federal governments new Department of Homeland Security) also highlights the importance of information sharing (Public Law 107-296). Unfortunately, this movement toward information sharing related to security breaches has ignored a large body of research that points out the need to create economic incentive mechanisms to facilitate the effective use of such sharing. Nowhere is the absence of these incentive mechanisms more apparent than in the federal government's recent initiatives to help protect critical infrastructure assets owned and operated in the private sector (e.g., in the formation of ISACS). The purpose of this paper is to analyze economic incentives and economic welfare aspects of information sharing among security-based information sharing organizations.[2]

Issues associated with information security are numerous and diverse. Many information security issues are directly related to both the fields of accounting and public policy, and to their intersection (as well as to a number of other disciplines, including computer science and engineering). Since the concepts of information or information systems is central to the very definition of accounting, a number of links between accounting and information security immediately come to mind. First, information security is paramount to accurate financial reporting and the provision of timely and relevant managerial accounting reports for decision-

making. Second, since information, like other organizational assets, is valuable and should be protected, information security comes under the purview of the internal control system designed and monitored by accountants. Third, whether viewed as capital expenditures or current expenditures, managerial accountants have a role in planning and monitoring information security expenditures to help the firm gain a competitive advantage (i.e., spending too much or too little on information security puts the firm at a competitive disadvantage).[3] Thus, this paper's analysis has clear relevance to the above noted links between accounting and information security.

Some links between public policy and information security are also clear. The security and reliability of the entire Internet is affected by the security measures taken by all users of the Internet (Anderson, 2001; Varian 2002). Hence, externalities play an important role in the study of information security. This fact, together with the threat of cyber terrorism aimed at shutting down critical infrastructure industries, has brought information security to the forefront of the public policy agenda. In the United States, for example, there have been numerous legislative acts and executive directives/orders that are focused on providing an environment conducive to facilitating information security among public and private organizations (e.g., The Computer Security Act of 1987; Presidential Decision Directive 63, May 1998; Executive Order 13231, 2001; Homeland Security Act of 2002). By examining the costs and benefits of information sharing as a means of reducing information security breaches and increasing social welfare, this paper has important public policy implications.

Using the modeling framework of Gordon and Loeb (2002), we examine the welfare eco-

nomic implications of sharing information related to the incidence and prevention of information security breaches. In the absence of information sharing, each firm independently sets its information expenditures at a level where the marginal benefits equals the marginal costs. We show that when firms are mandated to share security information, each firm spends less on information security. Nevertheless, the level of information security may increase, decrease, or remain at the optimal no-sharing level, depending on the ease of substitution between the firm's expenditures on information security and those of information sharing partner firms. Since sharing results in the cost of providing any given level of information security to decrease, sharing provides benefits to each firm, so total social welfare increases. However, due to free-riding on the security expenditures of other firms, decentralized information security decisions result in firms underinvesting in information security activities unless appropriate economic incentive mechanisms are put into place. In other words, while mandated information sharing offers the potential to increase each firm's profits and total welfare, without additional incentive mechanisms this potential is unlikely to be realized. This is because each firm will be motivated to renege on any sharing agreement, provide less information to other firms, and reap individual benefits.

The remainder of the paper is organized as follows. In the second section, we review the economics-based literature on information sharing. The third section contains the presentation of our basic model. The fourth section examines how sharing affects levels of information security and levels of information security expenditures. Section five contains an analysis of the incentives to share information. Some implications of our model are discussed in section

six. Concluding comments are offered in the paper's final section..

2 Economics-Based Literature on Information Sharing

Issues related to information sharing have been previously studied in the economics-based literature in the context of non-security related organizations. Of particular relevance, in this regard, is the extensive economics-based literature on trade associations (TAs), and joint ventures (JVs). Trade associations collect information from the membership and disseminate that information to the members (and sometimes also to non-members). Models of information sharing by Novshek and Sonnenshein (1982), Fried (1984), Gal-Or (1984, 1986), Shapiro (1986), Kirby (1988), Vives (1990), and Ziv (1993), among others, have been used to provide insights about the nature of TA's. Most of these papers (e.g., Novshek and Sonnenshein, 1982; Gal-Or, 1984, 1986; Shapiro, 1986; Kirby, 1988) model information sharing in an oligopoly or duopoly using a two-stage game in which each information is first shared and then the firms compete (without collusion) in the product market under the assumption of either Cournot or Bertrand competition. The information shared in these models is either information concerning an industry's demand parameter (common to all participants), or information concerning a cost parameter that is specific (a private value) to the individual firm.

Papers in this area usually do not address the question of incentives to report truthfully. Rather, it is usually assumed that if a firm joins a TA, then it would truthfully reveal information at the sharing stage. With this assumption, the ex ante value of joining the TA

is compared to the ex ante value of not joining to see whether information sharing or no information sharing is the equilibrium outcome. It turns out that the efficacy of information sharing is very sensitive to a number of assumptions, including the following: (1) the type of information shared - (common) demand or (private) cost, (2) the potential value associated with sharing information, (3) the type of competition - Cournot or Bertrand (4) the nature of the products produced - substitutes or complements, and (5) the firm's market share of such products.

In the literature on TAs, sharing information has two effects. First, the information each firm receives from the TA reduces the firm's uncertainty either about the demand for the final product or about the costs faced by competitors. Second, each firm, knowing that the other firms will also have this information, will adjust its decisions to take into account the adjustments by the other firms. This shared information allows the firm to generate higher expected profits by making better quantity and/or pricing decisions. As Vives (1990, p. 413) notes, "In general, the increased precision of the information for a firm has a positive effect on its expected profits, while the precision of the rivals and the increased strategy correlation have a different impact, depending on the nature of competition and uncertainty."

As mentioned earlier, most of the literature on TAs assumes that firms can (and will) pre-commit to truth-telling, and/or the TA can monitor or verify (i.e., audit) truth-telling. One noted exception, in this regard, is the paper by Ziv (1993). Ziv examines the case of a TA in which firm-specific cost information is to be shared and firms engage in Cournot behavior in the competition stage of the game. In this setting, information sharing is valu-

able assuming truthful behavior. However, in the absence of additional incentives, sharing combined with truth-telling is not an equilibrium outcome. Firms therefore have an incentive to understate their privately observed firm-specific cost so that competitors leave them more of the market. For the model examined, Ziv (1993) derives an optimal signaling charge that provides incentives for truth-telling, and for some parameter values that will result in information sharing remaining optimal. Since firms have an incentive to understate private costs, the optimal signaling fee has the characteristic that higher reported costs result in a smaller signaling charge. Furthermore, the signaling fees may be paid to the other TA members, so that overall TA costs are lessoned.

SB/ISOs, such as ISACs, are similar to TA's in that both are information sharing organizations. By sharing information about information security breaches and attempted breaches, SB/ISO members seek to promote the sharing of information about the common threat environment. In essence, the organizational members of SB/ISOs seek to minimize the sum of the costs associated with security breaches plus the costs of information security activities. Furthermore, one would expect truth-telling and verification issues to arise in security-based ISOs as they do in TA's.

SB/ISOs also seek to promote the sharing of the technology related to detecting and stopping information security breaches, as well as ways to repair damage caused by information breaches. Of course, since an organization must expend resources to develop technologies, methods and procedures to deal with information security breaches, sharing of this information is likely to be qualitatively different than sharing the type of information modeled in the

TA literature. In particular, a member may be tempted to free-ride and underinvest in new methods to deal with attempted and successful security breaches in the hope of obtaining solutions from other members for little or no cost.

Free-riding behavior is generally not addressed in the TA literature, although Vives (1990) does talk briefly about free riding in his discussion of disclosure rules. However, free-riding is addressed in the literature on research joint ventures (e.g., see Kamien et al., 1992). Firms form research JVs to pool their research resources and avoid wasteful duplication of effort. Kamien et al. (1992) use a two-stage non-cooperative game to model research JVs. In the first stage, members of the research JV invest in R&D seeking to reduce the costs of production, and in the second stage they face Cournot or Bertrand competition with each other. They show that the highest social welfare, as measured by producer plus consumer surplus, is achieved when firms coordinate the R&D decision and share R&D results for Cournot competition (and, in most cases, also under Bertrand competition). This view suggests that firms may actually be over-investing in security related activities (at least from a social welfare perspective) by not sharing security-based information.

Recent papers dealing with the economics of information security for computer systems have addressed issues relevant to the study of SB/ISOs. Anderson (2001) discusses a number of perverse incentives encountered in the information security arena, including incentives of organizations to free ride on the security efforts of others. Varian (2002) provides a formal model in which the free rider problem is analyzed in the context of providing system reliability. Gordon et al. (2002) present a general discussion of information sharing in the context of

SB/ISOs, but do not present a model or formal analysis. Schechter and Smith (2003), drawing upon an analysis of ordinary burglary by Goldberg and Nold (1980), provide an insightful analysis of the benefits of sharing information to prevent information security breaches. The model we present in the next section, unlike that of Schechter and Smith (2003), considers the costs of providing information security and free riding aspects of sharing information about computer security, in addition to the benefits provided by such sharing. Gal-Or and Ghose (2003) offer a model of information sharing that is complimentary to, although substantially different from, the model presented here. The Gal-Or and Ghose model examines how market characteristics affect the level of information sharing and posits functional forms expressing how security investments and shared information on computer security affects the demand for the final products, the marginal costs of producing the products, the costs of information security investments and the costs of information sharing. This contrasts with our model in which information sharing costs and benefits are derived implicitly by examining the effect on expected security breach losses. Thus, the focus of our model is on how sharing affects the overall level of information security.

3 The Model

Consider two firms, indexed by $i = 1, 2$, that form an SB/ISO. For simplicity, we suppose that each firm seeks to expend additional resources to enhance the security of a single information set. The information set, for example, could be the complete confidential details about all the firm's customers, suppliers, and creditors. Denote L_i as the loss to firm i, if the firm's

information set is breached. The loss could be associated with an attack on the information set's confidentiality, but could also be due to an attack on other dimensions of the information security (e.g., a denial of service attack or an attack on the integrity of the information set). In general, the loss L_i would include the value of profits lost from sales, and some of these sales (and profits) would be garnered by firm j, $j \neq i$. Moreover, the value of the lost sales and profits arising from an information security breach would, in general, also depend on whether or not firm $j \neq i$ also suffered an information security breach. If the profits of firm i were to increase when firm $j \neq i$ suffers an information security breach, then this fact alone would provide some incentive for firm i not to share security information (or take other actions) that would reduce the probability that firm j would suffer an information security breach. In order to focus on more subtle barriers to information sharing, our model takes L_i to be a constant, independent of whether or not the other firm suffers an information security breach and, similarly, assumes that each firm's profits, gross of any loss from breaches, do not depend on whether or not firm $j \neq i$ suffers a breach.

Members of SB/ISOs are typically asked to share information about security breach attempts (whether or not these attempts were successful), about methods used to prevent breaches, and methods to minimize the economic impact of a security breach once it has been detected. For the purposes of this paper, we suppose that if a firm shares security information with other member firms, a portion of the firm's information security expenditure will benefit each of the other member firms without diminishing (or enhancing) the benefit to the firm providing the information. Let $\theta_i \in [0, 1]$ be the portion of firm i's computer security

information that firm i shares with the other member firm.

The probability of a firm's information set being breached will depend on threat level and the information set's vulnerability. With information sharing facilitated by the SB/ISO, the probability (for given threat and vulnerability levels) that firm i's information set will be breached, denoted, P^i, will depend on the firm's level of monetary expenditures on information security, denoted x_i, the sharing partner firm's level of monetary expenditures, denoted x_j, and the amount of sharing by firm j, as captured by the sharing portion θ_j, $j \neq i$. We make the simplifying assumption that x_j and θ_j only affect the probability of a security breach to firm i through the product $x_j\theta_j$. Thus, firm i only benefits from firm j's information security expenditures when firm j shares information (i.e., when $\theta_j > 0$) and only benefits from increases in the sharing portion when firm j spends a positive amount on information security (i.e., when $x_j > 0$). We call P^i the firm's security breach probability function, write it as $P^i(x_i, y_j)$, where $y_j \equiv x_j\theta_j$, and assume that P^i is a continuously twice differentiable function.

Generalizing the Gordon and Loeb (2002) formulation, we assume that increases in expenditures on information security reduce the probability of a breach at a decreasing rate. Specifically, we assume $P_1^i(x_i, y_j) < 0$ and $P_{11}^i(x_i, y_j) > 0$, and $P_2^i(x_i, y_j) < 0$ and $P_{22}^i(x_i, y_j) > 0$, where $P_1^i(x_i, y_j) = \frac{\partial P^i(x_i, y_j)}{\partial x_i}$, $P_2^i(x_i, y_j) = \frac{\partial P^i(x_i, y_j)}{\partial y_j}$, $P_{11}^i(x_i, y_j) = \frac{\partial^2 P^i(x_i, y_j)}{\partial x_i^2}$, $P_{22}^i(x_i, y_j) = \frac{\partial^2 P^i(x_i, y_j)}{\partial y_j^2}$. That is, by increasing its own expenditures on information security, firm i's probability of having a security breach is reduced at a decreasing rate and, when firm $j \neq i$ shares some of its security information, increases in firm j's information security

expenditures decrease the probability of firm i having a security breach at a decreasing rate.

Assume that firm $j \neq i$ sets its information security investment level at x_j, and, for now, we let θ_j be an exogenously given sharing parameter. We interpret the exogenous selection of the sharing parameters as corresponding to an enforceable sharing arrangement specified by the SB/ISO. Assuming each firm is risk-neutral, each firm's problem is to select an information security expenditure level to maximize its expected net benefit from information security expenditures. This is equivalent to minimizing the total expected cost, where the total expected cost equals the expected cost of an information security breach plus the cost of the information security investment. Thus, we can write firm i's problem as:

$$\min_{x_i} \left[P^i(x_i, y_j) L_i + x_i \right] \tag{1}$$

The first-order condition characterizing the optimal investment in information security (assuming that the optimal level is positive), $\overline{x}_i$, is:

$$-P_1^i(\overline{x}_i, y_j) L_i = 1, \tag{2}$$

i.e., the marginal benefit from the last dollar spent on information security, should equal the marginal cost ($1) of the expenditure. For a given level of information sharing, θ_j, equation (2) characterizes firm i's reaction curve $\overline{x}_i(x_j)$. When there is no information sharing, i.e., when $\theta_j = 0$, $\overline{x}_i$ is independent of x_j. Thus, for the case of no information sharing, we can write firm i's optimal level of information security expenditures as a fixed amount, denoted as x_i^*, where for all x_j:

$$-P_1^i(x_i^*, 0)L \ = 1 \tag{3}$$

4 Effects of Sharing on Levels of Information Security Expenditures and Levels of Information Security

4.1 The Restricted Case

In order to gain some insights about the general effect of information sharing, we first study the effect of information sharing for a specific class of security breach probability functions. Consider security breach probability functions which can be written as:

$$P^i(x_i, y_j) = \phi^i(x_i + y_j) \tag{4}$$

where $\phi^i(z)$ is any continuously twice differentiable function from the set of nonnegative real numbers to $(0, 1)$ such that $\phi_1^i(\dot{z}) < 0$ and $\phi_{11}^i(\dot{z}) > 0$, and where ϕ_1^i represents the functions first derivative and ϕ_{11}^i represents the function's second derivative. Note that for this class of security breach probability functions we have:

$$P^i(x_i, y_j) = P^i(x_i + y_j, 0). \tag{5}$$

Thus, information sharing by firm j will shift the i^{th} firm's security breach probability function by $\theta_j x_j$, and the firms marginal benefit curve also shifts to the left by $y_j = \theta_j x_j$. In other words, if firm j spends x_j on information security and there is sharing, the effect on the probability of a security breach for firm i is the same as if firm i had increased its expenditures on information security by $\theta_j x_j$ in absence of information sharing.

For the security breach probability functions belonging to this class, the first order conditions (2) and (3) characterizing firm $i's$ information security expenditures with and without sharing become:

$$-\phi_1^i(\overline{x}_i + \theta_j x_j)L_i = 1 \tag{6}$$

and

$$-\phi_1^i(x_i^*)L \ = 1 \tag{7}$$

respectively. Note that when there is no information sharing, i.e., when $\theta_j = 0$, then $\overline{x}_i = x_i^*$. Otherwise, equation (4) characterizes firm i's reaction curve $\overline{x}_i(x_j)$. Note also, if $x_j = 0$, then $\overline{x}_i(0) = x_i^*$. Comparing conditions (6) and (7) and remembering that x_i, $x_j \geq 0$, one easily sees that for i, $j = 1, 2$ and $j \neq i$:

$$\overline{x}_i(x_j) = \max\{x_i^* - \theta_j x_j, 0\} \tag{8}$$

which can be rewritten as:

$$\overline{x}_i(x_j) = \begin{cases} x_i^* - \theta_j x_j & \text{for } x_j < \frac{x_i^*}{\theta_j} \\ 0 & \text{for } x_j \geq \frac{x_i^*}{\theta_j} \end{cases} \tag{9}$$

[Place Figure 1 here]

The reaction curves specified by equation (9) are shown for both firms in Figure 1. The point where the two reaction curves intersect, denoted $(\widehat{x}_1, \widehat{x}_2)$, represents the Nash equilibrium in information security expenditure levels for a noncooperative game in which each firm's strategy choice is their level of information security expenditures and their payoff is the expected cost savings from information security expenditures. That is, the payoff for firm i equals $[\phi^i(\theta_j x_j) - \phi^i(x_i + \theta_j x_j)]L_i - x_i$, for $i, j = 1, 2$ and $j \neq i$. In order for each firm to provide a positive level of information security expenditure in equilibrium, we assume $x_i^* > \theta_j x_j^*$ for $i, j = 1, 2$ and $j \neq i$. This condition means that the spillover from information sharing is less than each firm would spend on information security in the absence of any information sharing. The Nash equilibrium is found by solving the following simultaneous equations:

$$\widehat{x}_1 = x_1^* - \theta_2 \widehat{x}_2 \tag{10}$$

$$\widehat{x}_2 = x_2^* - \theta_1 \widehat{x}_1 \tag{11}$$

yielding:

$$\widehat{x}_1 = \frac{x_1^* - \theta_2 x_2^*}{1 - \theta_1 \theta_2} \tag{12}$$

$$\widehat{x}_2 = \frac{x_2^* - \theta_1 x_1^*}{1 - \theta_1 \theta_2}. \tag{13}$$

From the definition of the spillover effect, when firm 1 spends $\widehat{x}_1$ on information security and firm 2 spends $\widehat{x}_2$ on information security, the level of information security obtained by firm 1

is equivalent to the amount that would have been obtained had firm 1 spent $\widehat{x}_1 + \theta_2\widehat{x}_2$ in the absence of spillovers (sharing). From equation (10), $x_1^* = \widehat{x}_1 + \theta_2\widehat{x}_2$, so that firm 1 obtains the same level of information security (the level associated with spending x_1^*) that it would in the absence of information sharing. Note that although $\widehat{x}_1$ depends on the value of θ_2, the value x_1^*, determined by equation (7), is independent of θ_2. That is, the level of information security attained by firm 1 (i.e., the probability of a breach) in equilibrium does not depend on θ_2. Similarly, from equation (11), firm 2 attains the same level of information security (the level associated with spending x_2^*) as it would in the absence of information sharing, irrespective of the level of sharing.

While information sharing does not affect the levels of information security services attained by each firm, from equations (10) and (11), we see that when firms share information (i.e.,when $\theta_1,\theta_2 > 0$) each firm spends less on information security than they would have in the absence of sharing.[4] Since information sharing yields the same level of security, but at a smaller cost to each firm, total social welfare (excluding any administrative costs of operating the SB/ISO) is increased as a result of information sharing. We now return to the unrestricted model, in order to examine generality of these results.

4.2 The Unrestricted Case

When firm j shares computer security information, firm i's optimal level of information security expenditures will generally change. Whether these expenditures increase, decrease or remain the same, depends on how the shared security information changes the firm's marginal benefits from information security expenditures, $-P_1^i(x_i, y_j)L_i$. For the restricted

case, marginal benefits from information security expenditures decreased. We generalize this, and assume that $P_{12}^i(x_i, y_j) \equiv \frac{\partial^2 P}{\partial x_i \partial y_j} \geq 0$, so that the spillover from increased information security expenditures by firm j, decreases or leaves unchanged the marginal benefit of firm i's information security expenditures. Given this assumption, the firm's expenditures on information security under information sharing will be less than or equal to the level of expenditures without information sharing. This is formally demonstrated in the following proposition. (Proofs of the propositions appear in the Appendix.)

Proposition 1 *With information sharing, each firm's optimal level of expenditures for information security is less than or equal to the optimal level of expenditures for information security without sharing, i.e.,* $\overline{x}_i \leq x_i^*$.

Note that for the case where $P_{12}^i(x_i, y_j) > 0$, $\overline{x}_i < x_i^*$.[5]

The result that information sharing leads to each firm spending no more than it would have without sharing generalizes to the unrestricted case. However, the result that each firm's achieved level of information security, as measured by the probability of avoiding a breach, $1 - P^i$, is unaffected by the sharing of information does not generalize to the unrestricted case. The analysis of the restricted case showed that the level of information security may not be affected by information sharing. The following two examples show that sharing may also result in the level of information sharing increasing or decreasing.

To see that information sharing can lead to an increase in the level of information security, consider the following probability security breach function for firm i:

$$P^i(x_i, y_j) = \frac{1}{(x_i + 1)(y_j + 1)} \tag{14}$$

The firm, selecting $\overline{x}_i(y_j)$ to minimize $P^i(x_i, y_j)L_i + x_i$, would select:

$$\overline{x}_i(y_j) = \frac{\sqrt{L_i}}{\sqrt{y_j + 1}} - 1 \tag{15}$$

Thus, if there is no sharing, i.e., if $y_j = 0$, the firm spends $x_i^* \equiv \overline{x}_i(0) = \sqrt{L_i} - 1$ on information security and the probability of a breach becomes:

$$P^i(x_i^*, 0) = \frac{1}{\sqrt{L_i}} \tag{16}$$

When $y_j > 0$, the firm spends $\overline{x}_i \equiv \overline{x}_i(y_j)$ on information security, and the probability of a breach becomes:

$$P^i(\overline{x}_i, y_j) = \frac{1}{\sqrt{L_i}\sqrt{y_j + 1}} < \frac{1}{\sqrt{L_i}} \tag{17}$$

That is, $P^i(\overline{x}_i, y_j) < P^i(x_i^*, 0)$, so that information sharing leads to an increase in the level of information security.

Our second example shows that information sharing can lead to a decrease in the level of information security. Consider the following probability security breach function for firm i:

$$P^i(x_i, y_j) = e^{-x_i^2 - 2x_i} \cdot (y_j + 1)^{-1} \tag{18}$$

For this security breach function, we cannot find a closed-end expression for the firm's optimal level of information security expenditures. However, using numerical methods, we can find the optimal level for any given value of the parameters L_i and y_j. Let $L_i = 100$. For the no sharing case, i.e., $y_j = 0$, the firm's optimal level of security expenditures is found to be $x_i^* \approx 1.70$, and the probability of breach is $P^i(x_i^*, 0) \approx 1.8548 \times 10^{-3}$. For the sharing case, assume that $y_j = 1$ (e.g., $x_j = 4$ and $\theta_j = \frac{1}{4}$). Then, the firm's optimal level of security expenditures

is found to be $\overline{x}_i \approx 1.56$, and the probability of breach is $P^i(\overline{x}_i, 1) \approx 1.9367 \times 10^{-3}$. Hence, $P^i(\overline{x}_i, y_j) > P^i(x_i^*, 0)$, so that the level of security is decreased as a result of information sharing. Of course, the reduction in the firm's expenditures on information security (from 1.70 to 1.56) more than offsets the additional expected loss due to the decrease in the level of security.

One obvious sufficient condition for a firm's level of information security to be enhanced by sharing is that the other firm's investment in information security is so large that $P^i(0, y_j) \leq P^i(x_i^*, 0)$. The interesting case to examine is when this condition does not hold, i.e., when $P^i(0, y_j) > P^i(x_i^*, 0)$. For this case, let $x_i^E > 0$ be the level of firm $i's$ information security expenditures such that $P^i(x_i^E, y_j) = P^i(x_i^*, 0)$. Whether or not information sharing results in an increased level of security depends on the relative size of the firm's marginal benefit from an additional dollar of information security expenditure at (x_i^E, y_j) and $(x_i^*, 0)$ (see Figures 2a and 2b).

[Place Figures 2a and 2b here]

Noting that firm $i's$ marginal benefit at (x_i, y_j) equals $-P_1^i(x_i, y_j)L_i$, the necessary and sufficient condition for information sharing to result in increased security is given in the following proposition:

Proposition 2 *Firm $i's$ level of information security will increase as a result of firm j sharing security information if and only if firm $i's$ marginal benefits from additional information security expenditures at $\left(x_i^E, y_j\right)$ are greater than firm $i's$ marginal benefits from additional information security expenditures at $(x_i^*, 0)$. That is, $P\left(\overline{x}_i, y_j\right) < P\left(x_i^*, 0\right)$ if and only if $P_1\left(x_i^E, y_j\right) < P_1\left(x_i^*, 0\right)$.*

For given levels of (θ_1, θ_2), the reaction curves $(\overline{x}_1(x_2), \overline{x}_2(x_1))$ for firm 1 and firm 2 are specified by equation (2). Let $\widehat{x}_1 > 0$ and $\widehat{x}_2 > 0$ represent the (interior) Nash equilibrium in information security expenditure levels for the noncooperative game in which each firm's payoff is the net benefits shown in expression (1). The Nash equilibrium is the point where the two reaction curves intersect. Hence, we have

$$-P_1^i(\widehat{x}_i, \theta_j \widehat{x}_j) L_i = 1, \text{ for } i,\ j = 1, 2 \text{ and } i \neq j \tag{19}$$

Clearly, Propositions 1 and 2 hold at the Nash equilibrium.

Although Proposition 2 and the example preceding it shows that information sharing could lead to a decrease in a firm's level of information security, information sharing will always lead to a decrease in each firm's total expected costs. To see this note:

$$P^i(\widehat{x}_i, \theta_j \widehat{x}_j) L_i + \widehat{x}_i \leq P^i(x_i^*, \theta_j \widehat{x}_j) L_i + x_i^* < P^i(x_i^*, 0) L_i + x_i^* \tag{20}$$

where the first inequality holds because $\widehat{x}_i$ minimizes $P^i(x_i, \theta_j \widehat{x}_j) L_i + x_i$ with respect to x_i, and the second inequality holds since $P_2^i < 0$. Thus, the welfare of each firm individually, and hence the combined welfare of both firms, increases as a result of information sharing. The total social costs of all expenditures on information security, excluding any administrative costs of operating the SB/ISO and externalities to firms outside the SB/ISO, for given levels of sharing, (θ_1, θ_2), is represented by the following social cost function:

$$W(x_1, x_2) = P^1(x_1, \theta_2 x_2) L_1 + P^2(x_2, \theta_1 x_1) L_2 + x_1 + x_2. \tag{21}$$

From (20), the following proposition follows immediately:

Proposition 3 *Assuming positive levels of information sharing can be costlessly enforced by the SB/ISO, member firms will adjust their levels of information security expenditures so that social welfare increases (i.e., total social costs decrease). That is,* $W(\widehat{x}_1, \widehat{x}_2) < W(x_1^*, x_2^*)$.

Proposition 3 provides a theoretical justification for the promotion of information sharing organizations.

While one of the goals of information sharing is to increase the efficiency (i.e., reduce the cost) of securing computer systems, another goal is to increase the overall level of security. However, if firms are not responsible for the information expenditures of the other member firms and can still benefit from such expenditures, then each firm will have a tendency to free-ride on the information security of the others. In turn, such free-riding behavior generally leads to an under-investment in information security relative to the level that maximizes social welfare. The following proposition demonstrates that free riding is indeed a problem in the context of information sharing.

Proposition 4 *At the (decentralized) Nash equilibrium of the noncooperative information sharing game, a small increase in expenditures on information security by either firm would increase social welfare.*

Let $(\widetilde{x}_1, \widetilde{x}_2)$ denote the socially optimal levels of information security expenditures for firm 1 and firm 2, respectively (i.e., $(\widetilde{x}_1, \widetilde{x}_2)$ minimizes $W(x_1, x_2)$). Note that although at the Nash equilibrium total welfare would increase if either firm increased its level of expenditures for information security, this does not imply that the socially optimal expenditure levels for *both* firms are greater than the Nash equilibrium levels. While it is true that $\widetilde{x}_1 > \widehat{x}_1$ or $\widetilde{x}_2 > \widehat{x}_2$, it is possible one firm would spend more than the socially optimal level on information security in the Nash equilibrium. This could arise because one firm's productivity of information

security expenditures is much less than the other firm along with a significant spillover from expenditures in information security from the more productive firm.[6]

5 Incentives to Share Information

In the above analysis, we assumed the degree of sharing, as measured by the value of the θs, was exogenously determined by the coordinating agency and was costlessly enforced by the agency. Since $P_2^i < 0$ for $i = 1, 2$, we have:

$$\frac{\partial W}{\partial \theta_1} = x_1 P_2^2(x_2, \theta_1 x_1) L_2 < 0 \tag{22}$$

and

$$\frac{\partial W}{\partial \theta_2} = x_2 P_2^1(x_1, \theta_2 x_2) L_1 < 0. \tag{23}$$

Thus, if there were no enforcement costs associated with a sharing policy, increasing the mandated degree of sharing reduces total social costs. Hence, SB/ISO administrators should favor full sharing.

Now, suppose that each firm can select the amount it wishes to share, i.e., firm i selects, θ_i, for $i = 1, 2$. We also suppose that the sharing ratio selected by a firm is made known to the other firm, before each firm selects their information security expenditures. Let C^i denote firm i's total expected costs at the Nash equilibrium level of information security expenditures, $(\widehat{x}_1, \widehat{x}_2)$. That is,

$$C^i = P^i(\widehat{x}_i, \theta_j \widehat{x}_j) L_i + \widehat{x}_i, \text{ for } i,\ j = 1, 2 \text{ and } j \neq i. \tag{24}$$

The next proposition shows the inherent incentive problems with information sharing, viz., firms have incentives *not* to share computer security information.

Proposition 5 $\frac{\partial C^i}{\partial \theta_i} < 0$ *for* $i = 1, 2$. *If each firm is allowed to select its sharing ratio (as well as its level of information security investment), the only Nash equilibrium sharing ratio strategies are* $\left(\widehat{\theta}_1 = 0, \widehat{\theta}_2 = 0\right)$.

That is, if additional incentives are not provided, it is in each firm's self-interest to renege on previously agreed upon arrangements to share information on computer systems' security.

We now consider one possible way of altering the rewards to each firm to mitigate the incentive conflicts given in Proposition 4 and 5. Assume that the SB/ISO could verify the magnitude of the actual losses incurred (i.e., they could measure L_i, if the i^{th} firm actually suffered an information breach). Suppose the SB/ISO were to charge each member for the actual realized losses of the other member firms less an amount equal to the expected losses of all other member firms at the socially optimal level of sharing (i.e., the full sharing level $\widetilde{\theta}_i = 1$, $\forall i$ and the optimal information expenditure levels, $x_i = \widetilde{x}_i$, $\forall i$) . Note that (1) the losses of other firm depends on the amount shared by the given firm as well as the level of information expenditures selected by the given firm and (2) the expected losses of all other member firms at the socially optimal level of sharing and information expenditure levels are independent of the given firm's actions. Essentially, each firm receives a fixed subsidy (the expected losses of the other firms at the optimal) less a charge that depends on the given firm's actions.

To analyze the incentive effects of such an incentive mechanism, we consider the extreme case where the SB/ISO and each member firm knows the security breach function of each

member firm and the potential losses from security breaches. For the two firm case, firm 1 would be charged L_2, if firm 2 incurs a breach, and would receive the subsidy $P^2(\widetilde{x}_2, \widetilde{\theta}_1\widetilde{x}_1)L_2$, where $(\widetilde{x}_1, \widetilde{x}_2)$ and $\widetilde{\theta}_1 = 1$ are the socially optimal levels.[7] Firm 1's problem of selecting an information sharing level and a level of information security expenditures would be:

$$\min_{x_1,\theta_1}\{P^1(x_1, \theta_2 x_2)L_1 + x_1 + P^2(x_2, \theta_1 x_1)L_2 - P^2(\widetilde{x}_2, \widetilde{\theta}_1\widetilde{x}_1)L_2\}. \tag{25}$$

Comparing (25) with (21) and noting that $P^2(\widetilde{x}_2, \widetilde{\theta}_1\widetilde{x}_1)L_2$ is a constant, one sees that no matter what level of (x_2, θ_2) were selected by firm 2, firm 1 has the incentive to select (x_1, θ_1) to minimize the social cost function (conditioned on the decisions of firm 2). Similarly, firm 2 would have incentives to minimize the social cost function. This incentive mechanism fully internalizes externalities and makes each firm's objective of minimizing its cost less its subsidy identical to minimizing the social cost function up to a constant.

With this scheme, the SB/ISO's net total subsidy to the firms is:

$$S = \left[P^1(\widetilde{x}_1, \widetilde{\theta}_2\widetilde{x}_2)L_1 - P^1(x_1, \theta_2 x_2)L_1\right] + \left[P^2(\widetilde{x}_1, \widetilde{\theta}_2\widetilde{x}_2)L_2 - P^2(x_1, \theta_2 x_2)L_2\right]. \tag{26}$$

Note that $(\widetilde{x}_1, \widetilde{\theta}_1)$ and $(\widetilde{x}_2, \widetilde{\theta}_2)$ form a Nash equilibrium (or else $(\widetilde{x}_1, \widetilde{\theta}_1)$ and $(\widetilde{x}_2, \widetilde{\theta}_2)$ would not maximize social welfare), and at this equilibrium the net subsidy equals zero.

6 Implications

The U.S. federal government has encouraged the formation of security-based information sharing organizations (SB/ISOs) with the goal of helping to protect critical infrastructure assets that are largely owned and operated by the private sector. The government's underly-

ing assumption is that SB/ISOs could help to align the goals of both the business sector and the federal government, which in turn would improve the security of infrastructure assets. The first implication of the model and analysis provided above is that the federal government's assumption that information sharing would lead to a reduction in social costs (i.e., an increase in social welfare) seems to be correct (see Proposition 3). However, while informations sharing will allow firms to reduce the costs of attaining any given level of security, we showed (in Proposition 2 and the examples preceding it) that it is possible for SB/ISOs to lead a firm to reduce its level of information security.

The second implication of the model and analysis presented above is that SB/ISOs will only reach their potential when appropriate economic incentives to share security information are in place (see Propositions 4 and 5). In fact, without the appropriate economic incentives, free riding behavior on the part of members of the SB/ISOs will likely lead to underinvestment (in terms of what is socially optimal) in information security (see Proposition 4). Unfortunately, the available anecdotal and empirical evidence indicates that the appropriate economic incentives are not in place. For example, joining and reporting to Information Security Analysis Centers (ISACs) is voluntary, with no incentives in place to encourage full reporting and discourage free riding. As a consequence, members may underinvest in the development of information security measures in anticipation of obtaining them for free from other ISAC members and/or under-report breaches and attempted breaches of their computer systems. The free-rider problem is compounded by the fact that members of SB/ISOs are often concerned about providing competitive advantage to other member

firms and protecting their general reputation. This provides an additional motivation for members to renege on sharing security breach information with other member firms. Not surprisingly, the little empirical evidence available suggests that the existing information sharing among ISAC members is minimal.[8] The lack of well-designed economic incentives to encourage information sharing also appears to be a characteristic of most, if not all, of the other SB/ISOs, such as INFRAGARD.

A third implication of our analysis is the need to identify the appropriate economic incentives, and mechanisms for implementing such incentives, for improving the functioning of SB/ISOs. Such incentives could include, but are not limited to, subsidizing firms that are members of SB/ISOs based on the level of information sharing that takes place, government subsidized insurance, and other forms of government regulation. Of course, these incentives would have to be carefully constructed (with more formal auditing/monitoring of member reporting) and evaluated. Indeed, it is easy to envision situations where perverse economic incentives are created (i.e., incentives are created that actually encourage, rather than discourage, security breaches). Hence, the model presented above should be further developed to enable the comparison of the effectiveness and the impact of the different economic incentive schemes.

Examining the veracity of the argument that the appropriate incentives are not in place, and discovering the types of incentives that would work best are, in the final analysis, empirical issues. To date, the empirical data available related to these issues is largely anecdotal in nature or, at best, derived from studies that lack a rigorous empirical experimental de-

sign. Thus, the fourth implication of our model is that rigorous empirical studies related to the structure and activities of information sharing organizations are sorely needed. These studies would not only confirm the levels of information sharing taking place among members of SB/ISOs, but could also shed light on the issues related to the appropriate economic incentives that may be required to facilitate such sharing. In addition, such empirical studies could address the role of governance in resolving many of the thorny issues related to SB/ISOs.

7 Concluding Comments

Sharing of information about threats and breaches of computer security lowers the overall costs of achieving any particular level of information security, and thus has been promoted as an important tool in enhancing social welfare. As a result, the federal government has been at the center of a movement to develop security-based information sharing organizations such as ISACs. However, while our analysis shows that information sharing does indeed offer the *potential* to reduce overall information security costs and raise social welfare, some pitfalls exist that may well prevent the realization of the full potential benefits. These pitfalls revolve around the need to create economic incentives to facilitate effective information sharing.

The two pitfalls described in this paper are noted below. First, even if firms could be trusted to voluntarily share computer breach information, the firms would have an incentive to free-ride on the information security expenditures of the other members of an SB/ISO. Such free-riding will lead to levels of information security expenditures below the level that

maximizes social welfare. Second, and more importantly, without providing additional incentives for a firm to fully and truthfully reveal security breach information, firms will have an incentive not to share information, so that all benefits to information sharing disappear. Although only one incentive mechanism, a member-funded subsidy was examined in this paper, other potential incentive mechanisms that include variable SB/ISO fee structures, government subsidized insurance, and government regulation are possible. The design and analysis of such alternative incentive mechanisms awaits further research.

Acknowledgements

The authors thank Yun Liu, Stuart Schechter, Tashfeen Sohail, Krishnamurthy Surysekar and Lei Zhou for insightful comments on earlier drafts of this paper. Lawrence Gordon and Martin Loeb also gratefully acknowledge research support from the Laboratory for Telecommunications Sciences (within the Department of Defense) through a grant with the University of Maryland Institute for Advanced Computer Studies.

REFERENCES

Anderson, R., 2001. Why information security is hard – an economic perspective. In Proceeding of 17th Annual Computer Security Applications Conference, New Orleans, LA.

Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security 11 (3), 431-448.

Fried, D., 1984. Incentives for information production and disclosure in a duopolistic environment. The Quarterly Journal of Economics 99(2), 367-381.

Gal-Or, E., 1985. Information sharing in oligopoly. Econometrica 53(2), 329-343.

Gal-Or, E., 1986. Information transmission – Cournot and Bertrand equilibria. Review of Economic Studies 53(1), 85-92.

Gal-Or, E., Ghose, A., 2003. The economic consequences of sharing security information. In Proceedings of the Second Workshop on Economics and Information Security (May 29-30), University of Maryland.

United States General Accounting Office (GAO), 1998. Executive guide: information security management: learning from leading organizations. GAO/AIMD-98-68. US Government Printing Office, Washington, DC.

United States General Accounting Office (GAO), 1999. Information security risk assessment: practices of leading organizations. GAO/AIMD-00-33. US Government Printing

Office, Washington, DC.

Goldberg, I., Gold, F., 1980. Does reporting deter burglars? -an empirical analysis of risk and return in crime. The Review of Economics and Statistics, 62(3), 424-431.

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

Gordon, L., Loeb, M., Lucyshyn, W., 2002. An economics perspective on the sharing of information related to security breaches: concepts and empirical evidence. In Proceedings of the First Workshop on Economics and Information Security (May 16-17), University of California, Berkeley.

Gordon, L., Loeb, M., Lucyshyn, W., 2003. Information security expenditures and real options: a wait- and-see approach. Computer Security Journal 19(2), 1-7.

Hulme, G., 2002. With friends like this. InformationWeek, 896 (July 8), 22.

Kamien, M., Muller, E., Zang, I., 1992. Research joint ventures and R&D cartels. American Economic Review . 82(5), 1293-1306.

Kirby, A., 1988. Trade associations as information exchange mechanisms. RAND Journal of Economics 29 (1), 138-146.

Matthews, W., 2002. Horn: feds still fail security. Federal Computer Week (Dec. 2), http://www.fcw.com/fcw/articles/2002/1202/pol-horn-12-02-02.asp

Novshek, W., Sonnenschein, H., 1982.Fulfilled expectations in Cournot duopoly with information acquisition and release. Bell Journal of Economics 13(1), 214-218.

Public Law 107-296, November 25, 2002, "To establish the Department of Homeland Security, and for other purposes," http://www.cio.gov/documents/pl_107_296_nov_25_2003.pdf

Richardson, R., 2003. CSI/FBI 2003 computer crime and security survey. Computer Security Journal 19(2), 21-40.

Shapiro, C., 1986. Exchange of cost information in oligopoly. Review of Economic Studies 53(3), 433-446.

Schechter, S., Smith, C., 2003. How much security is enough to stop a thief? The economics of outsider theft via computer systems networks. In Proceedings of the Financial Cryptography Conference (January 27-30), Gosier, Guadeloupe.

Varian, H., 2002. System reliability and free riding. In Proceedings of the First Workshop on Economics and Information Security (May 16-17), University of California, Berkeley.

Vives, X, 1990. Trade association disclosure rules, incentives to share information, and welfare. RAND Journal of Economics 21(3), 409-430.

Ziv, A., "Information Sharing in Oligopoly: The Truth-Telling Problem," RAND Journal of Economics, Vol. 24 (1993), pp. 455-465.

8 Appendix

Proof of Proposition 1:

Since $P_{12}^{i}(x_i, y_j) > 0$

$$P_1^i(x_i^*, 0) < P_1^i(x_i^*, y). \tag{A1}$$

From equation (2) and equation (3), we have

$$P_1^i(\overline{x}_i, y_j) = -\frac{1}{L} = P_1^i(x_i^*, 0) \tag{A2}$$

Thus,

$$P_1^i(\overline{x}_i, y_j) < P_1^i(x_i^*, y_j). \tag{A3}$$

As $P_{11}^{i}(x_i, y_j) \geq 0$, this implies

$$\overline{x}_i \leq x_i^*. \blacksquare \tag{A4}$$

Proof of Proposition 2:

Suppose firm $i's$ marginal benefits from additional information security expenditures at $\left(x_i^E, y_j\right)$ are greater than firm $i's$ marginal benefits from additional information security expenditures at $(x_i^*, 0)$, i.e.,

$$-P_1\left(x_i^E, y_j\right) L_i > -P_1\left(x_i^*, 0\right) L_i. \tag{A5}$$

This condition holds if and only if

$$P_1\left(x_i^E, y_j\right) < P_1\left(x_i^*, 0\right). \tag{A6}$$

Since $P_1^i(x_i^*, 0) = -\frac{1}{L}$, and $P_1^i(\overline{x}_i, y_j) = -\frac{1}{L}$, we have

$$P_1^i(x_i^*, 0) = P_1^i(\overline{x}_i, y_j) \tag{A7}$$

Therefore, $P_1\left(x_i^E, y_j\right) < P_1\left(x_i^*, 0\right)$ holds if and only if

$$P_1\left(x_i^E, y_j\right) < P_1^i(\overline{x}_i, y_j). \tag{A8}$$

As $P_{11}^i > 0$, (A8) holds if and only if

$$x_i^E < \overline{x}_i. \tag{A9}$$

Since $P_1^i < 0$, (A9) holds if and only if

$$P\left(x_i^E, y_j\right) > P^i(\overline{x}_i, y_j). \tag{A10}$$

By the definition of x_i^E,

$$P\left(x_i^E, y_j\right) = P^i(x_i^*, 0). \tag{A11}$$

Hence, $P\left(x_i^E, y_j\right) > P^i(\overline{x}_i, y_j)$ if and only if

$$P\left(\overline{x}_i, y_j\right) < P(x_i^*, 0). \blacksquare \tag{A12}$$

Proof of Proposition 4:

The first-order conditions characterizing $(\widehat{x}_1, \widehat{x}_2)$, the Nash equilibrium levels of information security expenditures, are:

$$-P_1^1(\widehat{x}_1, \theta_2\widehat{x}_2)L_1 = 1 \tag{A13}$$

and

$$-P_1^2(\widehat{x}_2, \theta_1\widehat{x}_1)L_2 = 1 \tag{A14}$$

Note that since $\theta_1 P_2^2(\widehat{x}_2, \theta_1\widehat{x}_1)L_2 < 0$ and $\theta_2 P_2^1(\widehat{x}_1, \theta_2\widehat{x}_2)L_1 < 0$, we have:

$$-P_1^1(\widehat{x}_1, \theta_2\widehat{x}_2)L_1 - \theta_1 P_2^2(\widehat{x}_2, \theta_1\widehat{x}_1)L_2 > 1 \tag{A15}$$

and

$$-P_1^2(\widehat{x}_2, \theta_1\widehat{x}_1)L_2 - \theta_2 P_2^1(\widehat{x}_1, \theta_2\widehat{x}_2)L_1 > 1 \tag{A16}$$

The interpretation of inequality (A15) is that at the Nash equilibrium the benefits to both firms in terms of a reduction in the total expected breach costs for a small increase in firm 1's expenditures on information security is greater that the increase in the expenditure. Similarly, (A16) shows that at the Nash equilibrium, social welfare could be increased (i.e., total social costs cost be decreased), if firm 2 were to increase its expenditures on information security by a small amount. Hence, a small increase in expenditures on information security by either firm would increase social welfare. ■

Proof of Proposition 5:

At the Nash equilibrium,

$$-P_1^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) L_1 = 1 \tag{A17}$$

and

$$-P_1^2\left(\hat{x}_2, \theta_1\hat{x}_1\right) L_2 = 1. \tag{A18}$$

For Firm 1:

$$\begin{aligned}\frac{\partial C^1}{\partial \theta_1} &= P_1^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) L_1 \frac{\partial \hat{x}_1}{\partial \theta_1} + P_2^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) L_1 \frac{\partial \hat{x}_2}{\partial \theta_1}\theta_2 + \frac{\partial \hat{x}_1}{\partial \theta_1} \\ &= \left[P_1^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) L_1 + 1\right] \frac{\partial \hat{x}_1}{\partial \theta_1} + P_2^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) L_1 \frac{\partial \hat{x}_2}{\partial \theta_1}\theta_2\end{aligned} \tag{A19}$$

From (A17), we know $P_1^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) L_1 + 1 = 0$, so:

$$\frac{\partial C^1}{\partial \theta_1} = P_2^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) L_1 \frac{\partial \hat{x}_2}{\partial \theta_1}\theta_2 \tag{A20}$$

Taking the total differential of (A18), we find:

$$\begin{aligned}\frac{\partial \hat{x}_2}{\partial \theta_1} &= -\frac{P_{12}^2\left(\hat{x}_2, \theta_1\hat{x}_1\right) L_2\hat{x}_1}{P_{11}^2\left(\hat{x}_2, \theta_1\hat{x}_1\right) L_2} \\ &= -\frac{P_{12}^2\left(\hat{x}_2, \theta_1\hat{x}_1\right) \hat{x}_1}{P_{11}^2\left(\hat{x}_2, \theta_1\hat{x}_1\right)}\end{aligned} \tag{A21}$$

Since, $\hat{x}_1 > 0$, $P_{11}^2 > 0$ and $P_{12}^2 > 0$, $\frac{\partial \hat{x}_2}{\partial \theta_1} \leq 0$. Therefore, as $P_2^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) < 0$, $L_1 > 0$ and $\theta_2 > 0$:

$$\frac{\partial C^1}{\partial \theta_1} = P_2^1\left(\hat{x}_1, \theta_2\hat{x}_2\right) L_1 \frac{\partial \hat{x}_2}{\partial \theta_1}\theta_2 < 0. \tag{A22}$$

An analogous proof follows for firm 2. That is, firm i's total cost is increasing in its sharing ratio θ_i, i.e., without additional incentive mechanisms, each firm is motivated to renege on any sharing agreement.

FOOTNOTES

1. The CERT® Coordination Center (CERT/CC) is a federally funded research and development center operated by Carnegie Mellon University. CERT/CC publishes security alerts. See http://www.cert.org/nav/index_main.html

INFRAGARD is an is a cooperative undertaking between the U.S. Government (led by the FBI) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. See http://www.infragard.net/

Presidential Decision Directive/NSC-63 (PDD-63), Critical Infrastructure Protection, May 22, 1998, tasked administration officials to work with the National Economic Council and the owners and operators of critical infrastructures, and to encourage these owners to create private ISACs. The vision for the ISACs was that they would be a place where members could share information about security breaches with each other; share information about how to prevent computer breaches; and serve as a mechanism to provide members with government information on threats and attacks government agencies are experiencing.

CSORTs are regional initiatives that include a small number of Chief Security Officers who meet on a regular, but informal basis to discuss issues of common interest.

2. We recognize that there exist personal relationships that lead to informal sharing among individuals associated with SB/ISOs. Although useful, this type of sharing tends to be unpredictable and ephemeral. The focus of this paper is on the formally sanctioned sharing arrangements among the member firms of these organizations.

3. Gordon and Loeb (2002) and Gordon et al (2003) have analyzed problems associated with management's selection of a level to invest in information security.

4. From equations (12) and (13), it also follows that $\frac{\partial \widehat{x}_1}{\partial \theta_2}, \frac{\partial \widehat{x}_2}{\partial \theta_1} < 0$, i.e., as one would expect, the more the partner firm shares information, the less the firm will invest in information security in equilibrium. To see this for firm 1, note:

$\frac{\partial \widehat{x}_1}{\partial \theta_2} = \frac{\theta_1 x_1^* - x_2^*}{(1-\theta_1\theta_2)^2}$. Since $\theta_1, \theta_2 > 0$, $sign\left(\frac{\partial \widehat{x}_1}{\partial \theta_2}\right) = sign(\theta_1 x_1^* - x_2^*)$. As $x_1^* < \frac{x_2^*}{\theta_1}$ by assumption, we have the desired result $\frac{\partial \widehat{x}_1}{\partial \theta_2} < 0$.

5. Note also that if information sharing (unrealistically) resulted in an increase in a firm's marginal benefit curve, i.e., if $P_{12}^i(x_i, y_j) < 0$, a proof analogous to that of Proposition 1 would demonstrate that a firm's information security expenditures would increase as a result of sharing.

6. For example, suppose $P_i(x_i, y_j) = \frac{.5}{(.5[x_i + .\theta_j x_j]+1)^2}$ for $i = 1, 2$, $L_1 = 432$, $L_2 = 250$, $\theta_1 = .25$, $\theta_2 = .5$. One can easily verify that, $x_1^* = 10$, $x_2^* = 8$, $\widehat{x}_1 = 6.99$, $\widehat{x}_2 = 6.29$, and $\widetilde{x}_1 = 6.41$, $\widetilde{x}_2 = 8.45$. Thus, $\widehat{x}_1 > \widetilde{x}_1$, even though $\widehat{x}_1 + \widehat{x}_2 < \widetilde{x}_1 + \widetilde{x}_2$.

7. Note that under the information assumptions, the SB/ISO has enough information to calculate the value of $(\widetilde{x}_1, \widetilde{x}_2)$ for the full (and optimal) level of sharing,$(\widetilde{\theta}_1, \widetilde{\theta}_2)$.

8. A recent security survey by Hulme (2002) indicated that approximately 48% of respondents to the question "Who does your company notify after a security incident?" answered no one. Less than 10% of the survey respondents indicated that they notified an ISAC after a security incident.(p.22)