An Economics Perspective on the Sharing of Information Related to Security Breaches: Concepts and Empirical Evidence

By

Dr. Lawrence A. Gordon, Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance, Smith School of Business, University of Maryland

Dr. Martin P. Loeb, Professor of Accounting and Information Assurance, Deloitte & Touche Faculty Fellow, Smith School of Business, University of Maryland

Mr. William Lucyshyn, Research Director, Defense Advanced Research Projects Agency & Senior Research Scholar, School of Public Affairs, University of Maryland

Presented at

Workshop on Economics and Information Security

University of California, Berkeley, May 16-17, 2002

An Economics Perspective on the Sharing of Information Related to Security Breaches: Concepts and Empirical Evidence

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. Unfortunately, this arsenal has met with only limited success, as indicated by the fact that over 90% of the respondents to the 2001 survey conducted by the Computer Security Institute and Federal Bureau of Investigation had detected security breaches within the past 12 months (Power, 2001, p. 31). Further evidence of the continuing problems associated with computer security breaches is provided by the fact that Representative Stephen Horn, in his second annual report card on computer security within the federal government, gave the federal agencies an overall average grade of F (Dean 2001).

It is generally recognized that a key ingredient required to improve computer security is the gathering, analysis and sharing of information related to actual, as well as unsuccessful attempts at, computer security breaches. In the regard, in 1998 the U.S. federal government encouraged the establishment of industry-based

Information Sharing and Analysis Centers (ISACs) under Presidential Decision Directive/NSC-63. These ISACs are intended to be private sector-based, but with the assistance and participation of the federal government. One such ISAC is the Financial Services ISAC (FS/ISAC). As noted on its website (http://www.fsisac.com/): “The Financial Services Sharing and Analysis Center (FS/ISAC) offers a confidential venue for sharing security vulnerabilities and solutions. It facilitates trust among its participants. Members benefit from the FS/ISAC’s unique proactive means of mitigating cyber-security risks.”

As clearly noted in the above quote, “sharing security vulnerabilities and solutions” is a fundamental goal of the ISACs. However, there are a number of interesting economic issues that will affect achievement of this goal (for ISACs or any other organizational arrangement focused on the sharing information related to security breaches). These economic issues are most easily discussed in terms of the following series of questions. What is the economic incentive for an organization to join an ISAC? Once a firm joins an ISAC, what are the economic incentives to fully reveal information about actual security breaches? If such incentives are weak or non-existent, what types of security breaches are most likely to be revealed? Can the reward system be altered to provide economic incentives for complete and truthful revelation of security breaches? Do ISACs promote innovation in information security or do they promote free-riding behavior in which each ISAC member under invests and relies on the investments of fellow ISAC members? More generally, given the existing incentive structures, do ISACs increase social welfare?

Questions on information sharing, economic incentives, and social welfare, similar to those noted above, have been previously studied in the context of other organizations. This earlier work is able to shed light on the answers to these questions. Of particular relevance, in this regard, is the extensive literature on trade associations (TAs). TAs collect information from members and disseminate that information to 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 TAs. 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.[1] 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 value of information is very sensitive to a number of assumptions: whether the information is about (common) demand or (private) cost, whether the firms compete in a Cournot or Bertrand game, and whether or not the firms produce substitute or compliments products.[2] Moreover, as shown by Vives (1990), taking consumer as well as producer surplus into account, the

[1] In a Cournot game each firm selects a quantity to produce and sell, and in a Bertrand game the strategy choice is the selection of the output's price.

[2] Vives (1990) also shows that the value of sharing information to the individual firms and to society is sensitive to whether the TA shares (an aggregate statistic of) collected information only with TA members (an exclusionary arrangement) or with everyone (a non-exclusionary arrangement. In summarizing the previous literature, Vives (1990, p. 412) writes, "What are the general principles that explain the incentives to share information among oligopolists? Very few, if any, according to the by-now long literature on information transmission in oligopoly."

social welfare implications of information sharing are also quite sensitive to the model's specification.

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. This information allows the firm to generate higher *expected* profits by making better quantity and/or pricing decisions. 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.

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 verify truth-telling. Ziv (1993) makes no such assumptions. He 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 valuable assuming truthful behavior. However, in the absence of additional incentives, sharing combined with truth-telling is not an equilibrium outcome. Firms would have an incentive to understate their privately observed firm-specific cost so that competitors would 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.

ISACs are similar to TAs in that both are information sharing organizations. By sharing information about information security breaches and attempted breaches, ISACs seek to promote the sharing of information about the threat environment that is common to all its members. The organizational members of the ISACs seek to minimize the sum of the costs of security breaches plus the costs of information security expenditures. Furthermore, one would expect truth-telling and verification issues to arise in ISACs as they do in TAs. ISACs 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 technology, methods and procedures to deal with information security breaches, sharing of this information may be qualitatively different than sharing the type of information modeled in the TA literature. In particular, an organization may be tempted to free-ride and under invest in new methods to deal with attempted and successful security breaches in the hope of obtaining solutions from ISAC members for little or no cost.

Free-riding behavior is not addressed in the TA literature, but it is addressed in the literature on research joint ventures (e.g., see Kamien et al, 1992). Firms form research joint ventures (RJVs) to pool their research resources and avoid wasteful duplication of effort. Kamien et al (1992) use a two-stage non-cooperative game to model RJVs. In the first stage, members of the RJV 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).

The combination of the literature on TAs and RJVs provides the theoretical underpinnings to develop a model for examining information sharing related to security breaches. Such a model could be used to develop specific hypotheses for empirical testing. The empirical testing of such hypotheses could be done within the context of the ISACs or other information sharing arrangements related to security breaches.

References

Dean, J. "Feds Get an 'F' in Computer Security." *Government Executive Magazine*, November 9, 2001

Fried, D. "Incentives for Information Production and Disclosure in a Duopolistic Environment." *The Quarterly Journal of Economics*, Vol. 99 (1984), pp. 367-381.

Gal-Or, E. "Information Sharing in Oligopoly." *Econometrica*, Vol. 3 (1985), pp. 329-343.

______. "Information Transmission –Cournot and Bertrand Equilibria." *Review of Economic Studies*, Vol. 53 (1986), pp. 85-92.

Kamien, M., Muller, E. and Zang, I. "Research Joint Ventures and R&D Cartels." *American Economic Review*, Vol. 82 (1992), pp. 1293-1306.

Kirby, A. "Trade Associations as Information Exchange Mechanisms." *RAND Journal of Economics*, Vol. 19 (1988), pp. 138-146.

Novshek, W. and Sonnenschein, H. "Fulfilled Expectations in Cournot Duopoly with Information Acquisition and Release." *Bell Journal of Economics*, Vol. 13 (1982), pp. 214-218.

Power, R. "2001 CSI/FBI Computer Crime and Security Survey." *Computer Security Journal*, Vol. XVII, No. 2 (Spring 2001), pp. 29-51.

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

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

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