

The Economic Consequences of Sharing Security Information¹

Esther Gal-Or Anindya Ghose²

Abstract

Information technology (IT) security has emerged as an important issue in the last decade. To promote the disclosure and sharing of cyber-security information amongst firms, the US federal government has encouraged the establishment of many industry based Information Sharing & Analysis Centers (ISACs) under Presidential Decision Directive/NSC-63. We develop an analytical framework to investigate the competitive implications of sharing information about security breaches and investments in technologies which promote security. Using a game-theoretic model, we point out how firm and industry characteristics affect the incentives for information sharing amongst competing firms and their impact on firms' profits. We find that security technologies and information sharing act as "strategic complements in equilibrium". Our paper points out that by joining such alliances, firms can benefit from a "direct effect" which increases demand and a "strategic effect" which alleviates price competition. Our results suggest that information sharing is more valuable when product substitutability is higher, suggesting that information is of greater value in more competitive industries. We also highlight that sharing security information is more valuable for larger firms and in larger industries. Our model points out that "demand-side spillover" effects boosts sharing levels and lead to higher prices. Conversely, "cost-based spillovers" lead to lower sharing and lower technology investments. Finally we show that optimal levels of technology invested and information shared are higher in a sequential mode than in a Bertrand-Nash mode.

Keywords: *Security Technology Investment, Information Sharing, Security Breaches, Externality Benefit, Spillover Effect, Marginal Cost.*

¹This is an extended abstract of a preliminary draft : comments are very welcome. The full paper is available upon request. The contact author is: Anindya Ghose, e-mail: aghose@andrew.cmu.edu, phone : 412-2685798.

² The authors are Glenn Stinson Chair Professor of Business Administration and Economics, Katz School, University of Pittsburgh and Doctoral Student, Information Systems, GSIA, Carnegie Mellon University, respectively.

1 Introduction

The increasing pervasiveness and ubiquity of the Internet has provided cyber attackers with more opportunities to misappropriate or corrupt an organization's data resources. As e-commerce continues to grow, so does cyber crime. According to Jupiter Media Metrix, cyber-security issues could potentially cost e-businesses almost \$25 billion by 2006 - up from \$5.5 billion in 2001.³ With poor online security measures, many companies have experienced negative effects not only on their online sales over the past few years, but also in their off-line sales that shifted to competitors with a higher "perceived" security. There are many well known examples of cyber-hacking. Citibank lost business when it went public with the news that they had been hacked.⁴ Egghead.com faced a massive backlash from its customers after being hacked in 2000 by online intruders which led to its eventual bankruptcy filing. A security breach at Travelocity in 2001 exposed the personal information of thousands of customers who had participated in a promotion. Other victims in the recent past, include Yahoo, AOL and E-Bay. Not just restricted to the online world, this trend has been pervasive offline too where Microsoft and NASA, amongst others have been targeted. Hence corporations in many industries have recognized a strong need to beef up their cyber-security against potentially debilitating attacks and to treat computer security like a strategic marketing initiative, rather than a compliance burden.

For a while now, it has been recognized that a key factor required to improve information security is the gathering, analysis and sharing of information related to actual, as well as unsuccessful attempts at, computer security breaches. In this regard, the U.S. federal government has encouraged the establishment of industry-based Information Sharing and Analysis Centers (ISACs). ISACs facilitate sharing of information relating to members' efforts to enhance and to protect the security of the cyber infrastructure. In January 2001, nineteen of the nation's leading high tech companies announced the formation of a new Information Technology Information Sharing and Analysis Center (IT-ISAC) to cooperate on cyber security issues. Using the shared information, the IT-ISAC disseminates an integrated view of relevant information system vulnerabilities, threats, and incidents, to its members. It also shares best security practices and solutions among its members, and thus provides an impetus for continuous improvement in security products. Obviously, such mutual collaboration through information sharing is eventually intended for increases in the demand of security enhancing software and hardware.

Revealing information about security breaches entails both costs and benefits for the disclosing firm. The costs can accrue from loss of market share or stock market value from negative publicity (Cavusoglu, et al 2002, Campbell, et al. 2003). In a 2002 report by Jupiter Media Metrix, IT executives revealed they were more concerned with the impact of online security problems on consumer confidence and trust in e-business than the actual financial losses of physical infrastructure. Many companies have cited the FOIA (Freedom of Information Sharing Act) as a roadblock to the public-private partnership intended by ISACs. According to firms, the dual role played by the government - customer and regulator, will remain an obstacle to private sector cooperation. Ba-

³"Privacy Worries Plague E-Biz", <http://cyberatlas.internet.com/markets/retailing/article.html>

⁴"Information Sharing-Reactions are Mixed to Government Overtures," <http://networking.earthweb.com/netsecur/article,06/17/02>.

sically, companies are reluctant to give the government information on attacks and vulnerabilities that regulators may use against them later on.

One can think of losses from a scenario in which a competing firm or a third party can leverage the shared information and attempt to hack the databases of the breach reporting firms or malign its reputation by anonymously reporting it to the public. In January 2003, Next Generation Software Services (NGSS) claimed that CERT (Computer Emergency Response Team), the government-sponsored Internet security reporting center passed vulnerability information to third parties uninvolved with a problem about which NGSS had notified CERT. NGSS felt that this was a direct violation of trust, as the information was leaked to potential competitors of NGSS and it eventually severed ties with CERT.⁵

Other possibilities could include the hacking of the security breach correspondence between an ISAC and its member firms. The recent case of the leakage of a fatal flaw in an Internet software package from Sun Microsystems to a public mailing list proves this. The hacker posted an advisory containing the bug's specifics to the Full-Disclosure security mailing list. He also posted a warning about a separate security flaw discovered by researchers at MIT that wasn't supposed to be published until June. The hacker apparently intercepted both documents from CERT. According to CERT however, intruders may have hacked into systems operated by any of the dozens of affected vendors who received advance copies of the advisories. Irrespective of which party was hacked, the bottomline was that Sun Microsystems took a big hit in reputation.

However there are several positive aspects to reporting and sharing security breaches. The benefit from mutual sharing of actual or attempted security breaches can be partitioned into a private firm specific benefit and an external industry level benefit. This private benefit can be borne either directly by the prevention of further security breach and fraud losses in future (e.g., identifying and repairing vulnerabilities in their information security systems) or indirectly via increased sales emanating from a better security reputation and goodwill amongst consumers (NIPC 2001). Consumers' perceptions of security of financial information affects their satisfaction and purchases with the e-channel (Szymanski and Hise 2000, Parasuraman 2000).⁶ By reporting a security breach to central monitoring or law enforcement agency, a firm can send a strong message to its customers that the company takes information security seriously, is committed to developing rigorous information security procedures designed to protect sensitive information and detect security breaches and takes all necessary steps to mitigate damage from a future breach (Schenk and Schenk 2002). Such actions can boost the consumer comfort level while dealing with such firms, in terms of alleviating their "perceived security risk".

Once can envisage a situation in which customers of the ISAC members are many of the big corporations who buy goods or services from other firms, on a regular basis. For instance in the

⁵ "There is a conflict of interest for NGSS. One of the alliance members is one of our competitors, Digital Defense. We spend the time doing the research and working with the vendor to develop a patch and they get all this information! If the body of the Alliance was made of entirely government organizations, we wouldn't have a problem with this policy. Imagine if one of the commercial members used information on a new vulnerability delivered by CERT to gain access to one of their competitors's computers?" "www.inforworld.com," Mark Litchfield, CEO NGSS, 01/29/03.

⁶GVU surveys (<http://www.gvu.gatech.edu/usersurveys/survey> - 1998 - 10) have shown that consumers are quite concerned about security violations, with approximately 85% of respondents saying security concerns would be a significant factor in determining whether or not to do business with an online firm.

IT-ISAC, the customers of security vendors like Symantec and Computer Associates include big corporations like Proctor & Gamble, Lockheed Martin and Halliburton and hundreds of other firms.⁷ As corporations perceive improvement in the effectiveness of cyber security products – accruing from the information sharing behavior of security vendors (who are members of the IT-ISAC) – the overall customer confidence in stopping or apprehending cyber perpetrators increases, leading to increased demand for IT security products.

Hence, information security investments and sharing of security information can involve spillovers, which result in positive externalities for the industry as a whole. The industry benefits can accrue when enhancement in customers’ trust in transacting with a particular firm also expands the overall market size within the industry. A number of industries have experienced positive demand shocks by successful attempts at cross-selling and upselling, as a consequence of mitigating consumers’ fears of privacy and information security related issues.⁸ These benefits can indeed be significant in the realm of B2C e-commerce. For example, Amazon’s pioneering efforts in protecting the integrity of customer data, whether individuals or merchants also has had a positive ripple-effect on the size of potential market of its competitors like Barnes & Nobles and E-Bay. It has led to an increase in online purchases as consumers’ confidence in revealing credit card numbers and other personal information has grown considerably. In the online financial services industry, Ameritrade and DLJDirect have been able to reap the benefits of an increase in the customer comfort level in completing financial transactions on the Internet. In this regard, they have acknowledged the increased investment in security and privacy-enhancing technologies made by competitors like Charles Schwab and E-Trade as a potential factor for an increase in the online traffic. As pointed out above, sales of cyber security products have catapulted over the years, as security vendors become increasingly successful in producing an effective arsenal of weapons. One of the main purposes of this paper is to focus on such indirect “demand enhancing” benefits of information sharing alliances.

1.1 Research Questions & Prior Literature

For any organizational arrangement focused on the reporting and dissemination of information related to security breaches, there are a number of interesting economic issues that will affect achievement of this goal. We seek to address the following questions in this paper. What are the incentives for competing firms in a given industry, to share information about security breaches through a central organization? Does the degree of competitiveness in an industry hamper the economic incentives to fully reveal information about security breaches? Do smaller firms gain more from information sharing than larger firms? How does industry size impact such sharing behavior amongst competing firms? What is the nature of the relationship between investment in security enhancing technologies and the sharing of information pertaining to cyber-security attacks? Do

⁷Symantec’s success is punctuated by the continued growth of its worldwide enterprise customer base, featuring new contracts with 48 Global 500 and 18 Fortune 100 companies including 12 of the world’s largest banks, three of the world’s largest auto manufacturers, three of the world’s largest petroleum companies, three of the world’s largest pharmaceutical companies and four of the world’s largest telecom companies.

⁸The means by which firms have been enlightening customers about their efforts in security information sharing and security technology investments is through various advertising media.

spillover effects debar firms from sharing information and result in sub-optimal levels of technology investment or do they promote sharing and lead to increased technology investments?

Prior literature which is of relevance includes that of information sharing by Fried (1984), Gal-Or (1985), Shapiro (1986), the literature on mode of conduct and strategic effects such as Bulow, Geanakoplos and Klemperer, Gal-Or (1986) and extensive economics based literature on joint ventures such as d' Aspremont and Jacquemin(1988). Recent papers dealing with the economics of information security include Anderson(2001) who discusses various perverse incentives in the information security domain. Varian (2002) analyzes the free rider problem in the context of system reliability. Gordon and Loeb (2002) present a framework to determine the optimal amount to invest to protect a given set of information. Gordon, Loeb and Lucyshyn (2002) raise the issue of the need to study the economic benefits of security information sharing. Schechter and Smith (2003) provide an analysis of the benefits of information sharing to prevent security breaches.

2 Model

We analyze a market consisting of two firms producing a differentiated product in a two-stage non-cooperative game. In the first stage, firms simultaneously choose optimal levels of security technology investment which we denote as (t_i, t_j) and information sharing levels which we denote as (s_i, s_j) . In the second stage they choose prices (p_i, p_j) simultaneously. We consider a Subgame perfect equilibrium of this game using backward induction. We normalize the amount of security breach information being shared such that it always lies between 0 and 1, i.e., $s_i \in (0, 1)$. When $s_i = 0$, no information is shared and when $s_i = 1$, all the information is shared. Costs of production are assumed to be symmetric for both firms and are normalized to zero, without loss of generality. We explicitly model costs of sharing security information by imposing the variable costs $K_2 g(s_i)$, where K_2 is the information sharing cost parameter. We assume that $g(s)$ increases and is convex in s , i.e., $g' > 0$ and $g'' > 0$.

We denote the industry and firm specific benefits as B_I and B_F respectively. In such a scenario where investments in security enhancing technologies by one firm can lead to an overall demand expansion in the industry, thereby benefiting the competing firms as well, one can envisage the possibility of “demand side spillover” effects. Subsequently we also consider “cost-side spillover” effects which lead to technological cost reductions. In our basic model, spillovers lead to an incremental demand (arising from the industry benefit function) such that if a firm underinvests in technology, it faces a trade-off between a loss in demand and reduced costs. To model the technology spillover effect we introduce the variable λ . Keeping in mind that a higher knowledge of information security vulnerabilities leads to better investments in security enhancing technologies, we formulate the following production function for these two benefits.⁹

$$B_F^i = \alpha_F \left(\frac{1 + s_j}{2} \right) t_i, \quad i \in (1, 2)$$

$$B_I^i = \alpha_I \left(\frac{s_i + s_j}{2} \right) (t_i + \lambda t_j)$$

⁹The qualitative nature of most of our results hold irrespective of whether B_I^i is an additive or multiplicative function. Proof of this is available with the authors upon request.

Since the amount of information about its own security available to each firm is always complete, $s_i = 1$ in B_F^i . Notice that factor 2 in the denominator in the benefit functions ensures that the cumulative levels of information shared between the two firms never exceeds 1. Further, even if one firm decides to share zero information, it will still enjoy an increased demand due to the positive externality benefit created by the competing firm's decision to share information. The coefficients α_F and α_I denote the degree of change in the firm and industry specific benefits, with a change in the firm decision variables (s_i, t_i) .

The demand of each firm depends on its own price and the price of its competitor. Though it is uncertain, each firm obtains information about the level of security investment and information being shared from the central association and uses this in its pricing decision. In this context, we examine how the effect of information on profits is affected by firm and market characteristics. The demand functions for Firms 1 and 2 are assumed to be linear in self and cross-price effects (McGuire and Staelin 1983) and are written as follows.

$$q_1 = \gamma a - b_1 p_1 + b_2 p_2 + K_1(B_F^1 + B_I^1) - K_2 g(s_1) \quad (1)$$

$$q_2 = (1 - \gamma)a - b_1 p_2 + b_2 p_1 + K_1(B_F^2 + B_I^2) - K_2 g(s_2) \quad (2)$$

where b_1 and b_2 are the own and cross - price effects. Each of these effects are symmetric. We assume that $b_1 > b_2$ so that own price effects are greater than cross-price effects. Here the elasticity of demand b_1 can be interpreted as degree of consumer's loyalty to firms' products or "brand loyalty". a denotes the size of the industry. This particular demand model has been used extensively in marketing and economics and there is some research suggesting that comparative statics derived from simpler models may often hold more generally (Milgrom 1994). We assume that a in Equations (1) and (2) represents the base level of industry demand. The share of this demand going to Firm 1 is γa , and $(1 - \gamma)a$ goes to Firm 2. We assume for now, that the costs of investing in technologies which promote cyber-security are independent of the volume of sales but increasing in the amount of technology invested. We denote that these costs are convex given by $cf(t_i)$ such that $f' > 0$ and $f'' > 0$ and c is the technology cost parameter.

The first step in the analysis is to derive equilibrium pricing strategies and the resulting profits of each firm. These become the starting point for deriving comparative statics to examine how changes in the exogenous and endogenous variables affect profits under different market conditions.

¹⁰

Lemma 1 (i) *A firm's price increases with increase in both, its own and its competitor's investment in security enhancing technology, i.e., $\frac{dp_i}{dt_i} > 0$, $\frac{dp_i}{dt_j} > 0$*

(ii) *There exists a critical value of information shared s_i^c such that firm prices follow an inverted-U shaped curve with increase in information sharing, i.e. $\frac{dp_i}{ds_i} > 0$ for $s_i \in (0, s_i^c)$ and $\frac{dp_i}{ds_i} < 0$ for $s_i \in (s_i^c, 1)$*

Since we do not get closed form solutions for all decision variables, we adopt the implicit function approach to gain insights. From the first order conditions for the decision variables, (p_i, s_i, t_i) , we

¹⁰Proofs of Results are available with the authors upon request.

get multiple sets of simultaneous implicit functions for the exogenous and endogenous variables. This leads us to the Jacobian Matrix for each firm. Using Cramer's Rule, we can assign signs to the derivatives which enables us to derive the following results.

Lemma 2 *The reaction functions are upward sloping, i.e., $\frac{\partial s_i}{\partial s_j} > 0$, $\frac{\partial t_i}{\partial t_j} > 0$, $\frac{\partial s_i}{\partial t_j} > 0$ and $\frac{\partial t_i}{\partial s_j} > 0$*

A direct interpretation of these results is provided below.

3 Results

Result 1a: *(i) A higher level of security breach information sharing by one firm leads to a higher level of security breach information sharing by the other firm.*

(ii) A higher level of information sharing by one firm leads to a higher level of security technology investment by the other firm.

Result 1b: *Technology investment and information sharing act as strategic complements in equilibrium.*

Our analysis reveals that the reaction functions are upward sloping, that is, an increase in the investment in security enhancing technologies by firm i induces a higher level of information sharing by firm j . The two inputs act as strategic complements. This is evident from the fact that $\frac{\partial^2 \Pi_1}{\partial s_1 \partial t_2} > 0$, i.e., increase in profits with increase in technology investment is higher for higher levels of information sharing. Hence as we see from Lemma 1 & Lemma 2, firm i responds to less aggressive play by firm j by being less aggressive itself.

We would like to point out that there are two effects here : a direct effect and a strategic effect. The direct effect of increased information sharing $\frac{\partial \Pi_i}{\partial s_i}$ results in increased demand (market expansion) for both firms. From Lemma 1, we can isolate the strategic effect $(\frac{\partial \Pi_i}{\partial p_j} \frac{\partial p_j}{\partial s_i})$ which promotes higher prices with higher levels of information sharing. Thus, the strategic effect alleviates price competition, allowing firms to increase prices and make higher profits.

Result 2 : *(i) As the degree of product substitutability increases, the extent of information sharing and amount of security technology investment by both firms, increases.*

(ii) A lower level of "demand - side" spillover discourages a higher level of information sharing.

(iii) A higher level of firm loyalty leads to lower levels of information sharing and security technology investment.

Quite interestingly, to the extent that product substitutability is indicative of the degree of competition in an industry, we find that a higher level of competitiveness in the industry actually leads to higher levels of information sharing about security breaches and increased investment in security enhancing technologies by both firms. Firms generally respond to increased competition with aggressive price cuts. Since increases in s and t help in alleviating the price competition, in equilibrium both firms raise (s_i, s_j) and (t_i, t_j) to offset any possibility of Bertrand competition.

We also find that a higher spillover effect between the two firms is not detrimental to the firms since it promotes a higher level of information sharing. Increased spillover shifts the demand curve out which enables the other firm to increase its price. This facilitates less aggressive pricing by the technology investing firm.

We also find that higher the demand elasticity of the firm, lower is its propensity to invest in technology and share security breach information. If consumers are increasingly loyal to the firm, then firms would be able to charge higher prices without having to worry about an aggressive price cut by the other firm since such an action would have minimal effect on respective market shares. Hence this reduces its need to increase s or t to mitigate price competition.

Result 3 : *Security breach information sharing and security technology investment levels increases with firm size and with industry size.*

This suggests that sharing information is more valuable to larger firms and in bigger industries. Note, however, that whether or not a firm is large is measured not in absolute terms, but how large it is relative to the other firms in its industry. Our analysis suggests that larger firms may in fact assign a higher value to such information because the marginal benefit-cost ratio of sharing information, is higher for them than for smaller firms. This is similar to the intuition that a monopolist benefits more from cost-reducing innovations in R&D than a firm competing in a duopoly, because it can extract a higher proportion of the surplus from the market.

3.1 Impact of Marginal Costs

Organizations of all types and sizes are considering outsourcing the management of their security infrastructure. Some firms believe that information security like physical security is more efficiently applied as an outsourced function rather than an in-sourced one. One can expect that if the firm is managing its own infrastructure, then it would mostly incur fixed costs as we had modelled earlier. However many firms these days outsource their security and network management to an external entity. If there is managed security firm that is doing it as an outsourced contract, for different levels of service or for a larger number of machines etc., it would be more appropriate to model the firm's as incurring some additional costs which are also affected by the volume of sales. As the demand grows and firms' IT infrastructure grows, so would costs like those incurred for additional servers, software license fees, service agreements and importantly for associated security weapons like firewalls, intrusion detection systems, access control systems etc. In this section we analyze the impact of marginal costs of technology on firms' optimal profits and strategies, when such costs are increasing in the level of demand.

Having analyzed the impact of spillovers on the demand side, we now consider spillover effects on the cost side. One can envisage a situation in which a spillover in cost reduction occurs as a result of the knowledge accruing from the competitor's information sharing. This can happen when disclosure of vulnerabilities in a particular security technology by one firm leads the other firm to invest less in that technology. A direct consequence of such information sharing would be preemptive cost savings. Suppose the impact of sharing information by one firm is that spillover

effects lead to a reduction in marginal costs for the other firm. Hence the possibility of free riding or under investment becomes plausible in this situation. We model the new marginal cost function as $(c - \lambda s_j)\delta(t_i)$ where $\delta(t_i)$ is the marginal cost incurred for each unit of sales and λ is the “cost-side” spillover.

Result 4 : *When costs of security technology investment are affected by the volume of sales and there are “cost-side” spillovers, the propensity to share information or invest in technology of firm i decreases with increasing spillovers in technology invested or information shared by firm j .*

3.2 Sequential Entry

Analytical modelers have recognized that the qualitative insights regarding optimal strategies often depend on the assumed form of conduct in an industry. While Bertrand-Nash conduct is more common in fragmented industries, there are a number of reported incidences where one firm acts as the leader and the other firm follows it.

Firms maybe understandably reluctant to share sensitive proprietary information about prevention practices, intrusions, and actual crimes with either government agencies or competitors. To many firms information sharing is a risky proposition with less than clear benefits. For example, given the fierce competition amongst electronic retailers, a Internet retailer will not want information to surface that may jeopardize its market position, strategies, customer base, or capital investments. Due to the uncertainty involved with the outcome of information sharing alliances like ISACs, this may be specially true where some firms are more likely to be pioneering in their approach to disclosing critical information while others adopt a “wait and watch policy”.¹¹ This prompted our interest in comparing the amount of information and technology investment when firms behave in a sequential manner, with the value of information when the firms behave in a Bertrand- Nash manner.

We next consider a scenario in which there exists an incumbent firm which has already committed to sharing information and investing in technology, anticipating the entry and similar sharing behavior of the other firm. In stage 1, the incumbent chooses (s_1, t_1) . In stage 2 the entrant choose (s_2, t_2) . In stage 3, both firms choose prices (p_1, p_2) simultaneously.

Result 5 : *The optimal amount of security breach information shared and investment in security technology by firm 1(incumbent) will be higher in the sequential mode than in the Bertrand-Nash mode.*

The intuition for this is that such a precommitment by the incumbent will induce the entrant also to share even a higher level of information and invest more in security technology. Since increased sharing leads to softening of price competition and shared information acts complementary to technology invested, both firms’ profits will be strictly higher than in the simultaneous mode game.

¹¹The 2002 CSI/FBI survey study of computer crime and security revealed that over 85% of the companies polled had detected computer security breaches within the last 12 months, yet only 36% had reported the intrusions to law enforcement.

The sequential mode of conduct is considered less competitive than the Bertrand-Nash mode, and Result 5 suggests that sharing is higher in this than in the BN mode, leading to higher profits.

4 Conclusion

The U.S. federal government has encouraged the formation of Information Sharing & Analysis Centers (ISACs), with the goal of helping to protect critical infrastructure assets that are largely owned and operated by the private sector, in industries such as banking & finance, chemicals, telecommunications, oil & gas, electricity, etc. It is plausible that in the near future such centrally coordinated, security breach information sharing organizations will also be established in other industries, including the online e-commerce industry. Our results point out that there are indeed some very strong economic incentives for firms to indulge in such security breach information sharing. These incentives, become stronger with increases in the firm size, industry size and degree of competition. Importantly we point out that the nature of the cost function plays a pivotal role in determining whether spillovers are beneficial or detrimental to the firms' interests. Another implication of our model is that the sequence in which firms join such ISACs also influences the optimal sharing and technology investment levels.

It is important to note that while firms might gain unambiguously by sharing higher levels of information and investing more in information-security related technologies, the resultant increase in prices might have an adverse effect on consumer surplus. Despite the expansion in overall demand, social welfare may not always increase under such circumstances. This can have important implications for anti-trust issues and form a potential legal hurdle to information sharing. ISACs are not intended to restrain trade by restricting output, increasing prices, or otherwise inhibiting competition, on which the antitrust laws generally focus. We are exploring some of these issues in our ongoing research. In addition, empirical studies could address the role of government intervention at some stage in the form of optimal incentives or subsidies to prevent firms from increasing prices.

References

- [1] Anderson, R. (2001), "Why information security is hard : An economic perspective," Proceedings of 17th Annual Computer Security Applications Conference, Dec. 10-14.
- [2] Bulow, J., J. Geanakoplos and P. Klemperer (1985), "Multimarket Oligopoly : Strategic Substitutes and Complements," *The Journal of Political Economy*, Vol 93, Issue 3, pp 488-511.
- [3] Campbell, K., L. Gordon, M. Loeb and L. Zhou (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", forthcoming *Journal of Computer Security*.
- [4] Cavusoglu, H., B. K. Mishra and S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers," WISE 2002.

- [5] d'Aspremont, C. and A. Jacquemin (1988), "Cooperative and Non-cooperative R&D in a Duopoly with Spillovers", *American Economic Review*, 78 : 1133-1137.
- [6] Fried, D. (1984), "Incentives for Information Production and Disclosure in a Duopolistic Environment," *The Quarterly Journal of Economics*, Vol. 99, pp. 367-381.
- [7] Gal-Or, E. (1985), "Information Sharing in Oligopoly," *Econometrica*, Vol. 3, pp. 329-343.
- [8] Gal-Or, E. (1986), "First mover and second mover advantages," *International Economic Review*, 26 (3) 649-653.
- [9] Gordon, L.A. and M. P. Loeb (2002), "The Economics of Investment in Information Security," *ACM Transactions on Information and System Security*, Vol. 5, No.4 November, pp. 438-457.
- [10] Gordon, L. A., M. P. Loeb, and W. Lucyshyn (2002), "An Economics Perspective on the Sharing of Information Related to Security Breaches: Concepts and Empirical Evidence," *Proceedings of the First WEIS*, UC Berkeley, May 16-17.
- [11] McGuire, Timothy M., Richard P. Staelin (1983), "An industry equilibrium analysis of downstream vertical integration," *Marketing Science*, Vol. 2, pp 161-192.
- [12] Milgrom, P. (1994), "Comparing optima: Do simplifying assumptions affect conclusions?," *Journal of Political Economy*, 102(June), pp 607-615.
- [13] Miller, H. (2002), "Securing Our Infrastructure : Private/Public Information Sharing," *Testimony Presented to United States Senate Committee on Governmental Affairs*, May 8th, 2002.
- [14] (NIPC) National Infrastructure Protection Center (2001), "Information Sharing & Analysis Centers," *May 15th*.
- [15] Parasuraman, A. (2000) "Technology Readiness Index (TRI), A Multiple-Item Scale to Measure Readiness to Embrace New Technologies," *Journal of Services Research*, 2(4), pp 307-320.
- [16] Schechter, Stuart E., and Michael D. Smith (2003) , "How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems Networks," *Proceedings of the Financial Cryptography Conference*, Guadeloupe, January 27-30.
- [17] Schenk, M. and M. Schenk (2002), "Defining the Value of Strategic Security," *Secure Business Quarterly*, Vol. 1(1), pp 1-6.
- [18] Shapiro, C. (1986), "Exchange of Cost Information in Oligopoly," *Review of Economic Studies*, Vol. 53 (1986), pp. 433-446.
- [19] Szymanski, D. and T. Hise (2000), "e-Satisfaction: An Initial Examination," *Journal of Retailing*, 76(3), pp 309-322.
- [20] Varian, H. (2002), "System Reliability and Free Riding," *Proceedings of the First WEIS*, UC Berkeley, May 16-17.