The Economic Consequences of Sharing Security Information

Esther Gal-Or[1] Anindya Ghose[2]

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-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. Finally we show that "demand-side spillover" effects boosts sharing levels and lead to higher prices. Conversely, "cost-based spillovers" might lead to lower sharing and lower technology investments.

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

[1] The author is Glenn Stinson Chair Professor of Business Administration and Economics, Katz School, University of Pittsburgh. She can be reached at esther@katz.pitt.edu.

[2] The author is a Doctoral Candidate, Information Systems, GSIA, Carnegie Mellon University. He can be reached at aghose@andrew.cmu.edu.

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] 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 in the physical world 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 (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

[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.

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. Basically, 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.

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). 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 upon detection of security breaches can take 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".

One can envision 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

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. 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. 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 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, 1985, 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, 2003 raise the issue of the need to study the economic benefits of security information sharing. They show that sharing can benefit firms by reducing the costs incurred in security expenditures. Schecter and Smith, 2003 provide an analysis of the benefits of information sharing to prevent security breaches.

2 Economic Modelling

To answer these questions, 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 and information sharing levels. In the second stage they choose prices 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. Costs of production are assumed to be symmetric for both firms and are normalized to zero, without loss of generality. We explicitly model "leakage costs" of sharing security information and assume that these costs are increasing and convex in the amount of security information shared. These leakage costs affect demand adversely. The potential costs of security information leakage can have a snowball effect, accruing from the resultant loss of market share and stock market value from negative publicity (Campbell, et al. 2003).

In 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 envision the possibility of "demand side spillover" effects. We account for such spillovers, and subsequently also consider "cost-side spillover" effects which lead to technological cost reductions.

The demand of each firm depends on its own price and the price of its competitor. 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 depends upon firm and market characteristics. The demand functions for the two firms are assumed to be linear in self and cross-price effects (McGuire and Staelin, 1983).

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 initially assume 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, and that these costs are increasing and convex. Subsequently, we also consider variable costs of security technologies which increase with the volume of sales.

3 Results

Result 1: *(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.
(iii) 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 one firm induces a higher level of information sharing by the other firm. The two inputs act as strategic complements. This is evident from the fact that increase in profits with increase in technology investment is higher for higher levels of information sharing. Hence one firm responds to less aggressive play by the competing firm, 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 results in increased demand (market expansion) for both firms. We can also isolate the strategic effect 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 lower level of firm loyalty leads to lower levels of security 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 security information sharing and security technology investments help in alleviating price competition, in equilibrium both firms raise their investment and sharing levels as competition intensifies.

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 highlight that a steeper demand schedule, lowers a firm's propensity to invest in security technology and share security information. A steeper slope implies that each firm sells fewer units of the product for a given level of the equilibrium prices, i.e. consumers are more price sensitive. Smaller quantities imply, in turn, that the marginal return to any kind of technology investment is more limited. As a result, the firms have reduced incentives to invest in enhanced security technology. Further, the strategic complementarity between technology investment and information sharing implies also that the extent of sharing declines when demand schedules are steeper.

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.

How critical is the nature of the cost function? Of late, organizations of all types and sizes are considering outsourcing the management of their security infrastructure. 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., once could imagine a scenario where the firm also incurs some additional costs which are 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 an extension of the basic model, we analyze the impact of volume dependent costs of technology on firms' optimal profits and strategies.

Having analyzed the impact of spillovers on the demand side, we now also consider spillover effects on the cost side.[5] Consider 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.

Result 4: *When the costs of security technology investment are affected by the volume of sales, and there are "cost side spillovers" , an increase in the spillover parameter has ambiguous implications on the propensity to share security information or invest in security technology for both firms.*

Basically, changes in the spillover parameter introduce two countervailing effects. An increase in the parameter serves the purpose of making a firm's competitor more efficient by reducing its cost coefficient. This enables the competitor to price more aggressively. If a given firm increases its level of information shared, it further increases the cost efficiency of the competitor, which acts to the disadvantage of the firm. Since the improved cost efficiency precipitates further price competition, both firms respond strategically by reducing their levels of information sharing. On the other hand, an increase in the parameter also increases the profit margin of each firm, thus providing greater incentives for increased investment in technology and information sharing.

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. This has been witnessed in industries such as banking & finance, IT, chemicals, oil & gas, electricity, etc. The underlying assumption is that such centrally coordinated information sharing organizations would facilitate the alignment of goals for both the private sector and the federal government, which in turn would improve the security of cyber-infrastructure assets. However, all sectors do not have a fully established ISAC, and in those sectors that do, there is mixed participation. Specifically, five recently reviewed ISACs showed different levels of progress in implementing the PDD 63 suggested activities. These were the IT, Telecommunications, Energy, Water and Electricity ISACs. Hence, the government felt it important

[5] Introducing cost-side spillovers when the cost of the technology is independent of the volume of sales does not affect our main results.

to identify economic incentives to encourage the desired information sharing behavior in IT security (Dacey, 2003a).

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. 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. 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, Ross. (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] d'Aspremont, C. and A. Jacquemin. (1988). *Cooperative and Non-cooperative R&D in a Duopoly with Spillovers*, American Economic Review, 78: 1133-1137.

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

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

[7] Gal-Or, E. (1986). *First mover and second mover advantages*, International Economic Review, 26 (3) pp. 649653.

[8] Gordon, L.A. and M. P. Loeb. (2002). *The Economics of Investment in Information Security*, ACM Transactions on Information and System Security, Vol. 5, (4) November, pp. 438-457.

[9] Gordon, L. A., M. P. Loeb, and W. Lucyshyn. (2003). *Sharing Information on Computer Systems Security: An Economic Analysis*, Journal of Accounting and Public Policy, Vol 22, (6).

[10] McGuire, Timothy M., Richard P. Staelin. (1983). *An industry equilibrium analysis of downstream vertical integration*, Marketing Science, Vol. 2, pp. 161192.

[11] Milgrom, P. (1994). *Comparing optima: Do simplifying assumptions affect conclusions?*, Journal of Political Economy, 102(June), pp. 607 615.

[12] (NIPC) National Infrastructure Protection Center (2001). *Information Sharing & Analysis Centers*, May 15th.

[13] Schecter, 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.

[14] Schenk, M. and M. Schenk. (2002). *Defining the Value of Strategic Security*, Secure Busines Quarterly, Vol. 1(1), pp 1-6.

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

[16] Varian, H. (2002). *System Reliability and Free Riding*, Proceedings of the First WEIS, UC Berkeley, May 16-17.