2009

The Economic Ramifications of Strategic IT Security Information Sharing in the Financial Services Industry

Humayun Zafar
The University of Texas at San Antonio, hzafar@kennesaw.edu

Yoris A. Au
The University of Texas at San Antonio, yoris.au@utsa.edu

The Economic Ramifications of Strategic IT Security Information Sharing in the Financial Services Industry

Humayun Zafar
Department of Information Systems and
Technology Management
The University of Texas at San Antonio
San Antonio, TX 78249
humayun.zafar@utsa.edu

Yoris A. Au
Department of Information Systems and
Technology Management
The University of Texas at San Antonio
San Antonio, TX 78249
yoris.au@utsa.edu

ABSTRACT

We investigate the economic ramifications of strategic IT security information sharing among firms in the financial services industry. An IT security information sharing system can potentially minimize security breaches. However, although the Presidential Decision Directive/NSC-63 encouraged the establishment of such a system in the form of industry based information sharing and analysis centers (ISACs), it is injudicious to assume that firms will be willing to naively share their security information with their strategic competitors. We argue that without a proper mechanism some firms will try to put in minimum effort, potentially reducing the system's reliability, and aim to answer the following research question: "What will it take for a financial services firm to willingly share its strategic information technology security information with its competitors through an ISAC?" We use the theory of mechanism design in economics to develop an adverse selection model to address the question.

Keywords

Information security breach; financial services; competitive firms; information sharing; principal-agent; adverse selection.

INTRODUCTION

In January 2009, the Heartland Payment Systems, the sixth largest payment processor in the United States, announced that its processing systems had been breached. The effects of this IT security breach reverberated through the company's dozens of partners which included Forcht Bank of Kentucky, Farmers & Merchants Bank of Arkansas, and Adams Bank and Trust of New England (McGlasson, 2009a). The forensics team found that the hackers were able to grab numbers using sniffer malware at the time payments were being processed. However, it was not clear how long the malware had been present or how much the damage had cost (McGlasson, 2009b).

Earlier, in 2008, the Bank of New York Mellon reported that sensitive data of over four million customers who owned shares in public companies were compromised after the data were sent to a remote storage facility. The data included names, addresses, and social security numbers. The estimated cost of this breach was $197 per customer record. In another incident in 2008, an employee of Countrywide Financial Corporation was arrested by the Federal Bureau of Investigation for stealing and selling private information of over two million mortgage loan applicants. It was estimated that the employee profited from $50,000 to $70,000 from the sale (Mills, 2008).

The financial services industry has entered 2009 facing the prospect of an increase in regulations while at the same time having to combat persistent cyber threats. The Heartland breach incident shows that there is a need for increasing fraud detection efforts. Yet even with state-of-the-art mechanisms, the malware still remained undetected. Bank of New York Mellon which released data to a third-party realized how important it was to implement high level of data encryption on data both onsite and offsite. Countrywide Financial Corporation learned that insider threats were just as serious as any other IT security breaches.

None of the above IT security breach incidents represents a novel way of attack. Each of them has been well documented, and best practices for countering such threats have also been presented at length (Panko, 2004). At first glance, these cases appear to be independent. However, all three agencies actually belong to the Financial Services Information Sharing and Analysis Center (FS-ISAC). The center was established by the financial services sector under Presidential Decision Directive/NSC-63. The directive, which was later updated by the 2003's Homeland Security Presidential Directive 7, mandates that public and private sectors share information about the physical and security threats and vulnerabilities faced by financial services organizations. Its membership is limited to United States based entities such as FDIC insured financial institutions, specialized federal or state licensed banking companies, and other eligible entities as determined by the Board of Directors of FS-ISAC. Each member needs to provide evidence of their good standing with all appropriate regulatory bodies recognized by FS-ISAC (Financial Services ISAC, 2005). As of 2007, FS-ISAC has over 2000 members.

Even though FS-ISAC's mission is to encourage cooperation between financial institutions to prevent or limit instances of cyber attacks, the members of FS-ISAC continue to commit rudimentary mistakes. With thousands of active members, it would be reasonable to expect that FS-ISAC provides a sufficient information sharing facility that would help the Bank of New York Mellon, for example, to not make such a basic mistake as allowing its off-site storage facility to become a weak spot. The bank should be able to learn from a similar mistake other banks had made in the past, if such information were made available. However, without appropriate incentives and/or penalties, member firms may find no particular motivation to share their IT security incident information, hence impacting FS-ISAC's efficacy. This is especially true for the financial services industry, which consists of some of the most competitive firms. Consequently, we argue that without a proper mechanism to encourage information sharing, some firms will try to put in the minimum effort, potentially reducing the overall reliability of the endeavor. In this research, we aim to answer the following question: "What will it take for a financial services firm to willingly share its strategic IT security information with its competitors through FS-ISAC?" We use the theory of mechanism design to develop an adverse selection model to address the question. Adverse selection can also be described as a "principal-agent" problem. In our study, the principal is FS-ISAC and the agents are the financial services firms (e.g., banks). In the following sections we provide a literature review of current research in the area of economics of information systems security, a description of the adverse selection paradigm, a discussion of our proposed model, and conclusion.

LITERATURE REVIEW

The importance of research in IT security from the economic perspective has grown due to the increasing frequency and cost of security breaches. Cavusoglu et al. (2004) provided important elements of economics of security management: estimation of breach costs, strategic nature of security, configuration of security controls, and complementary and substitute nature of security controls. Most of the research in economics of IT security has occurred at the organizational level. Gordon and Loeb (2002) developed an economic model for information security investment decisions. They considered how vulnerability of information and its associated losses affected the optimal level of resources that should be devoted to securing information. Gal-Or and Ghose (2005) highlighted the existence of Information Sharing and Analysis Centers (ISACs) under Presidential Decision Directive (PDD) 63. They developed a model which investigated the benefits to firms from joining such security information sharing alliances. Not surprisingly, they concluded that in the presence of large positive implications on the demand facing the firms, there were strong economic incentives for firms to participate in sharing security information. However, pitfalls associated with sharing security information among organizations have also been recognized. Gordon et al. (2003) showed that information sharing might lead to situations where some firms would have an incentive to free ride on the information security expenditures of the other firms. In addition, without appropriate incentives firms may not fully share their security information, or for that matter neglect to share the information altogether.

Regardless of the current technical protection mechanism, security related incidents remain at an all-time high. These failures can be attributed not only to a lack of understanding of the fundamentals of IT security information sharing between firms (many of them are competitors in the financial services industry case), but also to perverse incentive strategies. Varian (2000) states that in a typical organization, security analysts should not only investigate weak points in a system, but also go one step further and examine the incentives of those responsible for the system.

The use of incentives in security research is not new. Cavusoglu et al. (2006) compared liability and cost-sharing as mechanisms for incentivizing vendors to work harder at patching their software. They found that depending on the incentive levels of the system, vendors should share either the burden (cost sharing) or the damage (liability), but not both, to reach the social optimality with minimum level of additional cost on the vendor side. Varian (2004) states that the reliability of a system depends on the contribution of the important stakeholders, which are potentially subject to incentive problems. The computation of reliability is based on total effort, weakest link, and the best shot. In total effort, reliability is dependent on the sum of the efforts exerted by each stakeholder; in weakest link, it depends on the least effort exerted by an agent; and in best shot, it depends on the greatest effort exerted by an agent. Our work relates to Varian's model due to the fact that the success of a strategic IT security information sharing depends on the efforts put forth by the willing agents.

ADVERSE SELECTION

Adverse selection is a principal-agent problem which involves two parties: a principal and an agent. The principal is responsible for offering a contract, whereas the agent decides whether to accept or reject the contract and can act on behalf of the principal as long as it follows the rules of the contract. The agent also has private information, not known to the principal, about some parameters of its utility function. These parameters may determine the agent's "type" which, as noted by Maskin and Tirole (1990), affects the principal's payoff because the type establishes the class of contracts that the principal will accept. Prior literature (e.g., Laffont and Maskin, 1982; Guesnerie and Laffont, 1984) has developed conceptual models that have been applied to economic problems such as insurance contracts, auctions, public goods, and regulation of monopoly.

The general idea of adverse selection can be illustrated through the following example. Suppose that the principal is an auto insurance company, and the agents are drivers who are required to purchase an auto insurance policy. There are different types of drivers, each of which represents a different level of risk. If the insurance company has no knowledge about the risk level of each driver, it will offer the same premium to all types of drivers. In this situation, one can argue that only the riskier drivers will end up purchasing an auto insurance policy (assuming there is no regulation that requires every driver to have an auto insurance policy). This presents an adverse selection problem and could cause losses to the insurance company. To alleviate the problem, the auto insurance company needs to assess the risk of each driver based on their age, gender, driving record, the neighborhood they live in, etc., and offer different premium levels attractive to different driver types.

Adverse Selection Applied to IT Security Information Sharing

We can apply the principle of adverse selection to the area of IT security information sharing in the financial services industry. The principal in our model is FS-ISAC. This is because FS-ISAC has the authority to not only accept or reject a prospective agent's (i.e., a financial firm's) membership to the organization but also serve as the primary communications channel for the financial services sector. FS-ISAC is designed, developed, and owned by the financial services industry; it includes private firms as well as US Government entities such as the US Department of Treasury. The FS-ISAC Board is responsible for administering multiple levels of membership offered by the organization. According to its website (www.fsisac.com), FS-ISAC offers different categories of membership ranging from $750 to $50,000 annually. A firm is assigned to a membership level based on its total assets.

The agents in our model are two financial firms, BankA and BankB, which are assumed to be equivalent in terms of their asset values and overall representation in the financial services arena. We also assume that BankA and BankB have similar risks with regard to their IT security. Furthermore, consistent with some of the requirements of FS-ISAC, they have the following qualities:

- Both banks are regulated;
- Both banks belong to the Platinum level membership tier;
- Both banks allow for anonymous incident submission;
- Both banks have signed a non-disclosure agreement;
- Both banks have agreed in principle to assist other members.

A principal-agent relationship is signified by a contract to carry out specific tasks. More importantly, an agent must not perform tasks that have not been either explicitly or implicitly authorized by the principal. Also, an agent should refrain from putting itself in a position that would encourage a conflict between the agent's own interests and the principal's. This holds true in the case of FS-ISAC and the two financial firms (i.e., BankA and BankB) in our model. As per the requirements of the contract, resolutions to specific incidents are posted to FS-ISAC's database, which is accessible to all members. The agents are also required to provide any practical knowledge discovered during their attempts to address specific vulnerabilities that may have a broader application to the financial sector (e.g., problems associated with Trojan horse programs). Therefore, in the event of an IT security breach the agents have three choices: (1) share all breach information completely, (2) partially share breach information, or (3) do not share any information. The last two options will result in the adverse selection problem because the agent is withholding information from the principal. This phenomenon is highlighted by the following scenario.

Suppose BankA suffered from a denial-of-service (DoS) attack, the effects of which lasted for three days. During that time period, BankA was prevented from offering some of its online services, one of which was access to its online banking system. BankA's online banking system offers services such as the ability to transfer funds to other financial institutions, as well as the ability to access brokerage account services for items such as Roth IRAs. For example, users could contribute to their Roth IRA account from the website. BankA's IT security division found that the source of the DoS attack was a botnet, which is a series of distributed compromised computers that have been infected with viruses set up to forward transmissions to other computers on the Internet. Once it is launched, a botnet attack is difficult to trace and counter. BankA also found that the botnet affected the brokerage account information in a peculiar manner: it confused the bank servers into thinking that the user was requesting brokerage account information for the year before, even though the date displayed on the web page was current. This means that if a user wanted to contribute to a Roth IRA account, she could potentially execute a valid transaction based on a mutual fund's value that was not current.

BankA decided to release preliminary findings about the attack to FS-ISAC but hold information about the impacts on Roth IRA accounts with the intention of releasing it at a later date once the entire problem had been resolved. In the meantime, FS-ISAC released BankA's preliminary findings to its members. Four days later, BankB suffered from a similar DoS attack by the same perpetrators that had attacked BankA. Based on what FS-ISAC had released, BankB was able to quickly detect the attack. However, not knowing about the attack's potential effects on Roth IRA accounts, BankB was under the impression that it had access to all the information regarding this form of attack based on what FS-ISAC had provided them. Unfortunately, many Roth IRA transactions were executed, causing heavy losses and a tarnished reputation to BankB.

The above hypothetical scenario shows how one agent may decide to withhold information from the principal, directly or indirectly impacting another agent. BankA fulfilled FS-ISAC's requirement by submitting information about the detection of the DoS attack but failed to report the impacts on its Roth IRA accounts. By not revealing the complete information, BankA has exerted only a minimal effort. BankB suffered from BankA's decision as a result and FS-ISAC failed to properly support BankB.

The scenario shows that BankA presents a greater risk as a member to FS-ISAC. We propose that this problem can be represented by a model which is normally seen in the insurance industry, as discussed by Salanié (2005). Similar to an insurer, FS-ISAC serves several risk categories. Furthermore, we believe that since FS-ISAC has support from the US Government and the private sector along with a large member base, it does have the necessary resources available to set up a model similar to that of an insurance agency. To prevent the problem of adverse selection, FS-ISAC can offer multiple insurance policies which are based on factors such as a financial institutions risk class, and its prior history of assisting organizations in a collaborative environment.

The Model

Let W_A denote an agent's (BankA's) initial wealth (in terms of total asset). An information security breach incident will reduce the agent's wealth by d_A dollars. Furthermore, let p_A denote the premium of the "insurance" offered by the principal (i.e., FS-ISAC). This premium includes the standard ISAC membership fee. If an information security breach event occurs, a reimbursement R_A will be given to the agent depending on the severity of the incident and the decision taken by the Principal regarding any complicity on the part of the agent. Therefore, the final wealth of the agent in the case of an information security breach incident is:

$$W_{FA} = W_A - d_A - p_A + R_A \qquad (1)$$

We propose that in order to truly encourage a more fluent exchange of security breach information, an immediate standard reimbursement is distributed to the agent based on a set of criteria. For example, if the agent suffers from a denial of service attack, then based on the agent's market value a certain percentage of the costs incurred be reimbursed to the agent. The principal (FS-ISAC) will need to look into the agent's affected system to estimate the amount of reimbursement. If later on it is determined that the agent was at fault, as is the case in the scenario where BankA purposefully withheld information, then the agent as the culprit will have to repay the funds in addition to a penalty in the form of an increased premium (p_A). This is similar to how the auto insurance companies raise premiums based on who is at fault.

In the event that the agent does not suffer from any information security breach incident the final wealth will be:

$$W_{NA} = W_A - p_A \qquad (2)$$

The premium in this case will be dependent on the agent's prior actions as a member of FS-ISAC. If the agent has a negative track record, then based on future performance the premium may change.

Based on the final wealth in the presence or absence of an IT security breach incident, the expected utility of the agent is:

$$U_A = r_A u_A W_{FA} + (1 - r_A) u_A (W_{NA}) \qquad (3)$$

Equation (3) holds if the agent belongs to a risk class whose probability of suffering from an information security breach incident is r_A, and u_A is an increasing concave function. For an increasing concave function, if $x_1 < x_2$ then it implies that $f(x_1)$

$< f(x_2)$. The value r_A is impacted by any previous occurrences of IT security breach incidents. This value can be significantly lower if the agent has participated actively in the FS-ISAC program, and/or has had a history of participating in agencies similar to FS-ISAC.

A Spence-Mirrlees condition in this case will hold (Mirrlees, 1971). Spence-Mirrlees condition allows agents types to be separated, while also enabling the Principal to offer multiple contracts based on the agent risk type. This can assist FS-ISAC to cater for all types of financial institutions, either the detrimental or beneficial ones. The marginal rate of substitution between the premium and reimbursement is:

$$-\frac{\partial U / \partial p}{\partial U / \partial R} = \frac{r_A u_A' W_{FA} + (1-r_A) u_A' (W_{NA})}{r_A u_A' W_{FA}} \tag{4}$$

This equation is a decreasing function of r_A, which makes it possible for FS-ISAC to offer better insurance options in combination with higher premiums to the financial institutions. Also in this case, FS-ISAC's profit is dependent on the risk class of the agents as well as on the contract:

$$o = p_A - r_A R_A \tag{5}$$

For FS-ISAC, the optimum condition will be to completely insure all categories of agents so that their final wealth does not depend on the occurrence of an IT security breach incident. Economically, the Spence-Mirrlees property implies that the indifference curves always move in the same direction. Figure 1 provides a graphical illustration of the indifference curves on the plane (W_{NA}, W_{FA}). The 45-degree line represents complete insurance, and point "O" represents the no insurance situation. Each of the subscripts "L" (low) and "H" (high) indicates the risks associated with insuring a particular agent. Since the slope of the indifference curve of low risks is steeper than that of high risks, and is in the same direction, the Spence-Mirrlees condition is supported. The principal's profit (isoprofit) curves are straight lines and define a function in vertical-horizontal space in which Q is some output. Any combination of coordinate values on the isoprofit curves has the same profit and is represented by the following equation:

$$Q = -\frac{1 - r_{AP}}{r_{AP}} \tag{6}$$

As already stated, the slope of these isoprofit curves depends on the agent's risk class. This is shown by the previous equation in which r_{AP} is the risk that the principal faces when insuring an agent. Therefore the risk for the principal is higher in the case where an agent's probability of not contributing to FS-ISAC is high. That is, the agent has committed acts in the past that are against the main tenets of the information sharing contract. For the agent, the objective is to check if the indifference curves are convex and decreasing, and the slope of the indifference curve of class r_A is

$$-\frac{1 - r_A}{r_A} \frac{u_A' W_{NA}}{u_A' W_{FA}} \tag{7}$$

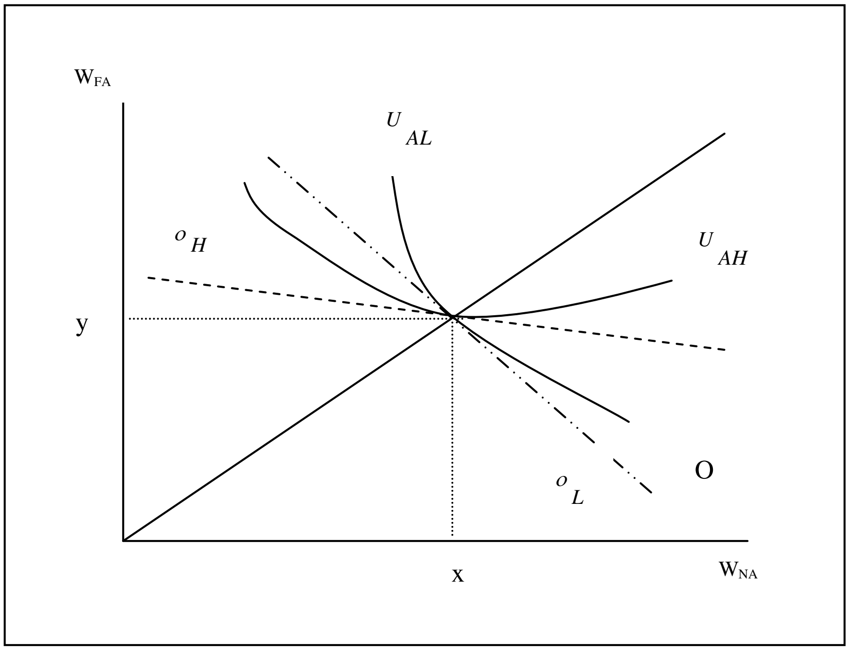

Figure 1: The Insurance Model

Figure 1 shows that utilities increase when going northeast, and profits increase when going southwest. This means that it is in the principal's interest to base its insurance policy on the optimum equilibrium point (*x*, *y*), where *y* and *x* are points on W_{FA} and W_{NA} respectively. At that point the principal can ensure that the agent that has a lower probability of a security breach event and the agent that has a higher probability of a breach event are each given the best possible premium while also maximizing the principal's profits. Also at that point, the isoprofit curve is tangent to the agent's utility function. Hence, the rate of change of a principal's profit is equal to the slope of the indifference curve of an agent. From equation (6) we can get the slope of the isoprofit curve,

$$\frac{\partial Q}{\partial r} = -\frac{1}{r_{AP}^2} \tag{8}$$

We also know that,

$$\frac{\partial Q}{\partial r} = -\frac{1}{r_{AP}^2} = -\frac{1-r_A}{r_A}\frac{u'_A x}{u'_A y} \tag{9}$$

Therefore solving for *y* and *x* from equation (9),

$$y = \frac{r_{AP}^2(1-r_A)x}{r_A} \qquad \because r_{AP}^2 > r_A \tag{10}$$

Equation (10) tells us that as FS-ISAC's risk of insuring a bank increases, it will become more beneficial for the bank to insure against IT security breach threats. At that point, the final wealth of the bank will increase at a rate which will be unfavorable for FS-ISAC. To reduce the possible losses that FS-ISAC may face in that case, FS-ISAC will have to not only reduce the probability of the bank from suffering a security breach incident, but also assist in preventing an erosion of the bank's wealth. This can be done if FS-ISAC encourages banks with a lower insurance risk to provide all appropriate IT security breach information in its most complete form. The bank that is not at risk has the incentive to protect the industry from potential damage due to negative reactions from consumers when security breach incidents occur. This is important because an IT security breach incident can have industry-wide financial implications, regardless of which bank was affected by the incident initially.

The specific value of *x* can be found by finding the minimum point of equation (7), where W_{NA} represents the value of *x*. Therefore,

$$x = \frac{-1}{r_A u_A^{'}} \tag{11}$$

Substituting value of *x* in equation (11) into equation (10) we get,

$$y = -\frac{r_{AP}^2 (1 - r_A)}{r_A^2 u_A^{'}} \tag{12}$$

Equation (12) provides a more holistic view of the link between FS-ISAC insuring a bank with a varying degree of insurance risk. It shows that the final wealth of a bank decreases as its risk of suffering from a security breach incident increases. From the perspective of FS-ISAC, insuring one high-risk member will necessitate the enrollment of multiple low-risk members. This will assist in sustaining FS-ISAC as an insurance provider, while also developing a wider base of financial institutions that will be more productive in foreseeing consequences of IT security breach incidents. This will also assist in countering the problem of adverse selection.

CONCLUSION

We have discussed how an adverse selection model can be used to address the question "What will it take for a financial services firm to willingly share its strategic IT security information with its competitors through FS-ISAC?" By allowing FS-ISAC to serve as an insurance provider, we can provide a dimension to IT security information sharing where financial service firms have the incentive to share their strategic IT security information. The idea of adding an insurance component to FS-ISAC can lead to questions about its feasibility. Although we have highlighted FS-ISAC's potential to become an insurance provider due to the presence of relevant stakeholders, future research (both quantitative and qualitative) is needed to support our proposal.

This study provides the practitioners with an approach towards consolidating losses incurred due to IT security breaches. It also provides a more practical approach that will encourage a better exchange of IT security information, regardless of differences in the risk classes of the financial firms. The introduction of insurance premiums that vary based on risk classes will discourage free riders and encourage more effort from each member. These practical implications are important, evidenced by the fact that some firms such as the American International Group, Inc. (AIG) have already offered a similar type of insurance (AIG, 2009), which fills the gaps left by the traditional lines of insurance are not all inclusive. Nevertheless, losses due to negative impact on reputation are more difficult to counter compared to those on the actual damage to an asset. Therefore, even in the presence of insurance options from companies like AIG, the best option is to prevent the loss in the first place. Consequently, we argue that a collaboration of various stakeholders under an umbrella agency will be more effective. We maintain that letting FS-ISAC provide an insurance service is the optimum option in this case because the organization is better positioned than companies like AIG to serve financial services firms due to its large membership base. It is also prudent to consider that even if security plans are implemented, there may still be incidents of IT security breaches that could prove to be costly due to inefficacy caused by non-conforming members. Our model addresses this issue by proposing penalties for members who disavow their contractual obligations by moving them to a higher risk class, hence impacting their respective premiums. This is similar to how the auto-insurance industry sets the premiums for drivers who are more prone to accidents. Finally, this study provides financial institutions with a reason to continue to join FS-ISAC, while also providing FS-ISAC with the necessary tools to effectively implement its objectives.

REFERENCES

1. AIG (2009) Network, Security and Privacy and ID Theft, http://www.aig.com/Network-Security-and-Privacy-Insurance-(AIG-netAdvantage)_20_2141.html. (Current: February 23, 2009)
2. Cavusoglu, H., Cavusoglu, H. and Zhang J. (2006) Economics of Security Patch Management, *The Fifth Workshop on the Economics of Information Security (WEIS 06)*, June 26-28, Cambridge, England.
3. Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. (2004) Economics IT Security Management: Four Improvements to Current Security Practices, *Communications of the Association for Information Systems*, 12, 65-74.
4. Financial Services ISAC (2005) FS ISAC Operating Rules, *FS/ISAC, INC*. www.fsisac.com. (Current: February 01, 2008)

5. Gal-Or, E. and Ghose, A. (2005) The Economic Incentives for Sharing Security Information, *Information Systems Research*, 16, 2, 186-208.
6. Gordon, L. A. and Loeb, M. P. (2002) The Economics of Information Security Investment, *ACM Transactions in Information System Security*, 5, 4, 438-457.
7. Gordon, L., Loeb, M. and Lucyshyn, W. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, 22, 461-485.
8. Guesnerie, R. and Laffont, J. (1984) A Complete Solution to a Class of Principal-Agent Problems with an Application to the Control of a Self-Managed Firm, *Journal of Economic Theory*, 39, 97-119.
9. Laffont, J. and Maskin, E. (1982) The Theory of Incentives: An Overview, in Hildenbrand, W. (ed) *Advances in Economic Theory*. Cambridge, 31-94.
10. Maskin, E. and Tirole, J. (1990) The Principal-Agent Relationship with an Informed Principal: The Case of Private Values, *Econometrica*, 58, 2, 379-409.
11. McGlasson, L. (2009a) Heartland Breach: Bigger than TJX? *BankInfoSecurity.com*, www.bankinfosecurity.com (Current: January 31, 2009).
12. McGlasson, L. (2009b) Heartland Payment Systems, Forcht Bank Discover Data Breaches, *BankInfoSecurity.com*, www.bankinfosecurity.com (Current: January 31, 2009).
13. Mills, E. (2008) Bank of New York Mellon Says Customer Data Exposed, *cnetNews*, news.cnet.com, (Current: February 02, 2009).
14. Mirrlees, J. A. (1971) An Exploration in the Theory of Optimum Income Taxation, *The Review of Economic Studies*, 38, 2, 175-208.
15. Panko, R. (2004) Corporate Computer and Network Security, Prentice Hall: New Jersey.
16. Salanié, B. (2005) Adverse Selection: General Theory, in *The Economics of Contracts: A Primer*. MIT Press: MA.
17. Van Eeten M. and Bauer, J. (2008) Economics of Malware: Security Decisions, Incentives and Externalities, *Organization for Economic Co-operation and Development*, www.oecd.org.
18. Varian, H. (2000) Managing Online Security Risks. New York Times, New York, NY.
19. Varian, H. (2004) System Reliability and Free Riding, in Camp, L. J., Lewis, S. (Eds.) *Economics of Information Security*. Norwell, Kluwer.