Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

Information Security Investment with Different Information Types: A Two-Firm Analysis

Dengpan Liu
University of Texas at Dallas, dengpan.liu@student.utdallas.edu

Yonghua Ji
University of Alberta, yji@ualberta.ca

Vijay M. Mookerjee
University of Texas at Dallas, vijaym@utdallas.edu

Information Security Investment with Different Information Types: A Two-Firm Analysis

Dengpan Liu
University of Texas at Dallas
dengpan.liu@student.utdallas.edu

Yonghua Ji
University of Alberta
yji@ualberta.ca

Vijay Mookerjee
University of Texas at Dallas
vijaym@utdallas.edu

ABSTRACT

We analyze information security investment decisions by two firms that possess imperfectly substitutable information assets. Information assets are imperfectly substitutable if information at each firm is valuable and becomes more valuable when combined. When compared to optimal investment decisions made by a central planner, we find diametrically opposite results in the case where these decisions are made independently: substitutable assets lead to an "arms race" in which both firms over-invest whereas complementary assets lead to under-provision of "public goods" in which both firms under-invest. We also find that firms with highly substitutable information assets may not necessarily increase the amount of security investment in a centralized investment environment as the intensity of the deflected cross traffic increases.

Keywords

Imperfectly substitutable information, security investment, over-invest, under-invest

INTRODUCTION

The importance of information security has increased in recent times as more firms use the internet to conduct business transactions. Businesses have begun to store a large amount of information in corporate networks relating to customer profiles, product sales, and R&D information. Furthermore, information security has become a major concern for e-businesses as the volume of cyber attacks has increased over the past few years.

Several researchers have studied the economic impacts of information security investments. Gordon & Loeb (2002) study how the level of information vulnerability and expected loss affects the optimal level of investment for a firm. Using a similar modeling framework, Gordon et. al (2003) examine how sharing information across firms affects the overall investment level. Gal-Or and Ghose (2002) analyze how the sharing of security information between two firms influences security investments and price competition between these firms. However, previous research has not studied how the changing of the behavior of a hacker may affect information security investment decisions made by two firms given the nature of information assets stored by these two firms.

Two pieces of information are ***substitutable*** to a hacker if a piece of information from one firm is of little additional value to her once she has obtained the other piece of information from the other firm. Thus having acquired one piece of information the hacker would stop since there is no economic incentive to risk being caught while hacking the second firm. If however, the first attempt at hacking is unsuccessful, the hacker would likely try to hack the second firm. Such unsuccessful hacking attempts lead to ***deflected cross traffic***.

Two pieces of information in two firms are ***complementary*** to a hacker if obtaining both pieces of information from both firms is very valuable while one piece of information alone has little value. The hacker therefore would continue to attack the second firm when the attempt at the first form is successful. Such successful hacking attempts lead to ***penetrated cross traffic***.

In reality, two pieces of related information are usually ***imperfectly substitutable***. For example, one firm might store information on customer addresses and the other might store information on customer bank accounts. Each piece of information is valuable in its own right to a hacker, so some hackers may be satisfied after obtaining only one piece of

information. Other hackers might attempt to steal both pieces of information so that they can match the records in order to commit financial fraud, such as making a money transfer out of an account. When two pieces of information stored by two firms are stolen and matched, each company could suffer a larger loss than when only one piece of information is stolen. For imperfectly substitutable information, some hackers may attempt to hack the second firm even if they fail to penetrate the first firm. Other hackers may attempt to hack the second firm only if they succeed in penetrating the first firm. Thus to make our analysis general, we need to consider both deflected and penetrated cross traffic.

The objective of this paper is to analytically compare individual (i.e., independent) investment decisions made by two firms with the optimal (i.e., centralized) investment decision in the presence of imperfectly substitutable information assets.

THE MODEL

In this model, we consider two firms with imperfectly substitutable information, i.e., information at each firm is valuable and becomes more valuable when combined. Hence, a firm will incur an additional loss when hackers obtain combined information. If hackers fail to penetrate the first firm, a fraction p of them will continue to attack the other firm. A fraction q of hackers who successfully penetrate the first firm continue to attack the second one to get more information. If only one firm is hacked, the cost of penetration to the hacked firm is u, if both firms are hacked, the cost to each firm is $u + v$.

Firms can improve information system security by investing in security technologies such as anti-virus software, firewalls or intrusion detection systems. Let Z be the investment amount and $f(Z)$ be the corresponding security breach function defined as the probability of being penetrated by an attack with the investment amount Z. Consistent with prior literature (Gordon and Loeb, 2002), we assume that $f(Z) \in [0,1]$, $f'(Z) < 0$ and $f''(Z) > 0$, that is, as the investment in security increases, the information system becomes more secure, but at a diminishing rate.

Our model is depicted in the Figure 1. Firms A and B invest amounts Z_A and Z_B to secure their systems. We assume N hackers attempt to attack the two firms with equal probability since hackers have no prior information of the vulnerability at each firm. For firm A, the number of initial hackers (= $N/2$) who succeed is given by $N/2 \cdot f(Z_A)$ and q portion of these hackers continue to attack the second firm (shown as E_{AB} in Figure 1). Of those who fail in the initial attack, p portion of hackers, denoted by D_{AB} ($= p \cdot N/2 \cdot [1 - f(Z_A)]$), switch to attack firm B. The remaining hackers exit the system. For firm B, we have a similar situation. We do not consider learning effects of hackers or the firms in this model. Since these two firms are homogeneous, the order of attacking on the firms does not affect the penetration probability and cost.

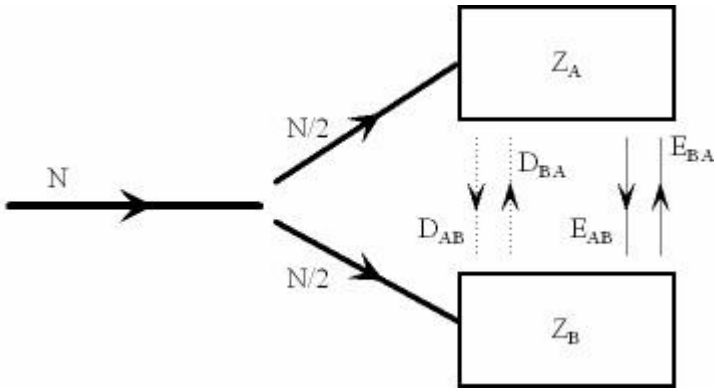

Figure 1: The hacking structure of the imperfectly substitutable information

The total cost $h(Z_A)$ for firm A that invests Z_A in information security, given that the investment level at firm B is Z_B, is given by

$$h_A(Z_A) = uN/2\, f(Z_A)\left[1 + q \cdot f(Z_B) + p(1 - f(Z_B))\right] + vqN \cdot f(Z_A) f(Z_B) + Z_A \quad (1)$$

The total cost $h(Z_B)$ is similarly obtained. Of the three terms in the square bracket in (1), the second one represents the cost due to penetrated cross traffic E_{BA} and the third one due to deflected cross traffic D_{BA}. The second term in (1) is the additional cost to firm A when both companies are penetrated. When firm B increases its spending Z_B, its system vulnerability $f(Z_B)$ decreases. This leads to an increase in the cost to firm A due to the cross traffic D_{BA} and a decrease in cost due to E_{BA}. Thus there are positive and negative externalities associated with security investments made by the two firms. The net effect due to E_{BA} and D_{BA} depends on the investment level and the damage cost u and v.

ANALYSIS OF MODEL

We consider two cases in the model. The first case studies firm investment level when firms make independent investment decisions. The second case studies a situation where the firms cooperate and make a centralized investment decision on information security.

Independent Investment Case

In the independent investment case, firm A and B make separate decisions on information security investment with a view to minimize their individual cost functions. The first-order conditions (FOCs) are given by:

$$uN \cdot f'(Z_A)[1 + q \cdot f(Z_B) + p(1 - f(Z_B))] + 2vqN \cdot f'(Z_A) f(Z_B) + 2 = 0 \quad (2)$$

$$uN \cdot f'(Z_B)[1 + q \cdot f(Z_A) + p(1 - f(Z_A))] + 2vqN \cdot f'(Z_B) f(Z_A) + 2 = 0 \quad (3)$$

These FOCs are symmetric and therefore we have a symmetric solution: $Z_A = Z_B = Z_D$. For certain functional forms such as the one given in Gordon and Loeb(2002), we can show that only symmetric solutions exist. To obtain an analytical solution, we need to assume a specific functional form for the security vulnerability function $f(Z)$. In this work, we are more interested in gaining insights about the cross traffic intensity parameter p and q affect the investment level. In the following propositions, without assuming a specific form of $f(Z)$, we characterize the impact of p and q on of Z_A and Z_B.

Proposition 1. In the decentralized case of imperfectly substitutable information, the security investment level at one firm will increase as more hackers switch to attack the other firm after an initial failure, i.e., $dZ_D / dp > 0$. (The proof is omitted for brevity)

From Proposition 1, we obtain the intuitive result that as the deflected cross traffic increases (p increases), both firms need to invest more to make their system more secure. However it is not obvious whether this result will hold if the two firms coordinate. Intuitively, when the cross hacking traffic to a firm increases, this firm would be expected to increase the investment to reduce the damage. We will later examine whether this intuition is correct in the centralized case. Proposition 2 below shows that the investment level at each firm in information security increases with cross traffic parameter q.

Proposition 2. In independent case of imperfectly substitutable information, the security investment level will increase as more hackers continue to attack the other firm after the first successful penetration. (The proof is omitted for brevity).

The result from Proposition 2 is also intuitive. If more hackers move from one firm to attack the other firm, then more security is needed. The interesting issue to explore next is whether this result in the independent case holds in the centralized case.

Centralized Investment Case

Two firms can form an alliance to coordinate their investments on information security so that the total cost to the firms is minimized. With coordinated investment, the benefit can be shared by the firms so they will be better off overall. The objective of the alliance is to minimize overall cost

$$H(Z_A, Z_B) = h(Z_A) + h(Z_B) \tag{4}$$

by choosing the optimal investment levels Z_A and Z_B.

The two FOCs with respect to Z_A and Z_B are symmetric, and we can show that for certain functional forms such as the one given in Gordon and Loeb (2002), there can only exist symmetric solutions. Therefore we limit out attention to the symmetric solution $Z_A = Z_B = Z_C$. The FOC is given by

$$uN \cdot f'(Z_C)[1 + 2q \cdot f(Z_C) + p(1 - 2f(Z_C))] + 4vqN \cdot f'(Z_C) f(Z_C) + 2 = 0 \tag{5}$$

Proposition 3. In the centralized case with imperfectly substitutable information, one firm's investment ($Z_A = Z_B = Z_C$) does not increase monotonically with p, the probability that a hacker will try to penetrate the second firm after failing at the first firm. The sign of dZ_C / dp is same as the sign of $1 - 2f(Z_C)$.

Proof: Taking the derivative of (5) w.r.t. p, we have

$$\frac{\partial Z_C}{\partial p} = \frac{(2f(Z_C) - 1)uNf'(Z_C)}{\partial^2 H / \partial Z_C^2} \tag{7}$$

Since Z_C minimizes the total cost H, we have $\partial^2 H / \partial Z_C^2 > 0$. The sign of dZ_C / dp is the same as the sign of $1 - 2f(Z_C)$ since $f'(Z_C) < 0$. **Q.E.D.**

Thus the result in the independent investment case does not carry over directly to the centralized investment case. Our numerical results verify that dZ_C / dp could be positive or negative in different regions of the parameter space. For certain types of retail firms that do not store sensitive customer information, security breach costs are relatively low (u and v are small). Hence it may be optimal to invest at a low level, i.e., $f(Z_C)$ is likely to be higher than 1/2. In such situations it is better to reduce the investment level so as to reduce deflected cross traffic if the cross traffic intensity p increases. On the other hand, for certain types of e-commerce or financial firms that have very valuable customer information, the security investment level is likely to be high (i.e., $f(Z_C)$ is likely to be lower than 1/2). Here the investment level Z_C increases with p. When two firms cooperate on security investments, a balance must be struck between the increase in direct penetration cost and the reduction of investment cost together with the burden on the other firm due to cross traffic. In the independent case, the two firms always increase the investment level to minimize individual losses when p increases. Similar to Proposition 2 in the independent case, Proposition 4 shows that the investment level Z_C increases as q increases.

Proposition 4. In the centralized case of imperfectly substitutable information, the security investment level $Z_C (= Z_A = Z_B)$ increases as more hackers continue to attack the other firm after the successful penetration at the first firm, i.e., $dZ_C / dq > 0.$

Proof: From (5), we take the derivative w.r.t. q,

$$\frac{dZ_C}{dq} = \frac{-2Nf(Z_C) f'(Z_C)(u + 2v)}{\partial^2 H / \partial Z_C^2} > 0. \qquad \textbf{Q.E.D.}$$

Contrasting Proposition 3 with Proposition 4, we can see that the effects of p and q on the information security investment are different because they measure cross traffic intensity from different aspects. The parameter q measures the proportion of further penetration at the second firm after a successful penetration at the first firm. Therefore, improving individual security levels should directly benefit each firm by reducing the chance of both initial and second penetration. Thus the investment decisions at the two firms exhibit positive externalities. The effect due to p is more complicated due to negative externalities. Increasing security at one firm comes at the expense of more attacks at the other firm since more hackers would fail to penetrate the first firm. In the centralized investment case, positive and negative externality effects are balanced to determine the coordinated investment level for each firm.

We have also compared the investment levels in the independent and centralized cases and summarized the results in Proposition 5.

Proposition 5. For the imperfectly substitutable information, compared with investment in information security in centralized case Z_C, investment in the independent case Z_D is higher when $q < q_0$, lower when $q > q_0$ and same when $q = q_0$ where $q_0 = p \cdot u/(u + 2v)$.

Proof(Sketch**)**: At $q = q_0$, Z_D and Z_C satisfy the same FOC: $uNf'(Z)(1+p) + 2 = 0$. Therefore, $Z_C = Z_D$ when $q = q_0$. Otherwise, $Z_C \neq Z_D$ in $Z - p$ plane. Also, at $q = q_0$, $dZ_C/dq = 2dZ_D/dq > dZ_D/dq > 0.$

Thus, we have $Z_D > Z_C$ when $q < q_0$ and $Z_D < Z_C$ when $q > q_0$. **Q.E.D.**

Proposition 5 provides some interesting results. When p is large relative to q, i.e., $q < q_0$, the firm compete in the independent environment to raise their individual security levels and deflect more hackers to their counterpart. Such negative externalities lead to an "arm race": both firms over invest. When q is relatively large, firms wait for each other to reduce cross traffic and under-invest. However the benefits of positive externality are not fully exploited in the independent case leading to a situation similar to the under-provision of "public goods".

CONCLUSION

We develop a model that studies how investment decision in information security is affected by the behavior of hackers in the presence of investment externalities. Compared to optimal investment decisions made by a central planner, we obtain opposite results when these decisions are made independently: holding substitutable information assets leads to an "arm race" in which both firms over-invest whereas holding complementary information assets leads to the under-provision of "public goods" in which both firms under-invest. Also we find the seemingly counter-intuitive result that the investment in the centralized case does not necessarily increase with an increase with the intensity of cross traffic *p*. Here the direction of change in the investment depends on the security breach cost u and v. With these insights in mind, a third party, which could be a social ware fare optimizer, can come up with a coordination scheme to achieve the optimum obtained in the centralized case.

In future work, we plan to incorporate learning effects into a hacker's behavior to study how the investment decision will change. This learning effect could intensify the "arm race" and lead to a further under-provision of "public goods".

REFERENCES

1. Gal-Or, E. and Ghose, A. (2003) The Economic Consequences of Sharing Security, *Proceedings of Workshop on Economics of Information Security*, University of Maryland.
2. Gordon, L. and Loeb, M. (2002) The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, 5, 4, 438-457.
3. 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.