Cyber Insurance and IT Security Investment: Impact of Interdependent Risk

Hulisi Ogut
Nirup Menon
Srinivasan Raghunathan
School of Management
The University of Texas at Dallas
Richardson, TX 75083
{hxo012000, menon, sraghu}@utdallas.edu

Abstract

IT security risk management has become a critical issue for many firms because of increasing scale and scope of virus and hacker attacks. As firms conduct more of their business over the Internet, security of IT assets of one firm becomes more intricately dependent on security of IT assets of other firms. While research in the IT security area has focused predominantly on developing software and hardware products to reduce security risks, we show in this paper that interdependency of IT security risks of different firms has a significant impact on firms' incentives to invest in these products. This interdependency also affects firms' insurance coverage, another important risk management tool, which is hampered by the still under-developed cyber-insurance market. Specifically, our analysis reveals that interdependence of cyber-risk reduces firms' incentives to invest in security technologies and to buy insurance coverage. Further, a higher degree of interdependence makes firms invest less in IT security and to buy less cyber-insurance even though it increases the risk. The security investment and the insurance coverage level are less than the corresponding socially optimal levels when cyber-risks are interdependent. A more developed insurance market may not increase firms' insurance coverage unless the development in insurance market reduces the price of insurance. We find that that a more mature insurance market may not necessarily result in lower insurance price because firms use insurance rather than investment to manage security risk in a mature insurance market, which increases the insurers' risk. Our results on the effect of cyber-risk interdependency on firms' strategies have significant implications for IT security policies. While developments in technology that reduce the interdependence and a mature and competitive insurance market may help firms, we find that traditional mechanisms such as punishment strategies (e.g., fines on the liable party) as well as cooperation mechanisms such as information sharing can mitigate the negative effect of interdependency and induce firms to invest at the socially optimal level.

1. Introduction

The scale and scope of hacker and virus attacks on computer systems is increasing (Power 2002, CERT/CC Statistics 2003), motivating firms to invest in security technologies such as firewalls, intrusion detection systems, encryption, biometric and other authentication systems (Doll 2002). Although deployment of these technologies may reduce security vulnerabilities and losses from security breaches, it is not clear to firms how much they must invest in IT security (Computerworld, July 16, 2003). Complete prevention of security breaches is technologically impossible and, in some cases, even undesirable because of high costs. Consequently, firms may buy insurance to hedge against loss due to security breaches. Investing in both prevention technologies and insurance to manage risks is common in numerous domains. What makes IT security risk management challenging is the interdependency of cyber-risk among firms. That is, IT security risk faced by a firm depends not only on its security posture and actions, but also on those of others.

Cyber-risk interdependence occurs in two ways. First, computers in different firms are physically linked via the Internet, and communication protocols allow access of machines by other trusted hosts (Camp and Wolfram 2001). If a hacker is able to penetrate one firm due its poor IT security, (s)he is able to access other linked firms. A second, and a more subtle, reason for interdependence of cyber-risk is the logical interdependence of systems. This type of interdependence occurs from ubiquitous computer technologies. Security experts argue that standardization of computer platforms across firms increases security vulnerability because a hacker that cracks the security of one firm may be able to crack the security of other firms that use the same technology as the first firm (Geer et al. 2003).

Industry experts argue that because inter-connection of computers increases the cyber-risk, firms should invest more in IT security technologies and buy more insurance to hedge against the increased likelihood of security breach (cf. D'Aquistino 2003). While firms have increased investments in security technologies in recent years, IT security experts suggest that investment in cyber insurance is significantly low considering the volume of business that occurs over IT networks (Kovacs et al 2004, IAAC 2002, Baer2003).[1]

[1] Current cyber-insurance coverage accounts for only about 1% for the potential US$20billion market world-wide. Only a few insurance companies such as American International Group, Lloyd's and Zurich offer commercial insurance against hacker attacks, disaster recovery, and network downtime, and third-party (or business partner) liability.

They attribute an immature insurance market characterized by few insurers and huge uncertainty in assessing cyber risk, and lack of awareness about cyber insurance products among firms for the low level of cyber insurance coverage.

Our analysis reveals that interdependence of cyber-risk may partly explain the IT security risk management strategies of firms. Though interdependence increases the magnitude of individual firm's risk, it reduces the effectiveness of IT security spending causing firms to invest less on IT security. Compared to independent risk, firms buy less insurance coverage when faced with interdependent risk. Interdependence causes insurers to raise insurance price because of the higher total risk that they bear now. An immature insurance market also affects the firms' risk management strategies significantly. In a less (more) mature insurance market, self-protection – IT security investment that affects probability of breach – is more (less) attractive compared to insurance to manage risk, and firms increase (decrease) IT security investment and decrease their insurance coverage. Whether a firm buys more or less insurance as the insurance market matures depends on its effect on the insurance premium vis-a-vis security investments. A more developed insurance market may not increase firms' insurance coverage unless the development in insurance market reduces the price of insurance. We find that that a more mature insurance market may not necessarily result in lower insurance price because firms use insurance rather than investment to manage security risk in a mature insurance market, which increases the insurers' risk. Consequently, conventional wisdom that firms will buy more cyber insurance if the insurance market matures may not hold.

In light of our result that interdependence of security risks causes firms to invest less than the socially optimal levels in IT security and insurance coverage, we analyzed two public policy mechanisms to induce firms to increase their investments. Developments in technology that reduce interdependence of security risks, while maintaining the benefits of interconnection, can certainly benefit the society. However, our analysis shows that, for a given level of interdependence, traditional mechanisms such as punishment strategies (e.g., fines on the liable party) as well as cooperation mechanisms such as information sharing can mitigate the negative effect of interdependence and induce firms to invest at the socially optimal level. In

particular, we find that information sharing, much debated in the IT security community, can be an effective tool for security risk management.

The most significant contribution of our research relates to the policy implications of two unique aspects of IT security – interdependency of IT security risks and a weak or immature insurance market – whereas prior research focused predominantly on security technology. Our insights about how interdependency and insurance market characteristics affect the efficiency of security investments, and consequently, the level of investments in IT security and insurance coverage are valuable to security managers and social planners alike in formulating their IT security risk management strategies.

The rest of the paper is organized as follows. We synthesize the relevant literature on IT security and insurance in the next section. In section 3, we describe the basic model. We derive and discuss the principal results about the effect of interdependency and insurance market on firms' risk management strategies in Section 4. In Section 5, we analyze fine on the liable firm and information sharing as mechanisms to reduce the negative effect of interdependency. We extend our basic model to n firms in Section 6. We conclude the paper with a summary in Section 7.

2. Literature Review

Planning for and management of IT security has been a focus of MIS literature for more than a decade (Neiderman et al 1991, Loch et al 1992, Straub and Welke 1998). This literature has focused on design of deterrent, preventive, and detection measures – collectively self-protection – and disaster recovery measures to enable an organization to control security risk by reducing both the probability and the severity of loss (Straub 1990). Qualitative research in IT security management has developed frameworks to manage IT security (Claffin 2001, Karofsky 2001). Technical research on IT security has focused on developing security products such as firewalls and intrusion detection systems (Axelsson 1999, Cheswick et al 2003, Pohlmann and Crothers 2002). Recently, researchers have initiated research on economic aspects of IT security such as evaluation of security technologies (Cavusoglu, Mishra, and Raghunathan 2004, 2005), patching policies (Beattie et al. 2002). Hoo (2000) proposes a decision analytic framework to evaluate different baskets of safeguards from a cost-benefit perspective for IT security investment decisions. Gordon and Loeb (2002)

present a model to analyze IT investment levels for given vulnerability. Varian (2002) analyzed the case when system reliability displays public good characteristics. None of these has investigated the impact of risk interdependence on firms' security risk management strategies. Our work complements the stream of research in the economics of IT security.

The motivation for our work is the increased risk and externalities caused by the growth of public and private networks using wired and wireless connections (Kunreuther and Heal 2003). Externalities imposed by networks have been extensively analyzed in the economics and IT literature. For example, in IT literature, Mendelson and Whang (1990) studied the role of externalities (congestion) in the pricing of computer services. Riggins et al. (1994) analyzed network growth in the presence of externalities in the context of electronic data interchange (EDI). Wang and Seidmann (1995) analyzed the negative externalities imposed by participants in an EDI network on the non-participants. In some cases, security devices generate positive externalities, as in the case of Lojack, a hidden radio transmitter used for retrieving stolen automobiles (Ayres and Levitt 1998). Ayres and Levitt empirically showed that the thefts of cars declined after Lojack was introduced, because perpetrators did not know if a car was actually protected by Lojack or not. In the IT security context, externalities arise because of hacker behavior and because of computer interconnections. When a firm protects its computer systems and makes it harder for a hacker to crack its system, hackers may shift their effort to other firms, and thus increasing the likelihood of successful attack on other firms (Anderson 2001). Anecdotal evidence shows that terrorists attack allied nations rather than their primary target when the primary target is well protected (Lakdawallah and Zanjani 2002). Physical and logical interconnections among computers of different firms also introduce externalities.

Recently the IT security community has proposed insurance as a means to cope with the residual risk after IT security investments are made (Gordon et al. 2003). Insurance is well-studied with at least three peer-reviewed academic journals dedicated to the study of risk and insurance (Dionne and Harrington, 1992). In their seminal article, Ehrlich and Becker (1972) showed that self protection and market insurance are complements when insurance price is actuarially fair, but are substitutes when prices increase with a decrease in self protection because of moral hazard commonly observed in the insurance market. Depending on the

level of loading on the insurance price due to moral hazard, organizations will pick more of one and less of the other between self-protection and insurance to manage their risk (Ehrlich and Becker 1972).

What distinguishes our work from general insurance research is that we examine managerial incentives of an insurance seeking firm in the presence of interdependent risks, heretofore not analyzed in literature. Unlike other insurance markets, interdependent risk is a significant aspect of cyber insurance. Cyber-insurance is impacted by correlated risks across firms and risk ambiguity caused by lack of data on frequency, scale, and scope of security breaches (Kunreuther 2004). Further, the current cyber-insurance market is considered to be immature with few firms offering insurance and few firms buying insurance and for low amounts of coverage (IAAC 2002).

3. The Model

Consider *n* risk-averse firms with inter-connected IT. All firms manage cyber-risk by investing in self-protection and by buying cyber-insurance. $U_j(\cdot)$ is firm *j*'s utility function that relates its payoff to its utility. We impose $U_j'(\cdot) > 0$ and $U_j''(\cdot) < 0$. Further, we assume constant absolute risk aversion (CARA) (or Arrow-Pratt absolute risk aversion coefficient) given by $r = -\frac{U''}{U'}$. We consider a single period. Firms invest in self-protection to decrease the probability of breach. A firm's investment on self-protection affects the probability of breach at all firms. That is, the probability of breach at any firm is affected not only by its security investments, but also by those of other firms. Consequently, the probability of breach at firm *j* is $B_j(z_1, z_2, \ldots, z_n)$, in which z_i represents the investment in self-protection by firm *j*. A higher level of investment by a firm reduces its own breach probability and that of others.[2] We also assume that these investments exhibit declining returns. Hence, $B_j'(z_i) < 0$ and $B_j''(z_i) > 0, \forall i, j$. The insurance premium paid by firm *j* to the insurer is a fraction, π_j, of amount of insurance, I_j, taken by the firm. π_j is the price of insurance and is set by the insurer (or the insurance market) after assessing the security risk of firm *j*. If an IT

[2] It can be argued that, *ceteris paribus*, a higher level of investment by a firm may *increase* the probability of breach of other firms because hackers may focus their efforts on firms that are easier to attack. We do not model this type of hacker-related externality in this paper. We assume that the interdependency occurs only because computers across firms are connected.

breach occurs at firm *j*, the firm incurs a loss of L_j, and is paid an amount, I_j, by the insurer, provided the firm had paid the premium $\pi_j I_j$ at the beginning of the period. Once a breach occurs, a firm loses the asset it was trying to protect. Firm *j* determines the optimal values of I_j and z_j by maximizing its expected utility

$$B_j(z_1, z_2, ...z_n)U_j\left(W_j - L_j + \left[1-\pi_j\right]I_j - z_j\right) + \left[1 - B_j(z_1, z_2, ...z_n)\right]U_j\left(W_j - \pi_j I_j - z_j\right),$$

where W_j is the initial wealth of firm *j*.

The insurance price is determined by the level of competition or number of insurers in the market, the level of security risk, the accuracy with which insurers can assess the security risk, and the availability of actuarial data to assess the risk. If the insurance market is perfectly competitive and the actuarial data about firms' security risks are available, then the insurance price will be such that each insurer makes zero profit, i.e., $\pi_j = B_j$. We refer to such an insurance market as mature. We model an immature insurance market through the parameter λ, commonly called the loading factor, so that $\pi_j = (1+\lambda)B_j$ (Spizro 1988)[3]. When the price of insurance is actuarially fair, λ=0. When λ>0, the insurers expect positive profits. The maturity level of the insurance market may be low when (i) there are a few firms in cyber insurance market and hence less competition, (ii) adequate data on IT security, breaches and damages is unavailable, and (iii) correlated damage that may cause catastrophic loss exists (IAAC 2003, Baer 2003, Froot and Posner 2000). Factors (i) and (ii) increase the premium through the impact of the loading factor, λ, while factor (iii) increases the assessed risk from the perspective of the insurer.

4. Interdependency, Immature Insurance Market, and IT Security Management

First, we consider the baseline case in which the firms are independent and the insurance market is mature. Second, we consider the IT security model with inter-dependent firms and an immature insurance market. Then, we compare the results of these two cases to derive the impacts of interdependency and insurance market maturity on firms' IT security risk management strategies.

4.1. Baseline Case: Independent Firms and Mature Insurance Market

[3] Insurer's expected profit is $\pi_j I_j - B_j I_j = (1+\lambda) B_j I_j - B_j I_j = \lambda B_j I_j$. If λ=0 then insurer's expected profit is 0.

In the baseline case, a firm's security investment affects only its breach probability. We drop subscript *j* for parsimony in notation. Assuming mature insurance market, we set $\lambda=0$. Thus, a firm maximizes its utility function given by:

$$\max_{z,I} \quad B(z)U\left(W-L+[1-B(z)]I-z\right)+\left[1-B(z)\right]U\left(W-B(z)I-z\right). \tag{1}$$

As shown in the appendix (proof 1), the optimal investment level is the solution to the equation

$$B'(z)=-\frac{1}{L}, \tag{2}$$

and the optimal insurance coverage is given by

$$I=L. \tag{3}$$

Thus, the firm takes insurance to cover the entire loss from a breach. Availability of cyber insurance reduces firms' incentives to spend on IT security because losses are now hedged through insurance. To see this, compare the above optimal security spending to that in a situation in which no cyber insurance exists. The objective function that maximizes the net utility function, without insurance amount and premium, is:

$$\max_{z} B(z)U\left(W-L-z\right)+\left[1-B(z)\right]U\left(W-z\right). \tag{4}$$

Solving for the optimal values of z, we get

$$B'(z)=-\frac{\left(B(z)+\left(1-B(z)\right)\dfrac{U'(W-z)}{U'(W-L-z)}\right)}{L}>-\frac{1}{L} \tag{5}$$

Comparing the values of z in equation (5) and equation (2), when W is relative to z, reveals that with insurance available at actuarially fair price, firms spend less on IT security {see proof 2 in the appendix}.

4.2. General IT Security Case: Interdependence and Immature Insurance Market

We analyze the interdependent risk case with two symmetric firms. Later in Section 6, we extend our analysis to *n* firms. We model interdependency in the following manner. The probability of breach for firm 1 is determined not only by firm 1's IT security investment level, but also by that of firm 2. A firm (e.g., firm 1) may be attacked directly or indirectly. A *direct* attack on a firm occurs if the breach occurs at the firm first. An *indirect* attack on a firm occurs when the hacker gains access to this firm's IT assets through the other firm after breaching the other firm first. A firm can only reduce the probability of its direct attack by self-

protection. The probability of indirect attack on a firm depends on the probability of direct attack on the other firm, i.e., on the security investment of the other firm, and on the level of interdependency between the two firms. Formally, the *direct* attack probability for firm 1 is $p(z_1)$ where z_1 is the investment by firm 1. The *indirect* attack probability for firm 1 is given by $q \cdot p(z_2), 0 \le q \le 1$. The parameter q measures the probability that firm 1 will be breached given that firm 2 has been breached and vice versa. q models the degree of interdependency or externality between the two firms' IT security. A higher q indicates a higher degree of interdependence. When $q = 0$, the firms have independent security risks. The breach probability for firm 1 is:

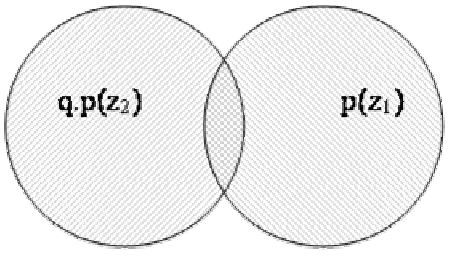
$$B_1(z_1, z_2) = p(z_1) + [1 - p(z_1)]qp(z_2) = 1 - [1 - p(z_1)][1 - qp(z_2)]. \quad (6)$$

The probability that a breach does not occur at firm 1 is $[1 - p(z_1)][1 - qp(z_2)]$. Subtracting from one gives the probability that direct or indirect breach occurs at this firm. The breach probability for firm 2 is a similar expression and can be obtained by interchanging the subscripts in equation 6. Figure 1 illustrates the IT security risk in the interdependent case. Without interdependence, a firm's probability of breach is the shaded circle on the right. The interdependence adds a second circle, shown as the left in Figure 1. The union of the two circles representing direct and indirect risks gives the total breach probability of firm 1.

Using λ as the loading factor for an immature insurance market, the insurance price is given by

$$\pi_1(z_1 : z_2) = [1 + \lambda] B_1(z_1, z_2). \quad (7)$$

Figure 1. Illustration of Breach Probability to Firm 1 with Interdependence



Equation 7 reduces to the baseline model when q =0, and $\lambda = 0$. Firm 1 maximizes its expected utility by solving

$$\max_{z_1, I_1} B_1(z_1, z_2)U_j\left(W - L + \left[1 - \pi(z_1 : z_2)\right]I_1 - z_1\right) + \left[1 - B_1(z_1, z_2)\right]U_j\left(W - \pi(z_1 : z_2)I_1 - z_1\right). \quad (8)$$

Firm 2 solves its expected utility (obtained by interchanging the firms' subscripts in 8). As shown in proof 3 of the appendix, for symmetric firms, a firm's IT security spending is given by the solution to the following differential equation:

$$p'(z)\left[1 - qp(z)\right] = -\frac{1}{\left[1+\lambda\right]L}. \quad (9)$$

The amount of insurance coverage demanded by the firm is:

$$I = L - \frac{\lambda}{r(1+\lambda)\left[1 - p(z)\right]\left[1 - qp(z)\right]}, \quad (10)^4$$

For a given functional form for $p(z)$, equations 9 and 10 are solved for the two decision variables. We have shown in proof 4 in the appendix that an unique equilibrium exists if

$$\left[p''(z)\left(1 - qp(z)\right)\right] - q\left[p'(z)\right]^2 > 0. \quad (11)$$

We make the technical assumption that constraint (11) is satisfied. Equation 9 is solved first to obtain the optimum investment, and then by substituting this investment in equation 10 and solving it, the optimum insurance coverage is obtained. Such a sequential solution procedure of simultaneous decision-making problem implies that firms can manage IT security risk by first reducing the risk through investments and then managing the residual risk through insurance. This is intuitive because the investment level affects security risk level and, consequently, the price of insurance, but the coverage amount does not affect the security risk. This result is consistent with the common practice of buying insurance only for the residual risk, which is either impossible or costly to manage through other mechanisms. (Counterpane Inc. 2004, Insurance Journal, February 23, 2004).

4.3. Impact of Interdependency and Insurance Market Maturity

[4] We can show that the second order conditions are satisfied in our model.

Comparing the solutions for the baseline case solutions (equations 2 and 3) with those for the general case solution (equations 9 and 10), we get the following result.

> *Proposition 1: All else kept constant, compared to when security risks are independent, (i) IT security investment is less, and (ii) the insurance coverage is less or equal (equality occurs when λ=0) when security risks are interdependent.*

{See proof 5 in the appendix.}

At first blush, the above result seems counter-intuitive because, for identical levels of investment, the probability of breach is higher when firms' risks are interdependent than when independent, i.e., $p(z)+\left[1-p(z)\right]qp(z) > p(z)$. The reasons for this counter-intuitive result are two-fold: lower efficiency of investment and higher insurance premium when firms are interdependent. We can observe from Figure 1 that interdependency increases the overall risk, represented as the union of the two circles,[5] but decreases the portion of risk controllable by security investment, represented as the right circle minus the intersection. That is, portion of the total risk controlled by investment reduces from $p(z_1)$ in the independent case to $p(z_1)\left(1-qp(z_2)\right)$ in the interdependent case. Further, the efficiency of investment, measured as the marginal reduction in risk because of investment, reduces from $\left|p'(z_1)\right|$ in the independent firm case to $\left|p'(z_1)\left(1-qp(z_2)\right)\right|$ in the interdependent case. In the interdependent risk case, the controllable portion of risk and the efficiency of investment are lower because a firm's investment is valuable (in terms of reducing the probability of attack) only under the condition that the firm does not suffer from an indirect attack, whereas in the independent risk case, there is no such condition. Thus, from the firm's perspective, reduction in controllable portion of risk and the efficiency of investment reduces its incentives to invest in IT security when firms are interdependent.

Not only does a firm spend less on IT security, but it also buys less insurance $\left(L-\frac{\lambda}{r[1+\lambda]\left[1-p(z)\right]\left[1-qp(z)\right]}\right)$ in interdependent risk, compared to the independent risk

[5] To be precise, the risk is equal to the probability represented in the figure multiplied by *L*, a contant.

$\left(L - \frac{\lambda}{r[1+\lambda][1-p(z)]}\right)$ {proof 5 in appendix}. The price per unit dollar of insurance coverage is higher for interdependent risk. This is so because from the insurer's perspective the total risk is higher. Note that insurance price is a product of loading factor and total risk to one firm. Consequently, a risk-averse firm reduces its coverage to lower the premium. The net effect of reduced investment and reduced insurance coverage combined with a higher total risk is that firms have a high breach probability and a higher loss in the interdependent risk case. The next proposition discusses the impact of the degree of interdependence and other firm specific parameters on firms' strategies through a comparative static analysis.

Proposition 2: For two identical firms,

(i) *As interdependency increases, IT security investment decreases and insurance coverage decreases or remains the same, ceteris paribus. That is,* $\frac{\partial z}{\partial q} < 0$, $\frac{\partial I}{\partial q} \leq 0$.

(ii) *As the amount at risk increases, IT security investment increases, and insurance coverage increases, ceteris paribus. That is,* $\frac{\partial z}{\partial L} > 0$, $\frac{\partial I}{\partial L} > 0$.

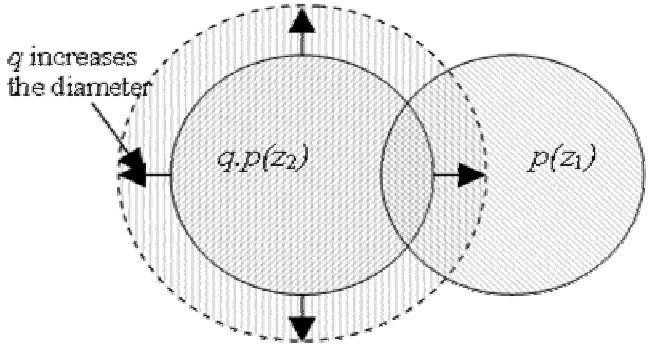
(iii) *As the degree of risk aversion increases, IT security investment remains constant, and the insurance coverage increases or remains the same. That is,* $\frac{\partial z}{\partial r} = 0$, $\frac{\partial I}{\partial r} \geq 0$.

{See proof 6 in the Appendix.}

Interdependency reduces the incentives of firms to invest in security and to buy insurance coverage, primarily due to reduced control over risk and reduced investment efficiency. As q increases, these two effects – reduced control over risk and reduced efficiency – increase (Figure 2). When q increases, the diameter of the circle at the left in Figure 2 (measure of indirect attack) increases. Hence, the size of the overlap region increases as well, which, in turn, decreases the portion of risk or residual risk that the firm can control. Similarly, the investment efficiency decreases with an increase in q, i.e., $\left|p'(z_1)(1-qp(z_2))\right|$ decreases as q increases. The result that firms reduce their insurance coverage when q increases, is an outcome of the following observation.

Corollary 1. The insurance price (π) increases with an increase in the degree of interdependence (q).

Figure 2. Illustration of Total Risk to One Firm with Increasing Externality



{See proof 7 in the Appendix.}

The insurance price is composed of two components: the loading factor and the risk assessed by the insurer. While the (insurance seeking) firm does not account for the risk that it imposes on another insurance seeking firm, the insurer accounts for the correlated risk when pricing insurance. Hence, though the loading factor could be the same for low or high interdependence, the probability of loss increases from the insurer's perspective thereby raising the insurance price.

An increase in loss (L) from a security breach increases the security spending as well as insurance coverage (part (ii) of proposition 2). An increase in L increases the efficiency of investment because an increase in L increases the expected loss. The higher efficiency causes firms to increase their security spending; the higher expected loss cause firms to increase their insurance coverage. Proposition 2(iii) is a standard result in the insurance literature: more risk-averse firms buy more insurance. The degree of risk aversion does not affect IT security investment because the degree of risk aversion does not affect the efficiency of security investment.

Proposition 2 showed the effects of firm-specific parameters on IT security spending and insurance coverage. We analyze the effects of insurance market characteristics on firms' strategies next. It is necessary to define the following variable for the next proposition,

$$\lambda^* = -\frac{p'(z)\left[1+q-2qp(z)\right]}{\left[1-p(z)\right]\left[1-qp(z)\right]L\left\{p''(z)\left[1-qp(z)\right]-p'(z)qp'(z)\right\}}. \tag{12}$$

Proposition 3: For two identical firms, as the insurance market becomes more immature (λ increases), IT security investment (z) increases. The insurance coverage (I) increases if $\lambda > \frac{1}{\lambda^* - 1}$, *and decreases if* $\lambda < \frac{1}{\lambda^* - 1}$.

{See proof 8 in the Appendix.}

Firms invest more in security when the insurance market is immature because security investment is more effective than insurance. However, the impact of the insurance market on insurance coverage is not uni-directional. This is because the loading factor affects firms' investments and the price of insurance. While a higher loading factor increases investment, it may not necessarily increase the insurance price, as shown by the following result.

Corollary 2: If $\frac{\partial \pi}{\partial \lambda} > 0$, *then* $\frac{\partial I}{\partial \lambda} < 0$.

{See proof 9 in the Appendix.}

When both the loading factor λ and the price of insurance (product of loading factor and probability of loss) decrease, firms buy more coverage because of two reasons. First, a smaller λ results in a lower security investment (as stated in the first part of proposition 3) and a higher breach probability, and consequently, a greater need for insurance. Second, the lower insurance price resulting from a lower λ increases demand for insurance. On the other hand, if the price of insurance increases and λ decreases, then depending on the increase in insurance price and on the increase in residual risk caused by the lower security investment, the firms may obtain more or less coverage. The increase in insurance price dominates the increase in risk when the insurance market is not significantly mature. If the maturity level of the insurance market is higher than a critical threshold value, any improvement in the maturity level contributes to a higher insurance coverage by firms.

4.4 Implications for IT Security Risk Management

The impact of interdependency on IT security risk management strategy is not well understood. Further, the nascent cyber-insurance market is hampered by lack of data about IT security risks and knowledge to assess such risks. Over time though, more insurers may enter the market, security risks are likely to be assessed more accurately, and the insurance market will mature. Technological innovation may also reduce the effect of

interdependence, even as more firms are interconnected by IT. This is an effect of maturity of the security technology. To analyze the combined impact of technology maturity and insurance market maturity on security investment and insurance coverage, we compare security spending and insurance coverage along two key dimensions, e.g., the degree of interdependence and the degree of insurance market maturity (Table 1). q=0 corresponds to mature security technology, in which firms are able to eliminate interdependence, and λ=0 specifies the situation in which the insurance market is mature.

Earlier we analyzed $\lambda > 0$ and $q>0$ (cell 4 of Table 1). Cell 1 corresponds to the baseline scenario, in which the insurance market is mature and the technology is such that interdependency of security risks is nil. The other two cells characterize the situations in which one of them, either the insurance market or the technology, is immature. The ordering of security investment and insurance coverage in these four regions is:

Proposition 4: (i) $z_2>z_1,z_4>z_3$ *(ii)* $I_1=I_3>I_2>I_4$.

{See proof 10 in the appendix}

Table 1. Comparison of Immature Insurance Market and Security Technology with Mature Market and Technology

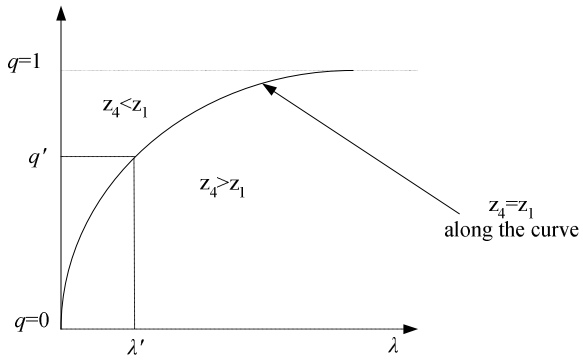
	Mature Insurance Market (Actuarially Fair Insurance price, λ =0)	Immature Insurance market (Imperfectly priced Insurance, λ >0)
Mature Security Technology (No interdependence or externality; q=0)	$p'(z_1^*) = -\frac{1}{L}$ $I_1^* = L$ I	$p'(z_2^*) = -\frac{1}{L[1+\lambda]}$ $r[L - I_2^*] = \frac{\lambda}{[1+\lambda][1-p(z_2^*)]}$ II
Immature Security Technology (Interdependence exists; $0<q<1$)	$p'(z_3^*) = -\frac{1}{L[1-qp(z_3^*)]}$ $I_3^* = L$ III	$p'(z_4^*) = -\frac{1}{L[1+\lambda][1-qp(z_4^*)]}$ $r[L - I_4^*] = \frac{\lambda}{[1+\lambda][1-p(z_4^*)][1-qp(z_4^*)]}$ IV

Firms invest the highest amount in security when security technology is mature and the insurance market is immature. Security spending is lowest when the insurance market is mature and security technology is immature. These findings are intuitive because the investment is attractive when the technology is more mature relative to the maturity of the insurance market. Further, for a given level of technology (insurance) maturity, any improvement in insurance (technology) maturity decreases (increases) firms' incentive to invest

in security. When both insurance market and technology improves, it is not clear whether firms increase or decrease their investments. Comparing diametrically opposite cases of mature technology and mature insurance (cell 1) and immature technology and immature insurance (cell 4), a firm invests more in security under two scenarios (Figure 3): (i) for a given insurance market, the level of interdependency (technology immaturity) is greater than a critical value *q'*, or (ii) for a given level of technology maturity, the insurance market maturity is less than a critical value *λ'*. The relationship between the IT security spending in these two regimes is governed by the condition $\frac{p'(z_1)}{p'(z_4)} = [1+\lambda]\left[1-qp(z_4)\right]$, which is plotted in Figure 3. This result shows that firms' security investment may not monotonically increase as technology and insurance market improves.

The insurance coverage is likely to increase, benefiting insurers, as the technology and insurance markets mature from cell 4 to other cells.

Figure 3: The Effect of Maturity in Insurance Market and Security Technology



5. Incentive Mechanisms for IT Security Management

When a firm acts in pure self-interest, it invests less both on security and on insurance when risks are interdependent. Consequently, with interdependent risk, the breach probability for each firm is higher, and the expected utility is lower. Joint decisions by firms internalize the negative externality of interdependency.

5.1. Joint Solution for Two Firms

The joint optimizing solution solves the following model:

$$\max_{z_1,z_2,I_1,I_2} \sum_{j=1}^{2} B_j U_{0j}\left(W - L + \left[1-\pi_j\right] I_j - z_j\right) + \left[1-B_j\right] U_{1j}\left(W - \pi_j I_j - z_j\right) \tag{13}$$

We show in the appendix (proof 11) that joint solution is:

$$p'(z)\left[1+q-2qp(z)\right] = -\frac{1}{(1+\lambda)L}. \tag{14}$$

$$I = L - \frac{\lambda}{r(1+\lambda)\left[1-p(z)\right]\left[1-qp(z)\right]}. \tag{15}$$

Thus,

> *Proposition 5: All else kept constant, the social planner's choice of IT security investment is higher than or equal to the firm's choice of IT security investment, and social planner's choice of insurance is higher than or equal to firms' choice of insurance.*

{See proof 11 in the appendix.}

Comparing the optimal security investments for joint decision (equation 14) with self-interested decision (equation 2), note that the marginal benefit of security investment for the joint solution, $p'(z)\left[1+q-2qp(z)\right]$, is higher than that for the self-interested firm, $p'(z)\left[1-qp(z)\right]$. This is because the former incorporates the impact of one firm's security investment on another. Firms therefore find it optimal to increase their investments under a joint (welfare) decision. Similar reasoning applies for the insurance level as well.

5.2. Mechanisms to Increase Firms' Investments and Insurance Coverage

The obvious question now is whether a social planner such as a government, regulatory body, or trade associations can induce firms to invest at the socially optimal level through mechanisms that mimic joint decision-making. Two such mechanisms are government-mandated fines on the liable firms, and information sharing arrangements to diffuse information about a security breach quickly.

5.2.1 Liability and Fine

Fine for liability is a commonly used mechanism to encourage desirable or discourage undesirable behavior. In this mechanism, the liable firm compensates for damages caused to other firms because of its negligence. Similar mechanisms have been analyzed in the contexts of fire prevention, airline security, and system reliability (Orszag and Stiglitz 2002, Kunreuther and Heal 2003, Varian 2002).

Consider the 2-interdependent firm case analyzed before. Now if an indirect attack occurs to the firm 1, firm 2 pays the full loss (L) to firm 1, and the insurance firm compensates firm 2 an amount I. There are 2 possible scenarios in which, say firm 1, incurs a loss. In scenario 1, firm 1 is attacked directly, and firm 2 is attacked indirectly through firm 1. In this situation, firm 1 not only incurs its own loss, but is also liable for the loss to firm 2. The probability of this event is $qp(z_1)(1-p(z_2))$. In scenario 2, firm 1 is directly attacked, but this attack does not be spread to firm 2. The probability of this event is $p(z_1)-qp(z_1)(1-p(z_2))$. Firm 1 does not incur any loss if it is indirectly attacked through firm 2 (because firm 2 will compensate it), and if there is no attack on firm 1. Therefore, the expected utility of firm 1 is

$$\begin{aligned} &qp(z_1)(1-p(z_2))U(W-2L+2I_1-\pi(z_1,z_2)I_1-z_1)+ \\ &\left[p(z_1)-qp(z_1)(1-p(z_2))\right]U(W-L+I_1-\pi(z_1,z_2)I_1-z_1)+ \\ &(1-p(z_1))U(W-\pi(z_1,z_2)I_1-z_1) \end{aligned} \tag{16}$$

where $\pi(z_1,z_2)=(1+\lambda)\left\{2qp(z_1)(1-p(z_2))+\left[p(z_1)-qp(z_1)(1-p(z_2))\right]\right\}$. For symmetric firms, the level of IT security investment will be the solution to the following equation.

$$\left[p'(z)+qp'(z)-qp'(z)p(z)\right]=-\frac{1}{(1+\lambda)L}+\frac{K}{L} \tag{17}$$

where $K=(1+\frac{\partial\pi(z,z)}{\partial z}I)\frac{\left[p(z)-qp(z)(1-p(z))\right]}{\pi(z,z)}\left[r(L-I)\right]>0$.

Proposition 6: (i) IT security investment level is higher with liability than without when firms maximize their individual utility (ii) IT security investment level with liability is higher than social optimum level of IT security investment without liability.

{See proof 12 in the appendix}

The intuition for Proposition 6 can be illustrated using Figure 3. Consider the overall system (both firms) risk given in Figure 3. Without liability, when firms make investment decisions in self-interest, the marginal efficiency of investments for firm 1 and firm 2 is the reduction in sizes of regions I and IV by a unit investment respectively (Figure 3). In the no liability case, when firms maximize joint utility, the marginal efficiency of investment for firm 1 and firm 2 is the reduction in sizes of regions (I+VI) and (IV+III) by a unit investment respectively. In the liability case, the marginal efficiency for firm 1 and firm 2 is the reduction

in sizes of regions (I+II+VI) and (III+ IV+V) by a unit investment respectively. The efficiency of investment is highest in the liability case followed by the joint utility maximization (no liability) case, followed by the individual utility maximization (no liability) case. Because higher marginal efficiency of investment results in a higher level of investment, proposition 6 follows.

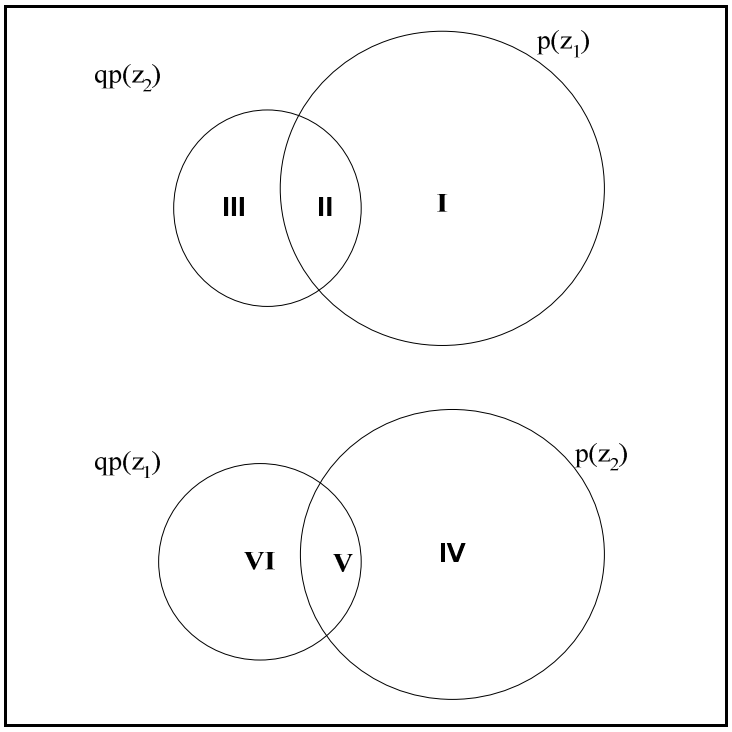


Figure 3: An illustration of the effect of liability on firms

Liability for loss to other firms makes firms over-invest in security compared to the socially optimal level. This is because liability forces each firm to minimize the risk it can control even though some portions of the risk are controlled by investments of both firms. Consequently, firms do not minimize the joint risk jointly, and they do not account for the effect the other firm's action on their own risk. Partial rather than full liability to the responsible firm remedies the over-investment problem. Because identifying the nature of attack, direct or indirect, and assigning blame on the responsible party is difficult in the cyber environment (Sagalow et al 2002), we analyze another mechanism, information sharing, that could alleviate externality associated with interdependency.

5.2.2 Information Sharing

Information sharing is touted as a "panacea" for hazard management problems (Farber 2004). For instance, the primary goal of federal agencies in the US such as the Department of Homeland Security, the Center for Disease Control, and the National Weather Bureau is to collect information from several sources, analyze and disseminate information to prevent or reduce damage from catastrophic events. The Center for Emergency Response Team (CERT) at Carnegie Mellon University plays a similar role in disseminating IT security information. Research in the IT security area has also investigated the impact of information sharing policies in different contexts (Gordon et al 2003, Gal-Or and Ghose 2003). For instance, Gordon et al. assumed that sharing of security information is equivalent to an increase in a firm's investment and showed that information sharing might actually reduce firms' incentives to invest in security. CERT's vulnerability disclosure policies have also been analyzed (Arora, Tealnd and Xu 2004, Cavusoglu, Cavusoglu and Raghunathan 2004). CERT (i) educates users about security vulnerabilities so that they can implement measures to prevent security breaches, and (ii) informs users about how to reduce damages and recover from security breaches such as virus attacks. The former reduces the probability of breach, p and the rate of spread of security attacks, q. The latter reduces the damage, L, from attacks. To analyze how a reduction in p or q enabled by information sharing affects firms' strategies, we analyze two models. First, information sharing affects the probability of breach but has no effect on the degree of interdependency. Second, information sharing affects the degree of interdependency but has no effect on the probability of breach.

Information sharing reduces direct attack probability, but not interdependency

Sharing of security best practices between firms enhances the effectiveness of IT security investments. Accordingly, we assume that the probability of direct attack will be lower with information sharing than without information sharing. if $p_i^I(z_i)$ and $p_i^N(z_i)$ represent the probability of direct attack on firm i when it makes an investment of z_i (the superscript I and N respectively stand for the information sharing and no-information sharing cases), then $p_i^I(z) < p_i^N(z)$. Assume that the marginal benefit from security investment is greater with information sharing, i.e., $p_i^{I'}(z) \le p_i^{N'}(z)$. Using an analysis similar to the one presented for the no-information sharing case in Section 4.2, the following optimal solution obtains for two identical firms.

$$p^{I'}\left(z^{I*}\right)\left(1-qp^{I}\left(z^{I*}\right)\right)=-\frac{1}{(1+\lambda)L} \tag{18}$$

Comparing (18) with (9) and noting that $p^{I'}(z)\left(1-qp^{I}(z)\right)<p^{N'}(z)\left(1-qp^{N}(z)\right)$, yields $z^{I*}>z^{N*}$. Similarly, the insurance coverage is also higher under information sharing than no-information sharing.

Information sharing reduces interdependency, not direct attack probability

In this case, the central agency informs firms on how to protect themselves from attacks propagated from other firms. Let q^{I} and q^{N} represent the probability of an indirect attack on a firm through another firm, so that, $q^{I} < q^{N}$. The results are similar to that of the no-information sharing scenario. Replacing the degree of interdependency to q^{I} in equations (9) and (10) gives the solution for the information sharing case. Because $q^{I} < q^{N}$, using Proposition 2(i), we can readily infer that $z^{I*}>z^{N*}$ and $I^{I*}>I^{N*}$.

In the extreme case of the information sharing agent disseminating information about an attack and how to staunch spread of this attack to other firms, and all firms following the advice of the information sharing agency instantaneously, interdependency is completely eliminated. That is, q^{I} becomes zero. When $q^{I} = 0$, individual firm's decisions are identical to the socially optimal decisions. The technology that has the ability to disseminate information about attacks instantaneously to the world can eliminate the negative effects of interconnections while retaining their positive contributions.

6. Model Extension: *n* Interdependent Firms

In the previous sections, the analysis used two firms for tractability. The principal result about the effect of interdependency easily extends to the *n* firm case. Consider *n* symmetric fully interconnected firms. That is, each firm is directly connected to every other firm. Further, consider only the first-order indirect attacks for tractability. That is, although the possibility of indirect attack on a firm from any of its neighbors when they are directly attacked is included in the model, indirect attacks caused by indirect attacks on neighbors are excluded. This assumption is reasonable when q is small. Without loss of generality, consider only the probability of breach of firm 1:

$$B_1(z_1,z_2,...,z_n)=1-\left[1-p(z_1)\right]\left[1-qp(z_2)\right]...\left[1-qp(z_n)\right].$$

The second term on the RHS is the probability that neither direct nor indirect breach occurs Thus

$$\pi(z_1 : z_2,...,z_n) = [1+\lambda]B_1(z_1, z_2,..., z_n) = [1+\lambda]\left(1-\left[1-p(z_1)\right]\left[1-qp(z_2)\right]...\left[1-qp(z_n)\right]\right) \quad (19)$$

Firm 1 solves the following maximization problem:

$$\max_{z_1,\, I_1} B_1 U_j\left(W - L + [1-\pi_1]I_1 - z_1\right) + [1-B_1]U_j\left(W - \pi_1 I_1 - z_1\right). \quad (20)$$

The optimal level of IT security investment and amount of insurance coverage respectively are

$$p'(z)\left[1-qp(z)\right]^{n-1} = -\frac{1}{[1+\lambda]L}, \quad (21)$$

$$r[L-I] = \frac{\lambda}{[1+\lambda]\left[1-p(z)\right]\left[1-qp(z)\right]^{n-1}}. \quad (22)$$

Proposition 6: For n identical firms,

(i) As interdependency increases, IT security investment decreases and insurance coverage decreases or remains the same. That is, $\frac{\partial z}{\partial q} < 0, \frac{\partial I}{\partial q} \le 0$.

(ii) As the number of firms (n) increases, IT security investment level by individual firm and insurance coverage decreases or remains the same, That is, $\frac{\partial z}{\partial n} < 0$, $\frac{\partial I}{\partial n} \le 0$.

{See proof 13 in the appendix.}

Comparing proposition 6 and propositions 1 and 2, we find that the effect of degree of interdependency does not change qualitatively in the *n*-firm case from the 2-firm case. Further, the effect of number of firms on firms' strategies is qualitatively similar to that of degree of interdependence in the 2-firm case. This is because the degree of interdependence and the number of firms affect investment efficiency and insurance price in the same way. In the 2-firm case, an increase in interdependency reduces investment efficiency and increases insurance price. In the *n*-firm case, an increase in the number of firms for a given level of interdependency has the same effect.

7. Conclusions

IT security researchers have focused primarily on providing technology based solutions or products to deal with security risks. While IT security products help in managing security risk, firms' incentives to invest in these products are governed by several factors. In this paper, we analyzed firms' IT security risk management strategies when their risks are interdependent. Interdependency of security risks arises because physical and

logical interconnections of computers across different firms have the ability to pass on harmful communication and software such as viruses and worms from one firm to another. We showed that interdependence of cyber-risk reduces firms' incentives to invest in security technologies and to buy insurance coverage. Further, a higher degree of interdependence reduces the incentive to invest in self-protection and to buy more cyber-insurance. The conventional wisdom that firms are reluctant to buy cyber insurance because insurance market is immature is not correct. A more developed insurance market may not increase firms' insurance coverage unless the development in insurance market reduces the price of insurance. We found that that a more mature insurance market may not necessarily result in lower insurance price because firms use insurance rather than investment to manage security risk in a mature insurance market, which increases the insurers' risk. Because interdependency reduces firms' incentives to manage IT security at a socially optimal level, social planners may find mechanisms such as information sharing and fines to be useful in inducing firms to increase their incentives.

As with any analytical model, our model has several limitations and offers different avenues for extensions. We assumed that security investments affect only the probability of direct attack. The loss when a security breach occurs and the probability of indirect attack are exogenously determined in our model. A more general model will have a firm making separate investment decisions for different dimensions of risk. An analysis of such a model will provide us insights into the interaction, e.g., substitution and complementary effects, among these investments. As we stated in Section 3, we modeled only the interdependency that arises because of interconnections of computers in different firms, but not the interdependency that stems from hacker behavior. A more complete model should incorporate the strategic interaction between firms and hackers.

References

1. Arora A., Telang R. and Xu H., "Timing Disclosure of Software Vulnerability for Optimal Social Welfare," Carnegie Mellon University working paper, April 2004
2. Anderson, R., "Why Information Security is Hard: A Economic Perspective," Cambridge University working paper, 2003.
3. Ayres, L., and Levitt S.D., "Measuring positive externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack," *Quarterly Journal of Economics*, vol 113, 1998, pg. 43-77.

4. Axelsson S., Research in Intrusion Detection Systems: A Survey, Technical Report No 98-17, Dept. of Computer Engineering, Chalmers University of Technology, Sweden, Aug. 19, 1999

5. Beattie, S., Cowan C., Wagle P., and Wright C., Timing the Application of Security Patches for Optimal Uptime. Proceedings of LISA 2002: 16th Systems Administration Conference, Philadelphia, PA, 2002

6. Baer W., "Rewarding IT Security in the Marketplace", accessed at http://tprc.org/papers/2003/190/BaerITSecurity.pdf

7. Camp, L.J., and Wolfram C., "Pricing Security," accessed at www.ljean.com/files/isw.pdf.

8. Cavusoglu, H., Cavusoglu, H., and Raghunathan, S., How should we disclose software vulnerabilities, *Proceedings of Workshop on Information Technology and Systems*, December 2004, pg. 243-248.

9. Cavusoglu, H., and Raghunathan S., Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches, *INFORMS Journal on Decision Analysis*, Vol. 1, No. 3, September 2004, pg. 131-148

10. Cavusoglu, H., Mishra, B., and Raghunathan S., A Framework for Evaluating IT Security Investments, *Communications of the ACM,* Vol. 47, No. 7, July 2004, pg. 87-92

11. Cavusoglu, H., Mishra, B., Raghunathan, S., The Value of Intrusion Detection Systems (IDSs) in Information Technology (IT) Security, *Information Systems Research*, 2005, Forthcoming

12. CERT (Computer Emergency and Response Team), *Detecting Sings of Intrusion*, CERT Security Improvement Modules, 2000.

13. Cheswick W., Bellovin S., and Rubin A., Firewalls and Internet Security: Repelling The Wily Hacker, Addison-Wesley, Boston, MA, 2003

14. Claflin, B., "Information Risk Management at 3Com," Secure Business Quarterly, Vol. 1, Iss. 2, 2001

15. Computerworld, "Update: Money seen as the biggest obstacle to effective IT security," July 16, 2003.

16. Counterpane Inc, www.counterpane.com/pr-lloydswp.html.

17. Dionne, G., and Harrington S.E., "An Introduction to Insurance Economics," *Foundations in Insurance Economics*, Kluwer Academic Publishers, Boston MA, 1992, pg. 1-47..

18. D'Aqostino, D, "Insuring Security," www.cioinsight.com/article2/0,1397,1216110,00.asp, accessed June 2004.

19. Doll, M., *Security & Technology Solutions: The 2002 Ernst & Young Digital Security Overview: An Executive Guide and Diagnostic*, Ernst & Young LLP, 2002.

20. Ehrlich, I., and G. S. Becker, Market Insurance, Self-Insurance, and Self-Protection *Journal of Political Economy,* Vol. 80,No. 4,1972, pg. 623-648.

21. Farber D., Information sharing is key to thwarting cyber attacks, http://techupdate.zdnet.com/techupdate/stories/main/Information_sharing_is_key_to_thwarting_cyber_attacks.html, February 25 2004

22. Gal-Or, E., Ghose, A., 2003. The economic consequences of sharing security information. In: Proceedings of the Second *Workshop on Economics and Information Security*.

23. Geer D., Bace R., Gutmann P., Metzger P., Pfleeger C., Querterman J., Scheier B., "Cyber Insecurity: The Cost of Monopoly How the Dominance of Microsoft's Product Poses a Risk to Security" accessed at www.ccianet.org/papers/cyberinsecurity.pdf

24. Gordon, L.A., and Loeb M.P., The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, Vol. 5, No. 4, November 2002, pg. 438-457.

25. Gordon, L.A., and Loeb M.P., "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, November 2002, pg. 438-457.

26. Gordon, L. A., Loeb, M. P., and Sohail T., "A Framework for using insurance for cyber-risk management," *Communications of the ACM*, 44, 9, March 2003, pp. 70-75.

27. Hoo, K. J. S. "How Much Security is Enough: A Risk Management Approach to Computer Security" *Ph.D. Dissertation*, Stanford University, 2000.

28. Hulme, H., Businesses Keep Spending on Security, *InformationWeek*, 873, p. 96, January 2002.

29. Information Assurance Advisory Council, "Insuring Digital Risk: A Roadmap for Action," accessed at www.iaac.org.uk.

30. Insurance Journal, Risk Management Solutions: Response to Cyber Threats and Cyberterrorism, accessed at **www.insurancejournal.com/magazines/west/2004/02/23/features/37008.htm**

31. Karofsky, E., "Insights into Return on Security Investment," Secure Business Quarterly, Vol. 1, Iss. 2, 2001

32. Kovacs P., Markham M and Sweeting R., "Cyber-Incident Risk in Canada and the Role of Insurance" April 2004, ICLR Research Paper Series- No.38

33. Kunreuther, H., "The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage," *RISQUES*, forthcoming.

34. Kunreuther H., and Heal G. "Interdependent Security," *Journal of Risk and Uncertainty*, 26: 231-249,2003

35. Ladkawalla, D., and Zanjani, G., "Insurance, Self-protection, and the Economics of Terrorism," Working paper, November 2002.

36. Loch, K.D., Carr H.C., and Warkentin M.E., "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, June 1992, pg. 173-186.

37. Mendelson, H. and S. Whang. Optimal Incentive-Compatible Priority Pricing for the M/M/1 Queue. *Operations Research*. Vol: 38. (1990) pp. 870-883.

38. Niederman, F., Brancheau J.C., and Wetherbe J.C., "Information Systems Management Issues for the 1990s," *MIS Quarterly*, December 1991, pg. 475-502.

39. Orszag p. and Stiglitz J.,Optimal Fire Departments: Evaluating Public Policy in the Face of Externalities, The Brookings Institution, Jan. 4, 2002. www.brookings.edu/views/papers/orszag/20020104.htm

40. Power, R., "2002 CSI/FBI Computer Crime and Security Survey," *Computer Security Isssues and Trends*, 8, 1, 2002.

41. Pohlmann N and Crothers T., *Firewall Architecture for the Enterprise*, Wiley Publishing Inc., New York, 2002

42. Riggins, F.J., Kriebel, C.H. and Mukhopadhyay, T., "The Growth of Interorganizational Systems in the Presence of Network Externalities," *Management Science*, vol. 40, no. 8, pp. 894-998, August 1994.

43. Sagalow, T.R., and Hammesfahr R.W., "@Risk Version 2.0," A Reactions Publication, accessed at www.aignetadvantage.com/content/netad/ty_atrisk.pdf.

44. Straub, D.W., "Effective IS Security: An empirical study," *Information Systems Research*, vol. 1, no.3, 1990, pg. 255-276.

45. Straub, D.W., and Welke R.J., "Coping with Systems Risk: Security Planning Models for managerial Decision Making," *MIS Quarterly*, December 1998, pg. 441-469.

46. Szpiro, G.G., "Insurance, Risk Aversion, and Demand for Insurance," *Studies in Banking and Finance*, vol. 6, 1988, pg. 1-125.

47. Tirole J., The theory of Industrial Organization, The MIT Press, Cambridge, MA, 1988

48. Varian H., "System Reliability and Free Riding", Workshop on Economics and Information Security, 2002.

49. Wang E. and Seidmann, A., "Electronic Data Interchange: Competitive Externalities and Strategic Implementation Policies," Management Science, Vol. 41, No. 3, 401-418,1995

Appendix

Proof 1. Baseline scenario:

Objective based on the expected utility function of the firm is

$$\max_{z,\,I} \quad B(z)U_B\left(W-L+[1-\pi(z)]I-z\right)+\left[1-B(z)\right]U_N\left(W-\pi(z)I-z\right)$$

The first order condition for IT security investment is

$$B'(z)[U_B-U_N]-\left\{1+\frac{\partial\pi(z)}{\partial z}I\right\}\left[B(z)U_B'+\{1-B(z)\}U_N'\right]=0. \qquad \text{(A1)}$$

First order condition for insurance is

$$B(z)[1-\pi(z)]U_B'-\pi(z)\left[1-B(z)\right]U_N'=0. \qquad \text{(A2)}$$

Since $\pi(z)=B(z)$, from the latter condition we see that $U_B'=U_N'$ and *I=L*. That is, the marginal utilities in both states are equal. From the first condition,

$$B'(z)=-\frac{1}{L} \qquad \text{(A3)}$$

Proof 2. IT Security Spending with No Insurance Market

Utility function of the firm is

$$\max_{z}\ B(z)U_B\left(W-L-z\right)+\left(1-B(z)\right)U_N\left(W-z\right)$$

The first order condition for IT security investment is

$$B'(z)[U_B-U_N]-\left\{B(z)U_B'+\left(1-B(z)\right)U_N'\right\}=0$$

For W large enough, first order Taylor series approximation gives

$$U_N\approx U_B+U_B'L \qquad \text{(A4)}$$

$$-B'(z)U_B'L-\left\{B(z)U_B'+\left(1-B(z)\right)U_N'\right\}=0$$

$$B'(z)=-\frac{\left(B(z)+\left(1-B(z)\right)\frac{U_N'}{U_B'}\right)}{L}$$

since $\left(B(z)+\left(1-B(z)\right)\frac{U_N'}{U_B'}\right)<1$, IT security investment when insurance is available at fair market price is lower than IT security investment when there is no insurance market available.

Proof 3. Interdependent case:

Utility function of the firm 1 is

$$\max_{z_1,\,I_1} \quad B_1(z_1,z_2)U_{B1}\left(W-L+[1-\pi(z_1:z_2)]I_1-z_2\right)+\left[1-B(z_1,z_2)\right]U_{N1}\left(W-\pi(z_1:z_2)I_1-z_2\right)$$

where $B_1(z_1,z_2)=1-\left[\left(1-p(z_1)\right)\left(1-qp(z_2)\right)\right]$

The first order condition for IT security investment is

$$\frac{\partial B_1(z_1,z_2)}{\partial z_1}\left(U_{B1}-U_{N1}\right)-\left[1+\frac{\partial\pi(z_1,z_2)}{\partial z_1}I_1\right]\left\{B_1(z_1,z_2)U_{B1}'+\left[1-B_1(z_1,z_2)\right]U_{N1}'\right\}=0 \qquad \text{(A5)}$$

First order condition for insurance is

$$B_1(z_1,z_2)(1-\pi_1(z_1,z_2))U_{B1}'-(1-B_1(z_1,z_2))\pi_1(z_1,z_2)U_{N1}'=0$$

If $\lambda=0$, then *I=L* and $\frac{\partial B_1(z_1,z_2)}{\partial z_1}=p'(z_1)(1-qp(z_2))=-\frac{1}{L}$

If λ >0, for W large enough, using first order Taylor series approximation

$$U_{N1} \approx U_{B1} + U'_{B1}(L - I_1);\ U'_{N1} \approx U'_{B1} + U''_{B1}(L - I_1)$$

Substituting in A5, dividing by U'_{B1} and using first order condition for insurance

$$\frac{U'_{N1}}{U'_{B1}} = \frac{B_1(z_1, z_2)\left(1 - [1+\lambda]B_1(z_1, z_2)\right)}{[1+\lambda]\left(1 - B_1(z_1, z_2)\right)}$$

we get

$$\frac{\partial B_1(z_1, z_2)}{\partial z_1} = \frac{-1}{[1+\lambda]L}$$

and assuming the CARA utility function we get from the FOC for insurance

$$r[L - I_1] = \frac{\lambda}{[1+\lambda]\left[1 - p(z_1)\right]\left[1 - qp(z_2)\right]}$$

where $r = -\frac{U''}{U'}$ is a constant and greater than 0. Using identical firms,

$$p'(z)\left[1 - qp(z)\right] = -\frac{1}{[1+\lambda]L} \qquad \text{(A6)}$$

$$I = L - \frac{\lambda}{r[1+\lambda]\left[1 - p(z)\right]\left[1 - qp(z)\right]} \qquad \text{(A7)}$$

Proof 4: Condition for Unique Equilibrium

From the first order condition of IT security investment (A6),

$$\Pi_1^1\left(R_1(z_2), z_2\right) = p'(z_1)\left[1 - qp(z_2)\right] + \frac{1}{[1+\lambda]L} = 0$$

The slope of reaction function for Firm 1 and 2 is

$$R'_1(z_2) = -\frac{\Pi_{12}^1\left(R_1(z_2), z_2\right)}{\Pi_{11}^1\left(R_1(z_2), z_2\right)} = \frac{p''(z_1)\left(1 - qp(z_2)\right)}{p'(z_1)qp'(z_2)};\ R'_2(z_1) = -\frac{\Pi_{21}^2\left(R_2(z_1), z_1\right)}{\Pi_{22}^2\left(R_2(z_1), z_1\right)} = \frac{p'(z_1)qp'(z_2)}{p''(z_1)(1 - qp(z_2))}$$

In order for reaction curve to intersect, the slope of R_1 should be higher than the slope of R_2. So

$$\frac{p''(z_1)\left(1 - qp(z_2)\right)}{p'(z_1)qp'(z_2)} > \frac{p'(z_1)qp'(z_2)}{p''(z_1)(1 - qp(z_2))}.$$

cross-multiplying and rearranging

$$\left\{\left[p''(z_1)(1 - qp(z_2))\right] - \left[p'(z_1)qp'(z_2)\right]\right\}\left\{\left[p''(z_1)(1 - qp(z_2))\right] + \left[p'(z_1)qp'(z_2)\right]\right\} > 0$$

Note that the second term in the LHS multiplicand is positive. Hence for an unique equilibrium,

$$\left[p''(z_1)(1 - qp(z_2))\right] - \left[p'(z_1)qp'(z_2)\right] > 0$$

Assuming symmetric firms, the condition for unique equilibrium can be written as

$$\left[p''(z)(1 - qp(z))\right] - q\left[p'(z)\right]^2 > 0$$

Proof 5:

Denote the level of IT security investment and insurance coverage taken in independent firm and dependent firms as z^I and z^D respectively and I^I and I^D .

$$p'(z^I) = -\frac{1}{[1+\lambda]L};\ r\left[L - I^I\right] = \frac{\lambda}{[1+\lambda]\left[1 - p(z^I)\right]} \qquad \text{(A8(a,b))}$$

$$p'(z^D)\left[1 - qp(z^D)\right] = -\frac{1}{[1+\lambda]L};\ r\left[L - I^D\right] = \frac{\lambda}{[1+\lambda]\left[1 - p(z^D)\right]\left[1 - qp(z^D)\right]} \qquad \text{(A9(a,b))}$$

Dividing A8a and A9a,

$$p'(z^I) = p'(z^D)\left[1 - qp(z^D)\right];\ p'(z^I) > p'(z^D) \Rightarrow z^I > z^D$$

If λ>0, dividing A8b and A9b,

$$\frac{\left[L-I^I\right]}{\left[L-I^D\right]}=\frac{\left[1-p\left(z^D\right)\right]\left[1-qp\left(z^D\right)\right]}{\left[1-p\left(z^I\right)\right]}$$

$$z^I>z^D \Rightarrow \left[1-p\left(z^I\right)\right]>\left[1-p\left(z^D\right)\right];\ \frac{\left[L-I^I\right]}{\left[L-I^D\right]}<1 \text{ or } I^I>I^D \text{ (if } \lambda=0,\ I^I=I^D\text{)}.$$

Proof 6:

$$\frac{\partial z}{\partial q}=\frac{p(z)\,p'(z)}{p''(z)\left[1-qp(z)\right]-p'(z)qp'(z)}<0 \quad \text{since denominator is less than zero.}$$

$$\text{(i) } \frac{\partial I}{\partial z}=-\frac{\lambda p'(z)\left[1+q-2qp(z)\right]}{[1+\lambda]r\left[1-p(z)\right]^2\left[1-qp(z)\right]^2}>0$$

$$\frac{\partial I}{\partial z}\frac{\partial z}{\partial q}=\frac{\lambda p'(z)\left[1+q-2qp(z)\right]}{[1+\lambda]r\left[1-p(z)\right]^2\left[1-qp(z)\right]^2}\frac{p(z)\,p'(z)}{\left\{p''(z)\left[1-qp(z)\right]-p'(z)qp'(z)\right\}}\le 0$$

$$\text{(ii) } \frac{\partial z}{\partial L}=\frac{1}{[1+\lambda]L^2\left[p''(z)\left(1-qp(z)\right)-p'(z)qp'(z)\right]}>0$$

$$\frac{\partial I}{\partial L}+\frac{\partial I}{\partial z}\frac{\partial z}{\partial L}=1-\frac{\lambda p'(z)\left[1+q-2qp(z)\right]}{[1+\lambda]r\left[1-p(z)\right]^2\left[1-qp(z)\right]^2}\frac{}{[1+\lambda]L^2\left[p''(z)\left(1-qp(z)\right)-p'(z)qp'(z)\right]}>0$$

$$\text{(iii) } \frac{\partial z}{\partial r}=0, \qquad \frac{\partial I}{\partial r}=\frac{\lambda}{r^2(1+\lambda)\left(1-p(z)\right)\left(1-qp(z)\right)}\ge 0$$

Proof 7:

$$\frac{\partial \pi}{\partial q}=(1+\lambda)\frac{\partial B}{\partial z}\frac{\partial z}{\partial q},\ B(z)=1-\left[1-qp(z)\right]\left[1-p(z)\right],\ \frac{\partial B}{\partial z}=p'(z)\left[1+q-2qp(z)\right]<0 \text{ and}$$

$$\frac{\partial z}{\partial q}<0 \text{ from proposition 2 (i): As a result, } \frac{\partial \pi}{\partial q}>0$$

Proof 8:

$$\frac{\partial z}{\partial \lambda}=\frac{1}{[1+\lambda]^2L\left\{p''(z)\left(1-qp(z)\right)-p'(z)qp'(z)\right\}}>0$$

$$\frac{\partial I}{\partial \lambda}=\frac{\partial I}{\partial z}\frac{\partial z}{\partial \lambda}+\frac{\partial I}{\partial \lambda}=-\frac{\lambda p'(z)\left[1+q-2qp(z)\right]}{[1+\lambda]r\left[1-p(z)\right]^2\left[1-qp(z)\right]^2}\frac{}{[1+\lambda]^2L\left\{p''(z)\left(1-qp(z)\right)-p'(z)qp'(z)\right\}}$$

$$-\frac{1}{\left[1-p(z)\right]\left[1-qp(z)\right]r[1+\lambda]^2}$$

$$=\frac{1}{\left[1-p(z)\right]\left[1-qp(z)\right]r[1+\lambda]^2}\left[-\frac{\lambda p'(z)\left[1+q-2qp(z)\right]}{(1+\lambda)\left[1-p(z)\right]\left[1-qp(z)\right]L\left\{p''(z)\left[1-qp(z)\right]-p'(z)qp'(z)\right\}}-1\right]$$

Denote $\lambda^*=-\dfrac{p'(z)\left[1+q-2qp(z)\right]}{\left[1-p(z)\right]\left[1-qp(z)\right]L\left\{p''(z)\left[1-qp(z)\right]-p'(z)qp'(z)\right\}}>0$

$$\frac{\partial I}{\partial \lambda}=\frac{1}{\left[1-p(z)\right]\left[1-qp(z)\right]r[1+\lambda]^2}\left[\frac{\lambda\lambda^*}{(1+\lambda)}-1\right]. \text{ If } \lambda>\frac{1}{\lambda^*-1},\ \frac{\partial I}{\partial \lambda}>0, \text{ else } \frac{\partial I}{\partial \lambda}<0.$$

Proof 9:

$$I=L-\frac{\lambda}{r(1+\lambda)\left[1-p(z)\right]\left[1-qp(z)\right]}=L-\frac{\lambda}{r(1+\lambda)[1-B(z)]}=L-\frac{\lambda}{r\left(1+\lambda-\pi(z)\right)}$$

$$\frac{\partial \pi(z)}{\partial \lambda} = B(z) + (1+\lambda)\frac{\partial B}{\partial z}\frac{\partial z}{\partial \lambda}$$

$$\frac{\partial I}{\partial \lambda} = -\frac{\partial\left(\frac{\lambda}{(1+\lambda-\pi(z))}\right)}{\partial \lambda} = -\frac{1-\pi(z)+\lambda\frac{\partial \pi(z)}{\partial \lambda}}{(1-\lambda-\pi(z))^2}$$

We know that insured amount will greater than premium paid.(i.e. $(1-\pi(z)>0)$As a result, if $\frac{\partial \pi(z)}{\partial \lambda}>0$, $\frac{\partial I}{\partial \lambda}<0$.

If loading factor increases, insurance coverage will decreases if price of insurance (π(z)) increases as well.

$$\frac{\partial \pi(z)}{\partial \lambda} = B(z) + (1+\lambda)\frac{\partial B}{\partial z}\frac{\partial z}{\partial \lambda} > 0 \text{ (if } \lambda > \frac{-\frac{\partial B}{\partial z}\frac{\partial z}{\partial \lambda}}{B(z)} - 1 = \lambda^{**} \text{ , } \frac{\partial \pi(z)}{\partial \lambda} > 0 \text{).}$$

Proof 10:

In region 1; $p'(z_1) = \frac{-1}{L}$, $I_1 = L$. In region 2; $p'(z_2) = \frac{-1}{(1+\lambda)L}$, $r(L-I_2) = \frac{\lambda}{(1+\lambda)\left[1-p(z_2)\right]}$. In region 3;

$p'(z_3) = \frac{-1}{L(1-qp(z_3))}$, $I_3 = L$. In region 4, $p'(z_4) = \frac{-1}{L(1+\lambda)(1-qp(z_4))}$,

$r(L-I_4) = \frac{\lambda}{(1+\lambda)\left[1-p(z_4)\right]\left[1-qp(z_4)\right]}$

$z_1 > z_3$, $z_2 > z_4$, $z_2 > z_1$ and since $\frac{\partial z}{\partial \lambda} > 0$, $z_4 > z_3$.

As a result, $z_2 > z_4, z_1 > z_3$. For the insurance amount, since $z_2 > z_4$, $I_1 = I_3 > I_2 > I_4$. Traditional Insurance Market (q=0 , λ=0) versus Current cyber insurance market. We will compare IT security investment level in region 4 and in region 1. For cyber insurance coverage taken $L = I_1 > I_4$. For the IT security investment,

$$\frac{p'(z_1)}{p'(z_4)} = \left[1+\lambda\right]\left[1-qp(z_4)\right] \text{ .}$$

If $\left[1+\lambda\right]\left[1-qp(z_4)\right]=1$, then $z_1 = z_4$.

If $\left[1+\lambda\right]\left[1-qp(z_4)\right]<1 \Rightarrow p'(z_1) > p'(z_4) \Rightarrow z_1 > z_4$

If $\left[1+\lambda\right]\left[1-qp(z_4)\right]>1 \Rightarrow p'(z_1) < p'(z_4) \Rightarrow z_1 < z_4$

Proof 11: Joint decision-making solution

Suppose that there are two firms; firm 1 and firm 2. Social planner will maximize the following

$B_1U_{B1}(W-L+(1-\pi_1)I_1-z_1)+(1-B_1)U_{N1}(W-\pi_1 I_1-z_1)+B_2U_{B2}(W-L+(1-\pi_2)I_2-z_2)+(1-B_2)U_{N2}(W-\pi_2 I_2-z_2)$

where $B_1 = 1-\left[(1-p(z_1))(1-qp(z_2))\right]$, $B_2 = 1-\left[(1-p(z_2))(1-qp(z_1))\right]$ and $\pi_1 = (1+\lambda)B_1$

FOC for self protection with respect to z_1;

$$\frac{\partial B_1}{\partial z_1}(U_{B1}-U_{N1})-\left[B_1U'_{B1}+(1-B_1)U'_{N1}\right]\left(1+\frac{\partial \pi_1}{\partial z_1}I_1\right)+\frac{\partial B_2}{\partial z_1}(U_{B2}-U_{N2})-\left[B_2U'_{B2}+(1-B_2)U'_{N2}\right]\left(\frac{\partial \pi_2}{\partial z_1}I_2\right)=0$$

FOC for insurance is;

$$B_1(1-\pi_1)U'_{B1}-(1-B_1)\pi_1U'_{N1}=0$$

Taylor 1st order approximation yields as before

$$\frac{\partial B_1}{\partial z_1}(I_1-L)-\left[B_1+(1-B_1)\frac{U'_{N1}}{U'_{B1}}\right]\left(1+\frac{\partial \pi_1}{\partial z_1}I_1\right)+\frac{\partial B_2}{\partial z_1}\left((I_2-L)\frac{U'_{B2}}{U'_{B1}}\right)-\left[B_1\frac{U'_{B2}}{U'_{B1}}+(1-B_1)\frac{U'_{N2}}{U'_{B1}}\right]\left(\frac{\partial \pi_2}{\partial z_1}I_2\right)=0$$

For identical agent, $U_{B1}=U_{B2}=U_B$ and $U_{N1}=U_{N2}=U_N$ and since $\frac{(1-(1+\lambda)B)}{(1-B)[1+\lambda]}=\frac{U'_N}{U'_B}$

$$p'(z)\left(1+q-2qp(z)\right)=-\frac{1}{(1+\lambda)L}$$

The above equation can be written as $p'(z)\left(1-qp(z)\right)+M=-\frac{1}{(1+\lambda)L}$; $M'=p'(z)\left(q-qp(z)\right)\le 0$

Comparing with individual firm's first order condition

$p'(z)\left(1-qp(z)\right)+M=-\frac{1}{(1+\lambda)L}$ where M=0 and since $\frac{\partial z}{\partial M}<0$.

Proof 12:

Utility of firm 1 will be

$qp(z_1)(1-p(z_2))U_A\left(W-2L+2I_1-\pi(z_1,z_2)I_1-z_1\right)+$

$\left[p(z_1)-qp(z_1)(1-p(z_2))\right]U_B\left(W-L+I_1-\pi(z_1,z_2)I_1-z_1\right)+(1-p(z_1))U_C\left(W-\pi(z_1,z_2)I_1-z_1\right)$

First order condition with respect to z_1

$qp'(z_1)(1-p(z_2))U_A+\left[p'(z_1)-qp'(z_1)(1-p(z_2))\right]U_B-p'(z_1)U_C$

$-(1+\frac{\partial\pi(z_1,z_2)}{\partial z_1}I_1)\left[qp(z_1)(1-p(z_2))U_A'+\left[p(z_1)-qp(z_1)(1-p(z_2))\right]U_B'+(1-p(z_1))U_C'\right]=0$

First order condition with respect to I_1

$\left(2-\pi(z_1,z_2)\right)qp(z_1)(1-p(z_2))U_A'+\left(1-\pi(z_1,z_2)\right)\left[p(z_1)-qp(z_1)(1-p(z_2))\right]U_B'-(1-p(z_1))\pi(z_1,z_2)U_C'=0$

Following first order Taylor series approximation,

$U_B\approx U_A+U_A'(L-I)$, $U_C\approx U_A+2U_A'(L-I)$ and $U_B'\approx U_A'+U_A''(L-I)$.

From first order condition with respect to I_1 and replacing $(1-p(z_1))U_C'$ in first order condition,

$\left[p'(z_1)-qp'(z_1)(1-p(z_2))\right]U_A'(L-I)-p'(z_1)2U_A'(L-I)$

$-(1+\frac{\partial\pi(z_1,z_2)}{\partial z_1}I_1)\left[\frac{2qp(z_1)(1-p(z_2))}{\pi(z_1,z_2)}U_A'+\frac{\left[p(z_1)-qp(z_1)(1-p(z_2))\right]}{\pi(z_1,z_2)}U_B'\right]=0$

Substituting the Taylor approximation, dividing by U_A', and since , and for symmetric firms,

$\left[p'(z)+qp'(z)-qp'(z)\,p(z)\right]=-\frac{1}{(1+\lambda)L}+K$, where $K=\frac{(1+\frac{\partial\pi(z,z)}{\partial z}I)\frac{\left[p(z)-qp(z)(1-p(z))\right]}{\pi(z,z)}\left[r(L-I)\right]}{L}>0$

The equation above can be written as $\left[p'(z)-qp'(z)\,p(z)\right]-K'=\frac{-1}{[1+\lambda]L}$, where $K'=K-qp'(z)>0$

For the individual choice of z earlier K'=0.From the previous equation $\frac{\partial z}{\partial K'}=\frac{1}{p''(z)\left[1-qp(z)\right]-qp'(z)\,p'(z)}>0$

As a result IT security investment with liability is greater than without liability. The equation above can be written as

$p'(z)\left[1+q-2qp(z)\right]-K''=\frac{-1}{[1+\lambda]L}$ where $K''=K-qp'(z)\,p(z)>0$.

For the joint choice of z earlier, K''=0. Thus, from the last equation

$$\frac{\partial z}{\partial K''}=\frac{1}{p''(z)\left[1+q-2qp(z)\right]-2qp'(z)\,p'(z)}>0$$

IT security investment level with liability is higher than social optimum level of IT security investment without liability.

Proof 13: Generalization to Several Interdependent Firms

Proof is omitted due to space limitation. However, proof is available from authors upon request.