Risk Analysis, Vol. 31, No. 3, 2011 DOI: 10.1111/j.1539-6924.2010.01478.x

Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection

Hulisi Öğüt,[1,*] Srinivasan Raghunathan,[2] and Nirup Menon[3]

The correlated nature of security breach risks, the imperfect ability to prove loss from a breach to an insurer, and the inability of insurers and external agents to observe firms' self-protection efforts have posed significant challenges to cyber security risk management. Our analysis finds that a firm invests less than the social optimal levels in self-protection and in insurance when risks are correlated and the ability to prove loss is imperfect. We find that the appropriate social intervention policy to induce a firm to invest at socially optimal levels depends on whether insurers can verify a firm's self-protection levels. If self-protection of a firm is observable to an insurer so that it can design a contract that is contingent on the self-protection level, then self-protection and insurance behave as complements. In this case, a social planner can induce a firm to choose the socially optimal self-protection and insurance levels by offering a subsidy on self-protection. We also find that providing a subsidy on insurance does not provide a similar inducement to a firm. If self-protection of a firm is not observable to an insurer, then self-protection and insurance behave as substitutes. In this case, a social planner should tax the insurance premium to achieve socially optimal results. The results of our analysis hold regardless of whether the insurance market is perfectly competitive or not, implying that solely reforming the currently imperfect insurance market is insufficient to achieve the efficient outcome in cyber security risk management.

KEY WORDS: Cyber security; insurance; risk management

1. INTRODUCTION

Managing information security risk, also known as cyber security risk, is challenging to firms and policymakers for several reasons. First, individual firms, whose sensitive information needs protection, share correlated risks due to common technologies and computer interconnectivity. Firms conduct their business through shared public networks, such as the Internet, which computer hackers use to propagate security breaches. In addition, the information technology infrastructure of firms is dominated by a few technologies, which expose many firms to the same vulnerabilities, leading to correlated risks.

Second, when the risk becomes reality and the security of a firm is breached, it is often unable to prove its loss from the breach to an insurance company. Consequently, it is unable to justify its claim for an insurance payout from the insurer that matches the loss. In addition to tangible losses incurred from a breach, a significant portion of the loss is intangible, such as loss of reputation, goodwill, and

[1]TOBB University of Economics, Ankara, Turkey.
[2]School of Management, University of Texas at Dallas, Richardson, TX, USA.
[3]School of Management, George Mason University, Fairfax, VA, USA.
[*]Address correspondence to Hulisi Öğüt, TOBB University of Economics, Sogutozu Cad. No. 43, Ankara, Turkey 06560; tel: 90-312-292-4218; fax: 90-312-292-41043 hogut@etu.edu.tr.

competitive intelligence.[1,2] This exacerbates the inability of a firm to receive compensation for the total losses from a breach. Another reason why a firm does not expect to receive full compensation from insurers for the losses from security breaches is that firms often fail to detect intrusions.[3] Managers are aware of their failure to detect breaches. A recent survey of information security professionals found that the perceived probability of detecting a large data breach (10,000 or more records) is 68%, and the perceived probability of detecting a small data breach (100 or fewer records) is 51%.[2]

Third, external parties, such as insurance companies and government agencies, are not able to fully observe a firm's self-protection efforts. Firms do not reveal their security efforts to anyone just in case the information gets in the hands of malcontents who are able to find security loopholes.

The purpose of this article is to examine the role of correlated risks and "unprovable losses" in self-protection and insurance coverage of firms from a public policy perspective. The need to secure national infrastructures is gaining prominence around the world. This work elucidates the impact of intervention by policymakers, such as a government or its agencies, in the cyber security and cyber insurance markets. We do this by first identifying the effect of correlated risks and imperfect ability to prove loss on firm's protection and insurance strategies. We use insights obtained from this analysis to examine how the interventions chosen by the government would affect the welfare of the firms involved. The interventions considered herein are: (1) requirement of disclosure of self-protection security efforts by all firms, that is, make security effort publicly observable, (2) provision of subsidies to firms based on security spending, and (3) imposition of a "sales" tax on insurance premium. The mathematical models examined in this article compare different combinations of interventions and public policies to provide insights into cyber security risk management.

Our results show that risk correlation and unprovable loss cause a firm to invest less in self-protection, compared to the socially optimal level, regardless of whether self-protection is observable by the insurer or not. Furthermore, a firm does not also buy the socially optimal insurance coverage because of risk correlation and imperfect proof of loss. Subsidizing self-protection and taxing insurance premiums improve risk management decisions of a firm. When the self-protection of firms is observable, a social planner could subsidize self-protection, whereas when self-protection is not observable, the government should tax insurance. Two different policy interventions arise because self-protection and insurance behave as complements when self-protection is observable and as substitutes when self-protection is not observable.

The rest of the article is organized as follows. We briefly summarize the relevant literature on risk management and insurance in the next section. In Section 3, we describe the model framework. In Section 4, we derive and discuss the results when insurers can observe firms' self-protection. In Section 5, we analyze the case when insurers cannot observe firms' self-protection levels. In Section 6, we show that our results are robust to model variations. We conclude the article with implications and a discussion of limitations of our model in Section 7.

2. RELEVANT LITERATURE

The risk analysis and insurance literature is extensive, and so we discuss only the literature most closely related to our work.[4] Ehrlich and Becker[5] and Rothschild and Stiglitz[6] are two of the seminal papers that consider both self-protection and insurance. The former paper showed that self-protection and insurance behave as complements, assuming that firms' risks are uncorrelated and that firms can prove their loss to an insurer. Rothschild and Stiglitz[6] studied the adverse selection problem associated with a heterogeneous risk population, and showed that low-risk individuals are worse off than they would be in the absence of high-risk individuals, thus exhibiting negative externalities. See Dionne and Harrington[7] for a review of literature in the self-protection and insurance area. More recently, Orszag and Stiglitz[8] analyzed the optimal size for fire departments when the risks of a fire for home owners are correlated, and explained that the positive externality of self-protection (against fire) led to lower self-protection by each home owner. Their model considered only self-protection and did not include insurance. Lakdawalla and Zanjani[9] showed that government subsidies for terror insurance discourage self-protection and limit the negative externalities of self-protection. We extend this stream of research and develop a model for cyber security risk management, in which risks are correlated and losses cannot be proven.

[4] The reader is referred to Harrington and Niehaus[4] for a thorough review.

Among the studies on the management of information security risk, Anderson[10] first identified the mismatched incentives among various participants in information security that makes cyber risk management hard. Gordon and Loeb[11] showed that cost considerations may cause a firm to decrease its security investment when the security vulnerability increases beyond a threshold. Varian[12] and Kunreuther and Heal[13] showed that risk correlation (which they termed interdependence) reduces a firm's incentives to invest in security, which is the result of the tendency of firms to free ride on the protection availed by others' efforts. Hausken[14] showed that the security effort by a firm is affected by correlated risk, attackers' income, and whether attackers are able to substitute their efforts among different targets. Cremonini and Nizovtsev[15] showed that when attackers can substitute their efforts between targets, firms with a strong defense reveal their protection levels to attackers.

Information sharing is a mechanism for mitigating the impact of correlated risk. Gordon, Loeb, and Lucyshyn[16] found that when firms share security information, they reduce investments in information security unless appropriate incentives are in place. Gal-Or and Ghose[17] found that security technology investments and security information sharing act as "strategic complements." Hausken[14] assumed that a firm's security effort and information received from another firm are substitutes, and that they are complements when the risk interdependence is negative. The papers in this group considered only self-protection as an instrument to manage risks, but not insurance and hence, do not provide a holistic view of risk management.

Research on cyber insurance is limited. Majuca *et al.*[18] trace the evolution of cyber insurance market. Gordon, Loeb, and Sohail[19] proposed a few qualitative prescriptions on using cyber insurance. Bohme and Kataria[20] developed models and measures of risk correlation in order to understand implications on cyber insurance and showed that risk correlation between systems within a firm influences a firm's decision to buy insurance and risk correlation among firms covered by an insurance company determines the premium. Mukhopadhyay *et al.*[21] used Bayesian belief networks to estimate probabilities associated with specific security breaches and used these probabilities to determine appropriate cyber insurance premiums. Herath and Herath[22] proposed that the copula methodology—combining one-dimensional distributions into a multivariate distribution functions—be used to price cyber insurance products. The papers in this group focused on developing methods to price cyber insurance. They did not study how much firms should invest in insurance to manage the information security risk. Recently, Bolot and LeLarge[23] showed that in the presence of network effects and discriminatory insurance pricing against firms that do not invest in protection, cyber insurance can motivate firms to invest in security. Shetty *et al.*[24] showed that competitive cyber insurers may not improve cyber security. The above mentioned papers did not consider the imperfect ability of a firm to prove loss to an insurer nor did they address public policy issues.

Table I. Notation

$U_i(.)$	Utility function (twice-differentiable, increasing, and strictly concave) of wealth for firm i
W	Initial monetary wealth of firms; $W > 0$
L	Monetary loss to a firm when it suffers from a loss-inflicting event; $L > 0$
z_i	Monetary self-protection of firm I; $z_i \geq 0$
$B_i(z_i, z_j)$	Probability of a breach for firm i; $B_i(z_i, z_j) > 0$
P	Probability that the loss is provable by a firm
I_i	Insurance coverage taken by firm I; $I_i \geq 0$
π_i	Insurance premium paid by firm I; $\pi_i \geq 0$
N_i	$W - \pi_i - z_i$; the wealth of firm i when it does not suffer any breach
C_i	$W - L + I_i - \pi_i - z_i$; the wealth of firm i when it suffers a breach
O_i	$W - L - \pi_i - z_i$; the wealth of firm i when it suffers a breach but the insurer does not cover the breach

3. MODEL FRAMEWORK

Consider two firms, $i, j = 1, 2$ $(i \neq j)$. Assume that both firms maximize expected utilities of wealth, are risk averse, face the possibility of loss-inflicting security breaches, and are able to affect the probability of loss by investing in self-protection. The notation used in our model is summarized in Table I.

The probability of a loss to a firm, $B_i(z_i, z_j)$, depends not only on its own self-protection investment, but also on the self-protection investment of the other firm; this feature models the correlated nature of risks across firms. $B_i(z_i, z_j)$ is decreasing in z_i and z_j implying that the breach probability of a firm is decreasing in a firm's own investment as well as the investment of the other firm in self-protection. If the firms' breach risks[5] are uncorrelated, then the

[5] We use the term risk to denote the probability of a security breach.

probability of breach for firm i would be denoted as $B_i(z_i)$. We assume that $B_i(z_i, z_j) \geq B_i(z_i)$. This assumption states that for a given level of a firm's investment, the presence of risk correlation can only increase the probability of breach for that firm. We also assume that marginal probability of breach is higher (weakly) when risks are correlated than when they are not, that is, $\frac{\partial B_i(z_i, z_j)}{\partial z_i} \geq \frac{\partial B_i(z_i)}{\partial z_i}$.

Unprovable loss is modeled by the parameter P, which is assumed to be independent of $B_i(z_i, z_j)$. A breach always inflicts loss L on the firm.[6] Loss L includes the tangible and intangible costs from a breach. We assume that firms are identical with respect to W, L, and P, so no firm-specific index is used for these parameters. Finally, we use the commonly used constant absolute risk aversion (CARA) utility function given by $U(x) = k - he^{-rx}$, where k and h are constants and r is the risk aversion factor. A higher value of r implies a higher risk aversion. Assume that all model parameters are common knowledge to both firms.

The decision variables for a firm are I_i and z_i. An insurance contract purchased by firm i can be succinctly described by three parameters: z_i, π_i, and I_i. If firm i invests z_i and pays a premium of π_i, then it is reimbursed I_i if it can prove that the loss has occurred. We first examine, in Section 4, the case in which the insurer is able to observe the self-protection of a firm before accepting an insurance contract.[7] This case models reality in two ways. First, many insurers partner with technology consulting firms so that they can audit the firms' security efforts.[30] A second scenario is that a government legislates that a firm seeking insurance must reveal its security efforts to insurance companies before insurance is taken. Both of these scenarios are modeled by the case that the insurer is able to observe the self-protection of a firm. Later, in Section 5, we analyze the case in which the insurer is not able to observe self-protection, in which case the insurance contract to firm i is described by only π_i and I_i, that is, firm i pays a premium of π_i, and is reimbursed I_i if it proves the loss.

We assume that insurers are risk neutral. Following earlier studies in the insurance literature, we assume that the insurance market is competitive.[28] Doing so allows us to isolate the effects of correlated risk and unprovable loss.[8] In a perfectly competitive insurance market, a *break-even* insurance policy, also known as the actuarially fair policy (results in zero expected profits to insurers), will be offered.[28] So, a firm's insurance premium is given by the expression for the expected payout as follows:

$$\pi_i - PB_i(z_i, z_j)I_i = 0, \ \forall i \Rightarrow \pi_i = PB_i(z_i, z_j)I_i, \forall i. \tag{1}$$

4. SELF-PROTECTION IS OBSERVABLE

The expected utility for firm i, assuming it always gets insurance, is given by the following:

$$E(U_i) = B_i(z_i, z_j)PU(C_i) + B_i(z_i, z_j)(1 - P)U(O_i) + [1 - B_i(z_i, z_j)]U(N_i). \tag{2}$$

Each firm will simultaneously maximize its expected utility with respect to I_i and z_i. The first-order conditions for the utility maximization objective of firm i are given by the following, after substituting $\pi_i = PB_i(z_i, z_j)I_i$ in Equation (2), and simplifying the expressions:

$$\frac{\partial E(U_i)}{\partial z_i} = \frac{\partial B_i(z_i, z_j)}{\partial z_i}\{PU(C_i) + [1 - P]U(O_i) - U(N_i)\} - \left(1 + P\frac{\partial B_i(z_i, z_j)}{\partial z_i}I_i\right)U'(C_i) = 0, \tag{3}$$

$$\frac{\partial E(U_i)}{\partial I_i} = \{1 - PB_i(z_i, z_j)\}U'(C_i) - [1 - P]B_i(z_i, z_j) \times U'(O_i) - \{1 - B_i(z_i, z_j)\}U'(N_i) = 0. \tag{4}$$

We show in the Appendix that a sufficient condition to obtain a unique interior equilibrium is given by $PB_i(z_i, z_j)L > 1$. This condition also ensures that firms buy insurance in the equilibrium. An equilibrium in which firms do not buy insurance is uninteresting for the public policy problem because insurance affects the degree of self-protection undertaken, and preferred public policy interventions are the ones that benefit the different parties involved.

[6] We assume that there is only one type of breach and it always inflicts a fixed damage of L on the firm. Later, in Section 6, we relax this assumption and allow L to come from a probability distribution.

[7] The insurance literature has analyzed the moral hazard arising from information asymmetry extensively.[25–28] Moral hazard problems arise in most principal-agent models.[29]

[8] At the present time, the cyber insurance market is neither perfect nor competitive because of various issues such as access to capital markets. While we do not analyze the impact of these issues, we speculate that these issues will increase the need for public policy intervention in the cyber risk management domain.

Rewriting Equation (4), we obtain:

$$U'(C_i) = \left(\frac{B_i(z_i, z_j)(1-P)}{1-PB_i(z_i, z_j)}\right) U'(O_i) + \left(\frac{1-B_i(z_i, z_j)}{1-PB_i(z_i, z_j)}\right) U'(N_i). \quad (5)$$

Thus, in equilibrium, $U'(C_i)$ is a convex combination of $U'(O_i)$ and $U'(N_i)$. Furthermore, substituting Equation (5) into Equation (3) and rewriting, we get the following equation for determining the self-protection level:

$$\frac{\partial B_i(z_i, z_j)}{\partial z_i} = \frac{\left\{1 + PI_i \frac{\partial B_i(z_i, z_j)}{\partial z_i}\right\} U'(C_i)}{PU(C_i) + (1-P)U(O_i) - U(N_i)}. \quad (6)$$

In Equation (6), $\frac{\partial B_i(z_i, z_j)}{\partial z_i}\{PU(C_i) + (1-P)U(O_i) - U(N_i)\}$ denotes the marginal increase in the utility from self-protection because of reduced breaches, and $\{1 + PI_i \frac{\partial B_i(z_i, z_j)}{\partial z_i}\}U'(C_i)$ denotes the marginal decrease in the utility from self-protection and associated impacts on insurance premium and insurance coverage. So, Equation (6) expresses the familiar condition that at the optimal self-protection level, the marginal increase equals the marginal decrease in utility. For the CARA utility function, we get the optimal symmetric insurance coverage and self-protection as the following:[9]

$$I^* + L - \frac{1}{r}\ln\left[\frac{\{1 - B(z^*, z^*)\} + B(z^*, z^*)(1-P)e^{rL}}{1 - B(z^*, z^*)P}\right], \quad (7)$$

$$\left.\frac{\partial B_i(z_i, z_j)}{\partial z_i}\right|_{z_i = z_j = z^*} = -\frac{1}{\left(PI^* + \frac{(1-P)(e^{rL}-1)}{r[1 - B(z^*, z^*) + B(z^*, z^*)(1-P)e^{rL}]}\right)}. \quad (8)$$

The following proposition is proved in Appendix.

Proposition 1: *When the self-protection by a firm is observable by insurers, then the firm*

(i) *buys less insurance, and*
(ii) *invests less in self-protection,*

when risks are correlated and the ability to prove loss is imperfect (provided that $P < \frac{r}{1+r}$*).*

Proposition 1 highlights the adverse consequence of correlated risk and unprovable loss in that there is free-riding behavior with respect to self-protection induced by risk correlation. By substituting $P = 1$ in Equation (7), we find that if a firm has the ability to detect and prove loss, then the firm will buy full insurance coverage whether their risks are correlated or not. Therefore, it is the imperfect ability to prove loss, and not the correlated risk, that reduces a firm's incentives to buy less than full insurance coverage. It is well known that the positive externality imposed by risk correlation causes a firm to reduce its self-protection effort.[31–33] From Equation (7), we have the following:

$$\frac{\partial I^*}{\partial P} = \frac{1}{r}\ln\left(\frac{1 - B_i(z^*, z^*)P}{1 - B_i(z^*, z^*) + B_i(z^*, z^*)(1-P)e^{rL}}\right) \times \left(\frac{B_i(z^*, z^*)\{1 - B_i(z^*, z^*)\}(e^{rL}-1)}{\{1 - B_i(z^*, z^*)P\}^2}\right) > 0. \quad (9)$$

Thus, as P decreases, insurance coverage decreases, *ceteris paribus*. To see how unprovable losses affect self-protection, consider the following:

$$\frac{\partial I^*}{\partial z^*} = \frac{\partial I^*}{\partial B(z^*, z^*)}\frac{\partial B(z^*, z^*)}{\partial z^*} = -\left[\frac{(1-P)(e^{rL}-1)}{\{1 - PB(z^*, z^*)\}^2}\right]\frac{\partial B(z^*, z^*)}{\partial z^*} > 0,$$

which shows that optimal self-protection and insurance are complements. This implies that when both risk correlation and imperfect ability to prove loss are present, the free-riding behavior with respect to self-protection level, induced by risk correlation, reduces a firm's incentive to buy insurance. The incentive of the firm to buy insurance, which is reduced by the firm's inability to prove its loss, further reduces its incentive to invest in self-protection.

Note the similarity of our result with respect to P, and the well-known result that moral hazard reduces insurance coverage. In models with moral hazard (but assuming that a firm can always prove its loss), the insurer does not offer full coverage in order to induce a firm to invest more effort in self-protection. In our model, even if the insurer does not face moral hazard and offers full insurance, a firm that is not able to reap full benefits from insurance will not buy full insurance coverage. Less than full coverage in our model is an outcome of disincentives

[9] For the symmetric equilibrium, we ignore the subscript so that $z_i^* = z_j^* = z^*$, $I_i^* = I_j^* = I^*$, $B_i = B_j$.

on the part of insured as opposed to the fact that less than full coverage in the moral hazard case is an outcome of the disincentives of the insurer.

Next, we model the probability of breach in a more specific and realistic manner. A firm incurs loss in two ways: directly or indirectly. A *direct* loss event occurs if the source of the event is the firm itself. An *indirect* loss event occurs when the event occurs on the other firm first and then spreads to the first firm. Let

$p(z_i) > 0$ be a twice-differentiable, decreasing, and strictly convex function denoting the probability of a direct loss on firm i when it invests z_i on self-protection,

q be the probability of the loss spreading to firm i given that firm j has incurred a loss.

The probability of a direct loss for a firm depends only on its own investment in self-protection. However, the probability of an indirect loss on firm i, $qp(z_j)$, depends on self-protection by the other firm and the spread probability, q. A higher value of q indicates that risks are more highly correlated. Current data suggest that the value of q is about 0.15 based on the U.S. Department of Justice and RAND Corporation survey of over 7,000 companies: http://www.ojp.usdoj.gov/bjs/abstract/cb05.htm. Thus, we model the probability of loss, $B_i(z_i, z_j)$, in the following manner:

$$B_i(z_i, z_j) = p(z_i) + [1 - p(z_i)]qp(z_j)$$
$$= 1 - [1 - p(z_i)][1 - qp(z_j)]. \quad (10)$$

We verified that the above $B_i(z_i, z_j)$ satisfied all the conditions we assumed for breach probability functions.

Using a numerical example as an illustration, Table II shows insurance coverage and self-protection levels (in absolute dollar values) for different q and P values when $p(z) = e^{-z}$, $L = \$10$, and $r = 1$ in the CARA utility function. Policymakers can follow similar steps and quantify various parameters in the model for comparing different scenarios. We make the following observations from the two tables.

(1) As risk correlation and the ability to prove loss increase (weakly), insurance coverage decreases (weakly). This result is consistent

Panel A

q\P	1	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1
0	10	7.05	6.61	6.33	6.10	5.88	5.66	5.42	5.12	4.66
0.1	10	6.08	5.23	4.60	4.05	3.51	2.91	2.16	0	0
0.2	10	5.38	4.40	3.68	3.02	2.33	0	0	0	0
0.3	10	4.88	3.81	3.00	2.16	0	0	0	0	0
0.4	10	4.47	3.32	2.30	0	0	0	0	0	0
0.5	10	4.11	2.80	0	0	0	0	0	0	0
0.6	10	3.75	0	0	0	0	0	0	0	0
0.7	10	3.38	0	0	0	0	0	0	0	0
0.8	10	2.74	0	0	0	0	0	0	0	0
0.9	10	0	0	0	0	0	0	0	0	0
1	10	0	0	0	0	0	0	0	0	0

Panel B

0	2.31	4.81	5.05	5.16	5.21	5.21	5.17	5.08	4.91	4.57
0.1	2.3	3.92	3.75	3.52	3.26	2.94	2.53	1.94	0	0
0.2	2.29	3.31	3.02	2.71	2.35	1.89	0	0	0	0
0.3	2.28	2.9	2.54	2.15	1.62	0	0	0	0	0
0.4	2.26	2.59	2.15	1.59	0	0	0	0	0	0
0.5	2.25	2.32	1.76	0	0	0	0	0	0	0
0.6	2.24	2.07	0	0	0	0	0	0	0	0
0.7	2.23	1.81	0	0	0	0	0	0	0	0
0.8	2.22	1.37	0	0	0	0	0	0	0	0
0.9	2.22	0	0	0	0	0	0	0	0	0
1	2.19	0	0	0	0	0	0	0	0	0

Table II. (A) Insurance Coverage for Risk Correlation (q) and Ability to Prove Loss (P); (B) Self-Protection for Risk Correlation (q) and Ability to Prove Loss (P)

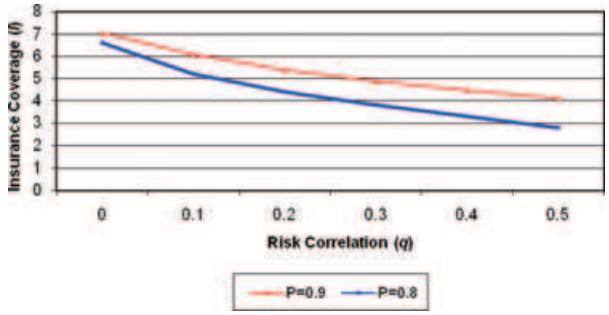

Fig. 1. Impact of risk correlation (q) on insurance coverage (I) for fixed values of ability to prove loss (P).

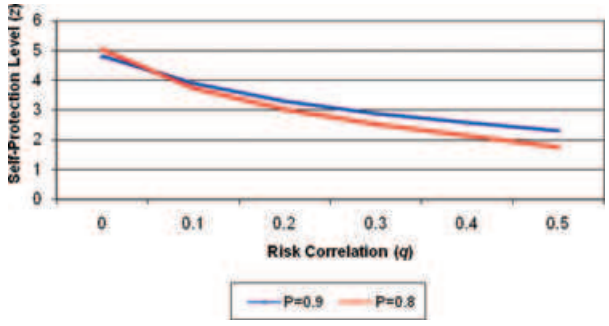

Fig. 2. Impact of risk correlation (q) on self-protection level (z) for fixed levels of ability to prove loss (P).

with Proposition 1(i). Self-protection decreases with risk correlation, as well as with unprovable loss (after increasing initially). This suggests that, while an increase in risk correlation diminishes self-protection and insurance, a decrease in the ability to prove loss may actually encourage a firm to invest in self-protection and rely less on insurance coverage to deal with security risks.

(2) When $P < 1$, insurance coverage is a decreasing convex function of q (see Fig. 1). Insurance coverage decreases faster as P decreases. This suggests that the marginal impact of risk correlation in reducing insurance is enhanced when the ability to prove loss decreases.

(3) Self-protection is a decreasing convex function of q (see Fig. 2). Self-protection decreases faster as the level of P decreases. This suggests that the marginal impact of risk correlation in reducing self-protection is enhanced when the ability to prove loss decreases.

So as P decreases, risk correlation plays a larger role in determining I and z. Therefore, the role of public policy is more important as P decreases.

4.1. Socially Optimal Self-Protection and Insurance

Until this point in the article, we analyzed a firm's self-protection level and insurance coverage in a free market in which firms make decisions independent of each other. When viewed as a problem for a government agency, the problem to be solved must maximize the benefits of both firms:

$$\underset{z_1,z_2,I_1,I_2}{Max} \sum_{i=1}^{2} E(U_i) = \sum_{i=1}^{2} \{PB_i(z_i, z_j)U(C_i) + (1-P)B_i(z_i, z_j)U(O_i) + [1 - B_i(z_i z_j)]U(N_i)\}. \tag{11}$$

The first-order conditions for the maximization problem, after simplification, are the following:

$$\frac{\partial}{\partial z_i}\sum_{i=1}^{2} E(U_i) = 0 = \frac{\partial B_j(z_i, z_j)}{\partial z_i}\{PU(C_j) + (1-P) \times U(O_j) - U(N_j) - PI_jU'(C_j)\} + \left(\frac{\partial B_i(z_i, z_j)}{\partial z_i}\{PU(C_i) + (1-P) \times U(O_i) - U(N_i)\} - \left\{1 + P\frac{\partial B_i(z_i, z_j)}{\partial z_i}I_i\right\} \times U'(C_i)\right), \tag{12}$$

$$\frac{\partial}{\partial I_i}\sum_{i=1}^{2} E(U_i) = 0 = [1 - PB_i(z_i, z_j)]U'(C_i) - (1-P)B_i(z_i, z_j)U'(O_i) - \{1 - B_i(z_i, z_j)\}U'(N_i). \tag{13}$$

Comparing Equation (12) with Equation (3), we find that the left-hand side of Equation (12) has an additional term, $(\frac{\partial B_j(z_i,z_j)}{\partial z_i}\{PU(C_j) + (1-P)U(O_j) - U(N_j) - PI_jU'(C_j)\})$, which represents the increase in self-protection to reduce negative externality for achieving the socially optimal self-protection levels. When firms make decisions independent of each other, they do not consider the externality effect. We also note that Equation (13) is identical to Equation (4), implying that if firms invest at the socially optimal level of self-protection, then they will also buy the socially optimal level of insurance coverage. We show the following result.

Proposition 2: *If risks are correlated and the ability to prove loss is imperfect, then a firm buys less than the socially optimal insurance coverage and invests less than the socially optimal level of self-protection.*

The principal reason that firms invest less than the socially optimal self-protection level is that when firms maximize their own utility, a firm considers the negative impact it suffers from the other firm's investment. But it does not take into account the negative effect of its own investment on the other firm, which is an externality. A government agency, by maximizing the benefits of both firms at the same time, internalizes such externalities. This results in the finding that the socially optimal self-protection for each firm is higher than the level of self-protection when each firm is maximizing its own benefit. Because of the complementary relationship between self-protection and insurance that we mentioned earlier, the socially optimal insurance coverage is also higher than the insurance coverage taken when each firm is maximizing its own benefit.

The most significant implication of Proposition 2 is that, for correlated risks and unprovable losses, a firm is more vulnerable to security breaches because of the lower self-protection levels at *all* firms. Each firm will also have to absorb more damages from a breach because of the lower amount of insurance coverage taken. Policymakers should address how to mitigate these adverse impacts. For example, assuming that self-protection is observable, a government can legislate that firms invest at the socially optimal level of self-protection and impose harsh penalties for the failure to do so. Firms will then automatically choose the socially optimal insurance. Recent compliance regulations (e.g., Sarbanes Oxley, HIPPA, Basel II) are efforts to legislate self-protection. However, enforcing self-protection by law and penalties could be very costly. It may be easier for the government to use incentives or subsidies to achieve the desired outcome.

4.2. A Subsidy on Self-Protection

Assume that the government offers a subsidy of $s < 1$ for each dollar of investment by a firm in self-protection. In order to fund the subsidy, the government charges, in advance, a lump-sum tax of $\kappa = sz$ on the firm. Assume that the insurance market is competitive as in the original model. In the presence of a self-protection subsidy, the expected utility of firm i is given by the following:

$$\begin{aligned} EU_i = {} & B_i(z_i, z_j)PU(W - L + I_i - \pi - [1 - s]z_i - \kappa_i) \\ & + B_i(z_i, z_j)(1 - P)U(W - L - \pi_i - [1 - s]z_i - \kappa_i) \\ & + \{1 - B_i(z_i, z_j)\}U(W - \pi_i - [1 - s]z_i - \kappa_i). \end{aligned}$$

We show the following result on the optimal subsidy level.

Proposition 3: *When*

$$s^* = \left. \frac{\dfrac{\partial B_j(z_i, z_j)}{\partial z_i}\{PU(C_j) + (1 - P)U(O_j) - U(N_j) - PI_jU'(C_j)\}}{U'(C_i)} \right|_{z_i = z_j = z_s^*, I_i = I_j = I_s^*},$$

a firm invests at the socially optimal self-protection level and buys the socially optimal insurance coverage, and $0 \le s^* \le 1$.

Note that when the expression for s^* in Proposition 3 is evaluated at the symmetric solution for z^* and I^*, one value is obtained for s^* that the policymaker is able to use for both firms. Proposition 3 shows that a subsidy on self-protection is optimal when self-protection is observable. A subsidy improves the marginal benefit from self-protection. At the optimal level of subsidy, this improvement in the marginal benefit from self-protection exactly offsets the reduction in marginal benefit caused by risk correlation, inducing firms to internalize the risk correlation effects and to adopt the socially optimal self-protection strategy. Once the externalities due to risk correlation are internalized, the firms also buy the socially optimal insurance coverage. While the policy of subsidizing self-protection can be effective, it still requires a government agency to monitor a firm's self-protection efforts. Thus, the question is whether the government can instead achieve the same result by intervening in the insurance market by subsidizing the insurance premium to achieve the socially optimal risk management strategy.

Proposition 4: *When self-protection is observable, there does not exist a subsidy on the insurance premium that will induce firms to adopt the socially optimal strategy.*

The above proposition reveals that a subsidy on insurance premiums cannot help coordinate a firm's risk management decision in a manner that is socially optimal. This is especially noteworthy because a subsidy on insurance premiums should have raised the self-protection level (recall that insurance and self-protection are complements). So why is it that a subsidy on self-protection works to coordinate a firm's risk management decision in a socially optimal

manner, but a subsidy on insurance premium does not? The reason is that a subsidy on self-protection has two effects. The *direct* effect is that it reduces the externality effects, thus causing firms to invest more in self-protection. The *indirect* effect is that the probability of breach is reduced by the increase in self-protection, which in turn reduces the insurance premium. Note that the premium price is a function of the breach probability ($\pi_i = PB_i I_i$). Though an insurance premium subsidy reduces the effective insurance premium, it does not have any impact on the externality effect due to risk correlation. Consequently, the insurance premium subsidy is unable to achieve a similar coordination.

5. SELF-PROTECTION IS UNOBSERVABLE

Now, more realistically, we assume that self-protection is not observable. For example, as is the case today, there are no regulated disclosures on self-protection. The insurance premium will be contingent only on the insurance coverage, so that Equation (1) is no longer applicable. Assume that the insurance premium is ϕ per unit dollar of coverage so that $\pi(I_i) = \phi I_i, \phi < 1$. Risks are correlated and the ability to prove loss is imperfect as before. The decision variables and the expression for the expected utility for a firm remain the same as when self-protection is observable (namely, Equation (2)). The first-order conditions are shown in the proof for Proposition 5 in the Appendix. Solving these conditions for the CARA utility function, we obtain the following conditions for insurance coverage and self-protection:

$$I^* = L - \frac{\ln\left[\dfrac{\phi(1-P)e^{rL}}{(1-\phi)P} + \dfrac{\phi\{1-B(z^*,z^*)\}}{[1-\phi]B(z^*,z^*)P}\right]}{r}, \tag{14}$$

$$\left.\frac{\partial B_i(z_i,z_j)}{\partial z_i}\right|_{z_i=z_j=z^*} = r\,B_i(z_i,z_j) \times \left.\left[\frac{1-B_i(z_i,z_j)+(1-P)B_i(z_i,z_j)e^{rL}}{B_i(z_i,z_j)-\phi-(1-P)B_i(z_i,z_j)e^{rL}}\right]\right|_{z_i=z_j=z^*}. \tag{15}$$

The condition $B_i(z_i,z_j)\{1-(1-P)e^{rL}\} < \phi$ must hold in order that a firm invests in self-protection in equilibrium.

Proposition 5a: *When the self-protection by a firm is not observable by an insurer and the firm's risks are uncorrelated with that of other firms, then the firm buys less insurance coverage and invests more in self-protection for unprovable losses.*

Proposition 5b: *When the self-protection by a firm is not observable by an insurer, and the firm's ability to prove loss is perfect, then the firm invests less in self-protection and buys more insurance for correlated risks.*

Table III compares the impact of risk correlation and imperfect ability to prove loss on a firm's self-protection and insurance decisions for the case of self-protection is observable and when self-protection is not observable.

In the case of unobservable self-protection, risk correlation increases insurance coverage, and unprovable loss increases its self-protection (column 2 in Table III). The intuition for this lies in the interaction between insurance and self-protection at equilibrium. Using Equation (14), we find that $\frac{\partial I^*}{\partial z^*} = \frac{\partial I^*}{\partial B(z^*,z^*)}\frac{\partial B(z^*,z^*)}{\partial z^*} < 0$. That is, now insurance and self-protection behave as substitutes, so that a reduction in self-protection is accompanied by an increase in insurance coverage, and vice versa. Because risk correlation decreases self-protection, it increases insurance coverage, and because the imperfect ability to detect loss decreases insurance, it increases self-protection.

Next, we consider the socially optimal levels of I_i and z_i from a policy analysis viewpoint. These results are found from the first-order conditions of Equation (11) as shown in the Appendix.

Proposition 6: *When the self-protection of a firm is not observable by the insurer, risks are correlated and the firm is not able to always prove loss from a breach, the firm buys more than the socially optimal*

Table III. The Impact of Observability of Self-Protection, Risk Correlation, and Imperfect Ability to Prove Loss

Presence of:	Self-Protection Is Observable (Assuming $P < \frac{r}{1+r}$)	Self-Protection Is Not Observable
1. Risk correlation	*Reduces* self-protection *Reduces* insurance coverage	*Reduces* self-protection *Increases* insurance coverage
2. Imperfect ability to prove loss	*Reduces* self-protection *Reduces* insurance coverage	*Increases* self-protection *Reduces* insurance coverage

insurance coverage and invests less than the socially optimal level of self-protection.

Comparing Proposition 2 with Proposition 6, we find that, unlike the case where self-protection is observable, the firm buys more insurance when its self-protection is not observable. The reason for this difference is that a firm's insurance and its self-protection are substitutes when self-protection is not observable, but are complements when self-protection is observable. This result shows that the adverse effects of risk correlation and unprovable loss exist even when a firm's self-protection is not observable. Because self-protection is not observable, risk management can be improved only by manipulating insurance.[10] Since firms rely more on insurance than the socially optimal level, taxation on insurance is one remedy to mitigate the adverse effects of risk correlation and unprovable loss.

Assume that the government charges an insurance "sales" tax of $\tau > 0$ per unit of insurance premium paid by a firm. The government maintains revenue neutrality by distributing the collected tax to all firms by other means. Assume that such a distribution amounts to d_i for each firm. We assume that the insurance market continue to price insurance at ϕ per unit dollar coverage. In the presence of the insurance tax, the expected utility of firm i is given by the following:

$$\begin{aligned} E(U_i) = {} & B_i(z_i, z_j)PU(W - L + I_i - [1+\tau]\pi_i - z_i + d_i) \\ & + B_i(z_i, z_j)(1-P)U(W - L - [1+\tau]\pi_i - z_i + d_i) \\ & + [1 - B_i(z_i, z_j)]U(W - [1+\tau]\pi_i - z_i + d_i). \end{aligned}$$

Solving the first-order conditions with respect to I_i and z_i as shown in the Appendix in the proof of Proposition 7, we have the following result highlighting the optimality of an insurance tax to achieve socially optimal outcomes.

Proposition 7: *When*

$$\tau^* = \left. \frac{\phi \dfrac{\partial B_j(z_i, z_j)}{\partial z_i}\{PU(C_i) + (1-P)U(O_i) - U(N_i) - PI_jU'(C_j)\}}{B_i(z_i, z_j)PU'(C_i) - \phi \dfrac{\partial B_j(z_i, z_j)}{\partial z_i}\{PU(C_i) + (1-P)U(O_i) - U(N_i)\}} \right|_{z_i = z_j = z_s^*, I_i = I_j = I_s^*} > 0,$$

firms invest at the socially optimal self-protection level and buy the socially optimal insurance coverage.

[10] Obviously, a subsidy on self-protection is impossible because self-protection is not observable.

In summary, our results in Sections 4 and 5 show that risk correlation and unprovable loss cause a firm to invest less in self-protection and buy less insurance, compared to the socially optimal level, regardless of whether self-protection is observable by the insurer or not. The corrective social policies that we proposed in this article, namely, subsidizing self-protection and taxing insurance premiums, improve risk management decisions of a firm. When the self-protection of firms is observable, a social planner could subsidize self-protection, whereas when self-protection is not observable, the government should tax insurance. The optimal policy interventions differ because self-protection and insurance are complements when self-protection is observable and are substitutes when self-protection is not observable.

6. ROBUSTNESS OF RESULTS

We consider two variations of our basic model to demonstrate that the results in this article are robust. First, we assume that the loss from a breach is not fixed. That is, we assume that the loss can be either low or high according to a probability distribution. This feature models the scenario that breaches are not homogenous with respect to the loss that they inflict on firms. In the second variation, we assume that firms invest in disaster recovery mechanisms to reduce the loss from a breach, in addition to investing in self-protection to reduce the probability of breach. We show in the following subsections that the results of Sections 4 and 5 hold for these model variations as well.

6.1. Heterogeneous Loss from Breach

We assume that the damage from a breach is L_H with probability p and L_L with probability $(1-p)$. The rest of the model is identical to the basic model discussed in Section 3. The expected utility of firm i is the following:

$$\begin{aligned} E(U_i) = {} & PB_i(z_i, z_j)[pU(W - L_H + I_i - \pi_i - z_i) \\ & + (1-p)U(W - L_L + I_i - \pi_i - z_i)] \\ & + (1-P)B_i(z_i, z_j)[pU(W - L_H - \pi_i - z_i) \\ & + (1-p)U(W - L_L - \pi_i - z_i)] \\ & + \{1 - B_i(z_i, z_j)\}U(W - \pi_i - z_i). \end{aligned}$$

For the CARA utility function, we have the following expression for the utility:

$$\begin{aligned} EU_i = {} & PB_i(z_i, z_j)e^{-r(W-\pi_i-z_i+I_i)}[pe^{rL_H} + (1-p)e^{rL_L}] \\ & + (1-P)B_i(z_i, z_j)e^{-r(W-\pi_i-z_i)}[pe^{rL_H} + (1-p) \\ & \times e^{rL_L}] + \{1 - B_i(z_i, z_j)\}e^{-r(W-\pi_i-z_i)}. \end{aligned}$$

Now define $\bar{L}$ as $e^{r\bar{L}} = pe^{rL_H} + (1-p)e^{rL_L}$. Firm i's utility can be written as:

$$\begin{aligned} E(U_i) = {} & PB_i(z_i, z_j)e^{-r(W-\pi_i-z_i+I_i-\bar{L})} \\ & + (1-P)B_i(z_i, z_j)e^{-r(W-\pi_i-z_i-\bar{L})} \\ & + \{1 - B_i(z_i, z_j)\}e^{-r(W-\pi_i-z_i)}. \end{aligned} \tag{16}$$

Equation (16) is identical to Equation (2) except that L is replaced by $\bar{L}$. Thus, all our results derived in Section 4 (and Section 5) can be shown to hold when the loss from a breach is not homogeneous by substituting L with $\bar{L}$ in the proofs.

6.2. Investments in Self-Protection and Disaster Recovery

In this variation, we assume that firm i invests z_i in self-protection and t_i in disaster recovery procedures. While self-protection reduces the probability of breach, disaster recovery procedures reduce the damage if a firm is breached. We assume that L is a decreasing convex function of t_i and $L(0) = L_0$. In this case, in addition to deciding optimal self-protection and insurance, firms also decide the optimal investment in disaster recovery. All other aspects of the model remain the same as in the basic model.

The expected utility of firm i is the following:

$$\begin{aligned} E(U_i) = {} & B_i(z_i, z_j)PU(W - L(t_i) + I_i - \pi_i - z_i - t_i) \\ & + B_i(z_i, z_j)(1-P)U(W - L(t_i) - \pi_i - z_i - t_i) \\ & + \{1 - B_i(z_i, z_j)\}U(W - \pi_i - z_i - t_i). \end{aligned} \tag{17}$$

The first-order conditions for expected utility maximization are given by the following:

$$\begin{aligned} \frac{\partial E(U_i)}{\partial I_i} = 0 = {} & \{1 - B_i(z_i, z_j)P\}B_i(z_i, z_j) \\ & \times PU'(W - L(t_i) + I_i - \pi_i - z_i - t_i) \\ & - B_i(z_i, z_j)PB_i(z_i, z_j)(1-P) \\ & \times U'(W - L(t_i) - \pi_i - z_i - t_i) \\ & - B_i(z_i, z_j)P\{1 - B_i(z_i, z_j)\} \\ & \times U'(W - \pi_i - z_i - t_i), \end{aligned} \tag{18}$$

$$\begin{aligned} \frac{\partial E(U_i)}{\partial z_i} = 0 = {} & \frac{\partial B_i(z_i, z_j)}{\partial z_i}[PU(W - L(t_i) + I_i - \pi_i \\ & - z_i - t_i) + (1-P)U(W - L(t_i) - \pi_i - z_i - t_i) \\ & - U(W - \pi_i - z_i - t_i)] - \left(1 + \frac{\partial B_i(z_i, z_j)}{\partial z_i} I_i\right) \\ & \times (B_i(z_i, z_j)PU'(W - L(t_i) + I_i - \pi_i - z_i - t_i) \\ & + B_i(z_i, z_j)(1-P)U'(W - L(t_i) - \pi_i z_i - t_i) \\ & + \{1 - B_i(z_i, z_j)\}U'(W - \pi_i - z_i - t_i)), \end{aligned} \tag{19}$$

$$\begin{aligned} \frac{\partial E(U_i)}{\partial t_i} = 0 = {} & -\{L'(t_i) + 1\}B_i(z_i, z_j)PU'(W - L(t_i) \\ & + I_i - \pi_i - z_i - t_i) - \{L'(t_i) + 1\}B_i(z_i, z_j) \\ & \times (1-P)U'(W - L(t_i) - \pi_i - z_i - t_i) \\ & - \{1 - B_i(z_i, z_j)\}U'(W - \pi_i - z_i - t_i). \end{aligned} \tag{20}$$

Comparing Equations (18) and (19) with Equations (4) and (3), respectively, we find that Equation (18) is same as Equation (4) and Equation (19) is same as Equation (3), except that L is now a function of t_i. Denote the optimal investment in disaster recovery as t_i^*. Then, the solution to the simultaneous Equations (18), (19), and (20) is obtained by substituting $L(t_i^*)$ for L in the solution to Equations (3) and (4). Since the qualitative nature of our results in Section 4 does not depend on the value of L, all of our results in Section 4 (and Section 5) hold when firms invest in disaster recovery in addition to self-protection. Both the analyses in this section show that our results about the impact of risk correlation and the inability to prove loss are applicable for a wide variety of situations.

7. CONCLUSIONS

An important challenge faced by governments is the management of national infrastructure security. Information technology infrastructure has been recognized as one of the critical elements of this national infrastructure. Cyber security is characterized by correlated risks and by the difficulty in proving the loss to an insurer. In this article, we analyzed the impact of risk correlation and unprovable loss on firms' risk management strategies. If self-protection can be observed so that insurance contracts are contingent upon self-protection levels, then self-protection and insurance behave as complements, and firms invest in less than socially optimal levels of self-protection and insurance coverage. In this case, the government can induce firms to choose socially optimal self-protection and insurance strategies by offering a

subsidy on self-protection. But the government cannot induce a similar behavior by offering a subsidy on insurance. If self-protection cannot be observed so insurance contracts depend only on the insurance coverage, then self-protection and insurance behave as substitutes, and firms buy more than the socially optimal insurance coverage and invest less than the socially optimal level in self-protection. Rather, the government should tax insurance premiums to achieve the desired result.

Several interesting policy implications emerge from our analysis. The most significant implication is that, since the public policy instrument (intervention in self-protection or insurance) and the type of intervention (subsidy or tax) critically depend on the observability of self-protection, the social policy should carefully evaluate the characteristics of the insurance industry before setting policies. For example, the regulatory body should assess whether insurers have access to firms' security-related data and to actuarial data. We found, contrary to the conventional wisdom, that controlling premium prices (which can be controlled by ensuring a competitive insurance market and access to actuarial data), and observability of self-protection will not result in firms taking adequate self-protection. Other intervention such as subsidies or taxation is required in the cyber risk domain.

As with any stylized model, our model also has several limitations. Our analysis and results were limited to a two-firm model, but the extension to n firms is straightforward. Our preliminary analysis of a model with more than two firms shows that increasing the number of firms is qualitatively equivalent to increasing the degree of risk correlation, and thus increasing the positive externality impact. Therefore, an increase in the number of firms is likely to exacerbate the adverse impact of risk correlation and the imperfect ability to prove loss, necessitating a more aggressive action by social planners to achieve socially optimal levels of risk management strategies. We also assumed that the two firms are homogeneous. In reality, the national information technology infrastructure includes firms of different sizes, information technology assets, and capabilities. It is certainly possible that smaller firms may free ride on larger firms in managing security. This may mean that the optimal strategy of a social planner is to use different intervention policies for different firms. Further research is required to understand the implications of heterogeneous firms in the cyber security context. We hope that this article provides a beginning.

ACKNOWLEDGMENTS

We are grateful to Cheryl Druehl for her comments on the article.

APPENDIX: PROOFS FOR PROPOSITIONS AND COROLLARIES

Recall that $C_i \equiv W - L + I_i - \pi_i - z_i$, $N_i \equiv W - \pi_i - z_i$, $O_i \equiv W - L - \pi_i - z_i$. C_i is the wealth of firm i when it suffers a breach and the insurer covers the breach, N_i is the wealth of firm i when it does not suffer any breach, and O_i is the wealth of firm i when it suffers a breach but the insurer does not cover the breach.

Second-Order Conditions for Utility Maximization in Section 4

The first-order conditions for firm i are given by Equations (3) and (4) given in the main text. The second derivatives for the firm's optimization model are given by the following:

$$\frac{\partial^2 EU_i}{\partial I_i^2} = PB_i[(1-PB_i)^2 U''(C_i) + P(1-P) \times B_i^2 U''(O_i) + P(1-B_i)B_i U''(N_i)] < 0,$$

$$\begin{aligned}\frac{\partial^2 E(U_i)}{\partial z_i^2} =& -PI_i \left(\frac{\partial B_i}{\partial z_i}\right)^2 [PU'(C_i) + (1-P) \\ & \times U'(O_i) - U'(N_i)] + \left(1 + P\frac{\partial B_i}{\partial z_i} I_i\right)^2 \\ & \times [B_i PU'(C_i) + B_i(1-P)U'(O_i) \\ & + (1-B_i)U'(N_i)] + \left(\frac{\partial^2 B_i}{\partial z_i^2}\right) B_i(1 - B_i PI_i) \\ & \times [PU'(C_i) + (1-P)U'(O_i)] \\ & - \left(\frac{\partial^2 B_i}{\partial z_i^2}\right) \{1 + (1-B_i)PI_i\} U'(N_i).\end{aligned}$$

We can verify that all terms on the right-hand side of the above equation except $(\frac{\partial^2 B_i}{\partial z_i^2})$ $B_i(1 - B_i PI_i)\{PU'(C_i) + (1-P)U'(O_i)\}$ are negative. Since every factor other than $(1 - B_i PI_i)$ in this term is positive, the whole term as well as $\frac{\partial^2 E(U_i)}{\partial z_i^2}$ is guaranteed to be negative if $(1 - B_i PI_i) < 0$.

Proof for Proposition 1

(1) Substituting $P = 1$ in Equations (7) and (8), we obtain $I^* = L$ and $\frac{\partial B_i}{\partial z_i} = -\frac{1}{L}$ for the scenario when the ability to prove loss is perfect. The result about insurance follows

from the fact $\frac{1}{r}\ln[\frac{1-B(z^*,z^*)+B(z^*,z^*)(1-P)e^{rL}}{1-B(z^*,z^*)P}] > 0$. The result about self-protection is proved if $(PI_i + \frac{(1-P)(e^{rL}-1)}{r[1-B+B(1-P)e^{rL}]}) < L$.

Substituting Equation (8) in the above, we get:

$$-P\frac{1}{r}\ln\left[\frac{1-B(z^*,z^*)+B(z^*,z^*)(1-P)e^{rL}}{1-B(z^*,z^*)P}\right] + \frac{(1-P)(e^{rL}-1)}{r[1-B+B(1-P)e^{rL}]} < L(1-P).$$

Since $-P\frac{1}{r}\ln[\frac{\{1-B(z^*,z^*)\}+B(z^*,z^*)(1-P)e^{rL}}{1-B(z^*,z^*)P}] < 0$, it is enough to show that:

$$\frac{(e^{rL}-1)}{r[1-B+B(1-P)e^{rL}]} < L$$

$$\Rightarrow \frac{(e^{rL}-1)}{r[1-B+B(1-P)e^{rL}]} < \frac{1}{PB} \text{ because } PBL > 1.$$

Algebraic manipulation shows that the above inequality holds.

Proof for Proposition 2

Comparing Equations (3) and (12), we find that Equation (12) has an extra term $(\frac{\partial B_j}{\partial z_i}\{PU(C_j)+(1-P)U(O_j)-U(N_j)-PI_jU'(C_j)\})$, which is positive because $\frac{\partial B_j}{\partial z_i} < 0$ and $PU(C_j)+(1-P)U(O_j)-U(N_j)-PI_jU'(C_j) < 0$. Thus, $\frac{\partial}{\partial z_i}\sum_{i=1}^{2}E(U_i) > \frac{\partial E(U_i)}{\partial z_i}$. We also know that both $\frac{\partial}{\partial z_i}\sum_{i=1}^{2}E(U_i)$ and $\frac{\partial E(U_i)}{\partial z_i}$ are declining in z_i. Consequently, z_i that satisfies $\frac{\partial}{\partial z_i}\sum_{i=1}^{2}E(U_i)=0$ is higher than the one that satisfies $\frac{\partial E(U_i)}{\partial z_i}=0$. So, the socially optimal level of self-protection is higher than that invested by individual firms.

Equations (4) and (13) are identical. Furthermore, $\frac{\partial}{\partial z_i}(\frac{\partial}{\partial I_i}E(U_i)) < 0$ and we know that z_i^* is higher for social welfare optimization. Therefore, I_i that satisfies Equation (13) is higher than I_i that satisfies Equation (4).

Proof for Proposition 3

The first-order conditions with respect to I_i and z_i for the maximization of utility of firm i are:

$$\begin{aligned}\frac{\partial EU_i}{\partial z_i} = {} & \frac{\partial B_i(z_i,z_j)}{\partial z_i}(PU(W-L+I_i-\pi_i-[1-s]z_i-\kappa_i)+(1-P)U(W-L-\pi_i-[1-s]z_i-\kappa_i)-U(W-\pi_i-[1-s]z_i-\kappa_i)) \\ & \times\left(1-s+P\frac{\partial B_i(z_i,z_j)}{\partial z_i}I_i\right)U'(W-L+I_i-[1-s]\pi_i-z_i-\kappa_i)=0,\end{aligned}$$

$$\begin{aligned}\frac{\partial EU_i}{\partial I_i} = {} & \{1-PB_i(z_i,z_j)\}U'(W-L+I_i-\pi_i-[1-s]\times z_i-\kappa_i)-(1-P)B_i(z_i,z_j)U'(W-L-\pi_i-[1-s]z_i-\kappa_i)-\{1-B_i(z_i,z_j)\}U'(W-\pi_i-[1-s]z_i-\kappa_i)=0.\end{aligned}$$

When we substitute

$$s^* = \left.\frac{\frac{\partial B_j}{\partial z_i}\{PU(C_j)+(1-P)U(O_j)-U(N_j)-PI_jU'(C_j)\}}{U'(C_i)}\right|_{z_i=z_j=z_s^*,\,I_i=I_j=I_s^*}.$$

and $\kappa_j = s^*z_s^*$ in the above first-order conditions, we obtain Equations (12) and (13), respectively. Consequently, the optimal self-protection and insurance when

$$S^* = \left.\frac{\frac{\partial B_j}{\partial z_i}\{PU(C_j)+(1-P)U(O_j)-U(N_j)-PI_jU'(C_j)\}}{U'(C_i)}\right|_{z_i=z_j=z_s^*,\,I_i=I_j=I_s^*}$$

must be identical to z_s^* and I_s^*, respectively.

Since $\frac{\partial B_j}{\partial z_i}\{PU(C_j)+(1-P)U(O_j)-U(N_j)-PI_jU'(C_j)\} > 0$ and $U'(C_i)$, $s^* > 0$. Furthermore, rewriting the first of the first-order conditions, we get:

$$\begin{aligned}\frac{\partial E(U_i)}{\partial z_i} &= 0 \\ &= \frac{\partial B_i}{\partial z_i}\{PU(W-L+I_i-\pi_i-[1-s]z_i-\kappa_i) \\ &\quad + (1-P)U(W-L-\pi_i-[1-s]z_i-\kappa_i) \\ &\quad - U(W-\pi_i-[1-s]z_i-\kappa_i)\} \\ &\quad - P\frac{\partial B_i}{\partial z_i}I_iU'(W-L+I_i-[1-s]\pi_i-z_i-\kappa_i) \\ &\quad - (1-s)U'(W-L+I_i-[1-s]\pi_i-z_i-\kappa_i).\end{aligned}$$

Since the first term is positive and the second term is negative, $(1-s)U'(W-L+I_i-[1-s]\pi_i-z_i-\kappa_i)>0$. So, $s^*<1$.

Proof for Proposition 4

Assume that the social planner offers a subsidy of $0<s<1$ for each dollar of premium paid by a firm. In order to fund the subsidy, the social planner charges, in advance, a lump-sum tax of κ_j equal to $s\pi_j$ on firm j. The external insurance market is competitive (i.e., $\pi_i = PB_iI_i$) as in our original model. The expected utility of firm i is given by the following:

$$\begin{aligned}E(U_i) = {} & B_iPU(W-L+I_i-[1-s]\pi_i-z_i-\kappa_i)\\ & + B_i(1-P)U(W-L-[1-s]\pi_i-z_i-\kappa_i)\\ & + (1-B_i)U(W-[1-s]\pi_i-z_i-\kappa_i).\end{aligned}$$

The first-order conditions for the maximization of utility for i are:

$$\begin{aligned}\frac{\partial E(U_i)}{\partial z_i} = 0 = {} & \frac{\partial B_i}{\partial z_i}(PU(W-L+I_i-[1-s]\pi_i-z_i-\kappa_i)\\ & + (1-P)U(W-L-[1-s]\pi_i-z_i-\kappa_i)\\ & - U(W-[1-s]\pi_i-z_i-\kappa_i))\\ & - \left(\frac{1+[1-s]P\dfrac{\partial B_i}{\partial z_i}I_i}{1-s}\right)U'(W-L+I_i\\ & - [1-s]\pi_i-z_i-\kappa_i),\end{aligned}$$

$$\begin{aligned}\frac{\partial E(U_i)}{\partial I_i} = 0 = {} & (1-[1-s]PB_i)U'(W-L+I_i-[1-s]\\ & \times \pi_i-z_i-\kappa_i)-(1-s)(1-P)B_iU'\\ & \times (W-L-[1-s]\pi_i-z_i-\kappa_i)-(1-s)\\ & \times (1-B_i)U'(W-[1-s]\pi_i-z_i-\kappa_i).\end{aligned}$$

Now, we prove the nonexistence of an s^* that forces firms to choose z_s^* and I_s^* by contradiction. Assume that when $s=s^*$, firms to choose z_s^* and I_s^*. Then,

$$\begin{aligned}\left.\frac{\partial E(U_i)}{\partial z_i}\right|_{z_i=z_j=z_s^*,\,I_i=I_j=I_s^*} & = 0 = \left.\frac{\partial B_i}{\partial z_i}\right|_{z_i=z_j=z_s^*,\,I_i=I_j=I_s^*}\{PU(W-L+I_s^*\\ & - [1-s^*]\pi_i-z_s^*-s^*\pi_i)+(1-P)\\ & \times U(W-L-[1-s^*]\pi_i-z_s^*-s^*\pi_i)\\ & - U(W-[1-s^*]\pi_i-z_i-\kappa_i)\}\\ & - \left(\frac{1+[1-s^*]P\left.\dfrac{\partial B_i}{\partial z_i}\right|_{z_i=z_j=z_s^*,\,I_i=I_j=I_s^*}I_s^*}{1-s^*}\right)\\ & \times U'(W-L+I_s^*-[1-s^*]\pi_i-z_s^*-s^*\pi_i).\end{aligned}$$

Equating the left-hand side of the above to the left-hand side of Equation (12), and simplifying, we get:

$$-\frac{s^*}{1-s^*} = \left.\frac{\dfrac{\partial B_j}{\partial z_i}\{PU(C_j)+(1-P)U(O_j)-U(N_j)-PI_jU'(C_j)\}}{U'(C_i)}\right|_{z_i=z_j=z_s^*,\,I_i=I_j=I_s^*}.$$

Note that the right-hand side of the above equation is positive, but the left-hand side is negative, which leads to a contradiction.

Proof for Proposition 5

The first-order conditions for firm i are given by the following:

$$\begin{aligned}\frac{\partial E(U_i)}{\partial z_i} = {} & \frac{\partial B_i(z_i,z_j)}{\partial z_i}[PU(C_i)+(1-P)U(O_i)\\ & - U(N_i)]-\frac{PB_i(z_i,z_j)U'(C_i)}{\phi}=0,\end{aligned}$$

$$\begin{aligned}\frac{\partial E(U_i)}{\partial I_i} = {} & (1-\phi)B_i(z_i,z_j)PU'(C_i)\\ & -[1-P]\phi B_i(z_i,z_j)U'(O_i)\\ & -\{1-B_i(z_i,z_j)\}\phi U'(N_i)=0.\end{aligned}$$

When $P=1$, Equation (15) becomes:

$$\left.\frac{\partial B_i(z_i,z_j)}{\partial z_i}\right|_{z_i=z_j=z^*} = \left.\frac{B_i(z_i,z_j)\{1-B_i(z_i,z_j)\}}{B_i(z_i,z_j)-\phi}\right|_{z_i=z_j=z^*}.$$

Since $\frac{\partial B_i(z_i,z_j)}{\partial z_i} > \frac{\partial B_i(z_i)}{\partial z_i}$ and $B_i(z_i,z_j) > B_i(z_i) \Rightarrow \frac{B_i(z_i,z_j)\{1-B_i(z_i,z_j)\}}{B_i(z_i,z_j)-\phi} < \frac{B_i(z_i)\{1-B_i(z_i)\}}{B_i(z_i)-\phi}$.

Hence, optimal z_i is smaller when there is risk correlation than when there is not.

When $P = 1$, Equation (14) can be written as:

$$I = L - \frac{\ln\left[\frac{\phi\{1 - B_i(z_i, z_j)\}}{(1-\phi)B_i(z_i, z_j)}\right]}{r}.$$

Since for the same z_i,

$$B_i(z_i, z_j) > B_i(z_i) \Rightarrow \frac{\phi\{1 - B_i(z_i, z_j)\}}{(1-\phi)B_i(z_i, z_j)} < \frac{\phi\{1 - B_i(z_i)\}}{(1-\phi)B_i(z_i)}.$$

Hence, optimal I_i is higher when there is risk correlation than when there is no risk correlation.

Proof for Proposition 6

$$\frac{\partial}{\partial I_i}\sum_{i=1}^{1} E(U_i) = 0 = (1-\phi)B_i(z_i, z_j)PU'(C_i) - (1-P)\phi B_i(z_i, z_j)U'(O_i) - \{1 - B_i(z_i, z_j)\}\phi U'(N_i),$$

$$\frac{\partial}{\partial z_i}\sum_{i=1}^{2} EU_i = 0 = \frac{\partial B_j(z_i, z_j)}{\partial z_i}[PU(C_j) + (1-P)U(O_j) - U(N_j)] + \frac{\partial B_i(z_i, z_j)}{\partial z_i}([PU(C_i) + (1-P) \times U(O_i) - U(N_i)]) - \left[\frac{PB_i(z_i, z_j)U'(C_i)}{\phi}\right]$$

Rewrite as:

$$\frac{\partial}{\partial z_i}\sum_{i=1}^{2} EU_i = 0 = K + \frac{\partial B_i}{\partial z_i}\{PU(C_i) + (1-P)U(O_i) - U(N_i)\} - \{PB_iU'(C_i) + (1-P) \times B_iU'(O_i) + (1-B_i)U'(N_i)\},$$

where $K = \frac{\partial B_j}{\partial z_i}\{PU(C_j) + (1-P)U(O_j) - U(N_j)\} > 0$. When $K = 0$, we obtain the first-order conditions for the scenario when firms maximize their own utility.

Maximization requires that $\begin{vmatrix} U_{zz} & U_{zI} \\ U_{Iz} & U_{II} \end{vmatrix} > 0$, $U_{II} < 0$, $U_{zz} < 0$. We also have:

$$U_{Iz} = \frac{\partial B_i}{\partial z_i}\left[\left(1 - \frac{\partial \pi_i}{\partial I_i}\right)PU'(C_i) - \frac{\partial \pi_i}{\partial I_i}(1-P)U'(O_i) + \frac{\partial \pi_i}{\partial I_i}U'(N_i)\right] - \left[\left(1 - \frac{\partial \pi_i}{\partial I_i}\right)PB_iU''(C_i) - \frac{\partial \pi_i}{\partial I_i}(1-P)B_iU''(O_i) - \frac{\partial \pi_i}{\partial I_i}(1-B_i)U''(N_i)\right] < 0$$

and $U_{zk} > 0$, $I_{Ik} = 0$. Therefore,

$$\frac{\partial z}{\partial K} = -\frac{\begin{vmatrix} U_{zk} & U_{zI} \\ U_{Ik} & U_{II} \end{vmatrix}}{\begin{vmatrix} U_{zz} & U_{zI} \\ U_{Iz} & U_{II} \end{vmatrix}} > 0; \frac{\partial I}{\partial K} = -\frac{\begin{vmatrix} U_{zz} & U_{zk} \\ U_{Iz} & U_{Ik} \end{vmatrix}}{\begin{vmatrix} U_{zz} & U_{zI} \\ U_{Iz} & U_{II} \end{vmatrix}} < 0.$$

So in the social planner case, z is higher and I is lower.

Proof for Proposition 7

$$\frac{\partial E(U_i)}{\partial z_i} = 0 = \frac{\partial B_i(z_i, z_j)}{\partial z_i}(PU(W - L + \{1 - [1+\tau]\phi\}I_i - z_i + d_i) + (1-P) \times U(W - L - [1+\tau]\phi I_i - z_i + d_i) - U(W - [1+\tau]\phi I_i - z_i + d_i)) - \frac{B_i(z_i, z_j)PU'(W - L + \{1 - [1+\tau]\phi\}I_i - z_i + d_i)}{(1+\tau)\phi},$$

$$\frac{\partial E(U_i)}{\partial I_i} = 0 = B_i(z_i, z_j)P\{1 - [1+\tau]\phi\} \times U'(W - L + \{1 - [1+\tau]\phi\}I_i - z_i + d_i) - (1+\tau)\phi(1-P)B_i(z_i, z_j) \times U'(W - L - [1+\tau]\phi I_i + z_i - d_i) - (1+\tau)\phi\{1 - B_i(z_i, z_j)\} \times U'(W - [1+\tau]\phi I_i - z_i + d_i).$$

After substituting $z_i = z_j = z_s^*$, $I_i = I_j = I_s^*$ in the above first-order conditions and equating them to the corresponding equations for the socially optimal solution, we obtain τ^* given in the proposition. Furthermore, rewriting the first of the two first-order conditions, we get:

$$\phi \frac{\partial B_j}{\partial z_i}\{PU(C_j) + (1-P)U(O_j) - U(N_j)\} + \phi \frac{\partial B_i}{\partial z_i}\{PU(C_i) + (1-P)U(O_i) - U(N_i)\} - PB_iU'(C_i) = 0.$$

Since the second term is positive, $\phi \frac{\partial B_j}{\partial z_i}\{PU(C_j) + (1-P)U(O_j) - U(N_j)\} < PB_iU'(C_i)$, So, $\tau^* > 0$.

REFERENCES

1. Cavusoglu H, Mishra B, Raghunathan S. The effect of Internet security breach announcements on market value: Capital market reaction for breached firms and Internet security developers. International Journal of Electronic Commerce, 2004; 9(1):69–105.
2. Ponemon L. National Survey on the Detection and Prevention of Data Security Breaches, 2006. Available at: http://www.csoonline.com/features/ponemon/ponemon102306.html, Accessed on September 11, 2006.
3. Pauli D, Crawford M. Cyber Insurance, What's That? 2006. Available at: http://www.cso.com.au/article/10744/cyber_insurance_what, Accessed on July 23, 2006.
4. Harrington SE, Neihaus GR. Risk Management and Insurance, 2nd ed. New York: McGraw-Hill/Irwin, 2003.
5. Ehrlich I, Becker GS. Market insurance, self-insurance, and self-protection. Journal of Political Economy, 1972; 80(4):623–648.
6. Rothschild M, Stiglitz J. Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. Quarterly Journal of Economics, 1976; 90(4):629–649.
7. Dionne G, Harrington SE. An Introduction to Insurance Economics, Foundations in Insurance Economics. Boston, MA: Kluwer Academic Publishers, 1992.
8. Orszag PR, Stiglitz JE. Optimal Fire Departments: Evaluating Public Policy in the Face of Externalities, 2002. Available at: http://www.brookings.edu/views/papers/orszag/20020104.pdf, Accessed on September 19, 2005.
9. Lakdawalla D, Zanjani G. Insurance, self-protection, and the economics of terrorism. Journal of Public Economics, 2005; 89(9–10):891–1905.
10. Anderson R. Why Information Security is Hard: A Economic Perspective, 2001. Available at: www.cl.cam.ac.uk/~rja14/Papers/econ.pdf, Accessed on September 19, 2005.
11. Gordon LA, Loeb MP. The economics of information security investment. ACM Transactions on Information and System Security, 2002; 5(4):438–457.
12. Varian H. System Reliability and Free Riding, Workshop on Economics and Information Security, College Park, MD, 2002.
13. Kunreuther H, Heal G. Interdependent security. Journal of Risk and Uncertainty, 2003; 26(2–3):231–249.
14. Hausken K. Income, interdependence, and substitution effects affecting incentives for security investment. Journal of Accounting and Public Policy, 2006; 25(6):629–665.
15. Cremonini M, Nizovtsev D. Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. Workshop on the Economics of Information Security, Cambridge, UK: 2006.
16. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer system security: An economic analysis. Journal of Accounting and Public Policy, 2003; 22(6):461–485.
17. Gal-Or E, Ghose A. The economic incentives for sharing security information. Information Systems Research, 2005; 16(2):186–208.
18. Majuca RP, Yurcik W, Kesan JP. The Evolution of Cyberinsurance, 2005. Available at: http://arxiv.org/ftp/cs/papers/0601/0601020.pdf, Accessed on September 19, 2005.
19. Gordon LA, Loeb MP, Sohail T. A framework for using insurance for cyber-risk management. Communications of the ACM, 2003; 44(9):70–75.
20. Böhme R, Kataria G. Models and Measures for Correlation in Cyber-Insurance. Workshop on the Economics of Information Security, Cambridge, UK: 2006.
21. Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Sadhukan SK. e-Risk Management with Insurance: A Framework Using Copula Aided Bayesian Belief Networks. Hawaii International Conference on System Sciences, Hawaii, 2006.
22. Herath H, Herath T. Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management. Workshop on the Economics of Information Security, Pittsburgh, PA, 2007.
23. Bolot J, LeLarge M. Cyber Insurance as an Incentive for Internet Security. Workshop on the Economics of Information Security, Hanover, NH, 2008.
24. Shetty N, Schwartz G, Felegyhazi M, Walrand J. Competitive Cyber-Insurance and Internet Security. Workshop on the Economics of Information Security, London, 2009.
25. Arrow KJ. Uncertainty and the welfare of medical care. American Economic Review, 1963; 53:941–973.
26. Pauly MV. The economics of moral hazard: Comment. American Economic Review, 1968; 58:531–537.
27. Spence M, Zeckhauser R. Insurance, information and individual action. American Economic Review, 1971; 61(2):380–387.
28. Shavell S. On moral hazard and insurance. Quarterly Journal of Economics, 1979; 93(4):541–562.
29. Hart O, Holmstrom B. The theory of contracts. In Bewley T (ed). Advances in Economic Theory. New York: Cambridge University Press, 1987.
30. Crews CW. 2005. Cyber Security Finger-Pointing, 2005. Available at: http://cei.org/pdf/4569.pdf, Accessed on September 19, 2005.
31. Pigou AC. Economics of Welfare. London: Macmillan, 1920.
32. Coase R. The problem of social cost. Journal of Law and Economics, 1960; 3:1–44.
33. Holmstrom B. Moral hazard in teams. Bell Journal of Economics, 1982; 13(2):324–340.