A Model to Analyze the Unfulfilled Promise of Cyber Insurance: The Impact of Secondary Loss

Tridib Bandyopadhyay • Vijay S Mookerjee • Ram C Rao

University of Texas at Dallas, School of Management, PO Box 830688, JO44
Richardson, Texas 75803-0688

tridib@utdallas.edu • *vijaym@utdallas.edu* • *rrao@utdallas.edu*

Abstract

Firms often manage cyber risks first by investing in security technologies and then by purchasing cyber insurance to cover for residual risk. However, despite the increasing dependence of firms on information assets, a mature market for cyber insurance is yet to emerge. Lack of actuarial data, market inexperience and accounting difficulties are widely cited as major reasons for slow growth of cyber insurance products. Here, we consider another possible explanation: filing cyber insurance claim for a previously undisclosed breach could constitute a tacit disclosure of the breach incident. Stakeholders use such information to adversely revise their risk perception about the firm - leading to a situation where an insured firm may avoid claiming losses incurred from a cyber attack. We develop a model that analyzes an insured firm's optimal claim strategy when hit by a cyber attack. We show that this claim strategy influences the conditions for a viable market for cyber insurance products, and also explains why cyber insurance products could end up being unattractive to the target clientele. We also discuss the policy implications of our analytical findings.

1. Introduction

The current level of sophistication in security technology does not offer complete immunity from IT security risk. One way that firms try to cover information security risk is first by investing in security technologies, and then buying cyber insurance cover for the residual risk (Gordon, Loeb and Sohail, 2003). Cyber insurance refers to contracts that stand to mitigate liability issues, property loss, and theft (Marsh e-business solutions, 2003). These contracts may also cover financial loss resulting from data damage, loss of income from network security failures, cyber-extortion, cyber-terrorism, post incident public relations fees, and criminal reward fund reimbursements (CIO Magazine, 2003).

Because it has the potential to provide umbrella coverage of several information security risks, cyber insurance offers significant promise in the strategic management of residual IT security risks. It is not surprising, therefore, that the size of the cyber insurance market was expected to reach $3.6 billion by 2005 in US (Insurance Information Institute, 2003). However, the market failed to perform anywhere near that mark; estimates indicate a sale of only $200 million of cyber insurance products in 2002, whereas potential losses ran in billions (Treasury and Risk Management, May 25, 2004). This suggests that cyber insurance has failed to play the role of an efficient vehicle to manage IT security risk. Accepted reasons for the underdevelopment of the cyber insurance market are industry inexperience, scant empirical data and history, and difficulties associated with estimating cyber losses (ICLR Research, April 2004).

1.1. Problem and Motivation

While the above reasons for the weak cyber insurance market are clearly plausible, we ask the question: Are there some characteristics inherent to the behavior of insured firms that make cyber insurance products an ineffective means to transfer cyber risk? Consider the following observations:

- Breach incident disclosures have been empirically shown to adversely affect stock prices, and hence the market capitalization of a firm (Cavusoglu et al, 2004).
- The FBI survey of 2002 found that about 90% of respondents detected computer security breaches in the past year but only 34% reported those attacks to authorities (USA Today, April 2002).
- Firms fear that consumer confidence will decrease with occurrence of cyber attacks (ICLR Research, April 2004).
- The Ernst and Young Global Information Security Survey (2003) suggest that a section of IS managers fear that filing an insurance claim could expose security and intelligence breaches (Information Security Magazine, August 2004).

Given these observations, it is possible that regulatory restrictions permitting, firms may not claim a cyber loss if the act of making a claim discloses the cyber attack event to stakeholders.[1] Managers must therefore take into account the secondary loss that may be triggered by the act of

[1] An insurance claim process constitutes investigation by the insurer (or a third party specialist), and involvement of the insured firm's accounting affiliates and other groups, rendering it difficult to keep a breach event private.

claiming, while calculating the expected indemnity payout of the claim. If this altered claiming behavior is not apparent to the insurer, the expected indemnity calculated by the contracting parties may differ. Hence the offered premium structure may appear unattractive to the insured firm. We examine the impact of secondary (subsequent, uninsured) loss associated with cyber (direct, insurable) loss on the cyber insurance market.

1.2. Contributions and Findings

The main contributions and findings of this study are:

1. We build an economic model that describes an optimal cyber insurance contract and the optimal claim strategy for the insured firm. The model captures the effect of secondary loss associated with a cyber breach incident.

2. It is shown that the offered premium of a cyber insurance contract is always more expensive when the claiming strategy of the insured firm is not apparent to the insurer (*Information Asymmetry*), than when it is (*Information Symmetry*).

3. We show that insured firms optimally transfer more risk through cyber insurance contracts under information symmetry than otherwise.

4. In some situations the insurer prefers to consider the insured party's claim strategy. In these situations we speculate that the cyber insurance market will strengthen. However, there are situations where the provider does not benefit from considering the insured firm's claim strategy. We predict that these situations may result in an underdeveloped market, or worse, even market failure. We also discuss the policy implications of these situations.

Our work is significant in that it characterizes the special nature of an insurance contract in the domain of cyber risk. The overall contribution of this work is to provide an additional explanation for the underdeveloped cyber insurance market. Over time, it is possible that the extant reasons for the weakness in the cyber insurance market may be removed with technological advances. This paper identifies a more fundamental reason for market weakness that is based on economic, rather than technological factors. The rest of the paper is organized as follows. In Section 2, we review related work. In Section 3, we set up the basic model after providing the model background, and assumptions. Section 4 analyzes our model under different scenarios (information symmetry and asymmetry) of the cyber insurance market. In Section 5, we report the results and insights from a variety of numerical experiments. Section 6 discusses results, and provides managerial policy implications. Section 7 provides directions for future research, and concludes our work.

2. Related Work

Our research brings together issues of insurance economics and IT security that jointly impact IT risk management within an organization. Specifically we adopt a traditional insurance contract, and have it perform under the new paradigm of IT security risks. Thus we review literature in two main areas: (1) Insurance Economics and (2) IT risk management.

2.1. Insurance Economics

Mossin and Smith (1968) analyze the rational purchase of insurance by an individual who faces risk of loss of her wealth, and exhibits a defined preference structure. In their work, an insurance contract is exogenously determined and a balance is sought between the incremental levels of premium and incremental coverage, where the insured chooses the level of deductible or the cap of the contract, and shares a chosen part of her risk with the insurer. On the other hand, using the endogenous framework of optimal insurance of Borch (1960), Arrow (1971) derives Pareto optimal insurance policies for risk-averse insurers (where coinsurance is optimal) and risk neutral insurers (where full coverage over a deductible is optimal). In line with Arrow's work in this research we assume that the insurer is risk neutral and that the insured is risk averse., such that the offered cyber insurance contract is Pareto optimal above a deductible. Raviv (1979) extends and generalizes Arrow's work and shows that risk preferences do not necessarily determine the forms of optimal insurance contract and that an optimal contract may feature both deductible and coinsurance. Although we do not employ this generalized nature of an optimal contract, we do provide a partial analysis of our problem (Appendix-B) with an insurance contract where both deductible and cap provisions exist. Schlesinger (1981) investigates optimal levels of deductibles in insurance contracts and has shown that under certain assumptions -

conditions of higher loss probability, higher degree of risk aversion or lower level of initial wealth - ensure lower deductibles (more insurance). The variations in the level of optimal deductible in our research builds over and above the above effects, and is a result of the information asymmetry in the cyber insurance market. Through the concept of 'Risk Vulnerability', Gollier and Pratt (1996) explain how the introduction of an unfair risk affects the willingness of the insuring parties to bear the risks of the existing assets, concluding that all standard and proper utility functions are vulnerable to risk. In another contemporary work, Gollier (1996) investigates optimal insurance contracts when some risks affecting wealth remains uninsured, and then shows how presence of this uninsurable background risk reduces the policy deductible when the insured behaves in an economically prudent fashion. In contrast to Gollier's work, our uninsurable (secondary) risks are subsequent in nature, and could get triggered only when a claim is made – rendering 'claiming the realized loss' a strategic decision. Ermoliev and Flam (2000) investigate issues of Pareto optimal insurance contracts under the conditions where the probabilities and distribution of losses are unavailable, and use a scheme of adaptive optimization using Monte Carlo simulation and already observed losses. While the above technique may extend this research in a subsequent phase, our current effort is limited to bringing out the optimal levels of deductible under information symmetry and asymmetry; and we employ numerical experiments to augment our analytical results. Breuer (2004), in his current work relaxes the nonnegativity constraints on the coverage function and investigates how optimal insurance contracts may evolve where for certain ranges of losses, the insured could actually compensate the insurer. Although this is an interesting dimension in itself, we have no indication of such exotic behavior in the cyber insurance domain, and this research considers strictly those contracts where under no circumstances does an insured firm compensates the insurer – barring the upfront premium that buys the contract.

2.2. IT risk management

Gordon, Loeb, and Tashfeen (2003) propose a framework of using cyber insurance in mitigating information risk exposure that may not be addressed through technology. In their framework, an organization needs to appreciate and assess its own information risk exposure and organizational risk profile, and then fill the technology gap (residual risk) through the use of pertinent financial instruments (cyber insurance contracts). Ogut et al. (2005) show how firms could distribute their risk mitigation efforts in technology and financial domains. Unlike the above, we develop our research in the sole premise of residual information risks, which may not be mitigated with the use of currently available technologies. Cavusoglu et al. (2004) investigate the observed effects of breach exposure on stock prices of affected firms through an event study, concluding negative impact under general considerations. Moderating the outcome of the event study by Cavusoglu et al. (2004), Campbell et al. (2003) argue that economic consequences of a reported breach depend on the underlying assets affected by the breach: clarifying that security breaches that involve unauthorized access of confidential data bring higher negative economic impact than otherwise.

In essence, the framework of our model brings together the intuitions developed by the seminal work of Borch (1960) and the observed secondary loss of realized breach (Cavusoglu et al., and Campbell et al.), whereas our model background somewhat resembles that of Gollier (1996). However, unlike Gollier's work where an uninsurable background risk exists per se, in our work, the secondary loss (and risk thereof) is triggered by the act of breach disclosure (explicit or implicit), and is partly or fully controllable at the insured firms' end. Unlike the works of Cavusoglu et al. and Campbell et al., secondary loss from an IT breach is not the effect, but the driver for downstream strategies in our model.

3. The Model

We first state some preliminaries, our assumptions, and describe the background useful for development of the model before we present notation (*Table-1*) used to develop the model. Notation used in later sections of this paper is also included here for convenience. Next we derive the claiming strategy of an insured firm when a cyber insurance contract is in place. Finally we develop the model, and solve it to provide an optimal cyber insurance contract from the perspective of an insured firm.

3.1. Preliminaries

Types of IT security breach: We classify IT security breaches in two main categories: *pandemic* and *directed*.

1. *Pandemic breaches* (typically outsider initiated) exploit system vulnerabilities of those IT systems, which are widely employed across firms (e.g. Microsoft Internet Information Services Remote Buffer Overflow). These breaches often propagate through network connectivity, and affect many firms in a short period of time (e.g. the rampant breaches caused by virus/worms such as ‘love-bug’, ‘I love you’ etc.). The discerning characteristics of these breaches are that a) there is no firm-specific malice intended, and that b) no firm-specific vulnerabilities are exploited. Given the scale and scope of these breaches, an affected firm has no *motivation* (and often no *ability* either) to conceal pandemic breaches.
2. A *directed breach,* on the other hand, exploits a firm specific flaw, or system/personnel vulnerability (flawed security policy, social engineering vulnerability etc.), and may be insider or outsider initiated. Because this is a firm specific attack, the breach often reveals the health and dependability of the information security practices of the specific firm. A firm, affected by a directed breach, has the *motivation* to mask the breach/vulnerability information from its stakeholders, and may do so (as suggested by FBI survey 2002, and the event study of Cavusoglu et al., 2004) within the bounds of accounting norms and other

regulatory obligations. When a firm is able to hide the breach information and does so, we term the directed breach '*private*'. When an affected firm discloses a directed breach publicly, we define the breach as '*public*'. The definition of a breach being private or public is *ex-post*: an affected firm's decision in this regard necessarily follows the actual realization of the breach event.

In this research, we further assume that for an insured firm directed and pandemic breaches occur randomly in proportions δ and (1- δ), and within directed breaches, private and public breaches occur randomly in proportions γ and (1- γ).

Types of Loss: We categorize losses from security breaches into the following *two* types, *Cyber Loss* and *Secondary Loss;* and define them as follows:

1) *Cyber losses* are business, and other losses caused directly by a breach incident. This may include property, rights or transactional losses, maintenance and recovery expenses, contractual losses, as well as liability and other losses. In essence, all first party and third party losses that are directly attributable to the breach event are cyber losses. Such losses are direct, and may be covered in a cyber insurance contract.

2) *Secondary losses* stem from the 'loss in stakeholder confidence' when information about a breach incident reaches them. We differentiate secondary loss exposure from cyber (primary) loss exposure in the following manner: the first is a second-degree exposure, subsequent to the first-degree (direct) exposure of a realized breach. By the very fact that the secondary loss is a subsequent loss, it may not be covered in an insurance contract written for cyber loss.

It is important to realize the relationships between the types of breach, and the losses that stem from them. A public breach automatically begets both cyber and secondary losses to the firm (by our definition, the public breach incident is readily disclosed to the stakeholders). On the other hand, a private breach brings cyber loss to the firm anyway, but the secondary losses accrue only when the breach information is available to the stakeholders in a direct or tacit manner (e.g., by the act of claiming). The pandemic breaches expose no firm-specific vulnerabilities, and the attacked firm suffers only cyber losses.

Nature and magnitude of secondary loss: Although studies have empirically established post-disclosure secondary losses for information compromises (Cavusoglu et al., 2004, and Campbell et al., 2003), the nature of such losses may vary. The secondary losses can be event oriented, loss oriented, claim oriented or some combinations thereof as we discuss below.

1. A breach is event oriented when the loss in stakeholders' confidence, that translates to the secondary losses is constant - implying that all breach events erode stakeholder confidence by the same amount.
2. A breach is loss oriented when stakeholders revise their risk perception in relation to the magnitude of the cyber loss suffered. Here the loss in stakeholder confidence, and hence the secondary loss depends on the cyber losses suffered, which is known to the stakeholders.
3. A breach is claim oriented when stakeholders revise their risk perception in proportion to the magnitude of claim realized by the insurance firm after a breach. Now the secondary loss depends on the realized indemnity I (assuming that not the primary loss, but the realized indemnity is known to the stakeholders from accounting and other statements).
4. When the risk perception is some combination of the breach event, losses, and claims made/realized, a weighted average method could be employed to appreciate the secondary loss.

For the sake of simplicity we treat secondary loss to be event oriented (and hence a constant) in this research[2].

3.2 Assumptions

To model the claiming as well the contracting strategy of an insured firm (hereafter) in relation to a cyber insurance instrument, we make the following assumptions.

1. The secondary loss faced by a firm from a realized IT security breach is constant.
2. The decision to claim is a subsequent decision taken after the breach has been realized.

[2] **Appendix-1** provides a treatment (towards optimal claim strategy of an Insured firm) of secondary loss that is claim oriented, $G = G\ (I)$.

3. For private breach, the claiming process implicitly exposes the breach incident to the stakeholders (through formal or informal channels). For example, the breach information may reach the stakeholders through accounting statements, organizational grapevines, business analysts, or independent technology/trade watch groups.

4. The loss function for cyber losses $f(x)$, the probability of directed breach δ, and the loading factor λ are common knowledge between the contracting parties of cyber insurance. This is done to separate out the effect of secondary loss and the claiming strategy on the cyber insurance market.

5. The expected indemnity payout is proportional to a constant loading factor λ. This is a common assumption in the insurance literature (Raviv 1979) and allows the model to capture a market in which insurance prices (premiums) are set though the action of competitive forces.

3.3. Notation

F_i	Insuring firm, offering cyber insurance (assumed risk neutral)
F_d	Insured firm, buying cyber insurance (assumed risk averse)
W	Insured firm's beginning wealth, a constant
q	Probability of an IT security breach
δ	Conditional probability of a *directed* breach: $P(\textit{directed breach} \mid \textit{breach})$
γ	Conditional probability of a private breach: $P(\textit{private breach} \mid \textit{directed breach})$
x	Insured firm's realization of cyber (primary) loss, given a breach
$f(x)$	Conditional distribution of the Insured firm's cyber loss (transparent between the contacting parties), given a breach
P	Upfront premium for the cyber insurance contract
Γ	Insured firm's claim strategy for a private breach
I	Indemnity payout, $I(x) \geq 0$, $I'(x) \geq 0$,
G	Secondary loss subsequent to a realized breach
U	Insured firm's utility function (assumed concave)
λ	Insured firm's market loading factor (known to both the contracting parties)

TABLE-1. Model Parameters and Decision Variables

3.4 The insurance contract

A cyber insurance contract is a couple (P, I), so that when the insured firm F_d pays an upfront premium P, the insurer firm F_i promises an indemnity payment $I(x)$ in the event of a cyber loss of magnitude x. The upfront premium P depends on the probability distribution of cyber losses $x\,(0 \le x \le \infty)$ of insured firm F_d, and the market-loading factor λ, which includes (among others) third party security readiness assessment fees, and contract writing costs. Because we assume that the market-loading factor is proportional to the expected indemnity payout of the insurer, and that the insurer is risk neutral, F_i offers a Pareto-optimal cyber insurance contract above a deductible x_1 (Borch, 1960). Assuming claims for losses above the deductible are payable in full, the indemnity payout is given by:

$$\begin{array}{ll} I = 0 & 0 \le x \le x_1 \\ I = x - x_1 & x_1 < x \end{array} \qquad \textbf{(\textit{1})}$$

The insurer requires the insured firm to make an upfront payment

$$P = q.(1+\lambda)\int_{x_1}^{\infty}(x - x_1)f(x)dx\ , \qquad \textbf{(\textit{2})}$$

Where q is the probability of breach, and the loss distribution $f(x)$ is conditionally defined on a given breach. The insured firm has an option to choose the deductible x_1 (assumed continuous here), that influences the level of the premium charged by the insurer.

3.5 The contract time line and payoffs to the parties

At the beginning of the contract period (typically a year), a cyber insurance contract is written. This requires the insured firm to communicate an optimal deductible x_1 *. For every deductible x_1 *, the insurer offers a Pareto optimal contract (P^*, I^*), the form of which is represented by (*1*) and (*2*) above. If the optimal deductible is *0*, the insured firm buys full insurance (100% transfer of IT security risk). In case the optimal deductible is infinitely high, the charged premium is $P^* = 0$, there is no contract and the insured firm accepts all risks (or ‘self insurance’). Between these two extreme deductible amounts, all contracts may be feasibly written to optimally transfer partial IT risk to the insurer. Note that the loss function $f(x)$, and the loading factor λ are common knowledge in our model, thus an offered contract (P^{*}, I^{*}) in response to a communicated 'optimal' deductible $x_1{}^{*}$ is always acceptable to the insured firm (assuming no secondary loss). A breach is realized with probability q, and the probability that a realized breach is a directed one is δ. A directed breach becomes public with probability $(1-\gamma)$. The disclosure of a public breach incident is automatic, and the secondary loss G occurs along with the cyber loss x. The insured firm then claims for the cyber loss, and accrues the indemnity payout. On the other hand, a directed breach is private with probability γ and the secondary loss G is incurred only if the insured firm claims. Otherwise, only a cyber loss x is incurred[3].

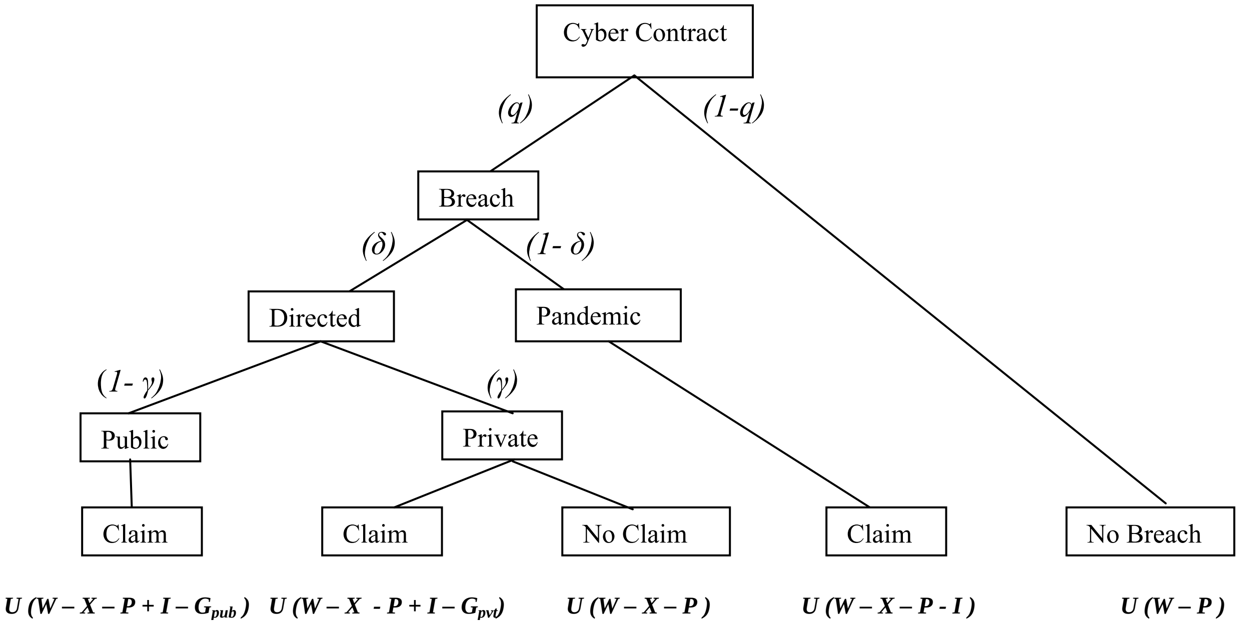


Figure-1. The contingency tree for payoffs to the insured firm in a cyber insurance contract

[3] The utility of the insured firm F_d under all possible situations have been depicted in *Figure-1*. The payoff to the risk neutral insurer F_i is the upfront premium, which is the expected indemnity payout, loaded with the factor λ**.** The 'claim' decision could include full/partial/no claim, depending on the optimized strategy of the Insured firm.

3.6 The insured firm's decision problem

The insured firm first decides its optimal deductible $x_1 *$, and communicates it to the insurer. Having a contract in place, and having realized a *private breach*, the insured firm implements its optimal claim strategy (for *public breach*, the insured firm always claims its realized losses as per the contract provisions). However, the claim strategy in private breach affects the optimal deductible $x_1 *$ in the first place. Here, we utilize a standard backward induction method to find out the optimal claim strategy in the private breach first, and then the optimal deductible $x_1 *$, which maximizes the expected utility to the insured firm. Note that the claiming strategy in private breach implicitly comprises two decisions: '*when to claim*', and '*how much to claim*'.

Define an indicator variable: $\Gamma(x)=1$ when the insured firm claims a realized cyber loss x through a private breach; else $\Gamma(x)=0$. Because we assume an event-oriented, constant secondary loss G, $\Gamma(x)=1$ could include only full claim decision[4]. Given the downstream claim strategy $\Gamma(x)$, the insured firm maximizes the following to arrive at its optimal deductible $x_1 *$.

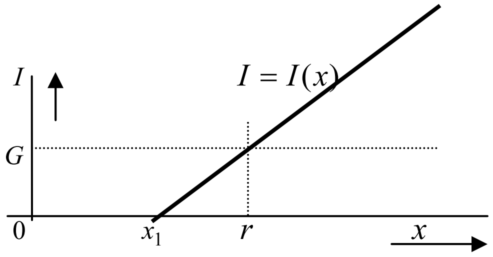
$$\underset{x_1,\ \Gamma(x)}{Max} \left[\begin{array}{l} q\delta\left\{ \gamma\int\limits_0^\infty U\big(W-x-P+\Gamma(x)I(x)-\Gamma(x)G\big)f(x)dx+(1-\gamma)\int\limits_0^\infty U\big(W-x-P+I(x)-G\big)f(x)dx \right\} \\ +q(1-\delta)\int\limits_0^\infty U\big(W-P-x+I(x)\big)f(x)dx+(1-q)\int\limits_0^\infty U\big(W-P\big)f(x)dx \end{array} \right] \qquad \textbf{(3)}$$

The fist term in (*3*) refers to a private breach (probability $q\delta\gamma$). Claiming a private breach means tacit exposure of the breach: but the firm is able to strategize here - thus the realized claim is $I=\Gamma(x)I(x)$. Note that the secondary loss in the private breach is incurred only if a claim is

[4] The act of claiming and NOT the amount of claim begets the constant secondary loss *G*. Thus it is a dominant strategy to claim all losses truthfully once it is optimal to claim losses from a private breach (vide *Figure-2*, and *proposition-1*). Claiming more than realized loss is illegal by contract design.

made (i.e. $\Gamma(x)=1$). The second term represents the case of a public breach (probability $q\delta(1-\gamma)$). The information regarding a public breach reaches stakeholders directly - the secondary loss is always incurred - and the managers have no reason to deviate from contract intended behavior. The third term refers to the situation where the firm has suffered a pandemic breach (probability $q(1-\delta)$). The firm suffers cyber loss x, but there are no secondary losses to consider: the firm claims the cyber loss, and realizes the indemnity payment. The fourth term refers to a situation where the firm does not suffer breach, the probability mass of which is given by $(1-q)$.

Proposition 1: *For constant secondary loss G associated with a realized private breach, there exists a minimum loss $r\ (=x_1+G)$ up to which the insured firm does not claim its losses, for losses above r, the insured firm claims its actual loss.*
Proof: *Appendix – 1.*



The net revenue R that the insured firm realizes from Indemnity payment $R(x)=I(x)-G$

Figure-2. The strategized deductible *r* in a private breach, and the contracted deductible x_1

The implications of proposition-1 are the following:

1. In case of private breaches, the existence of secondary loss increases the effective deductible of the cyber insurance contract. Contrary to the (contract) designed behavior, in the range $x_1 \le x \le r$, the insured firm does not claim its losses in private breach.
2. The unclaimed loss in the range $x_1 \le x \le r$ (although contractually realizable) reduces the overall expected indemnity receipt from the cyber insurance contract.

Importantly, an insurance contract with a *fixed* deductible cannot alter this '*no claim*' strategy of the insured firm in range $x_1 \le x \le r$.

3.7 The optimum deductible for the contract

Knowing the exact claiming strategy in case of a private breach (*Proposition-1*), and the concomitant indemnity payouts, (*3*) now modifies to the following:

$$\underset{x_1}{Max}\left(\begin{array}{l} q\,\delta\,\gamma\left(\int\limits_0^{x_1+G} U\left(W - x - P\right) f(x)\,dx + U\left(W - x_1 - P - G\right)\left(1 - F(x_1 + G)\right)\right) \\ +\, q\,\delta\,(1-\gamma)\left(\int\limits_0^{x_1} U\left(W - x - P - G\right) f(x)\,dx + U\left(W - x_1 - P - G\right)\left(1 - F(x_1)\right)\right) + \\ q\,(1-\delta)\left(\int\limits_0^{x_1} U\left(W - x - P\right) f(x)\,dx + U\left(W - x_1 - P\right)\left(1 - F(x_1)\right)\right) + (1-q)\,U\left(W - P\right) \end{array}\right) \qquad \textbf{(4)}$$

The solution of the above problem yields the optimal deductible $x_1{}^*$, which is now communicated to the insurer for the cyber insurance contract. However, as we show in the next subsection, the communicated deductible $x_1{}^*$ prices the cyber insurance contract differently depending upon whether the insurer is cognizant of a) the existence of the secondary loss G and b) the distribution of private and public breaches γ .

3.8 The insurer's pricing decision

We define an insurer *uninformed* when s/he is not cognizant of *either* the secondary loss G , *or* the distribution of the breaches γ . An *informed* insurer is cognizant of G and γ . The possibility of a *partially informed* insurer (who knows only one of the factors, G or γ) in the market is plausible, but that is of no particular consequence here. Knowing G alone, the insurer does not change the premium structure (subsequent losses are outside contract consideration); knowing γ alone, the insurer cannot discern altered claim behavior. As a result, the pricing decisions (our concern here) of the uninformed and the partially informed insurers remain identical. In order to appreciate the deviated claiming strategy of the insured firm, the insurer necessarily needs to know both G and γ; thus we subsume the partially informed insurer in to our uninformed insurer category. Having categorized the insurers, their pricing structures for a cyber insurance contract for a deductible x_1 are as follows:

1. The uninformed insurer offers the contract for a premium

$$P_u = q.(1+\lambda)\int_{x_1}^{\infty}(x-x_1)dF(x) \tag{5}$$

2. The informed insurer offers the contract for a premium

$$\begin{aligned} P_i = q\,\delta(1+\lambda)\left(\gamma\int_{(x_1+G)}^{\infty}(x-x_1)\,f(x)dx + (1-\gamma)\int_{(x_1)}^{\infty}(x-x_1)\,f(x)dx\right) + \\ q\,(1-\delta)(1+\lambda)\int_{(x_1)}^{\infty}(x-x_1)\,f(x)dx \end{aligned} \tag{6}$$

While the above equations are self-explanatory, the following lemma is in order now:

Lemma 1: *For any given deductible, the informed insurer offers a cyber insurance contract that is never priced higher than that offered by the uninformed insurer i.e.* $P_u \geq P_i$.

Proof: *Appendix-1.*

The expected utility of the insured firm depends on the structure of premium (*5*) or (*6*) used in (*4*). As a result, the optimal deductible $x_1{}^*$ (which is to be communicated to the insurer) is now affected depending on the type of the insurer.

4. Analysis

In section-3 we have argued that the a) the secondary loss (G) from a realized breach and b) the distribution of private and public breaches (γ) together alter the optimal deductible in the consumption side, and also the pricing structure in the supply side. Here we are concerned with the comparative performance of the insurance instrument, as G and γ are revealed to the contracting parties. In order to facilitate the comparison, we introduce specific functional forms for the utility and the cyber loss function of the insured firm. We employ the standard logarithmic function $U(.) = Ln\,(.)$ for the utility of the insured firm. The logarithmic utility function of the insured firm preserves the concavity assumption in our model, thereby ensuring risk averseness of the insured. For the cyber loss x, we employ a uniform loss distribution function given by $f(x) = {}^{1}\!\big/_{(b-a)},\ a \geq x \geq b,$. In absence of an empirically established cyber loss distribution, our assumption of uniform loss function is of general interest in the sense that any malevolent breach could be equally probable, and that depending on the target asset, the losses incurred could fall in a known range.

Under the assumed logarithmic utility and uniform loss functions, the insured firm now optimally selects its deductible $x_1{}^*$ ($0 \leq x_1 \leq b$), which maximizes the following:

$$\underset{x_1}{Max}\left(\begin{array}{l} \dfrac{q}{b-a}\left\{\begin{array}{l} \delta\,\gamma\left(\displaystyle\int_0^{Min\{(x_1+G),b\}} Ln\big(W-x-P\big)dx + Ln\big(W-x_1-P-G\big)\big(b-Min\{(x_1+G),b\}\big)\right)+ \\ \delta\,(1-\gamma)\left(\displaystyle\int_0^{Min\{x_1,b\}} Ln\big(W-x-P-G\big)dx + Ln\big(W-x_1-P-G\big)\big(b-Min\{x_1,b\}\big)\right)+ \\ (1-\delta)\left(\displaystyle\int_0^{Min\{x_1,b\}} Ln\big(W-x-P\big)dx + Ln\big(W-x_1-P\big)\big(b-Min\{x_1,b\}\big)\right) \end{array}\right\} \\ +\,(1-q)\;Ln\big(W-P\big) \end{array}\right) \tag{7}$$

$$\textit{Subject to}\text{: } W > Max\{\,(G+a+P(a)),(G+b),(P(0)+Max\{G,a\})\,\}$$

Note that:

a) The constraint introduced above is the minimum initial wealth required for the insured firm: this is needed to conserve the integrity of the logarithmic utility function of our model.

b) We have conveniently restricted the bounds of search for optimal deductible in (*7*). Given our uniform loss function, the upper bound of the search space for x_1 is *b*: beyond that point $f(x) = 0, F(x) = 1$ everywhere, and neither the structure of expected utility $E[U]$ of the insured firm (*4*), nor the premium $P(x_1)$ i.e. (*5*) *or* (*6*) undergoes any change. In other words, $\forall\, b \leq x_1$, $E[U]$ is constant. The search range includes $a \leq x_1 \leq b$, because the location of x_1 directly affects the limits of integration in the premium structure, which affects $E[U]$. Although the limits of integration in the premium structure is unaffected for $0 \leq x_1 < a$; the premium $P(x_1)$ does change in that range because the integrand $(x - x_1)$ varies, which in turn affects the expected utility $E[U]$ of the insured firm. In essence, the insured firm could optimally select its deductible in the restricted range $0 \leq x_1 \leq b$, without sacrificing any performance in solution.

4.1 IT security risk and information asymmetry in cyber insurance

In view of the fact that IT security risks are new, and that our understanding of the field is still maturing; we conjecture that the cyber insurance market participants may exhibit lag in their recognition and appreciation of the secondary loss G, and the cases of private and public breaches, γ. Accordingly, we define the following 2 distinct *scenarios* of the evolving cyber insurance market:

1. The cyber insurance market is in *'information asymmetry*', when the insured firm (and not the insurer) recognizes secondary loss from a realized breach, and formalizes the nature of a realized breach (private or public) in its claiming strategy and optimal deductible selection (*informed insured*). The insurer is not cognizant of G and γ, and hence utilizes the schedule of (*5*) to price a contract. While the insured firm's behavior is now modified, neither the behavior nor the underlying reason is apparent to the insurer (*uninformed insurer*).
2. The cyber insurance market is in *'information symmetry*' when the idiosyncratic characteristics of IT risks (G and γ) are transparently known to the insurer (and also to the insured firm: the insured firm cannot have coarse information set than the insurer), and the insurer appreciates the changed behavior (claiming and contracting strategy) of the insured

firm. The *informed insurer* then readjusts its behavior (now utilizes the schedule of (*6*) to price a contract) in order to accommodate the new information.

We conjecture that the cyber insurance market may initially begin from a scenario of *'naïve symmetry'*, where neither the insurer nor the insured firm has yet realized the idiosyncratic characteristics (G and γ) of IT security risks. Over time, the insured firm first realizes the effect of G and γ, (and modifies its claiming and buying behavior) and the market quickly makes a transition to *'information asymmetry*'. Finally, when the insurer knows the altered claiming and buying behavior as well as the underlying reasons, the pricing schedule (premium) is altered. The market then makes a transition to *'information symmetry*'.

Under our assumed functional forms, the insurer now offers the following premium structure[5]:

Scenario-1, Information Asymmetry:

$$P_1 = \frac{q(1+\lambda)}{2(b-a)}\left(b - Max\{a, x_1\}\right)\left(b + Max\{a, x_1\} - 2x_1\right),$$

Scenario-2, Information Symmetry:

$$P_2 = Max\left\{\frac{q(1+\lambda)}{2}\left(b+a-2x_1\right), 0\right\} \quad \forall\, x_1 + G < a,$$

$$P_2 = Max\left\{\frac{q(1+\lambda)}{2(b-a)}\left\{(b-a)(b+a-2x_1) - \gamma\delta\left(G^2 - (a-x_1)^2\right)\right\}, 0\right\} \quad \forall\, x_1 < a, \quad a \le x_1 + G \le b \tag{8}$$

$$P_2 = Max\left\{\frac{q(1+\lambda)(1-\gamma\,\delta)}{2}\left(b+a-2x_1\right), 0\right\} \quad \forall\, x_1 < a, \quad x_1 + G > b$$

$$P_2 = Max\left\{\frac{q(1+\lambda)}{2(b-a)}\left\{(b-x_1)^2 - \gamma\,\delta\, G^2\right\}, 0\right\} \quad \forall\, x_1 \ge a, \quad x_1 + G \le b$$

$$P_2 = Max\left\{\frac{q(1+\lambda)(1-\gamma\,\delta)}{2(b-a)}(b-x_1)^2, 0\right\} \quad \forall\, x_1 \ge a, \quad x_1 + G > b$$

4.2 Systemic overpricing of the offered premium in information asymmetry:

Before we analyze the optimal deductible under the scenarios, it is important to understand the intensity of information asymmetry caused by the levels of secondary loss G, and the

[5] The offered premiums are written in view of the restricted search space for deductible is $0 \le x_1 \le b$.

probability of private breach γ between the scenarios. *Lemma-1* already suggests that an insurance contract in information asymmetry is generally overpriced. Under our assumed functional forms, the following is in order now:

Lemma 2: *Ceteris paribus, for a selected deductible* $x_1, x_1 \geq 0$, *the apparent premium overpricing* $(P_1 - P_2)$ *in information asymmetry:*

1) *Does not exist in the range* $x_1 \leq Max\{(a-G), 0\}$
2) *Increases linearly with the probability of private breach* γ *in the range* $x_1 > Max\{(a-G), 0\}$
3) *Exhibits quadratic increase with the secondary loss G in the range* $a < x_1 + G \leq b$
4) *Remains invariant of the secondary loss G in the range* $x_1 > Max\{(b-G), 0\}$

Proof: *Appendix – 1.*

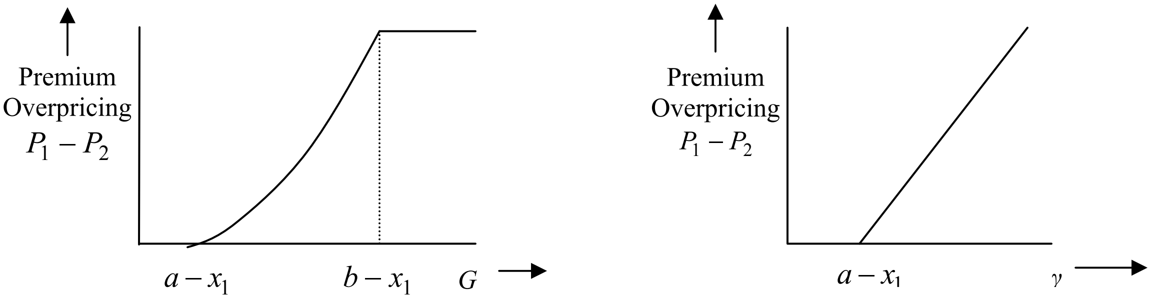


Figure-3. Premium overpricing at deductible levels ${}^i x_1$ when secondary loss *G* increases

The information set of the insurer becomes finer as the market moves from information asymmetry to information symmetry. This alters the premium structure (*8*) offered by the insurer, which in turn impacts the expected utility structure (*7*) of the insured firm. In effect, the chosen optimal deductible (x_1 *) differs under the 2 scenarios of the cyber insurance market. Importantly, the chosen level of optimal deductible not only affects the contract premium; it also impacts the proportion of cyber security risk that could be optimally transferred to the insurer (efficiency of the instrument). A lowering in deductible, ceteris paribus, indicates that the contract transfers proportionally higher risk to the insurer.

5. Numerical Analysis

The goal of this section is to compare the optimal deductible that the insured firm selects under the scenarios of information asymmetry symmetry. The FOC of (*7*) is transcendental in nature, and is not amenable for variable separation. Thus the optimal deductibles cannot be isolated analytically. In what follows we report our numerical experiment, and investigate the optimal deductibles when the parameters vary, and the information scenario changes.

5.1 Parameters and variables of experiment:

We use wealth W as the normalized scaling parameter (base value *600*), which we swing *15%* upwards of base value to test for the firm's wealth effect on optimal deductibles. The range of direct cyber loss x is chosen in a wide range, from *8%* to *80%* of the initial wealth. This is done in order to emphasize the IT intensity and pervasiveness in the operations of the insured firm F_d, for whom the cyber insurance contract is an important alternative to manage IT security risks. The secondary loss G varies from *0%* to *15%* of the initial wealth of the firm. At the upper range, this ratio is indeed high, but such a choice is purposely exercised to accentuate the intensity of asymmetry between the insurer and the insured, and test the levels of risk transfer[6]. The probability mass q signifies the basic level of security readiness of the insured firm. In our experiment we vary q from *0.1* to *1.0*, to compare the effect of information asymmetry on the range of firms where some firms are almost impregnable (low q), and others have high probability of breach (high q). The base value of the directed breach δ is *0.9*, signifying that pandemic breaches are none too frequent for the insured firm under consideration. This could also mean that the insured firm regularly updates its systems with the security patches that popular vendors regularly deliver free of cost. As such, general experience suggests infrequent

[6] Cavusoglu et al. (2004) estimate losses some what below 4% for the firms in their dataset.

attacks of pandemic nature. In view of the FBI survey, our base value of private breach γ is fixed at *0.7*. The market-loading factor λ has a high base value of *0.5*. This is deliberately done to emphasize the fact that the cyber insurance market is in a nascent stage, and the insurer must operate on a higher mark up (very high cost of third party security assessment, and high contract writing costs). The base values and the ranges of the parameters (and their symbols) are tabulated below:

Parameters and decision variables	Symbol	Base value and range
Secondary loss	G	*50, 0* to *90*
Initial wealth	W	*600, 600* to *690*
Minimum loss	a	*50, 20* to *200*
Maximum loss	b	*500, 200* to *560*
Conditional Probability of directed breach	δ	*0.9, 0.1* to *1.0*
Conditional Probability of private breach	γ	*0.7, 0.1* to *1.0*
Market loading factor	λ	*0.5, 0.2* to *0.7*
Probability of a breach	q	*0.9, 0.1* to *1.0*
Optimal deductible in information asymmetry	x_{11}	--, *0* to *500*
Optimal deductible in information symmetry	x_{12}	--, *0* to *500*

Table 2. Parameters and decision variable in numerical experiment

5.2 Search space for the optimal deductible x_1 *; and discontinuity in expected Utility

The numerical experiment of this work centers on (*7*), which captures the expected utility of the insured firm; and (*8*), which represents the reaction function of the insurer. Recall that given the functional form of the cyber loss, it is sufficient to restrict the search in $0 \le x_1 \le b$, and note that (*7*) and (*8*) are already adjusted to facilitate the restricted search. It is also sufficient to dissociate the discontinuous expected utility in to a set of adjacent problems, and then select the best solution among them (*Appendix-3*).

5.3 Results

Secondary loss *G*, optimal deductible x_1 *, and upfront premium *P:** The direction in which changes in *G* affects the deductible depends on its level, whereas the intensity of the effect depends on the scenario of cyber insurance market.

1. There are two effects of the secondary loss *G* on the way the optimal is chosen by the insured firm. First, it works as an unmitigated background risk, which when realized, has a reducing effect on the wealth of the insured firm. Secondly, *G* has an overpricing effect on the premium (vide lemma-*2*), because it reduces the range in which the insured firm can claim its loss (private breach), thereby reducing the expected indemnity receipt from the contract. Between these two opposing forces, an equilibrium deductible is established. *Figure-4* depicts the trajectory of this deductible for the scenarios of information a/symmetry. These opposing effects are apparent when (*4*) is investigated closely:
    a. The secondary loss *G* appears on the limits of integration: here it affects (negatively) the range of claim, and hence indemnity realization of the insured firm. Increase in *G* works against the motivation of insurance purchase here. Form this perspective, we may expect an increase in deductible as the secondary loss increases. In symmetry, the reduction of expected indemnity receipt is compensated, which is however not the case in information asymmetry. Thus the increasing effect of deductible could be relatively higher in case of information asymmetry.
    b. The secondary loss *G* also appears in the argument of the utility function of the insured firm (we may approximate the effect as $W_{effective} = W - G$, thereby creating a wealth effect in the negative direction). Here, introduction of *G* causes the insured firm to slide leftwards on its concave utility curve, where it is more risk averse and is amenable to buy more insurance. Increase in *G* here works as a motivating factor for purchase of more cyber insurance.

2. When *G* is small, the wealth effect is small in comparison to the indemnity effect (the insured firm operates in a flatter region of its utility curve), thus the resultant effect increases the deductible, and the insured firm chooses to buy less insurance. However, between the scenarios of asymmetry and symmetry, the following is important: When *G* is very small, the difference between the deductibles in symmetry and asymmetry is insignificant, and the trajectories are almost coincident (*figure-4*). However, note that as *G* increases further (about 20), the systemic premium overpricing effect picks up (lemma-*2*, quadratic increase in the range $G < b - x_1 *$). The trajectory of $x_{11} *$ visibly rises above that of $x_{12} *$, and exhibits accelerated rise till $G = b - x_1 *$. After that, the systemic overpricing remains constant, and the trajectories of x_{11}*, and $x_{12} *$ are about parallel.

3. At high level of *G*, the wealth effect is more significant; the insured firm slides farther leftwards on its concave utility curve, where the gradient is steeper. As a result, the insured is much more risk averse and is ready to buy more insurance/more costly insurance. This arrests the rising trend of deductible before bringing in a decreasing trend. As the deductible starts to decrease, the firm increasingly regains its ability to claim in private breaches. Although it increases the premium payment, very high level of *G* is able to compensate this increase in premium, and the decreasing trend sustains.

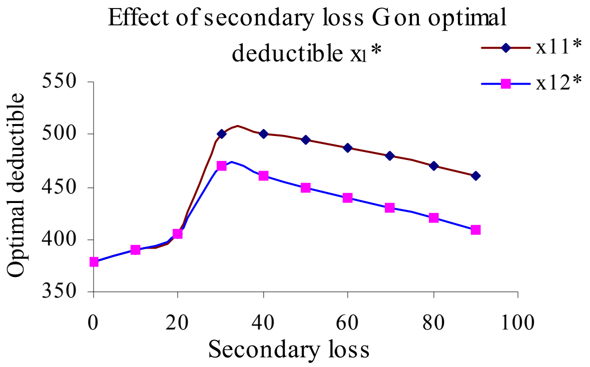


Figure-4. The effect of increasing secondary loss G on optimal deductible

The trend of the trajectories of P_1* and P_2* can be explained in light of the movement of the deductibles $x_{11}*$, and $x_{12}*$, as the secondary loss *G* changes.

1. The general movement of the deductible $P*$ mirrors the movement of the deductible x_1*. Thus for small levels of *G*, we find a decreasing trend in premium, whereas at high levels of *G*, the premium rises (*figure-5*) with increasing *G*. Here we will just concentrate on explaining the difference in the equilibrium (optimal) premiums under the scenarios of a/symmetry.
2. Because there is no apparent premium overpricing in information symmetry, the increasing effect on P_2* for high and increasing *G* is purely attributed to decreasing deductible. In case of information asymmetry, however, for high and increasing *G,* the pure effect of decreasing deductible on P_1* (increase) could be augmented by the effect of increased overpricing in premium (lemma-*2*). However note that, under information asymmetry (*figure-4*), the optimal deductible, while it is decreasing, is chosen such that $G > b - x_{11}*$ (in a range, where the systemic premium overpricing curve is flat). This ensures that falling deductible does not further increase the overpricing of the premium. As a result, the overpricing (augmenting) effect for P_1* is absent in *figure-5*. Thus, the rising curves of P_1* and P_2* for high and increasing G are virtually parallel.

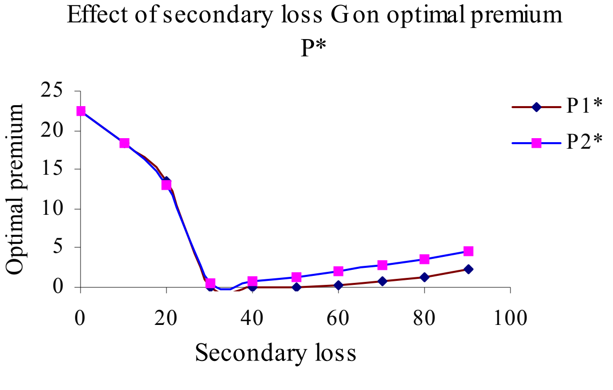


Figure-5. The effect of increasing secondary loss *G* on optimal premium

Probability of private breach γ, optimal deductible x_1* and upfront premium $P*$

When the conditional probability of private breach *(*γ*)* rises without any changes in secondary loss G, there is no immediate effect in the no-claim range of the insured firm. However, two important things happen: (i) it now increases the relative probability (frequency) that a 'private claim' will be made. It also means that a loss x $(x < x_1 + G)$ in private breach will remain unclaimed with higher frequency. These together, provides incentive for the insured firm to reduce its deductible in the 'private breach'. (ii) Because an increase in γ necessarily implies a decrease in $(1-\gamma)$, it now decreases the probability that a 'public claim' will be made. Because the chances for a public claim are reduced, the insured firm would like to increase the deductible for the 'public breach'.

However, the cyber contract is defined on a unique deductible, and the expected utility, in part, is a weighted average of the expected utilities of the insured firm between the private and the public breaches, such that the relative weights of the reclaimable loss (indemnity) from private/public breach decide the unique action that the insured firm takes.

When γ is small, the increasing tendency in deductible for the public breaches preponderates over the decreasing tendency in deductible for the private breaches. So, the overall effect in the initial values of γ on the deductible is increasing. However as γ increases further, the decision suitable for the private breach gains more importance, and the rate of increase in deductible starts falling till it is finally arrested (*figure-6*)[7].

[7] Whether the overall effect could initiate decrease in the deductible at higher values of γ depends on the other parametric values of the problem. In our current set up that overall decreasing effect is not reached before γ reaches its maximum value of 1.

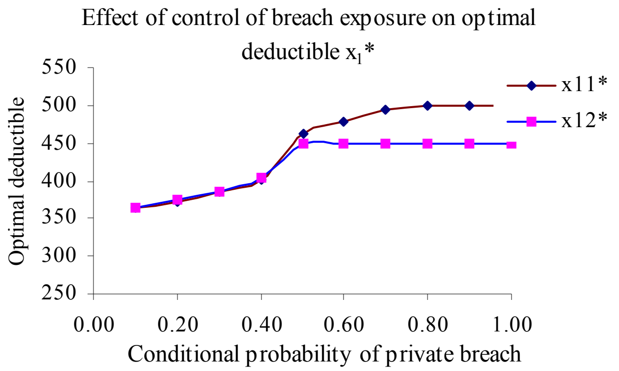


Figure-6. The effect of increasing γ on optimal deductible

In line with the above discussion, the premium in general falls as a reaction to the deductible selection criteria of the insured firm. Under information asymmetry the optimal premium P_1 * falls, as γ increases. Here, the optimal deductible rises almost linearly with γ; the rate of fall in premium is increasingly lower (flat) at higher levels of γ ($-dP/dx_1$ flattens out at elevated x_1 *).

For the symmetric scenario, the effect of the choice of increasing deductible in public breach needs to overcome that of decreasing deductible in the private breach (on the expected utility of the insured firm) at lower level of γ . This is possible only when the optimal premium P_2 *could exhibit steeper initial fall. The same is depicted in *Figure-7*. Fall in both P_2 * and P_2 * flatten out at higher levels of γ .

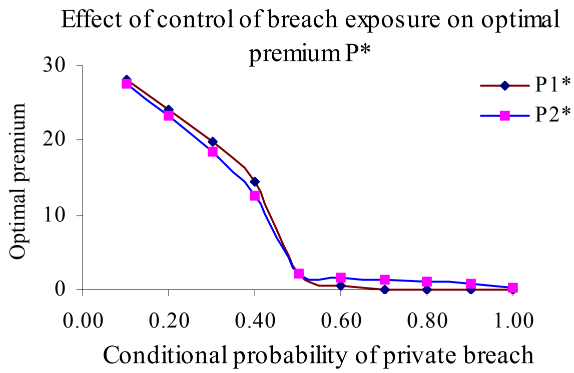


Figure-7. The effect of increasing γ on optimal premium

Firm wealth W, intensity of IT operations k, and optimal deductible x_1 *

Prudence from traditional insurance suggests that everything remaining same, increase in wealth reduces the optimal deductible of an insurance contract. Similarly, as the wealth of a firm increases, smaller cyber losses become relatively insignificant, and the firm finds it optimal to insure only large and catastrophic losses. However, facing a secondary loss, it is not readily apparent how the increase in initial wealth W would modify the level of optimal deductible. In order to put the secondary loss in proper perspective, we argue that the magnitude of the secondary loss G in IT security breaches depends on how IT intensive the firm's operations are[8]. Thus holding the secondary loss of a firm at a fixed proportion ($k = G/W$) of its total wealth, a convenient surrogate for the intensity of IT operation of a firm can be achieved in our present context.[9]

In information asymmetry, at constant G, the insured firm is motivated to buy less of insurance (rise in deductible) when wealth W increases, because smaller losses become relatively insignificant. We have also observed that an increase in G (at low G) at constant W increases the deductible (*Figure-4*), such that, the wealth effect of G could be partly reduced. When k remains constant, i.e. when both G and W increase keeping their ratio fixed, the movement of the deductible is governed by the resultant effect of the above two forces. However, as the magnitude of the wealth W is much larger than the magnitude of the secondary loss G ($k < 1$), the wealth effect predominates; and the rise in deductible is arrested. In other words, a similar firm with higher wealth could exhibit relatively lower interest in cyber insurance.

[8] By definition the root cause of the secondary loss is the risk revision done by the stakeholders of an insured firm, which has direct bearing on the intensity of IT operations in the firm's business. An IT security breach exposes the vulnerabilities and the security readiness of a firm in IT domain only. Higher the IT intensiveness of a firm, the larger is the downward risk revision by its stakeholders for a given IT security breach.

[9] We conveniently denote firms with high W value as '*large firms*', and with identical k values as *'similar firms'*.

On the other hand, when *k* increases (i.e. a firm becomes more IT intensive), an increase in *G* is established in real terms. In order to compensate for the lost indemnity from an increased *G*, and also to combat the indirect reducing wealth effect of *G*, the deductible falls. As *G* keeps on increasing (unabated rise in *k*), the effective wealth and the deductible fall. By this argument, large and IT intensive firms could exhibit heightened interest in a cyber insurance instrument in information asymmetry (*figure-8*).

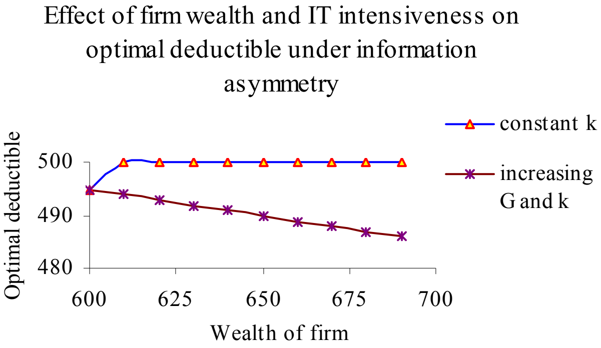


Figure-8. The effect of firm wealth on optimal deductible in asymmetry

During information symmetry (*Figure-9*), the loss in indemnity because of no-claim range is fully compensated in the premium structure. So, in general, for all the above situations, the firm buys more insurance (less deductible). For constant *k*, the only difference in information symmetry is the absence of apparent overpricing (which has a tendency to increase deductible). As a result, the constant *k* curve is unlike the corresponding one in information asymmetry at the beginning: the initial increase in deductible is absent. By the same argument, when both *G* and *k* increase (i.e. when the increase in *k* is caused by increase in *G* alone) in information symmetry, the (reducing) wealth effect first monotonically decreases the deductible. This also helps the insured firm to reclaim its no-claim range in part in case of private breaches. The equilibrium premiums under these circumstances are predictable from the movement of the deductibles in *Figure-8* and *9,* and are not presented here.

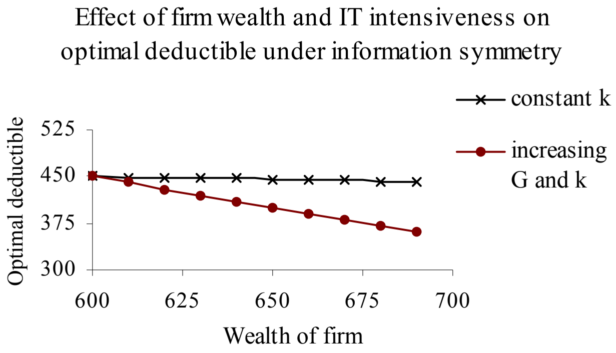


Figure-9. The effect of firm wealth on optimal deductible in symmetry

Firm wealth *W*, Secondary loss *G*, Types of breach γ, and Contract performance

Everything remaining same, a higher deductible transfers less risk through an insurance contract. Comparing the relative levels of optimal deductibles between the scenarios of information symmetry and asymmetry, it is thus possible to compare the performance of a cyber insurance contract in transferring IT security risk. In our earlier discussion of the results, we have generally observed that $(x_{11}* - x_{12}*)$ is positive. A positive value of $(x_{11}* - x_{12}*)$ refers to the fact that the contract optimally transfers higher risk under information symmetry. The general explanation of this is that under information symmetry, the insurer is cognizant of the under claiming strategy of the insured firm, and revises the offered premium downwards. As a result, the contract is generally more attractive to the insured firm, and the insured firm buys more of cyber insurance.

As *k* increases (i.e. increase in *G* without affecting the value of *W*) in information asymmetry, in order to recover part of her lost claiming range in private breach, and also for the reducing wealth effect of increasing *G*, both $x_{11}*$ and $x_{12}*$ fall. The overall level of $(x_{11}* - x_{12}*)$ shows rising trend because reducing deductible is cheaper in symmetry than in asymmetry (*Figure-10*).

Increasing *W* (but keeping *k* constant) has a net positive wealth effect in both scenarios (both $x_{11}*$ and $x_{12}*$ rises). With increasing *W*, *k* falls, and both $x_{11}*$ and $x_{12}*$ increases in unison, before they could max out at the limit of the maximum primary loss. Thus the contract transfers more risk in information symmetry, and the increment in risk transfer remains virtually constant.

On the other hand, when γ increases initially, both $x_{11}*$ and $x_{12}*$ increase, but remain almost coincident(*figure-6*). Thus there is hardly any gain in risk transfer at lower levels of γ between the scenarios of information a/symmetry ($x_{11}*-x_{12}*\approx 0$). This is also understood from the fact that the lost frequency in claiming private breaches of the nature $x < x_1 + G$, being low, has a minimal effect on the deductibles. However, the initial rate of rise in $x_{12}*$ falls below that of $x_{12}*$ (*figure-6*), and then ($x_{11}*-x_{12}*$) rises fast in the mid range of γ. Then the rate of rise of $x_{12}*$ trails off followed by that of $x_{11}*$ as well. Thus the increase in risk transfer remains constant at higher levels of γ. In effect, for the whole mid to high range of the value of γ, the contract transfers higher risk in information symmetry than otherwise (*Figure-10*).

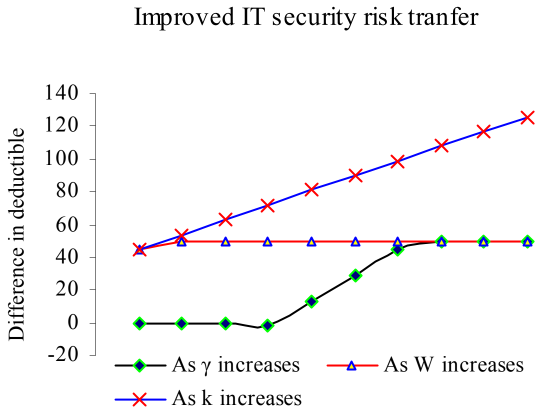


Figure-10. Increased risk transfer in information symmetry

Information asymmetry and the value of cyber insurance to the contracting parties:

When $x_{11}*-x_{12}*\geq 0$, from a *market perspective*, the cyber insurance contract optimally transfers more IT security risk in information symmetry than otherwise. However, from the *perspective of the contracting parties*, the value of the contract lies in their expected utility, which is moderated under the scenarios of information a/symmetry.

The insured firm is risk averse, and its expected utility is governed by (*7*) in conjunction with (*8*). Denote the optimized expected utility of the insured firm in information asymmetry (symmetry) as $U_{11}*$ ($U_{12}*$). The insurer is risk neutral, and asks for premium $P_i = (1+\lambda) I_i$, where I_i is the expected indemnity payout. A risk neutral insurer's utility (V_i) from an insurance contract with premium P_i is given by $V_i = \lambda I_i$ such that $P_i = V_i \frac{1+\lambda}{\lambda}$. Because we assume that information asymmetry does not alter λ, it is apparent that $P_1 * (P_2 *)$ effectively represent a scaled up measure of the expected utility of the insurer in our context.

Also note that a positive $U_{12}*$ - $U_{11}*$ ($P_2 * - P_1 *$) represent an increase in utility of the insured (insurer) when the market has moved from information asymmetry to information symmetry. These incremental gains (losses) in utility of the insurer and the insured firms have been depicted in *figure-11* below, which also warrant the observations that follow *figure-11*:

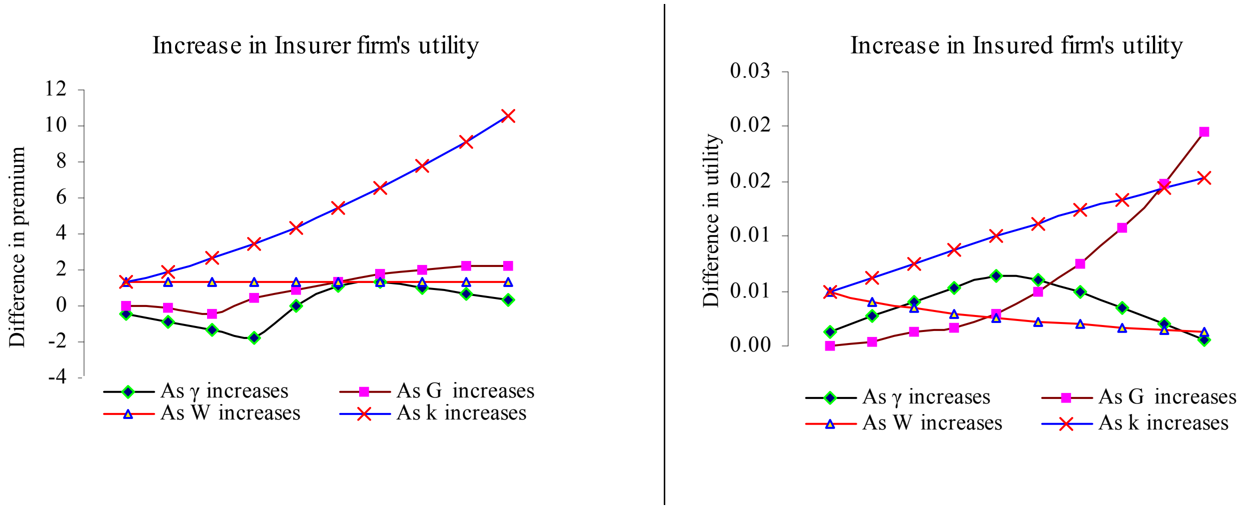


Figure-11. Increase in expected utility under information symmetry

1. Between asymmetry and symmetry, the insured firm is always better off in information symmetry ($U_{12}* - U_{11}* \geq 0$). This is however, not necessarily the case with the insurer.

2. In our model, it is the insured firm who pays the price of information asymmetry. Thus when information asymmetry is dispelled, a cyber insurance contract brings more value to the insured firm. On the other hand, under certain circumstances, the price of information asymmetry paid by the insured firm alters the balance, and the insurer could be better off in information asymmetry.

3. As G increases, the insured firm forfeits increasingly more of its indemnity receipt from the private breach because of the strategic claiming behavior. In information asymmetry, this remains uncompensated in the premium structure, which adds to the utility of the insurer. The higher the G; the better off the insurer is in information asymmetry: the insurer is now able to derive this extraordinary economic rent of information asymmetry. On the other hand, as asymmetry is dispelled, the insured firm is increasingly better off as G rises.

4. As conditional probability γ of private breach increases, the deductible in information asymmetry increases, with which increases the no-claim range as a cascading effect. The uncompensated premium structure adds to the utility of the insurer, and makes him better off in information asymmetry. At mid to high levels of γ, the deductible in information asymmetry is higher than in information symmetry, and the difference in earned premium become more pronounced than the benefit from overpricing in information asymmetry. Now the insurer is better off in information symmetry.

5. Under increase in W, an insured firm buys less insurance as a rule (wealth effect): but in information symmetry, the insured firm buys comparatively more insurance, and so the utility of the insurer improves from a (almost constant) higher stream of premium payment.

6. Discussion:

We have shown that in presence of the idiosyncratic characteristics of IT security risk (secondary losses *G* and breach distribution γ), an insured firm strategizes its claiming behavior - resulting in an off-contract 'no-claim range' in a private breach. Under information asymmetry, the insurer does not know this, and cannot appreciate the now reduced expected indemnity payout. As a result, the offered premium appears overpriced to the insured firm, and lower amount of risk is optimally transferred through the cyber insurance contract. Once the insurer comes to know of *G* and γ , the information asymmetry between the parties is resolved, and the indemnity payout as calculated by the insurer coincides with that of the insured firm. Consequently, the insurance contract transfers more risk in information symmetry. However, an efficient instrument alone may not guarantee a successful market for cyber insurance products, as we discuss below.

We conjecture that initially the market for cyber insurance could begin in *naïve symmetry* (*Quadrant-I, Figure-12*) where neither the insured nor the insurer firm knows about *G* and γ , and the cyber insurance contract is written with business prudence derived/experienced from other established insurance markets.

However, soon the insured firm realizes secondary loss *G*, when stakeholders adversely reassess the post-breach IT security risk profile of the firm. The insured firm now formalizes an optimized claiming strategy, which differs from the contract-intended behavior, and the market makes a transition from '*naïve symmetry'* to '*information asymmetry'* (*Quadrant-II, Figure-12*). We understand that the current market for cyber insurance is in this state of information asymmetry. We have shown that lower amount of IT security risk is optimally transferred in information asymmetry, and that the contract is overpriced - causing the instrument to lose its appeal to the insured firms. This may explain, in an aggregate scenario, the relatively small size of the cyber insurance market today. But what could provide impetus for the market to move to information symmetry, where more IT security risks could be transferred?

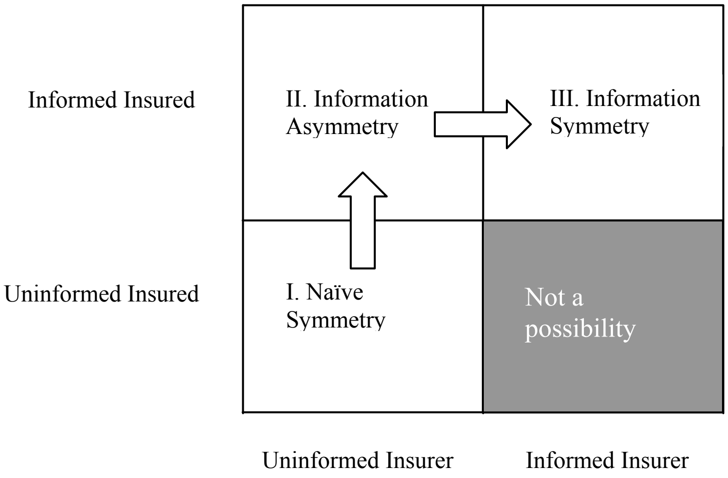


Figure-12. Scenarios of cyber insurance market

The insured firm pays for the information asymmetry, and has clear motivation to move to information symmetry where the premium structure is softer, and its expected utility is enhanced (*Figure-11*). It is thus appropriate to assume that the insured firm would signal its off-contract claiming strategy to the insurer. Because there is published research (e.g. Cavusoglu et al., 2004) about post breach secondary loss, we understand that the insurer would also find the signal credible. Even if we assume that the insurer could include the signal of the new claiming strategy, and enforce it in the contract; the insurer may not necessarily do so. The revised utility of the insurer in information symmetry is not necessarily higher on a contract-by-contract basis (*Figure-11*). For example, in presence of high secondary loss *G*, the insurer is better off in information asymmetry than otherwise. Thus, even after receiving a credible under claiming signal from the insured firm, an insurer may still refuse to revise the premise of a cyber contract. In that case, the cyber insurance market is likely to remain locked in information asymmetry.

The lock-in in information asymmetry could be overcome under the following circumstances:

1) As pricing of cyber insurance contract falls in information symmetry, increase in demand may be realized. Once demand picks up, the overall revenue of the insurer from its operations in the cyber domain may be positively impacted, causing the insurer to move to information symmetry.

2) Competitive forces in the supply side may cause some insurers to offer contracts that incorporate the under claiming strategy, and hence a lower premium. As these contracts more closely capture the expected payout, the generated market forces will bring information symmetry in the whole market.

Firms with high secondary loss G (synonymous with intensive IT utilization in their operations) find cyber insurance contracts highly overpriced in today's market of information asymmetry. These are also the firms who potentially need cyber insurance more than those with less intense IT practices. Interestingly, this also brings the traditional dilemma of insurance in a new envelope: *those who need cyber insurance more, find the contracts more expensive, and are less likely to buy!* We believe that this is one important reason why cyber insurance products have failed to fulfill buoyant expectations.

Firms with low G (who do not find the cyber products highly expensive), or firms under regulatory or other obligations are more likely to buy cyber insurance in information asymmetry. Our model suggests that these firms may constitute the majority buyers of cyber insurance products today. There appears to be another segment of firms who currently use cyber insurance for strategic and competitive posture[10]. These firms buy cyber insurance to assure their stakeholders, but choose very high deductible with no serious intention or possibility to ever reclaim cyber losses.

Although occurrence of secondary losses has been empirically confirmed, the exact nature of these losses is yet to be ascertained. However, we do not foresee any major changes in the

[10] This was pointed out by a graduate student (who is also the CIO of a medium size IT intensive firm at Dallas) in an MBA class discussion at UT Dallas

outcome of our model when other forms/nature of secondary losses is substituted for the constant loss in our model. We have investigated a firm's claim strategy for a claim/indemnity oriented convex loss (*Appendix-2*). The results indicate that similar information asymmetry, and premium overpricing would exist there too.

The issue of accounting materiality of losses and regulatory requirement of reporting them[11] can potentially alter the ex-post classification of a breach as private or public. Experience suggests that breaches in organizational information systems are numerous in nature, and small rather than very large losses are prevalent. Quite often the incursions are tracked before much damage is done, and for moderately large companies, these fall below their accounting materiality considerations (typically 3-5% of assets), thereby providing accounting freedom to employ the claim strategy as suggested in our analysis. Moreover, a detailed loss assessment of information breach is a time-consuming affair, and breach incident occurrences and accounting disclosures are discrete and unrelated actions of organizations.

This research rests on the premise of secondary loss exposure, which an insured firm faces while claiming a previously undisclosed breach of information systems/assets. Our future efforts thus involve testing our model with empirically supported secondary losses, and also the nature of such losses. This could then objectively estimate the stream of indemnity payouts, and bring out the deviations that may be caused by information asymmetry.

7.0 Conclusion:

Our model examines a standard insurance contract (Borch (1960) and Raviv (1979)) under the circumstances of the nascent cyber insurance market, where insured firms foresee secondary losses while claiming indemnity for a realized cyber loss. Through an analysis in the expected utility regime, we explain how this secondary loss exposure 1) may affect claiming behavior of

[11] This issue was brought up during presentation of an earlier version of this paper in the proceedings of the XIV th. Workshop of Information Technology and Systems (WITS) at Washington DC, December 2004.

an insured firm, 2) give rise to information asymmetry between the insurer and the insured firms, and 3) may thwart development of this nascent market in an aggregate scenario. We also discuss factors that could help move the market to information symmetry, where cyber insurance products are less expensive, and higher demand could be expected. Although information symmetry is likely to reduce the pricing of cyber insurance contract substantially, the private nature of firm specific assessment of cyber loss exposures swells the contract writing costs. So long large-scale actuarial data is generated and iso-risk groups of firms are identified, cyber insurance products are likely to remain somewhat pricey in near future.

References:

Becca, Mader, "Cyber insurance's higher rates make it a long-term sell", http://sanjose.bizjournals.com/sanjose/stories/2002/11/04/focus2.html

Borch, Carl, "The Mathematical Theory of Insurance", Lexington Press, 1974, USA

Borch, K., "The Safety Loading of Reinsurance Premiums", Skand. Akturietidskrift, 162-184, 1960.

Breuer, Michael, "Optimal Insurance Contracts without the Non-Negativity Constraints on Indemnities Revisited", University of Zurich Working Paper No. 0406, April 2004.

Cavusoglu, H., Mishra, B., and Raghunathan S., "The Effect of Security Breach Announcement on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", UT Dallas Working Paper, 2004.

Doherty, N and Schlesinger, H., "Optimal Insurance in Incomplete markets", Journal of Political Economy, 91: 1045-1054, 1983

Borch, K., "Economics of Insurance", North Holland publishing company, 1990

Ermoliev, Yuri M., and Flam, Sjur Didrik, "Finding Pareto Optimal Insurance Contracts", International Institute for Applied Systems Analysis Interim Report IR-00-033, June 2000.

Gollier, Christian, "Optimal Insurance of Approximate Losses", The Journal of Risk and Insurance, volume 63, No 3, 369-380, 1996.

Gollier, Christian, and Pratt, John W., "Risk Vulnerability and the Tempering Effect of Background Risk", Econometrica, Vol. 64, No. 5, 1109-1123, 1996.

Gordon, Lawrence A., Loeb, P Martin and Sohail Tashfeen, "A framework for using insurance for Cyber risk Management", Communications of the ACM, Vol. 46, No. 3: 81-85.

Wood Lamont, "When all else fails, there's cyber insurance" http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss446_art920,00.html

Institute for Catastrophic Loss Reduction, "Cyber-Incident Risk in Canada and the Role of Insurance", Paper Series - No.38, ISBN: 0-9733795-4-5, April 2004.

Mossin, J., "Aspects of rational insurance Purchasing", Journal of political Economy, July/August, 76, 533-68, 1968

Ponssard, J., Pierre, "Competitive strategies, - an advanced text book in game theory for business students", North Holland publishing company, 1981

Raviv, A., "The design of an optimal Insurance policy", American Economic Review, 69: 84-96, 1979.

Schlesinger, Harris, "The Optimal Level of Deductibility in Insurance Contracts", The Journal of Risk and Insurance, Vol. 48, No. 3, 465-481, 1981.

Schlesinger, Harris, "Insurance Demand without the Expected-Utility Paradigm", The Journal of Risk and Insurance, Vol. 64, No. 1, 19-39, 1997.

Sethi, Suresh P., and Thompson, Gerald L., "Optimal Control Theory, Applications to Management Science and Economics", Kluwer Academic Publishers, Second Edition, 2000, USA

Stadler, Macho Ines, and Castrillo, David Perez, "An Introduction to the Economics of Information – Incentives and Contracts", Oxford University Press, 1997.

Campbell, K., Gordon, Lawrence A., Loeb, Martin P., Zhou L, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", The Journal of Computer Security, Vol. 11, No. 3, 431-448, 2003

USA Today, April 8, 2002, "FBI survey finds computer attacks up" (http://www.usatoday.com/tech/news/2002/04/08/fbi-survey.htm)

Appendix-1

Proposition 1: *For constant secondary loss* G *associated with a private breach, there exists a minimum realized loss* $r\ (= x_1 + G)$ *up to which the insured firm does not claim its losses, for losses above* r *the insured firm claims its actual loss.*

Proof: The local optimization problem is reduced to locate an arbitrary point r in the loss axis (*Figure-2*) such that the expected revenue $E[R(r)] = \int_r^{\infty} I(x) f(x) dx - (1 - F(r))$ is maximized. The FOC of the above yields the optimal r: $r = I^{-1}(G)$. However, the point r must lie towards the right of point x_1 (the firm has no reason to claim below the deductible and absorb just the secondary losses). Thus in general: $r = I^{-1}(r - x_1)$. This fixes the point r conclusively, $r = x_1 + G_{pvt}$. The point r marks the boundary; beyond which the insured firm claims a suffered loss in the private breach.

Lemma 1*: For any given deductible, the informed insurer offers a cyber insurance contract that is never priced higher than that offered by the uninformed insurer, i.e.* $P_1 \geq P_2$.

Proof: It can be shown that $P_i = P_u - q\,(1+\lambda)\,\gamma\,\delta \int_{x_1}^{x_1+G} (x - x_1)\, f(x)\, dx$, such that for nonnegative values for G, δ, γ, and λ, $P_u \geq P_i$.

Lemma 2*: Ceteris paribus, for a selected deductible* $x_1, x_1 \geq 0$*, the apparent premium overpricing in information asymmetry* ($P_1 - P_2$)

5) *Does not exist in the range* $x_1 \leq Max\{(a - G), 0\}$
6) *Increases linearly with the probability of private breach* γ *in the range* $x_1 > Max\{(a - G), 0\}$
7) *Exhibits quadratic increase with the secondary loss G in the range* $a < x_1 + G \leq b$
8) *Remains invariant of the secondary loss G in the range* $x_1 > Max\{(b - G), 0\}$

Proof: The overpricing is denoted as $\Delta P = q\,(1+\lambda)\,\gamma\,\delta \int_{x_1}^{x_1+G} (x-x_1)\, f(x)\, dx$

$$Case{-}1: \Delta P = q\,(1+\lambda)\,\gamma\,\delta \int_{x_1}^{x_1+G} (x-x_1)\,0\,dx = 0, \qquad x_1+G<a$$

$$Case{-}2: \Delta P = q\,(1+\lambda)\,\gamma\,\delta \int_{a}^{x_1+G} (x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)\gamma\delta}{2(b-a)}\left(G^2-(a-x_1)^2\right), \qquad x_1<a,\quad a\le x_1+G\le b$$

$$Case{-}3: \Delta P = q\,(1+\lambda)\,\gamma\,\delta \int_{a}^{b} (x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)\gamma\delta}{2}\left(b+a-2x_1\right), \qquad x_1<a,\quad x_1+G>b$$

$$Case{-}4: \Delta P = q\,(1+\lambda)\,\gamma\,\delta \int_{x_1}^{x_1+G} (x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)\gamma\delta}{2(b-a)}G^2, \qquad a\le x_1\le b,\quad a\le x_1+G\le b$$

$$Case{-}5: \Delta P = q\,(1+\lambda)\,\gamma\,\delta \int_{x_1}^{b} (x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)\gamma\delta}{2(b-a)}(b-x_1)^2, \qquad a\le x_1\le b,\quad x_1+G>b$$

Derivation of the offered premium in information a/symmetry:

Scenario-1, Information Asymmetry:

$$Case\,1: P_1 = q(1+\lambda)\int_a^b (x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)}{2}(b+a-2x_1) \qquad x_1<a$$

$$Case\quad 2: P_1 = q(1+\lambda)\int_{x_1}^b (x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)}{2(b-a)}(b-x_1)^2 \qquad x_1\ge a,$$

Thus in general:

$$P_1 = \frac{q\,(1+\lambda)}{2(b-a)}\left(b-Max\{a,x_1\}\right)\left(b+Max\{a,x_1\}-2x_1\right)$$

Scenario-2, Information Symmetry:

$$Case\ -1: P_2 = q(1+\lambda)\left\{\int_a^b (x-x_1)\frac{1}{b-a}\,dx - \gamma\delta\int_{x_1}^{x_1+G}(x-x_1).0.dx\right\} \qquad \forall\ x_1+G<a$$

$$P_2 = Max\left\{\frac{q\,(1+\lambda)}{2}\left(b+a-2x_1\right), 0\right\} \qquad \forall\ x_1+G<a$$

$$Case{-}2: P_2 = q(1+\lambda)\left\{\int_a^b (x-x_1)\frac{1}{b-a}\,dx - \gamma\delta\int_{a}^{x_1+G}(x-x_1).\frac{1}{b-a}.dx\right\} \qquad \forall\, x_1<a,\quad a\le x_1+G\le b$$

$$P_2 = Max\left\{\frac{q(1+\lambda)}{2(b-a)}\left\{(b-a)\left(b+a-2x_1\right)-\gamma\delta\left(G^2-(a-x_1)^2\right)\right\}, 0\right\} \qquad \forall\, x_1<a,\quad a\le x_1+G\le b$$

$$Case-3: P_2 = q(1+\lambda)\left\{\int_a^b (x-x_1)\frac{1}{b-a}dx - \gamma\delta\int_a^b (x-x_1).\frac{1}{b-a}.dx\right\} \qquad \forall\, x_1 < a, \quad x_1+G > b$$

$$P_2 = Max\left\{\frac{q\,(1+\lambda)(1-\gamma\,\delta)}{2}\left(b+a-2x_1\right), 0\right\} \qquad \forall\, x_1 < a, \quad x_1+G > b$$

$$Case-4: P_2 = q(1+\lambda)\left\{\int_{x_1}^b (x-x_1)\frac{1}{b-a}dx - \gamma\delta\int_{x_1}^{x_1+G} (x-x_1).\frac{1}{b-a}.dx\right\} \qquad \forall\, x_1 \geq a, \quad x_1+G \leq b$$

$$P_2 = Max\left\{\frac{q(1+\lambda)}{2(b-a)}\left\{(b-x_1)^2 - \gamma\,\delta\,G^2\right\}, 0\right\} \qquad \forall\, x_1 \geq a, \quad x_1+G \leq b$$

$$Case-5: P_2 = q(1+\lambda)\left\{\int_{x_1}^b (x-x_1)\frac{1}{b-a}dx - \gamma\delta\int_{x_1}^b (x-x_1).\frac{1}{b-a}.dx\right\} \qquad \forall\, x_1 \geq a, \quad x_1+G > b$$

$$P_2 = Max\left\{\frac{q\,(1+\lambda)(1-\gamma\,\delta)}{2(b-a)}(b-x_1)^2, 0\right\} \qquad \forall\, x_1 \geq a, \quad x_1+G > b$$

Derivation of the expected utility of the insured firm:

Range of ***x₁***	Expected Utility of the insured ***E [U]***
General	$q\delta\gamma\left(\int_0^{x_1+G} U(W-x-P)f(x)dx + U(W-x_1-P-G).(1-F(x_1+G))\right) + q\delta(1-\gamma)\left(\int_0^{x_1} U(W-x-P-G)f(x)dx + U(W-x_1-P-G).(1-F(x_1))\right) +$ $q(1-\delta)\left(\int_0^{x_1} U(W-x-P)f(x)dx + U(W-x_1-P).(1-F(x_1))\right) + (1-q).U(W-P)$
$x_1+G<a$	$q\delta\,\gamma\big(Ln(W-x_1-P-G).1\big) + q\delta\,(1-\gamma)\big(Ln(W-x_1-P-G).1\big) + q\,(1-\delta)\big(Ln(W-x_1-P).1\big) + (1-q)Ln(W-P)$ $=$ $q\delta.Ln(W-x_1-P-G) + q.(1-\delta).Ln(W-x_1-P) + (1-q).Ln(W-P)$
$x_1<a,$ $a \leq x_1+G$	$q\delta\gamma\left(\int_a^{x_1+G} Ln(W-x-P)\frac{1}{b-a}dx + Ln(W-x_1-P-G).\frac{(b-x_1-G)}{b-a}\right) + q\delta(1-\gamma)\ Ln(W-x_1-P-G) + q(1-\delta)\ Ln(W-X_1-P) + (1-q).U(W-P)$ $=$ $\frac{q\delta\gamma}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)- \\ (W-b-P).Ln(W-x_1-P-G)-(x_1+G-a)\end{array}\right) + q\delta(1-\gamma).Ln(W-x_1-P-G) + q.(1-\delta).Ln(W-x_1-P) + (1-q).Ln(W-P)$

$x_1 < a,$ $x_1 + G > b$	$q\delta\gamma\left(\int_a^b Ln(W-x-P)\frac{1}{b-a}dx+0\right)+q\delta(1-\gamma)\,Ln(W-x_1-P-G)+q(1-\delta)\,Ln(W-X_1-P)+(1-q).U(W-P)$ $=$ $\frac{q\delta\gamma}{b-a}.\left(\begin{array}{l}(W-a-P-G).Ln(W-a-P-G)-\\(W-b-P-G).Ln(W-b-P-G)-(x_1-a)\end{array}\right)+q\delta(1-\gamma).Ln(W-x_1-P-G)+q.(1-\delta).Ln(W-x_1-P)+(1-q).Ln(W-P)$
$x_1 \geq a,$ $x_1 + G \leq b$	$q\delta\gamma\left(\int_a^{x_1+G} Ln(W-x-P)\frac{1}{b-a}dx+Ln(W-x_1-P-G)\frac{b-x_1-G}{b-a}\right)+q\delta(1-\gamma)\left(\int_a^{x_1} Ln(W-x-P-G)\frac{1}{b-a}dx+Ln(W-x_1-P-G).\frac{b-x_1}{b-a}\right)+$ $q(1-\delta)\left(\int_a^{x_1} Ln(W-x-P)\frac{1}{b-a}dx+Ln(W-x_1-P).\frac{b-x_1}{b-a}\right)+(1-q).Ln(W-P)$ $=$ $\frac{q\delta\gamma}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-x_1-P-G)-(x_1+G-a)\end{array}\right)+\frac{q\delta(1-\gamma)}{b-a}.\left(\begin{array}{l}(W-a-P-G).Ln(W-a-P-G)-\\(W-b-P-G).Ln(W-x_1-P-G)-(x_1-a)\end{array}\right)+$ $\frac{q(1-\delta)}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-x_1-P)-(x_1-a)\end{array}\right)+(1-q).Ln(W-P)$
$x_1 \geq a,$ $x_1 + G > b$	$q\delta\gamma\left(\int_a^b Ln(W-x-P)\frac{1}{b-a}dx+0\right)+q\delta(1-\gamma)\left(\int_a^{x_1} Ln(W-x-P-G)\frac{1}{b-a}dx+Ln(W-x_1-P-G).\frac{b-x_1}{b-a}\right)+$ $q(1-\delta)\left(\int_a^{x_1} Ln(W-x-P)\frac{1}{b-a}dx+Ln(W-x_1-P).\frac{b-x_1}{b-a}\right)+(1-q).U(W-P)$ $=$ $\frac{q\delta\gamma}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-b-P)-(b-a)\end{array}\right)+\frac{q\delta(1-\gamma)}{b-a}.\left(\begin{array}{l}(W-a-P-G).Ln(W-a-P-G)-\\(W-b-P-G).Ln(W-x_1-P-G)-(x_1-a)\end{array}\right)+$ $\frac{q(1-\delta)}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-x_1-P)-(x_1-a)\end{array}\right)+(1-q).Ln(W-P)$

Appendix-2

<u>Claim Oriented Risk Perception Loss and Claim Strategy</u>:

Firms differ in the way they are exposed to post-claim risk perception loss $g(I(y(x)))$. Companies dealing in sensitive personal information, engaged in major e-commerce activities, or with little brick and mortar presence may likely experience high exposure from $g(I(y(x)))$. These firms are also highly exposed to cyber risks because of the nature of their business. Consider F_d to be one such firm and represent its market losses by a convex $g(I(y(x)))$, such that $g(0)=0,\ g'(I)\geq 0,\ g''(I)>0$. What this means is that as stakeholders come to know of larger breaches through a realized indemnity, the risk perception about the company is adversely revised at an increasing rate. Also consider that the cyber risk loss is free to assume any value in the positive line and the cyber contract is written with a deductible x_1 and a cap x_2.

<u>Assertion 1</u>: *Facing a convex risk perception loss $g(I(y))$, for every realization x of its random cyber loss $\widetilde{X}$, an insured firm claims $y = Min\{x, x_2, \xi^*\}$, $(\xi^* = I^{-1}(g'^{-1}(1)))$, when $Min\{x, x_2, \xi^*\} > x_1 + g(Min\{x, x_2, \xi^*\} - x_1)$; else the firm does not claim.*

Proof:

Let net revenue from indemnity be $R(y) = I(y) - g(I(y))$; From F.O.C., $g'(I(y)) = 1$ is the condition for optimal claim because the second order derivative

$R''(y) = I''(y)\{1 - g'(I(y))\} - I'(y)^2 g''(I(y))$ is clearly negative at $g'(I(y^*)) = 1$.

Denote $\xi^* = I^{-1}(g'^{-1}(1))$, and consider the following cases:

Case-1: $x \leq x_1$

Because $y \leq x$, and $x \leq x_1$, $I(y) = 0,\ g(I(y)) = 0,\ R(y) = 0$, insured firm does not claim.

Case-2: $x_1 < x$

Sub case 2A: $\xi^* > x$

Knowing $g(0) = 0$, $g'(I(\xi^*)) = 1$ and $\xi^* > x$, $1 - g'(I(y))$ is positive in the range $x_1 < x < \xi^*$**.** Thus $R'(y) = I'(y)\{1 - g'(I(y))\}$ is positive when $I'(y) > 0$, ($I'(y) > 0$ in the range $x_1 < y \leq x_2$)

and 0 when $I'(y) = 0$ (true in the range $x_2 < y$). Beginning at *x₁,* the value of *I (y)* increases monotonically till $y = x_2$, beyond which it remains constant. However, if $x < x_2$, the firm may claim only up to $y = x$. In other words, the firm claims Min $\{x, x_2\}$. $R = Min\{x, x_2\} - x_1 - g(Min\{x, x_2\} - x_1)$, And the firm claims when $R > 0$. Thus the effective claim strategy is: $Claim\, Min\{x, x_2\}$, $when\, Min\{x, x_2\} > x_1 + g(Min\{x, x_2\} - x_1)$ *; else do not claim.*

Sub case 2B: $\xi^* \le x$

Here F_d claims $Min\{\xi^*, x_2\}$ when $Min\{x, x_2\} > x_1 + g(Min\{x, x_2\} - x_1)$.

This defines an effective under claiming range $x - \xi^*$ when $\xi^* < x$. *Q.E.D.*

Appendix-2

Along the search space of deductible x_1, the expected utility of the insured firm is discontinuous. This is so because of the following reasons:

a) The indemnity structure of the Pareto-optimal contract (*1*) induces jump at $x = x_1$. This manifests itself in the limits of integration in (*7*).

b) Our assumed functional form of the loss function is *Uniform* [*a, b*]: this induces jumps at the points $x = a, and\ x = b$. This is manifested in the ranges of premium in (*8*), which in turn, modifies the argument of the expected utility of the insured firm.

c) Existence of the secondary loss *G* causes the contract intended behavior to alter in the private breaches, which shifts the location of jump from $x_1\ to\ x_1 + G$ in point *a*) above

d) Depending on the relative magnitudes of the secondary loss *G*, and the parameters of the loss function *a,* and *b* (in comparison to the choice of the deductible x_1 in the search range), the jumps in point *b*) above may or may not be realized, which in turn potentially changes the upfront premium (and hence the argument of the utility function of the insured firm) in information symmetry.

In our experiment we circumvent the maximization problem of this discontinuous expected utility of the insured firm in the following fashion. Note that the maximization problem of (*7*) can be construed as a set of adjacent sub problems defined by the pertinent ranges of the deductible. The insured firm could concurrently maximize each of these sub problems to yield the corresponding optimal deductibles, each of which is now specific to the deductible range. Finally, among all these range-specific optimal deductibles, the deductible that yields the highest expected utility among all the maximized solutions of the sub problems could then be selected for onward communication to the insurer. The dissociation of the maximization problem in to a set of sub problems is sufficient without any loss in quality of solution; so long the restricted range of deductible $0 \le x_1 \le b$ is exhaustively searched. The above process is represented in the following table, which is also how we conduct our numerical experiment[12]. Every row in table-3 represents a sub problem, which is numerically maximized twice: once under information asymmetry (*column-3*), and then under information symmetry (*column-4*). The process is repeated for 10 different values of each of the parameters.

Range of deductible $\boldsymbol{x_1}$	Expected Utility of the insured ***E [U]***	Offered premium in Asymmetry $\boldsymbol{P_1}$	Offered premium in Symmetry $\boldsymbol{P_2}$
$x_1 + G < a$	$q\delta.Ln(W - x_1 - P - G) +$ $q.(1-\delta).Ln(W - x_1 - P) + (1-q).Ln(W - P)$	$\frac{q(1+\lambda)}{2}(b + a - 2x_1)$	$Max\left\{\frac{q(1+\lambda)}{2}(b + a - 2x_1), 0\right\}$
$x_1 < a,$ $a \le x_1 + G$	$\frac{q\delta\gamma}{b-a}.\left(\begin{array}{l}(W - a - P).Ln(W - a - P) - \\ (W - b - P).Ln(W - x_1 - P - G) - (x_1 + G - a)\end{array}\right) +$ $q\delta(1-\gamma).Ln(W - x_1 - P - G) + q.(1-\delta).Ln(W - x_1 - P) +$ $(1-q).Ln(W - P)$	$\frac{q(1+\lambda)}{2}(b + a - 2x_1)$	$Max\left\{\frac{q(1+\lambda)}{2(b-a)}\left\{\begin{array}{l}(b-a)(b + a - 2x_1) - \\ \gamma\delta\left(G^2 - (a - x_1)^2\right)\end{array}\right\}, 0\right\}$
$x_1 < a,$ $x_1 + G > b$	$\frac{q\delta\gamma}{b-a}.\left(\begin{array}{l}(W - a - P - G).Ln(W - a - P - G) - \\ (W - b - P - G).Ln(W - b - P - G) - (x_1 - a)\end{array}\right) +$ $q\delta(1-\gamma).Ln(W - x_1 - P - G) + q.(1-\delta).Ln(W - x_1 - P) +$ $(1-q).Ln(W - P)$	$\frac{q(1+\lambda)}{2}(b + a - 2x_1)$	$Max\left\{\frac{q(1+\lambda)(1-\gamma\delta)}{2}(b + a - 2x_1), 0\right\}$

[12] Please note that for the range of practicable values of parameters of our experiment (*Table-1*), some of these sub problems are not valid.

$x_1 \geq a$, $x_1 + G \leq b$	$\frac{q\delta\gamma}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)- \\ (W-b-P).Ln(W-x_1-P-G)-(x_1+G-a)\end{array}\right)+$ $\frac{q\delta(1-\gamma)}{b-a}.\left(\begin{array}{l}(W-a-P-G).Ln(W-a-P-G)- \\ (W-b-P-G).Ln(W-x_1-P-G)-(x_1-a)\end{array}\right)+$ $\frac{q(1-\delta)}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)- \\ (W-b-P).Ln(W-x_1-P)-(x_1-a)\end{array}\right)+$ $(1-q).Ln(W-P)$	$\frac{q(1+\lambda)}{2(b-a)}(b-x_1)^2$	$Max\left\{\frac{q(1+\lambda)}{2(b-a)}\{(b-x_1)^2-\gamma\delta G^2\}, 0\right\}$
$x_1 \geq a$, $x_1 + G > b$	$\frac{q\delta\gamma}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)- \\ (W-b-P).Ln(W-b-P)-(b-a)\end{array}\right)+$ $\frac{q\delta(1-\gamma)}{b-a}.\left(\begin{array}{l}(W-a-P-G).Ln(W-a-P-G)- \\ (W-b-P-G).Ln(W-x_1-P-G)-(x_1-a)\end{array}\right)+$ $\frac{q(1-\delta)}{b-a}.\left(\begin{array}{l}(W-a-P).Ln(W-a-P)- \\ (W-b-P).Ln(W-x_1-P)-(x_1-a)\end{array}\right)+$ $(1-q).Ln(W-P)$	$\frac{q(1+\lambda)}{2(b-a)}(b-x_1)^2$	$Max\left\{\frac{q(1+\lambda)(1-\gamma\delta)}{2(b-a)}(b-x_1)^2, 0\right\}$

Table-3. Sub problems of expected utility maximization under information a/symmetry