

# On Economic Perspectives of Internet Security: The Problem of Designing Optimal Cyber-Insurance Contracts

Ranjan Pal  
University of Southern California  
rpal@usc.edu

Leana Golubchik  
University of Southern California  
leana@usc.edu

## 1. INTRODUCTION

In Internet security, traditional protection mechanisms such as anti-virus software, firewalls, and other add-ons are not capable of completely eliminating security risks [3]. As noted in [7], the management of information security needs to be addressed through economic, psychological, and policymaking approaches, in combination with engineering approaches. As a realistic and futuristic solution, recent efforts suggest alleviating existing Internet security problems through cyber-insurance schemes [5][6] - an alternative approach to handling residual risk, where residual risk is transferred to a different entity, i.e, insurance companies, in return for a fee, termed the insurance premium. Cyber-insurance is analogous to the widely popular technique of ‘insurance’ in modern life [1]. Cyber-insurance companies could take the form of government agencies or public/private Internet service providers (ISPs) such as phone and cable companies (e.g., AT&T, Comcast). For instance, ISPs could act as insurance agencies and make it mandatory for its clients to certify their computing devices, and in return provide them with insurance services that include monetary compensations, data backups, real-time network traffic monitoring and filtering [4].

Existing research [5][6] has shown that cyber-insurance is a powerful incentive mechanism that increases the level of self-protection amongst Internet users, and thereby the overall network security (social welfare). The works are based on the notion that increasing level of self-protection amongst Internet users makes individual users robust to the success of threat attacks, and in turn makes the whole network more threat-proof. In this extended abstract, we address the problem of enforcing *optimal* cyber-insurance contracts between the insurer and the insured, where optimality may be defined w.r.t to maximizing social welfare or w.r.t maximizing insurer commercial profits. We define an insurance contract as a (*premium, coverage*) tuple that is enforced between the insurer (say an ISP) and the insured, prior to the ISP providing Internet service, as part of terms of the agreement between the two.

Our problem is important for the following reasons. In general, an insurance contract is first imposed between the insurer and the insured followed by end users deciding on their self-defense investments. Previous research efforts assume a *given* insurance contract in their models and derive the results for incentivizing self-protection and improving network security; they do not compute an optimal cyber-insurance contract that must operate in practice. An *optimal* insurance contract is important for an insurer to impose, mainly due to commercial profit reasons. *Given* an optimal insurance contract, co-operative and non-co-operative Internet users can decide on their *optimal amounts* of self-defense investments to improve network security [8]. Thus, the optimal insurance contract in addition to optimal user self-defense investments, form the optimal economic parameters for each user in the network. *Given* that optimal contracts could be defined w.r.t social welfare, or w.r.t business profits, it would be useful to *compare* the social welfare obtained in these cases, as it is not necessary for the welfare to be the same for both. The difference in the values of social welfare would in turn promote the design of mechanisms to reduce the gap.

The main goal of this abstract is two fold: (1) to derive optimal cyber-insurance contracts between the insurer and its clients, where the insurer could have either a social welfare maximizing mindset or a profit maximizing mindset, and (2) to compare the optimal contracts for both types of insurers and analyze the differences in the social welfare and commercial profits generated in both scenarios.

## 2. CYBER-INSURANCE MODEL

We consider the scenario where a single cyber-insurance agency provides service to all Internet users in a geographical locality. We consider two types of cyber-insurers in our model: (1) insurers aiming to maximize social welfare (without making negative profits) by increasing the level of security in the network, and (2) insurance agencies whose sole motive is to maximize profit whilst providing insurance services to its customers. Examples of organizational agencies that could offer insurance solutions solely for social welfare purposes are non-profit Internet service providers (ISPs) like MAIN (<http://www.main.nc.us>). Profit-maximizing cyber-insurance agencies are likely to mainly include commercial Internet service providers (ISPs) in the form of broadband cable companies or phone companies (e.g., Comcast, AT&T).

We assume that Internet users are uniformly distributed on the line segment  $[0,1]$ , i.e., the location  $p \in [0,1]$  of a particular user on the unit interval denotes its probability of

facing a substantial risk of size  $R$ . This is the risk a user faces *after* some initial investments, which are precautionary efforts both in the monetary, as well as in the non-monetary sense. We assume that the ISP (or any other insurance agency) could have an estimate of this risk probability via the answers to some general questions (e.g., the type of anti-virus protection one uses, the security mindset of a user, and some basic general knowledge on Internet security) it requires its potential clients to answer before signing up for service and from the network topology (which can help determine the probability of each user being affected by threats). Apart from the probability of facing risk, the Internet users are assumed to be homogenous in terms of their initial wealth  $w$  and the size  $R$  of risk faced, where a risk represents the negative wealth accumulated by a user when it is affected by Internet threats. We assume that the potential risk faced by an Internet user is less than its initial wealth  $w$ . Each user may buy at most one cyber-insurance policy from the insurer by agreeing to pay a premium  $z$  for an insurance coverage amount  $c$ . The cyber-insurance company advertises only one contract to all its customers. We assume that the level of coverage is not bigger than size  $R$  of risk. We also assume that the initial wealth of a user, the size of risk, the cyber-insurance premium, and the level of coverage have the same measurable units. We also account for the fact that the system does not face the *moral hazard* problem and the *adverse selection* problem [2]. We apply a risk-averse utility function  $U_p(z, c)$  to Internet users, where  $U_p(z, c)$  is defined as

$$U_p(z, c) = \begin{cases} w - pKR & \text{if it buys no insurance} \\ w - z - pK(R - c) & \text{if it buys insurance,} \end{cases}$$

where  $K \geq 1$  is the degree of risk aversion of a user, assumed to be the same for all users in the network. When  $K = 1$ , a user evaluates its loss to be exactly  $R$ . When  $K > 1$ , the user adds an additional negative utility of  $(K - 1)R$  for an idiosyncratic pain due to facing the risk.

We assume that the cyber-insurance agency is risk-neutral, i.e., it is only concerned with its expected profits. For an insurance policy  $(z, c)$  sold to a user, the contract is worth

$$(1 - p)z + p(z - c) = z - pc$$

to the insurer. Thus, the overall expected profit made by the cyber-insurance agency by providing the same insurance service to its entire geographical locality is

$$G(z, c) = \int_0^1 (z - pc)dp$$

Here, we use ‘contract’ and ‘policy’ interchangeably.

### 3. WELFARE MAXIMIZING INSURANCE

We now determine an optimal cyber-insurance policy,  $(z, c)$ , a cyber-insurance agency interested in maximizing social welfare would provide to its customers. We assume here that the insurer values the welfare of each of its customers equally and is not inclined to making negative profit. We also assume that a user can decide whether to buy the policy or not, and that the insurer also has the power to decide whether to provide insurance to a customer, based on its probability of facing risk.

**Problem Formulation.** Let the insurer offer a contract  $(z, c)$ . An Internet user facing a probability of risk,  $p$ , will

want to buy cyber-insurance if  $U_p(z, c) \geq U_p(0, 0)$ . Thus, the following condition must hold for a user to buy cyber-insurance:  $w - z - pK(R - c) \geq w - pKR$ , or  $p \geq \frac{z}{Kc} = p_L(z, c)$ . Therefore, a user buys insurance only if its risk probability is higher than some *lower bound*  $p_L$ . The lower bound is dependent on  $z, c$ , and  $K$ . We observe that for a fixed  $K$ , the lower the value of premium per unit coverage, the higher is the incentive for a user to buy cyber-insurance.

On the other hand, the cyber-insurance agency may not allow every interested user to buy insurance. There exists a particular value,  $p_H$ , of the probability of risk, for which  $z = p_H c$ . In such a case, the cyber-insurance company breaks even and the resulting  $z$  is the fair premium. The insurance agency denies insurance service to users whose probability of risk is greater than  $p_H$ . Thus,  $p_H$  is the *upper bound* of the risk probability that a user requiring insurance can afford if it wants to claim insurance.

A cyber-insurer primarily interested in social welfare advertises a contract  $(z, c)$  that *maximizes* the total welfare of all Internet users in its geographical locality without it making negative profits. Formally, we frame our optimization problem as follows.

$$\operatorname{argmax}_{(z, c)} TW = A + B + C$$

$$\text{subject to } D,$$

where

$$A = \int_{p_L}^{p_H} [w - z - pK(R - c)]dp,$$

$$B = \int_0^{p_L} (w - pKR)dp,$$

$$C = \int_{p_H}^1 (w - pKR)dp,$$

$$D = \int_{p_L}^{p_H} (z - pc)dp \geq 0$$

$A$  is the expected utility of all Internet users whose risk facing probability,  $p$ , lies in the interval  $[p_L, p_H]$ .  $B$  represents the expected utility of users who have no incentive to buy insurance. The risk probability of these users lies in the interval  $[0, p_L]$ .  $C$  stands for the expected utility of users who want to purchase cyber-insurance, but are denied by the insurance agency. Their risk probabilities lie in the interval  $[p_H, 1]$ . Finally,  $D$  represents the constraint of the optimization problem, which states that the expected profits of the cyber-insurer are non-negative.

**Results.** We state our results through a theorem. We omit the proof due to lack of space. We note that the terms ‘profits’ and ‘total user welfare’ refer to the expected values of profits and social welfare.

**Theorem 1.** *For a welfare-maximizing cyber-insurance contract, the optimal (premium, coverage) pair is  $(R, R)$ ; the risk probability lower bound,  $p_L$ , equals  $\frac{1}{K}$ ;  $p_H = 1$ ; total user welfare,  $TW$ , is  $(w - R\frac{2K-1}{2K})$ ; and the insurer profit,  $P$ , equals  $R\frac{(K-1)^2}{2K^2}$ .*

**Theorem Implications:** We infer that the optimal insurance coverage in a welfare maximizing scenario is ‘full coverage’. For  $K = 1$  the lower bound of risk facing probability,  $p_L$ , is 1, and a user buys full cyber-insurance if its sure to face a risk, and in this case the insurer charges its client a fair premium  $R$ , i.e., probability of facing risk  $\times$  coverage ( $R$ ) =  $R$  = premium charged. However, as the degree of risk

averseness of a user increases, the value of  $p_L$  is less than one, and a user decides to buy insurance for risks that occur with probability less than or equal to 1. Intuitively, this result makes sense as more risk averse users are more inclined to buy cyber-insurance even for risks that do not occur with probability (w.p.) 1. However, for  $K > 1$ , the insurer charges an unfair premium  $R$  (i.e., probability of facing risk  $\times$  coverage  $<$  premium charged) to users who face risks that occur w.p.  $< 1$ , and charges a fair premium to users who are sure to face risk. Thus, the cyber-insurance agency de-incentivizes *higher* risk-averse users to buy insurance when they do not face risk for sure, to prevent itself from making negative profits. The profits made by the insurance company also increase with increase in  $K$ , and this is true as more users buy cyber-insurance, i.e,  $p_L$  value decreases with increase in  $K$ . However, the total user welfare decreases with increase in its degree of risk averseness. This is due to the fact that our utility function for each user is wealth based and a user loses more of its initial wealth with increase in its risk averseness. We emphasize here that the total user welfare is calculated by implicitly taking into account initial precautionary investments of a user. After a contract is signed between the cyber-insurer and its client, a user can decide on its optimal self-defense investments and evaluate a different utility function for welfare [8].

#### 4. PROFIT MAXIMIZING INSURANCE

In this section, we determine the optimal cyber-insurance policy,  $(z, c)$ , a cyber-insurance agency solely interested in maximizing profits (a monopolist) would provide to its customers. As in Section 3, we assume that a user can decide whether to buy the policy or not, and that the insurer also has the power to decide whether to provide insurance to a customer based on its probability of facing risk.

**Problem Formulation.** A cyber-insurer primarily interested in making business profits chooses a contract  $(z, c)$  that *maximizes* its total profit over all users it services. Formally, we frame our unconstrained optimization problem as follows.

$$\operatorname{argmax}_{(z,c)} \int_{p_L}^{p_H} (z - pc) dp,$$

where  $p_L$  and  $p_H$  are defined as above.

**Results.** We state our result through the following theorem. We omit the proof for lack of space.

**Theorem 2.** *For a profit-maximizing insurance contract, the optimal (premium, coverage) pair is  $(R \frac{K^2}{2K-1}, R)$ ;  $p_L = \frac{K}{2K-1}$ ;  $p_H = \frac{K^2}{2K-1}$ ; and the insurer profit,  $P$ , equals  $R \frac{(K-1)^2}{2(2K-1)}$ .*

**Theorem Implications:** We observe that full insurance coverage is the optimal insurance coverage in case of a profit maximizing scenario. Apart from the case when  $K = 1$ , in all other cases of  $K$ , the insurer charges an unfair premium to its client for a reason similar to that mentioned in the implications of Theorem 1. Taking the limit as  $K$  tends to infinity, we infer that the the probability lower bound,  $p_L$ , for a user lies in the interval  $[0.5, 1]$ . The value of  $p_H$  is obtained from the equation  $R \frac{K^2}{2K-1} = p_H R$ . As for insurer profits and individual user welfare, they increase and decrease with  $K$  for reasons similar to those provided in the implications of Theorem 1.

#### 5. COMPARISON

We now draw a comparison between parameters we have evaluated in welfare-maximizing contracts and profit-maximizing contracts cases. From the results in Sections 3 and 4, we observe that the optimal premium charged by the cyber-insurers is more in the case of monopolistic insurers than in the case of social welfare-maximizing insurers. For Internet users who are sure to face a risk, the monopolistic insurer charges them an unfair premium for coverage, i.e., premium  $>$  coverage (except when  $K = 1$ ), whereas for welfare-maximizing insurers, the users who are sure to face risk are charged a fair premium. We also observe that the profits made by a monopolistic insurer are higher than its welfare-maximizing counterpart.

The total user welfare in the profit-maximizing scenario is  $\int_0^{\frac{K}{2K-1}} (w - pKR) dp + \int_{\frac{K}{2K-1}}^1 (w - R \frac{K^2}{2K-1}) dp$ , which evaluates to  $w - R \frac{K^2(3K-2)}{2(2K-1)^2}$ . To compare the total user welfare in a profit-maximizing scenario with that of a welfare-maximizing scenario, we need to compare the expressions,  $\frac{K^2(3K-2)}{(2K-1)^2}$  and  $\frac{2K-1}{K}$ . Clearly, the former expression is greater or equal to the the latter for all  $K \geq 1$ , equality holding when  $K = 1$ . Therefore, the total user welfare in the case of a welfare-maximizing contract is always greater than or equal to that of a profit-maximizing cyber-insurance contract, equality holding when  $K = 1$ . The welfare gap for general values of  $K$  is  $\frac{R}{2} \cdot [\frac{K^2(3K-2)}{(2K-1)^2} - \frac{2K-1}{K}]$ . We observe that the welfare gap is linear with  $K$ , the degree of user risk averseness.

#### 6. FUTURE WORK

As part of future work, we are interested in developing a game-theoretic model for an oligopolistic insurance market scenario, where multiple Internet service providing companies, like Comcast, AT&T, etc. are in competition with each other in providing cyber-insurance to Internet users in a geographical locality. We are also interested in designing optimal cyber-insurance contracts under moral-hazard and adverse selection scenarios.

#### 7. REFERENCES

- [1] H.Kunreuther and G.Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26, 2002.
- [2] H.R.Varian. *Microeconomic Analysis*. Norton, 1992.
- [3] J.Kesan, R.Majuca, and W.Yurcik. Cyber-insurance as a market-based solution to the problem of cyber-security. In *WEIS*, 2005.
- [4] J.Walrand. *Personal Communication*.
- [5] M.Lelarge and J.Bolot. Cyber insurance as an incentive for internet security. In *WEIS*, 2008.
- [6] M.Lelarge and J.Bolot. Economic incentives to increase security in the internet: The case for insurance. In *IEEE INFOCOM*, 2009.
- [7] R.Anderson. Why information security is hard - an economic perspective. In *ACSAC*, 2001.
- [8] R.Pal and L.Golubchik. Analyzing self-defense investments in internet security under cyber-insurance coverage. In *IEEE ICDCS*, 2010.