Improving Cyber-Security via Profitable Insurance Markets

Ranjan Pal, Leana Golubchik, Konstantinos Psounis
University of Southern California
{rpal, leana, kpsounis}@usc.edu

ABSTRACT

Recent work in security has illustrated that solutions aimed at detection and elimination of security threats alone are unlikely to result in a robust cyberspace. As an orthogonal approach to mitigating security problems, some researchers have pursued the use of cyber-insurance as a suitable risk management technique. In this regard, a recent work by the authors in [1] have proposed efficient monopoly cyber-insurance markets that maximize social welfare of users in a communication network via premium discriminating them. However, the work has a major drawback in the insurer not being able to make strictly positive profit in expectation, which in turn might lead to unsuccessful insurance markets. In this paper, we provide a method (based on the model in [1]) to overcome this drawback for the risk-averse premium discriminating monopoly cyber-insurer, and prove it in theory. More specifically, we propose a non-regulatory mechanism to allow monopoly cyber-insurers to make strictly positive profit in expectation. To investigate the general effectiveness of our mechanism beyond a monopoly setting with full coverage, we conduct numerical experiments (comparing social welfare at market equilibrium) on (a) practical Internet-scale network topologies that are formed by users who are free to decide for themselves whether they want to purchase insurance or not, (b) settings of perfect and imperfect market competition, and (c) scenarios with partial insurance coverage.

Categories and Subject Descriptors

C.4 [**Performance of Systems**]: Modeling Techniques—*Economics*

Keywords

security, cyber-insurance, market, market equilibrium

1. INTRODUCTION

Despite continual improvements in risk protection techniques over the last decade due to hardware, software and cryptographic methodologies, it is impossible to achieve perfect or near-perfect cyber-security protection due to several techno-socio-economic reasons (see [2] [3]). In view of these reasons, the need arises for alternative methods for risk management in cyberspace In this regard, some security researchers in the recent past have identified *cyber-insurance* as a potential tool for effective risk management. Cyber-insurance is a risk management technique via which network user risks are transferred to an insurance company, in return for a fee, i.e., the *insurance premium*. Examples of potential cyber-insurers might include ISP, cloud provider, traditional insurance organizations. Proponents of cyber-insurance believe that cyber-insurance would lead to the design of insurance contracts that would shift appropriate amounts of self-defense liability to the clients, thereby making the cyberspace more robust. Here the term 'self-defense' implies the efforts by a network user to secure their system through technical solutions such as anti-virus and anti-spam software, firewalls, using secure operating systems, etc. Cyber-insurance has also the potential to be a market solution that can align with economic incentives of cyber-insurers, users (individuals/organizations), policy makers, and security software vendors. i.e., the cyber-insurers will earn profit from appropriately pricing premiums, network users will seek to hedge potential losses by jointly buying insurance and investing in self-defense mechanisms, policy makers would ensure the increase in overall network security, and the security software vendors could experience an increase in their product sales via forming alliances with cyber-insurers.

1.1 Research Motivation

Despite initial hopes, current cyber-insurance markets are moderately competitive, non-sustainable, and specialized with large to medium scale business being the sole insurance clients. There are currently over 60 insurance companies offering cyber-insurance contracts in the United States. Many insurers had reported growths of 10-25% in premiums in a 2012 survey of the market, with some companies even reporting higher rates [4]. We refer the interested reader to [5] [6] [7] for additional information on both the US and UK insurance markets, as well as common types of coverage offered through these policies, and the typical exclusions. The important thing to note from these studies is that the total cyber-insurance business currently amounts to approximately US$ 5 billion per year, *whereas* the total cost of security breaches to the global economy amounts to a whopping US$ 445 billion per year [8].

The inability to bridge this huge financial gap and form a successful and sustainable cyber-insurance market is mainly due to the fact that current cyber-insurance markets primarily target businesses and fail to reach out to the common population mass. A plausible reason for this trend is the existence of a number of unresolved research challenges and practical considerations [9], the most prominent amongst them being (i) *information asymmetry* between the insurer and the insured on loss information, and (ii) the *interdependent and correlated* nature of cyber-risks[1].

In this paper, we investigate via theory and experiments, the following important question: *can cyber-insurance solutions induce efficient sustainable markets that improve the security of a network consisting of network individuals as well as organizations?* In this regard, a recent work by the authors in [1] have proposed efficient monopoly cyber-insurance markets that maximize social welfare of users in a communication network via premium discriminating them. However, the work has a major drawback in the insurer not being able to make strictly positive profit in expectation, which in turn might lead to unsuccessful insurance markets. In the case when the insurer is a government agency primarily interested in social welfare, making strictly positive profit in expectation might not be a concern - however, there might be cases in future where big commerical companies (e.g., Amazon) might act as an insurance agency for it clients (e.g., for providing cloud services to a majority of population on the Internet). In addition, not every government mght have equal preferences for social welfare. As an example, it is popularly known that Hong Kong and Singapore governments are profit inclined.

1.2 Research Contributions

We make the following primary research contributions in this paper.

- In order to allow risk-averse cyber-insurers to make strictly positive profit, we derive in theory, non-regulated premium discriminating contracts in a monopoly scenario that allow a risk-averse cyber-insurer to make a certain amount of expected profit, and at the same time maximize social welfare at market equilibrium, and subsequently make the market efficient and sustainable. In this regard, we also study contracts that completely internalize all network externalities caused by user security efforts, and at the same time maximize social welfare at market equilibrium (See Section 3).

- For Internet-scale network topologies that are generated via a power-law degree distribution, we perform a detailed numerical experimental analysis of monopoly cyber-insurance markets, when network users are perfectly rational. The experimental results validate our claims made via theory (See Section 4).

2. SUPPLY-DEMAND MODEL

We propose a model of a cyber-insurance market in this section. In the first part we describe our model from a *demand* (network user) perspective. In the second part we describe our model from a *supply* (cyber-insurer) perspective.

2.1 Model from a Demand Perspective

We structure this section in several components which when combined together form the demand side of the cyber-insurance market.

2.1.1 Network Topology

We consider a communication network comprised of a continuum of *risk-averse* users. Here we use the notion of 'users' as per the *individual risk model* in the indemnity insurance literature, where users are considered as atomic *nodes* (individuals, organizations, enterprise, data center elements, etc.) in the network, each controlling a possible collection of devices [9]. The *links* between the nodes need not necessarily be physical connections (e.g., network link), and could also represent logical or social ties amongst the nodes (e.g., for social engineering attacks). We emphasize here that for different types of threats (e.g., targeted attacks, viruses and worms, social engineering attacks, etc.) we will have different network topologies.

2.1.2 Network User Utility Function

Each risk-averse user i in the communication network is assumed to be perfectly rational and has the standard *von Neumann-Morgenstern (VNM)* utility, $U_i(\cdot)$ [10]. VNM utilities are a function of a user's final wealth, and is twice continuously differentiable, increasing, and strictly concave. By the term 'final wealth', we imply a user's resulting wealth after being affected by threats, and (potentially) paying a premium to his cyber-insurer. We assume that each user in the network initially starts with a net worth of w_0.

2.1.3 Cost of Investing in Self-Defense Solutions

Each threat type has the potential to inflict loss of a particular amount on a user. However, depending on his latent security strength profile, each user is heterogenous and incurs a different cost to prevent the loss. For example, a user knowledgable about Internet security might adopt safe browsing practices, use secure OSs, and hence invest less in self-defense solutions compared to a user ignorant about safe security practices. More formally, for a *particular* loss size of r (the loss amount corresponding to a given threat), each user i incurs a cost x_i^r to invest in self-defense mechanisms to prevent the loss. Recall that self-defense mechanisms include antivirus and anti-spam softwares, firewalls, buying secure OSs, etc. We assume that x_i^r lies in the interval $[0, r]$, i.e., a user does not invest more in self-defense mechanisms than the total loss amount. We also assume that a user does not completely avoid loss on self-defense. In this paper we will use the terms 'self-defense' and 'self-protection' interchangeably.

For a given threat type, we define x_r^m to be the marginal cost of investing in self-defense mechanisms, i.e., it is the cost to a user who is indifferent between investing and not investing in self-defense. Such a user's net utility on investment in self-defense solutions is the same as his net utility on non-investment. In the remainder of the paper, we assume that such a user always invests in self-defense. All other risk-averse users either decide to invest or not invest in self-defense mechanisms, depending on whether their cost of investment is lower or higher than x_r^m. Throughout the paper we let r and x_i^r's have the same units.

2.1.4 Loss Types

Following the model by Kunreuther and Heal [11], we assume that a user is subject to two types of losses: *direct* and *indirect*. A direct loss to a user is caused when it is directly attacked by a malicious entity (threat). An indirect loss to a user is caused when it is indirectly affected by direct threats to other users in the network. A user can be indirectly af-

[1] In this work we use the terms 'risk' and 'expected loss' interchangeably.

fected only by a user who is already directly affected. Most common threats are of the direct/indirect type. A brief description of some examples of direct and indirect threats is given in Section 7. Regarding attacks, we assume them to be exogenous in nature rather than them being launched by *strategic* players.

2.1.5 *Loss Probabilities*

Let $p_d^{i,r}$ denote the probability of a direct loss to a user for a given threat type that has the potential to incur a loss of amount r on user i. Here $p_d^{i,r}$ is a function of x_i^r, i.e., $p_d^{i,r} = p_d^r$ if user i invests does not invest in self-defense solutions and $p_d^{i,r} = 0$ if he invests an amount x_i^r in self-protection. Thus, conditioned on the fact that a user i invests a non-zero amount x_i^r, he incurs a constant probability of loss that is the same for all other investing users, given a particular threat type. Let $p_{ind}^{i,r}(l)$ denote the probability of a user i getting indirectly affected by other network users for a given threat type, where l is the *proportion of users in the network not adopting self-defense (self-protection) mechanisms*, which in turn is a function of x_r^m, i.e., the marginal cost to a user indifferent to investing in self-defense investments. x_r^m is a function of (i) the vector of user investments, (ii) the network topology, and (iii) the number of users in the network who are already affected by a threat. Thus, $p_{ind}^{i,r}(l) = p_{ind}^{i,r}(l(x_r^m))$. Note that the proportion of individuals without self-defense investments is strictly decreasing in x_r^m as more users find it preferable to invest in self-defense with increasing marginal costs.

Regarding the connection between $p_{ind}^{i,r}(l)$ and $l(x_r^m)$, the higher the value of $l(x_r^m)$, the greater is the value of $p_{ind}^{i,r}(l)$. Therefore, $p_{ind}^{i,r}(l(x_r^m)) > 0$, and $0 \leq p_{ind}^{i,r}(l(x_r^m)) \leq p_{ind}^{max}$. Here p_{ind}^{max} is the maximum value of the function $p_{ind}^{i,r}(l)$ taken at an argument value of 1, and we assume that $p_{ind}^{i,r}(0) = 0$. The interpretation behind $p_{ind}^{i,r}(l)$ is that if nobody invests in self-defense, a user gets indirectly affected with probability p_{ind}^{max}, and if everyone invests in self-defense, the probability of indirect loss to a user is zero. Note that x_r^m is dependent on the investment of one's neighbors in the communication network, which in turn is dependent on the investment of neighbor's neighbors and so on.

The events where a user incurs a direct loss and an indirect loss are assumed to be *statistically* independent. In the case when a user does not completely avoid loss on self-defense, we assume that he has no direct loss on investing in self-protection but incurs an indirect loss. We denote p_i^r to be the probability of a user i facing a loss for a given threat type. In this case, when i invests in self-protection, p_i^r, is given by

$$p_i^r = p_{ind}^{i,r}(l(x_r^m)).$$

In a similar fashion, when i *does not* invest in self-defense mechanisms, p_i^r is given by

$$p_i^r = p_d^r + (1 - p_d^r)p_{ind}^{i,r}(l(x_r^m)).$$

We note that one particular way of computing the value of p_i^r as a function of parameters $p_d^{i,r}$ and $p_{ind}^{i,r}$ in a network graph, is using *Local Mean Field Analysis* (LMFA), [12] [13] [14], and is illustrated in [15].

Symbol	Meaning
U	VNM user utility function
w_0	Initial wealth of a user
$R = r$	Risk r.v. taking a value of r
x_i^r	cost to a user to invest in self-defense
x_r^m	marginal cost of investing in self-defense (risk size r)
x_r^{eq}	equilibrium investment cost
x_r^{sopt}	welfare maximizing investment cost
$l(x_r^m)$	proportion of non-investing network users
p_i^r	probability of a user i facing a risk
p_d^r	probability of a user facing direct risk
$p_{ind}^{i,r}(l(x_r^m))$	probability of a user i facing indirect risk
λ	loading factor of a cyber-insurance contract

Table 1: Summary of Important Symbols

2.2 Model from a Supply Perspective

The supply side of the market comprises of cyber-insurers selling insurance solutions. We assume that cyber-insurers bundle contracts for every threat type. In this paper, our analysis is for a particular threat type with potential to inflict a loss of r per user. Similar to the section on demand perspectives, we structure this section into multiple parts comprising the supply side of a cyber-insurance market.

2.2.1 *Regulation and Market Types*

In this paper we consider monopolistic cyber-insurance markets under a regulated setting. A regulatory agency is typically a government agency whose role is to ensure (i) monopoly insurers are limited to exercising certain client options and make profits under certain limits, (ii) insurers make the contract under-writing process effective and transparent, (iii) effective sharing of cyber-security information by establishing an anti-trust exemption to allow insurers to pool data on vulnerabilities and attacks, and (iv) the practical implementation of certain collective action mechanisms that potentially mitigate undesirable externalities and help improve network security. Of course, in environments of high risk interdependence and global correlation, regulatory steps might not result in the desired level of success (else widey adopted cyber-insurance markets would be a success by now), nonetheless the steps ensure smoother market operation.

2.2.2 *Insurer Types*

A cyber-insurer could be any combination of an ISP, security product vendor, traditional insurance company, and a security third party. We assume that insurers are *risk-averse* (in contrast to common assumption in insurance economics [16]). This assumption makes sense in the light of the fact that risks in cyber-space are highly interdependent and globally correlated; as a result the insurer can get bankrupt.

2.2.3 *Insurance Parameters*

In this work we assume that cyber-insurers provide full or partial coverage to their clients (users), who *must* buy cyber-insurance. We consider mandatory insurance as a regulator's tool to improve cyber-security. The authors in [17] [4] address the need for mandatory insurance, primarily stating the inability of voluntary cyber-insurance to maximize social welfare due to the public nature of security goods. In this paper, we consider social welfare maximization as the primary goal of a market and so enforce compulsory insurance. As a matter of fact, in a recent article [18], the authors cite the need of the US government to impose mandates on ISPs to increase cyber-security. From a policy viewpoint, compulsory insurance might raise some eyebrows [9], however we envision a future where proper incentives would be in place to make sure that network users voluntarily buy insurance.

As mentioned before, in a correlated and interdependent risk environment such as the Internet, a cyber-insurer cannot afford to be *risk-neutral* as it could become bankrupt if the expected aggregate loss in a period is greater than what it could afford to cover. Unlike in tradition, we do not model the insurer via concave utility functions that characterize risk-averse mindset. However, we assume/approximate the risk-averse behavior of the insurer by requiring it to hold ***safety capital***. A safety capital is an amount of money that a cyber-insurer buys from an agency to cover the risk of being bankrupt in the case of a catastrophic event caused by the factor of global correlation and risk interdependence. The cost of holding safety capital is distributed across the clients through the premiums charged to them. We assume that the share of safety capital cost per client is less than his expected risk value. Each client is charged a premium of $(1 + \lambda)E(R)$, where $\lambda \geq 0$ is the ***loading factor*** per contract, and $E(R)$ is the expected loss value of the client. Here, $E[R]$ equals $p_i^r \cdot r$, for a given threat type. The loading factor represents the amount of profit per contract the cyber-insurer is keen on making and/or the share of the safety capital cost of each user. Thus, in a sense, through λ, we capture the risk-averse behavior of the cyber-insurer. In a networked setting, heterogenous values of λ per network user can be determined using techniques proposed in [19] [20]. A premium is said to be *fair* if its value equals $E(R)$, and is *unfair* if its value is greater than $E(R)$.

2.2.4 Information Asymmetry

Information asymmetry has a significant negative effect on most insurance environments, where typical considerations include inability to distinguish between users of different (high and low risk) types, i.e., the so called *adverse selection* problem, as well as users undertaking actions that adversely affect loss probabilities after the insurance contract is signed, i.e., the so called *moral hazard* problem. The scale of information asymmetry is larger in the Internet than in other practical insurance scenarios, due to the interdependent and correlated nature of cyber-risks.

We assume that cyber-insurers can *approximately* resolve the information asymmetry problem, i.e., it can stochastically estimate loss probabilities for different risk categories via proper information sharing policies[2], and effective computational tools (e.g., the local mean field method), thereby resolving the *adverse selection* problem to an extent[3]. In a series of recent works, [22] [23] states ways to effectively estimate loss distributions in a computationally tractable manner for real world network (formed by individuals and organizations) topologies, and on a global scale. The works duly account for the uncertainty and inability to get information related to cyber-losses on a large geographical scale. In the organizational network context, the authors in [24] [25] provide statistical tools to appropriately compute cyber-insurance premiums under loss information uncertainty settings. Regarding the moral hazard problem, we assume that it exists and we will design a mechanism in this paper that will alleviate this problem (refer to Section 6.). We also assume that cyber-insurers can appropriately estimate losses. In this context, cyber-insurers can resort to a mixture of actuarial, normative, and emotional considerations proposed in [26] to measure losses in cyber-space, apart from resorting to information sharing pools.

Given the challenges of (i) uncertainty in computing risk, (ii) loss dependencies, and (iii) risk correlations, the cyber-insurers can overprice contracts and make clients unhappy [27], despite adopting best estimation practices. To prevent network users from not signing up for insurance, regulatory agencies need to design incentives for users to mandatorily or voluntarily buy insurance.

3. MAKING STRICTLY POSITIVE PROFIT

In [1], we showed that premium discrimination in a monopoly setting leads to social welfare maximization, but does not necessarily guarantee a strictly positive expected profit for the cyber-insurer. This in turn is strong enough a disincentive for the cyber-insurer to drop out of the market. In this section, we aim to alleviate this problem by designing contracts that allow the monopolistic insurer to make strictly positive profit, and at the same time ensure social welfare maximization. We take a non-regulated approach of charging fines and rebates to insurance clients so that the insurer always makes positive profit in expectation. Our solution is more theoretical in nature, primarily looking at a way to *internalize all externalities.* In a practical setting, our solution technique requires the assumption of *perfect information* and the possibility of no *outside options* - both of which are really hard to satisfy in reality. The goal of our theoretical analysis is to get some insights into developing practically viable solutions as part of future work.

We start off with the concept that marginal users will be indifferent beween investing in self-defense and not investing if

$$U_i(w_0 - x_r^m - ((1 + \lambda)p_{ind}^{i,r}(l(x_r^m)) \cdot r - b)) \qquad (1)$$
$$= U_i(w_0 - (1 + \lambda)p_i^r \cdot r + a)).$$

Thus, for a monopolist cyber-insurer to ensure a profit margin of k, the following relation needs to hold:

$$a \cdot l(x_r^m) - b \cdot (1 - l(x_r^m)) = k.$$

For a given threat type with the potential to inflict a loss of r on any user, we now have the following lemma characterizing the lower bound for k achieved when market equilibrium ensures a social welfare maximum, and the correspnding optimal and rebate values. *The proof of the lemma is in the Appendix.*

LEMMA 1. *For a given threat type, the lower bound of profit k made by a monopoly cyber-insurer at market equilibrium is given by*

$$k \geq \{x_r^{sopt} - p_d^r(1 - p_{ind}^{i,r}(l(x_r^{sopt})))r\}l(x_r^{sopt}) - p_{ind}^{i,r}(x_r^{sopt})r$$

[2] Precedents include the Information and Readiness Disclosure Act (1998), and Electronic Freedom of Information Act (1996).

[3] It is fair to assume that we cannot have a perfect scenario where information asymmetry will not exist. Such a state is impractical and infeasible. We can at best strive to achive a state where users will be happy to bear some cyber-risk, the insurers will be satisfied with the loss information they have, and the regulatory agencies will approve of the strength of cyber-security. [21]

, and corresponding fine and rebate values are respectively given by

$$a = x_r^{sopt} - p_d^r(1 - p_{ind}^{i,r}(l(x_r^{sopt})))r - b;\ \text{where}\ b$$
$$= \{x_r^{sopt} - p_d^r(1 - p_{ind}^{i,r}(x_r^{sopt}))r\}l(x_r^{sopt}) - k,$$

and $x_r^{sopt} = x_r^{eq} = x_r^m$, i.e., the market equilibrium solution leads to social welfare maximum.

Practical Implications: The above analysis shows that an efficient market equilibrium can be reached by ensuring a strictly positive profit of k for the cyber-insurer. Note that we performed our analysis constraining $\lambda = 0$. This is useful from both a theory perspective, as it makes analysis easier (need only deal with utility arguments), and also from a practical perspective, as it saves the insurance company the hassle of computing the optimal loading factor. In addition, in a non-regulated monopoly setting, the insurer can easily tune its fines and rebates to extract profit without requiring the loading factor. *An interesting question that arises out of the analysis of a monopoly market with premium discrimination is whether all externalities could be completely internalized.* This would happen only if the network users without self-protection had to be fully responsible for the externalities caused by them. In that case, the users making self-defense investments should be fully compensated by allowing them pay a zero premium. In practice, this scenario is hard to achieve (due to it being difficult to measure exact value of externalities caused by each user), however from a theory perspective, it is an interesting question to answer whether such an ideal situation can indeed be achieved. In this regard, we have the following theorem that can be derived using Lemma 1. *The proof of the lemma is in the Appendix.*

THEOREM 1. *With (i) a premium fine α for users without self-defense such that α enables the internalization of all externalities, and (ii) a zero premium for network users with self-defense adoption, the socially optimal prevention level is achievable. Under a profit restriction of $k > 0$, an optimal α must satisfy*

$$k \geq \alpha \cdot l(x_r^{sopt}) - (1 - l(x_r^{sopt}))p_{ind}^{i,r}(l(x_r^{sopt}))r > 0.$$

Proof Sketch. The proof method is based on the rationale that we show the monotonicity of a potential function related to the cases when a user invests and does not invest in self-defense mechanisms, which leads us to a unique set of parameters at market equilibrium.

Practical Implications. The main takeaway message from this theorem is that we need to charge a premium fine high enough for high risk users to internalize all the externalities. In Lemma 1 we had derived a lower bound of the expected profit k and the associated fine and rebate values, but these parameters do not ensure that all network externalities are internalized. As mentioned before, there are practical challenges to implementing a parameter setting in practice that internalizes all externalties, primarily due to the inevitability of imperfect information and the presence of outside options. In addition, under a non-regulated environment, the monopoly cyber-insurer can charge exorbitant fines, leading to a dictatorial setting. However, there is an important practical intuition conveyed by Lemma 1 and Theorem 1: between the case of k having a lower bound and the case of the cyber-insurer "dictatorially" making a profit margin as it desires, there is a range of k which could be exploited through properly designed premium discrimination mechanisms that might lead to strictly profit making scenarios for the cyber-insurer. Such mechanisms could be supported via regulatory agencies and be practically viable solutions. As part of future work, we plan to design price discrimination mechanisms in practice by closely studying the properties of user network communication graphs, and their relationship with user investment patterns.

4. PRACTICAL EVALUATION

In this section, we conduct a numerical experimental evaluation of our cyber-insurance market settings proposed in the paper. Our main goal here is to not only validate the theoretical result derived in the paper under the assumption of compulsory insurance, but at the same time study market efficiency trends under the assumption of non-compulsory insurance for the monopoly market setting. This section is structured as follows: , we describe the network topology and risk contagion setting used for our experiments; *second*, we describe the security adoption setting for network users who can either be perfectly rational or boundedly rational; *third*, we describe our cyber-insurance market setting; and *finally*, we plot and analyse our numerical evaluation results.

4.1 Network Topology and Contagion Setting

We consider a large graph with power-law degree distribution [28], to be representative of Internet-scale network topologies. A typical example of such a topology is a large social/logical network on which social engineering attacks propagate. We use the popular Generalized Linear Preference (GLP) method to generate power law graphs [29] using the power law exponent value, γ = -3. We generate graphs with 10,000 nodes and approximately 30,000 edges. For the generated graphs, we observe the minimum node degree in the graphs to be 3 and the maximum degree to be 180. With respect to risk contagion in the network, we assume each network user to initially get *directly* infected (when not investing in security measures) with a probability that is a function of its node degree. As example of this probability function, for a given user degree k, we choose the probability to equal $\frac{0.15}{k}^{\frac{1}{3}}$. A user also initially infects its neighbors in the graph *indirectly* with a probability q, which for our work lies in the set {0.1, 0.2, 0.3}.

4.2 Security Adoption Setting

We model the utility function, U_i, of final wealth of a network user i to be the widely used *Cobb-Douglas* function in economics [10], with risk aversion parameter σ. Mathematically we represent this function as

$$U(w) = \frac{w^{\sigma}}{1 - \sigma},$$

where w is the final wealth of a user, and $\sigma \in [0, 1)$ is the degree of risk aversion of U. In this paper, we set the degree of risk of aversion of the utility function σ to be uniformly distributed in the range [0.5, 0.8] for all nodes. Unlike our proposed theory, we assume the initial wealth of nodes to be a function of their degree k to represent heterogeneity of initial wealth amongst network users. In this regard, we choose $w_0^k = 10k + 50$. We assume that the loss for each user follows a uniform distribution from 0 to half of its initial wealth. We also set the cost of security measure, i.e., self-defense, of all nodes to be uniformly distributed in the range [0.3, 0.6]. Initially, all nodes without (with) security measures are infected initial with probability $\frac{0.15}{k}^{\frac{1}{3}}$ (0).

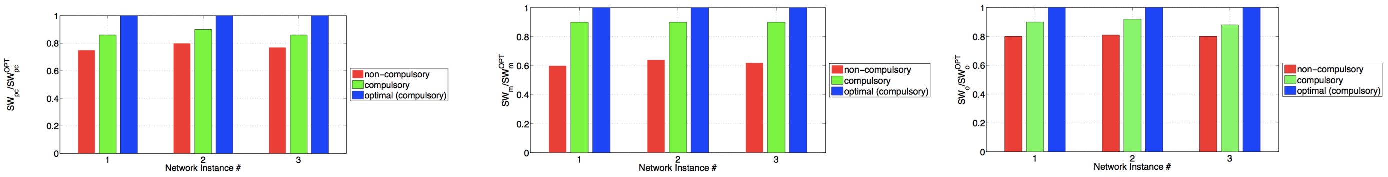

Figure 1: $\frac{Equilibrium\ Welfare}{Optimal\ Welfare}$ Ratios for (a) Perfect Competition (left), (b) Monopoly (middle), and (c) Oligopoly (right) - Case of [full coverage, premium non-discrimination]

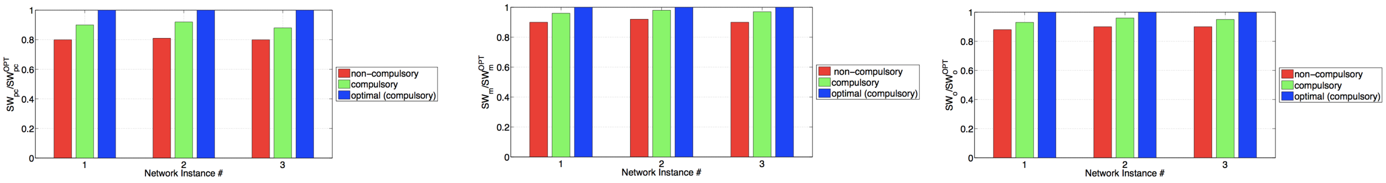

Figure 2: $\frac{Equilibrium\ Welfare}{Optimal\ Welfare}$ Ratios for (a) Perfect Competition (left), (b) Monopoly (middle), and (c) Oligopoly (right) - Case of [full coverage, premium discrimination]

4.3 Cyber-Insurance Market Setting

We consider monopoly markets in our evaluations. For this market structure, we assume both full or partial coverage provided to network users by the insurer. With respect to the cyber-insurer providing partial coverage to its clients, we assume that the cyber-insurer uniformly randomly chooses its partial coverage from the set {70%, 75%, 80%} of percentage coverage of total loss values. For the premium discrimination setting in monopolistic markets, we assume that the insurance provider determines its loading factor via a topological mechanism as proposed in [20]. We also randomly prelock network users to a monopoly cyber-insurance provider prior to running simulations.

4.4 Performance Results

In this section, we plot and analyze performance results related to efficiency of cyber-insurance markets under our above-mentioned experimental setting. For this setting, we emphasize here that results related to (i) the infection probability of nodes in a network with different degrees, and (ii) security adoption behavior of users in the network are already discussed in [15], and is not the focus of this paper. Here, we only focus on the efficiency of cyber-insurance markets under environments of (i) compulsory/non-compulsory insurance, (ii) discriminatory/non-discriminatory premium pricing, and (iii) full/partial insurance coverage.

Figures 1-4 illustrate the welfare ratio $\frac{SW_{\{pc,m,o\}}}{SW^{OPT}_{\{pc,m,o\}}}$ at market equilibrium for difference cyber-insurance parameter settings. Each plot projects the results for three randomly chosen network instances generated via a power law degree distribution. We observe the following trends:

- Compulsory insurance generates more social welfare at market equilibrium compared to that when insurance is made non-compulsory, for all settings considered in our experimentation. The reason for this is the compulsory insurance forces network users to be liable for their security behavior (and hence internalize externalities in the network to a greater degree), else they could end up paying more premiums, something that conflicts with rational behavior of users forced to buy insurance.

- For all the experimental settings, monopoly markets result in the best social welfare performance, i.e., higher social welfare, at market equilibrium when compared to perfect competition and oligopoly markets. The reason for this is the additional pricing control a monopolistic cyber-insurer enjoys over insurers in competition. The monopoly insurer tunes its prices to maximize its profit, but at the same time makes network users invest enough in self-defense at market equilibrium to improve social welfare.

- For all market types, price discrimination results in better social welfare performance at market equilibrium compared to the non-discrimination setting, and alleviates the problem of moral hazard. The reason for this trend is that differentiated premiums relatively optimally (via fines and rebates) allow network externalities to be internalized by the network users, compared to the case of non-differentiated pricing that fails to penalize network users with high risk and reward network users with low risk.

- For all market types, partial coverage by an insurer results in better social welfare performance at market equilibrium compared to full coverage scenarios. This trend is evident because full coverage leads to moral hazard issues for network users, where the latter has a lesser incentive to protect themselves to the best of abilities, compared to the partial coverage setting, and knowing that they would be fully covered on facing a loss. Thus, social welfare suffers. On the other hand, partial coverage transfers liability on a network user to invest more in self-defense and improve social welfare in the network.

5. RELATED WORK ON MARKET SUCCESS

Recent research works on cyber-insurance [30] [3] [31] have mathematically shown the existence of inefficient insurance

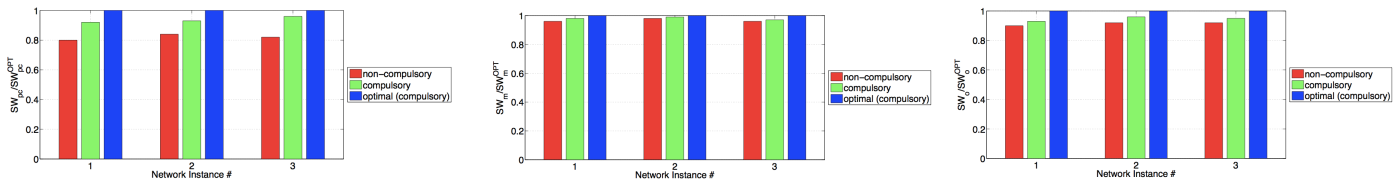

Figure 3: $\frac{Equilibrium\ Welfare}{Optimal\ Welfare}$ Ratios for (a) Perfect Competition (left), (b) Monopoly (middle), and (c) Oligopoly (right) Case of [partial coverage, premium differentiation]

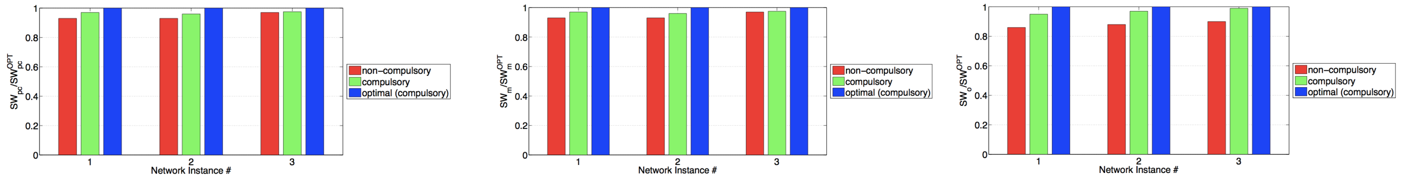

Figure 4: $\frac{Equilibrium\ Welfare}{Optimal\ Welfare}$ Ratios for (a) Perfect Competition (left), (b) Monopoly (middle), and (c) Oligopoly (right) Case of [partial coverage, premium discrimination]

markets. Intuitively, an efficient market is one where all stakeholders (market elements) mutually satisfy their interests. These works state that cyber-insurance satisifies every stakeholder apart from the regulatory agency (e.g., government), and sometimes the cyber-insurer itself. The regulatory agency is unsatisfied as overall network robustness is sub-optimal due to network users not optimally investing in self-defense mechanisms, whereas a cyber-insurer is unsatisfied due to it potentially making zero expected profit at times. Lelarge et.al in [3] recommended the use of fines and rebates on cyber-insurance contracts to make each user invest optimally in self-defense and make the network optimally robust. However, their work neither mathematically proves the effectiveness of premiums and rebates in making network users invest optimally, nor does it guarantee the strict positiveness of insurer profits at all times. In [14] [15], the authors state that cyber-insurance incentivizes self-defense investments only if the quality of self-defense is not very good and the initial security level of user is poor. Cyber-insurance does not incentivize self-defense investments if the quality of self-defense is good or the initial security level of a user is good. These conditions might be necessary to ensure efficient markets but are practically not feasible to achieve, or commonly realizable in the real world. In a recent work [1], we overcome the drawbacks of the mentioned existing works, and propose ways to form provably efficient monopolisitc cyber-insurance markets by satisfying market stakeholders, including a risk-averse cyber-insurer, in environments of interdependent risk. We also account for information asymmetry and correlated risks in a partial manner. In doing so we also extend and strengthen our own works in [32] and [33] that account for market stakeholders and information asymmetry respectively, in a weak manner. However, a drawback of the work in [1] is that there is no strict guarantee provided to the monopolistic cyber-insurer that it would always make positive profits. The notion of making zero expected profits at times is enough for cyber-insurers to opt out of the market, leading to an insurance market failure. *In this paper, we make a theoretical effort to address the problem of a monopoly insurer always making positive profit in expectation, using non-regulatory mechanisms.*

6. CONCLUSION AND FUTURE WORK

In this paper we alleviated in theory, the problem of a risk-averse monopoly insurer not making positive profit in expectation by fixing an insurer profit choice of value k, and designing premium discriminating contracts that ensure a profit of k and at the same time maximize social welfare, thereby making the market efficient and sustainable. We took a non-regulated approach of charging fines and rebates to insurance clients so that the insurer always makes positive profit in expectation. Our solution insight here is to find a way to internalize all network externalities. We validated our proposed theory in the paper using extensive numerical experiments conducted on practical Internet-scale network topologies obeying the power-law degree distribution.

The problem of making strictly positive profit can also be addressed in a regulated manner using a symbiotic relationship between a market entity and a cyber-insurer, as in [**?**]. For example, a security vendor (e.g., Symantec or Microsoft) can enter the cyber-insurance ecosystem and via a symbiotic relationship between the insurer (through exchange of logical/social client topological information and lock-in privileges for profit shares of the SV) can increase its profits and subsequently enable the cyber-insurer to always make strictly positive profit keeping the social welfare state identical. As a special case, the security vendor could be the cyber-insurer itself. One advantage of this approach is that fines and rebates could be fairly split amongst the network users based on network structure, and the amount of externalities each user generates in the network via his investments, instead of just charging a fixed fine/rebate for high and low risk users, as suggested in this paper. In addition, the symbiotic approach would also allow a cyber-insurer to appropriately allocate its safety capital costs amongst clients.

One drawback of our work is we assume that an insurer can stochastically observe user investment amounts and infer their risk type. This *partially* incorporates the adverse selection problem in the model. However, as part of future work we want to investigate the existence of efficient cyber-insurance markets when the insurer can make no observations on client investments, or is given false information by the clients. We strongly feel that the theory of mechanism and ontract design in economics should be a good starting point in allowing us to address the information asymmetry problem in network settings a nice manner. Another problem we want to explore in theory is to find ways to satisfy all market stakeholders under non-compulsory cyber-insurance in an oligopolistic setting.

7. REFERENCES

[1] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security: A market analysis," in *To Appear in IEEE INFOCOM*, 2014.

[2] R. Anderson and T. Moore, "Information security economics and beyond," in *Information Security Summit*, 2008.

[3] M. Lelarge and J. Bolot, "Economic incentives to increase security in the internet: The case for insurance," in *IEEE INFOCOM*, 2009.

[4] P. Naghizadeh and M. Liu, "Voluntary participation in cyber-insurance markets," in *WEIS*, 2014.

[5] S. Romanovsky, *Comments to the Department of Commerce on Incentives to Adopt Improved Cyber-Security Practices*. April 2013, 2013.

[6] Betterly, *The Betterly Report: Cyber/Privacy Insurance Market Survey*. June, 2012, 2012.

[7] Arimic, *Arimic Review of Recent Developments in the Cyber-Insurance Market*. 2013, 2013.

[8] M. Thompson, "Why cyber-insurance is the next big thing," in *CNBC Report*, 2014.

[9] R. Bohme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework," in *WEIS*, 2010.

[10] A. Mas-Collel, M. D. Winston, and J. R. Green, *Microeconomic Theory*. Oxford University Press, 1995, 1995.

[11] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty*, vol. 26, 2002.

[12] M. Lelarge and J. Bolot, "A local mean field analysis of security investments in networks," in *ACM NetEcon*, 2008.

[13] M. Lelarge and J. Bolot, "Network externalities and the deployment of security features and protocols in the internet," in *ACM SIGMETRICS*, 2008.

[14] Z. Yang and J. Lui, "Security adoption in heterogenous networks: The influence of cyber-insurance market," in *IFIP Networking*, 2012.

[15] Z. Yang and J. C. S. Lui, "Security adoption and influence of cyber-insurance markets in heterogenous networks," *Performance Evaluation*, vol. 74, 2014.

[16] G. Dionne and S. E. Harrington, *Foundations of Insurance Economics: Readings in Economics and Finance*. Springer, 1992.

[17] R. Pal, L. Golubchik, and K. Psounis, "Aegis: A novel cyber-insurance model," in *IEEE/ACM GameSec*, 2011.

[18] A. Khouzani, S. Sen, and N. Shroff, "An economic analysis of regulating security investments in the internet," in *IEEE INFOCOM*, 2013.

[19] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Security pricing as an enabler of cyber-insurance: A first look at differentiated pricing markets," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[20] R. Pal and P. Hui, "Cyber-insurance for cyber-security: A topological take on modulating insurance premiums," *Performance Evaluation Review*, vol. 40, no. 3, 2012.

[21] A. Odlyzko, "Economics, psychology, and sociology of security," in *Financial Cryptography*, 2003.

[22] B. Johnson, A. Lazska, and J. Grossklags, "The complexity of estimating systematic risk in networks," in *IEEE CSF*, 2014.

[23] A. Lazska, B. Johnson, J. Grossklags, and M. Felegyhazi, "Estimating systematic risk in real-world networks," in *FC*, 2014.

[24] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukan, "Cyber-risk decision models: To insure it or not?," *Decision Support Systems*, vol. 56, 2013.

[25] S. B. Herath and C. T. Herath, "Copula based actuarial model for pricing cyber-insurance policies," *Insurance Markets and Companies: Analyses and Actuarial Computations*, vol. 2, 2011.

[26] M. Baddeley, "Information security: Lessons from behavioral economics," in *SHB*, 2011.

[27] C. Toregas and N. Zahn, *Insurance for Cyber-Attacks: The Issue of Setting Premiums in Context*. George Washington University, 2014.

[28] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the internet topology," in *ACM SIGCOMM computer communication review*, vol. 29, pp. 251–262, ACM, 1999.

[29] T. Bu and D. Towsley, "On distinguishing between internet power law topology generators," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, pp. 638–647, IEEE, 2002.

[30] A. Hoffman, "Internalizing externalities of loss prevention through insurance monopoly," *Geneva Risk and Insurance Review*, vol. 32, 2007.

[31] N.Shetty, G.Schwarz, M.Feleghyazi, and J.Walrand, "Competitive cyber-insurance and internet security," in *WEIS*, 2009.

[32] R. Pal and L. Golubchik, "On economic perspectives of internet security," in *ACM SIGMETRICS Workshop on Mathematical Performance Modeling and Analysis (MAMA)*, 2010.

[33] R. Pal and P. Hui, "Modeling internet security investments: The case of tackling topological information uncertainty," in *IEEE/ACM GameSec*, 2011.

Appendix

In this section we prove Lemma 1 and Theorem 1.
Proof of Lemma 1. Consider $\lambda = 0$. In such a case, because premiums are marginally fair, risk-averse users act as if they were risk neutral [16]. The social welfare expression, $SW_{M_{ncd}}(x_r^m)$, in the monopoly scenario (when insurer wants a profit of k) is then given by

$$SW_{M_{ncd}} = \int_0^{x_r^m} (w_0 - x - (p_{ind}^{i,r}(l(x_r^m)) \cdot r - b))f(x)dx + \chi,$$

where

$$\chi = (w_0 - (p_i^r \cdot r + a))l(x_r^m) + k.$$

Now, we know that

$$\int_0^{x_r^m} bf(x)dx - al(x_r^m) = b(1 - l(x_r^m)) - al(x_r^m) = -k.$$

Thus, using the relation, $al(x_r^m) - b(1 - l(x_r^m)) = k$, $SW_{M_{ncd}}(x_r^m)$ can be expressed as

$$SW_{M_{ncd}}(x_r^m) = \int_0^{x_r^m} (w_0 - x - p_{ind}^{i,r}(l(x_r^m)) \cdot r)f(x)dx + (w_0 - p_i^r \cdot r)l(x_r^m).$$

We also have the participation constraint of the cyber-insurer expressed as

$$p_d^r(1 - p_{ind}^{i,r}(l(x_r^m)))r - x_r^m + \frac{a}{1 - l(x_r^m)} - \frac{k}{1 - l(x_r^m)} = 0. \quad (2)$$

The Lagrangian function, $\mathcal{L}(a, x_r^m, L, k)$ subject to the previous equation is given by

$$\mathcal{L}(a, x_r^m, L, k) = \int_0^{x_r^m} (w_0 - x - p_i^r \cdot r)f(x)dx + L \cdot C, \quad (3)$$

where

$$C = p_d^r(1 - p_{ind}^{i,r}(l(x_r^m)))r - x_r^m + \frac{a}{1 - l(x_r^m)} - \frac{k}{1 - l(x_r^m)},$$

and L is the Lagrange multiplier. The necessary first-order condition for a maximum of $\mathcal{L}$ is

$$\frac{\delta \mathcal{L}(a, x_r^m)}{\delta a} = L \cdot \left\{ \frac{1}{1 - l(x_r^m)} \right\} = 0. \quad (4)$$

Since the term inside braces of Equation (4) is positive, we have $L = 0$. Thus, the optimal self-defense investmen cost is x_r^{sopt} at market equilibrium. Correspondingly, the values of a (fine) and b (rebate) for a given k, are given by

$$a = x^{sopt} - p_d^r(1 - p_{ind}^{i,r}(l(x_r^{sopt})))r - b,$$

where

$$b = \{x_r^{sopt} - p_d^r(1 - p_{ind}^{i,r}(l(x_r^{sopt})))r\} - k.$$

Since the rebate, b, does not exceed the fair premium value, we have

$$k \geq \{x_r^{sopt} - p_d^r(1 - p_{ind}^{i,r}(l(x_r^{sopt})))r\} - l(x_r^{sopt})r.$$

Thus, we have proved Lemma 1 **Q.E.D.**

Proof of Theorem 1. Without a premium fine, the expected utility of network users who invest in self-defense is $U_i(w_0 - x_i^r)$, and $U_i(w_0 - p_i^r \cdot r)$ for users who do not invest in self-defense mechanisms. In that case we have

$$\Psi(l(x_r^m), x_r^m) = U_i(w_0 - x_r^m) - U_i(w_0 - p_i^r \cdot r).$$

We also have $\frac{d\Psi}{dx_r^m}$ evaluate to

$$-U_i(w_0 - x_r^m) + U(w_0 - p_d^r r - (1 - p_d^r)p_{ind}^{i,r}(l(x_r^m))r)(1 - p_d^r)\frac{dp_{ind}^{i,r}(l(x_r^m))}{dx_r^m}r,$$

which is less than zero, and thus $\frac{d\Psi_2}{dx_r^{m_2}}$ is strictly decreasing in $x_r^{m_2}$. Again, $\Psi(l(x_r^m), 0) > 0$, and $\Psi(l(x_r^m), r) < 0$. Thus in most practical cases, there is a unique interior solution (according to monotonicity properties), x_r^{sopt} such that

$$\Psi(l(x_r^m), x_r^{sopt}) = U_i(w_0 - x_r^{sopt}) - U_i(w_0 - p_i^r \cdot r) = 0,$$

where $p_i^r \cdot r$ is evaluated at x_r^{sopt}. Introducing a premium fine of α for users who do not invest in self-defense, the following two must hold:

$$U_i(w_0 - x_r^m) = U_i(w_0 - p_i^r \cdot r + \alpha). \quad (5)$$

and

$$U_i(w_0 - p_i^r \cdot r) - U_i(w_0 - x_r^{sopt}) = \frac{dU_i(w_0 - p_i^r \cdot r)}{dx_r^m} l(x_r^m), \quad (6)$$

where $x_r^m = x_r^{sopt}$. In order to attain the optimal self-defense cost value, x_r^{sopt}, Equation (5) can be written as

$$U_i(w_0 - x_r^{sopt}) = U_i(w_0 - p_i^r \cdot r + \alpha),$$

where $p_i^r \cdot r$ is evaluated at x^{sopt}. Thus, there exists an α that satisfies

$$U_i(w_0 - p_i^r \cdot r) - U_i(w_0 - (p_i^r \cdot r + \alpha)) = \frac{dU_i(w_0 - p_i^r \cdot r - \alpha)}{dx_r^m} l(x_r^m), \quad (7)$$

where $x_r^m = x_r^{sopt}$. The latter expression is greater than zero and thus the socially optimal level of self-defense, x_r^{sopt} is achievable by a fine of α, and for the insurer-desired profit margin, k, the following must hold:

$$k \geq \alpha \cdot l(x_r^{sopt}) - (1 - l(x_r^{sopt}))p_{ind}^{i,r}(l(x_r^{sopt}))r > 0. \quad (8)$$

Here $p_{ind}^{i,r}(l(x_r^{sopt}))r$ denotes the expected loss of users whose self-defense investment cost level is x_r^{sopt}. Equation (8) results because the quantity, $p_{ind}^{i,r}(l(x_r^{sopt}))r$, which must be indemnified by the cyber-insurer in case of a loss, but for which it has no premium income from users adopting self-defense, must be gained by the quantity $\alpha(p_{ind}^{i,r}(l(x_r^{sopt})))$ - the proportion of network users who do not invest in self-defense, in order for the insurer to make strictly positive expected profits. Thus, we have proved Theorem 1 **Q.E.D.**