Will Cyber-Insurance Improve Network Security? *A Market Analysis*

Ranjan Pal
University of Southern California
Email: rpal@usc.edu

Leana Golubchik and Konstantinos Psounis
University of Southern California
Email: {leana, kpsounis}@usc.edu

Pan Hui
HKUST, and T-Labs - Germany
Email: pan.hui@telekom.de

***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 have pursued the use of cyber-insurance as a suitable risk management technique. Such an approach has the potential to jointly align with the incentives of security vendors (e.g., Symantec, Microsoft, etc.), cyber-insurers (e.g., ISPs, cloud providers, security vendors, etc.), regulatory agencies (e.g., government), and network users (individuals and organizations), in turn paving the way for comprehensive and robust cyber-security mechanisms.**

To this end, in this work, we are motivated by the following important question: can cyber-insurance really improve the security in a network? To address this question, we adopt a market-based approach. Specifically, we analyze regulated monopolistic and competitive cyber-insurance markets, where the market elements consist of risk-averse cyber-insurers, risk-averse network users, a regulatory agency, and security vendors. Our results show that (i) without contract discrimination amongst users, there always exists a unique market equilibrium for both market types, but the equilibrium is inefficient and does not improve network security, and (ii) in monopoly markets, contract discrimination amongst users results in a unique market equilibrium that is efficient, which in turn results in network security improvement - however, the cyber-insurer can make zero expected profits. The latter fact is often sufficient to de-incentivize the insurer to be a part of a market, and will eventually lead to its collapse. This fact also emphasizes the need for designing mechanisms that incentivize the insurer to permanently be part of the market.

***Keywords:* security, cyber-insurance, market, equilibrium**

I. Introduction

The infrastructure, the users, and the services offered on computer networks today are all subject to a wide variety of risks posed by threats that include distributed denial of service attacks, intrusions of various kinds, eavesdropping, hacking, phishing, worms, viruses, spams, etc. In order to counter the risk posed by the threats, network users have traditionally resorted to antivirus and anti-spam softwares, firewalls, intrusion-detection systems (IDSs), and other add-ons to reduce the likelihood of being affected by threats. In practice, a large industry (companies like *Symantec, McAfee,* etc.) as well as considerable research efforts are currently centered around developing and deploying tools and techniques to detect threats and anomalies in order to protect the cyber infrastructure and its users from the negative impact of the anomalies.

Inspite of improvements in risk protection techniques over the last decade due to hardware, software and cryptographic methodologies, it is impossible to achieve a perfect/near-perfect cyber-security protection [3][12]. The impossibility arises due to a number of reasons: (i) scarce existence of sound technical solutions, (ii) difficulty in designing solutions catered to varied intentions behind network attacks, (iii) misaligned incentives between network users, security product vendors, and regulatory authorities regarding each taking appropriate liabilities to protect the network, (iv) network users taking advantage of the positive security effects generated by other user investments in security, in turn themselves not investing in security and resulting in the free-riding problem, (v) customer lock-in and first mover effects of vulnerable security products, (vi) difficulty to measure risks resulting in challenges to designing pertinent risk removal solutions, (vii) the problem of a lemons market [2], whereby security vendors have no incentive to release robust products in the market, (viii) liability shell games played by product vendors, and (ix) user naiveness in optimally exploiting feature benefits of technical solutions. In view of the above mentioned inevitable barriers to near 100% risk mitigation, the need arises for alternative methods of risk management in cyberspace [1]. 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 (e.g., ISP, cloud provider, traditional insurance organizations), in return for a fee, i.e., the *insurance premium*. 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 on 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 softwares, 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, the policy makers would ensure the increase in overall network security, and the security software vendors could go ahead with their first-mover and lock-in strategies as well as experience an increase in their product sales via forming alliances with cyber-insurers.

A. Research Motivation

Despite all promises, current cyber-insurance markets are moderately competitive and specialized. As of 2010, there are approximately 18 insurance organizations in the United states insuring $800 million worth of organizational IT resources only [4], and there is little information as to whether the current cyber-insurance market improves network security by incentivizing organizations to invest aptly in security solutions. The inability of cyber-insurance to become a common reality (i.e., to form a successful market) amongst non-organizational individual users is due to a number of unresolved research challenges as well as practical considerations.

[1] To highlight the importance of improving the current state of cyber-security, US President Barack Obama has recently passed a security bill that emphasizes the need to reduce cyber-threats and be resilient to them.

The most prominent amongst them is *information asymmetry* between the insurer and the insured, and the *interdependent and correlated* nature of cyber-risks [5].

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 challenge due to the interdependent and correlated nature of cyber-risks is particular to cyber-insurance and differentiates traditional insurance scenarios (e.g., car or health insurance) from the former. In a large distributed system such as the Internet, risks span a large set of nodes and are correlated. Thus, user investments in security to counter risks generate positive externalities (See Section I-C) for other users in the network. The aim of cyber-insurance here is to enable individual users to internalize the externalities in the network so that each user optimally invests in security solutions, thereby alleviating moral hazard and improving network security. In traditional insurance scenarios, the risk span is quite small (sometimes it spans only one or two entities) and uncorrelated, thus internalizing the externalities generated by user investments in safety, is much easier.

In this paper we investigate the following important question: *can cyber-insurance solutions induce efficient markets that improve the security of a network?* By the term network security we imply the *average probability* of a user being successfully attacked by malicious threats [15]. This is our security metric. In the process of studying improvement and the optimality of network security, we are interested in analyzing the welfare of elements (stakeholders) that form a cyber-insurance market (if there exists one).

B. Research Contributions

We make the following primary research contributions in this paper.

- We propose a supply-demand model of regulated cyber-insurance markets that accounts for inter-dependent risks in a networked environment as well as the externalities generated by user security investments. (See Section II.)
- We show that a monopoly cyber-insurer providing full coverage to its clients without contract discriminating them enables the existence of an inefficient cyber-insurance market that does not improve network security. However, with client contract discrimination, the cyber-insurer is successful in enabling an efficient cyber-insurance market that alleviates the moral hazard problem and improves network security. In the process the insurer makes non-negative expected profits. (See Section IV.)
- We show that in perfectly competitive and oligopolistic cyber-insurance settings, there exists an inefficient insurance market that does not improve network security. (See Section V.)

C. Basic Economics Concepts

In this section we briefly review some basic economics concepts as applicable to this work in order to establish terminology for the remainder of the paper. Additional details could be found in a standard economics textbook such as [13]. Basic concepts related to insurance economics will be discussed in Section II.

externality: An externality is an effect (positive or negative) of a purchase of self-defense investments by a set of users (individuals or organizations) on other users whose interests were not taken into account while making the investments. In this work, the effects are improvements in individual security of network users who are connected to the users investing in self-defense.

risk probability: It is the probability of a network user being successfully attacked by a cyber-threat and incurring a loss of a particular amount.

initial wealth: It is the initial amount of wealth a network user possesses before expending in any self-defense mechanisms and/or insurance solutions.

user risk propensity: A risk-neutral investor (either the insurer or the insured) is more concerned about the expected return on his investment, not on the risk he may be taking on. A classic experiment to distinguish between risk-taking appetites involves an investor faced with a choice between receiving, say, either $100 with 100% certainty, or a 50% chance of getting $200. The risk-neutral investor in this case would have no preference either way, since the expected value of $100 is the same for both outcomes. In contrast, the risk-averse investor would generally settle for the "sure thing" or 100% certain $100, while the risk-seeking investor will opt for the 50% chance of getting $200.

market: In regard to a cyber-insurance context, it is a platform where cyber-insurance products are traded with insurance clients, i.e., the network users. A market may be perfectly competitive, oligopolistic, or monopolistic. In a perfectly competitive market there exists a large number of buyers (those insured) and sellers (insurers) that are small relative to the size of the overall market. The exact number of buyers and sellers required for a competitive market is not specified, but a competitive market has enough buyers and sellers that no one buyer or seller can exert any significant influence on premium pricing in the market. On the contrary, in monopolistic and oligopolistic markets, the insurers have the power to set client premiums to a certain liking.

equilibrium: An equilibrium refers to a situation when both, buyers, as well as the sellers are satisfied with their net utilities and no one has any incentive to deviate on their strategies. In this paper we consider two equilibrium concepts: (i) the Nash equilibrium (for monopoly markets and imperfectly competitive markets), and (ii) the Walrasian equilibrium (a standard solution concept for perfectly competitive markets).

stakeholders: The stakeholders in a cyber-insurance market refer to entities whose interests are affected by the dynamics of market operation. In our work we assume that the entities are cyber-insurers (e.g., ISPs, cloud providers, security vendors, traditional insurance companies), the network users, a regulatory agency such as the government, and security vendors such as Symantec and Microsoft.

market efficiency: A cyber-insurance market is called efficient if the social welfare of all network users is maximized at the market equilibrium. The market is inefficient if it fails to achieve this condition. Here, 'social welfare' refers to the sum of the net utilities of network users after investing in self-defense and/or cyber-insurance.

II. Supply-Demand Model

In this section we propose a supply-demand model of a cyber-insurance market. The section has two parts: in the first part we describe our model from a demand (network user) perspective, in the second part we describe our model from the supply (cyber-insurer) perspective. Important notation[2] used in the paper is summarized in Table 1. Additional notation is explained when used in subsequent sections.

A. Model from a Demand Perspective

We consider a communication network comprised of a continuum of *risk-averse* users. Here we use the notion of 'users' as mentioned in [5], where users are considered as atomic nodes (individuals, organizations, enterprise, data center elements, etc.) in the network, each controlling a possible collection of devices. The links between the nodes need not necessarily be physical connections and could also represent logical or social ties amongst the nodes. For example, social engineering attacks are conducted on overlay networks. Each

[2] Variations of certain notations as applicable to the section at hand are described in the respective sections.

user has initial wealth w_0 and faces a risk of size $r < w_0$ with probability p, i.e., he either faces a risk of size r with probability p or faces no risk with probability $1 - p$. Here p is a function of the proportion of users not investing in security measures *(read on for a more formal description.)*. Each risk-averse user has the standard *von Neumann-Morgenstern (VNM)* utility[3], $U(\cdot)$[13], that is a function of his final wealth, is twice continuously differentiable, increasing, and strictly concave. Each user also incurs a cost x to invest in self-defense mechanisms, which is drawn from a random variable X having distribution function F and density function f, each defined over the support $[0, r]$. We define x^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 is the same as his net utility on non-investment. From now on in 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^m.

We assume that a user does not completely avoid loss on self-protection, i.e., self-protection is not perfect, and 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. Let p_d denote the probability of a direct loss to a user. Let $q(l)$ denote the probability of a user getting indirectly affected by other network users, 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^m, i.e., the marginal cost to a user indifferent to investing in self-defense investments. Thus, $q = q(l) = q(l(x^m))$. We have the following relationship between l and x^m:

$$l = l(X = x^m) = \int_{x^m}^{r} f(\theta)d\theta = 1 - F(x^m). \qquad (1)$$

Thus, $\frac{dl(x^m)}{dx^m} = -f(x^m) < 0$, implying the proportion of individuals without self-defense investments is strictly decreasing in x^m as more users find it preferable to invest in self-defense with increasing marginal costs.

Regarding the connection between q and $l(x^m)$, the higher the value of $l(x^m)$, the greater is the value of q. Therefore we assume $q'(l(x^m)) > 0$, and $0 \leq q(l(x^m)) \leq q^{max}$. Here q^{max} is the value of the function q taken at an argument value of 1, and we assume that $q(0) = 0$. The interpretation behind q is that if nobody invests in self-defense, a user gets indirectly affected with probability q^{max}, and if everyone invests in self-defense, the probability of indirect loss to a user is zero. Note that x^m is dependent on the investment of one's neighbors in the contact graph *(our work assumes any general contact graph)*, which in turn is dependent on the investment of neighbor's neighbors and so on. The events that 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. In this case, his probability of facing a loss on investing in self-protection is given as

$$p = p(x^m) = q(l(x^m)).$$

The probability of a user facing a loss when he *does not* invest in self-defense mechanisms is given as

$$p = p(x^m) = p_d + q(l(x^m)) - p_d q(l(x^m)) = p_d + (1 - p_d)q(l(x^m)).$$

Symbol	Meaning
U	VNM user utility function
U^i_{def}	user utility (defense adopted, Scenario i)
U^i_{ndef}	user utility (no defense, Scenario i)
w_0	Initial wealth of a user
$R = r$	Risk r.v. taking a value of r
x	cost to a user to invest in self-defense
x^m	marginal cost of investing in self-defense
x^{m_i}	marginal investment cost in Scenario i
x^{eq_i}	equilibrium investment cost in Scenario i
x^{sopt_i}	welfare maximizing investment cost in Scenario i
$SW_i()$	social welfare of users in Scenario i
$l(x^{m_i})$	proportion of non-investing network users (Scenario i)
$p(x^{m_i})$	probability of a user facing a risk (Scenario i)
p_d	probability of a user facing direct risk
$q(l(x^{m_i}))$	probability of a user facing indirect risk (Scenario i)
P^2_{jk}	user premium for Case jk of Scenario 2
Case jk	Case j in Scenario 2 with investment scenario k
P^3_k	user premium in Scenario 3, $k \,\epsilon\, \{1, 2\}$
λ	loading factor of a cyber-insurance contract
$\Pi_{monopoly}$	expected profit by a monopolistic cyber-insurer

TABLE I
LIST OF IMPORTANT SYMBOLS

B. Model from a Supply Perspective

In this paper we consider regulated monopolistic and competitive (both perfect and oligopolistic) cyber-insurance markets. A regulatory agency is typically a governmental agency whose role is to ensure (i) insurers make profits under certain limits, and (ii) the network security is improved. A cyber-insurer could be any combination of an ISP, security product vendor, traditional insurance companies, and security third parties. We assume that insurers are *risk-averse* and provide full coverage to their clients (users), who must buy cyber-insurance in the monopolistic case (not necessarily in the competitive case). Mandatory insurance is considered as a regulator's tool in [12], but the flip side to it is that it might be politically inviable or difficult to implement [5]. However, in a recent article [8], the authors cite the need of the US government to impose mandates on ISPs to increase cyber-security[4]. In this regard, we could also foresee the use of compulsory cyber-insurance if it were to increase cyber-security[5]. Another reason why compulsory insurance could be mandated is to prevent high-risk users from adopting unsafe protection measures. In a non-compulsory system, high risk users might opt out of buying cyber-insurance knowing that they would have to pay high premiums. This would imply that these users could adopt unsafe security measures that result in negatively affecting cyber-security. With insurance being made compulsory, high risk users would take steps to protect their systems more in order to pay lesser premiums, and hence positively affect cyber-security. We ensure full coverage from the insurer side in return for clients committing to buy cyber-insurance.

In a correlated and interdependent risk environment such as the Internet, a cyber-insurer cannot afford to be *risk-neutral* as it could

[3] Von-Neumann-Morgenstern utility functions are standard in expected utility-theoretic economics.

[4] As a matter of fact, in [18], the authors show that when insurable and non-insurable risks (for example those caused by hardware/software reliability faults) co-exist together, even under conditions of no information asymmetry between the monopolistic insurer and the insured, cyber-insurance needs to be made mandatory for a market to exist. From a policy viewpoint, this seems tough to implement, but as mentioned above, in the interest of cyber-security, such measures might be adopted in the near future.

[5] In practice, for reliability purposes, it is possible to enforce compulsory insurance in data center and enterprise networks where the network is generally owned by a single entity providing application services to numerous customers.

get bankrupt if the expected aggregate loss in a period is greater than what it could afford to cover. We assume the risk-averse behavior of the insurer by requiring it to hold ***safety capital***. A safety capital is the additional amount over the expected aggregate loss in a period such that the probability of an insurer incurring of a loss of value greater than the sum of the capital and expected aggregate loss in that period does not exceed a particular threshold. The threshold value is defined by a regulator. 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. The loading factor resembles 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. A premium is said to be *fair* if its value equals $E(R)$, and is *unfair* if its value is greater than $E(R)$.

III. Scenario 1: No Insurance Case

In this section we analyze the case when network users do not have access to any form of insurance coverage. This case is useful for the comparison of optimal user investments in security between scenarios of no insurance coverage and those with coverage.

The expected utility of a user in Scenario 1 who does not invest in self-defense mechanisms is given as

$$E[U^1_{ndef}] = E[U^1_{ndef}(l(x^{m_1}))] = p_d U(w_0 - r) + (1 - p_d)Q_1,$$

where Q_1 is the probability of the user facing indirect loss in Scenario 1 and is given as

$$Q_1 = q(l(x^{m_1}))U(w_0 - r) + (1 - q(l(x^{m_1}))U(w_0),$$

where $q = q(l(x^{m_1}))$. Here, x^{m_1} is the marginal cost of investment in Scenario 1. Similarly, the expected utility of the same user when he invests in self-defense mechanisms is given as

$$E[U^1_{def}] = E[U^1_{def}(l(x^{m_1}), x)]$$

or

$$E[U^1_{def}] = q(l(x^{m_1}))U(w_0 - x - r) + (1 - q(l(x^{m_1}))U(w_0 - x).$$

A user would want to invest in loss prevention only if $E[U^1_{def}] \geq E[U^1_{ndef}]$.
Define $\Psi_1(l(x^{m_1}), X = x)$ as

$$\Psi_1(l(x^{m_1}), x) = E[U^1_{def}(l(x^{m_1}), x)] - E[U^1_{ndef}(l(x^{m_1})]. \quad (2)$$

When $X = r$, we have

$$\Psi_1(l(x^{m_1}), r) = (1 - p_d)\{U(w_0 - r) - U(w_0)\} < 0, \quad (3)$$

and at $X = 0$ we have

$$\Psi_1(l(x^{m_1}), 0) = p_d(1 - q^{max})\{U(w_0) - U(w_0 - r)\} > 0. \quad (4)$$

In most practical cases, Equations 3 and 4 jointly indicate the monotonicity of $\Psi_1(\cdot)$ (due to Ψ being often strictly decreasing) and imply that (i) if no user invests in self-protection and the risk of loss is very high, it is worth to undertake defense measures to reduce expected loss, when cost to invest in self-defense is zero, (ii) if every user invests in self defense and the risk is zero, an investment is not worth being undertaken, and (iii) there exists an interior solution x^{eq_1}, where $0 < x^{eq_1} < r$, such that

$$\Psi_1(l(x^{m_1}), x^{eq_1}) = E[U^1_{def}(l(x^{m_1}), x^{eq_1})] - E[U^1_{ndef}(l(x^{eq_1}))] = 0. \quad (5)$$

Nash Equilibrium: The solution to $E[U^1_{def}] = E[U^1_{ndef}]$ gives us the investment cost to a user who is indifferent between investing and not investing in self-defense. Thus $x^{eq_1} = x^{m_1}$, the marginal cost of making self-defense investments in Scenario 1. The interior solution, x^{eq_1}, in the equation is the competitive Nash equilibrium (NE) cost of protection investment. It implies the fact that users whose cost of self-defense is less than x^{eq_1} invest in self-defense as their expected utilities of investing would be greater than that without it, whereas the others do not invest in any protection mechanisms as it would not be profitable for them to do so. Mathematically, the expression for the Nash equilibrium can be derived from the following equation arising due to [19].

$$U(w_0 - x^{eq_1} - q(l(x^{eq_1}))\cdot r - \pi[q(l(x^{eq_1}))]) = U(w_0 - p\cdot r - \pi[p]),$$

where $p = p(x^{eq_1})$, which leads to a NE value given by

$$x^{eq_1} = p_d(1 - q(l(x^{eq_1}))\cdot r - \pi[q(x^{eq_1})] + \pi[p(x^{eq_1})].$$

Here $\pi[p]$ is the risk premium and denotes the maximum amount a user is willing to pay to securely receive the expected value of the probability distribution of risk instead of the probability distribution itself.

Social Welfare Maximization: We define the social welfare of a network of users in the no insurance case as the sum of the expected utility of all the users. Mathematically, we denote social welfare in Scenario 1 as $SW_1(x^{m_1})$ and express it as

$$SW_1(x^{m_1}) = \int_0^{x^{m_1}} E[U^1_{def}(l(x^{m_1}, x)]f(x)dx + E[U^1_{ndef}(l(x^{m_1})]l(x^{m_1}).$$

The first term in $SW_1(x^{m_1})$ denotes the sum of the expected utility of all agents with adopting self-defense, the second term denotes the sum of the expected utilities of all agents not investing in self-defense. Equating the first order condition for $SW_1(x^{m_1})$ results in finding x^{sopt_1}, the cost of investment that maximizes social welfare. The first order condition (FOC) for an interior maximum is

$$\frac{dSW_1(x^{m_1})}{dx^{m_1}} = A_1 + B_1 + C_1 + D_1, \quad (6)$$

where

$$A_1 = E[U^1_{def}(l(x^{m_1}), x^{m_1})]f(x^{m_1}),$$

$$B_1 = E[U^1_{ndef}(l(x^{m_1}))]\frac{dl(x^{m_1})}{dx^{m_1}},$$

$$C_1 = \frac{dE[U^1_{ndef}(l(x^{m_1}))]}{dx^{m_1}}l(x^{m_1}),$$

and

$$D_1 = \int_0^{x^{m_1}} \frac{\delta E[U^1_{def}(l(x^{m_1}, x)]}{\delta x^{m_1}} f(x)dx.$$

In the light of Equation 1, Equation 6 can be written as

$$\frac{dSW_1(x^{m_1})}{dx^{m_1}} = F + C_1 + D_1, \quad (7)$$

where

$$F = \{E[U^1_{def}(l(x^{m_1}), x^{m_1})] - E[U^1_{ndef}(l(x^{m_1}))]\}f(x^{m_1}).$$

The term inside brackets of F is the excess of expected utility, $\Psi_1(l(x^{m_1}), x^{m_1})$. C_1 and D_1 are non-negative and non-decreasing in x. Since the excess of expected utility is positive at $x = 0$ and negative at $x = r$, there exists x^{sopt_1} such $\frac{dSW_1(x^{m_1})}{dx^{m_1}}$ is zero, and the social welfare in the network is maximized. We represent this mathematically as

$$x^{sopt_1} = argmax_{x^{m_1}} SW_1(x^{m_1}). \quad (8)$$

Substituting x^{eq_1} in Equation 7, and using Equation 5 we get

$$\frac{dSW_1(x^{m_1})}{dx^{m_1}}|_{x^{m_1}=x^{eq_1}} > 0. \quad (9)$$

This implies that $x^{sopt_1} > x^{eq_1}$ and $l(x^{sopt_1}) < l(x^{eq_1})$. i.e., the proportion of users not resorting to self-defense mechanisms is higher in the Nash equilibrium than in the welfare optimum. **The analysis above proves the following theorem.**

Theorem 1. *In the case of imperfect prevention, when network users do not have cyber-insurance protection, there exists a unique Nash equilibrium (NE) cost to invest in self-defense, x^{eq_1}. Users facing protection costs below x^{eq_1} invest in self-defense mechanisms, whereas other users do not. This NE cost of self-defense does not result in maximizing user social welfare in the network, i.e., i.e., the proportion of users not resorting to self-defense mechanisms is higher in the Nash equilibrium than in the welfare optimum.*

Theorem Intuition and Practical Implications: The intuition behind Theorem 1 follows from the *first fundamental theorem in welfare economics* [13] which states that the network externalities generated by user investments are not internalized (i.e., users do not pay for externality benefits), by the users for public goods such as security measures, and results in the free-riding problem. Thus, risk - averse users do not end up putting in optimal self-defense efforts, and this results in sub-optimal network security, i.e., the average of the sum of user risk probabilities (denoted as $p(x^m)$), is not minimized. With respect to the welfare of users, the ones who face a cost of investment above the NE cost do not buy security products and are not satisfied because they cannot defend themselves on being attacked. The ones who do invest in security measures are better off but are still susceptible to indirect risks. Security vendors like Symantec and Microsoft make profits as per their current security product market scenario. The case of no insurance is currently the situation in Internet security, apart from a few organizations that are insured.

IV. Scenario 2: Monopoly Markets

In this section we analyze a regulated monopolistic cyber-insurance market under conditions of imperfect prevention (self-protection does not guarantee risk removal). Here the term ‘regulated’ implies the role of the government to (i) ensure Internet users buy compulsory cyber-insurance, (ii) enable insurers to adopt premium discrimination amongst clients based on the user risk types , and (iii) allow basic user security behavior monitoring by insurance agencies. We divide this section in two parts: in the first part we analyze the case when there is no contract discrimination amongst clients. In the second part we analyze the case with clients being contract discriminated.

A. Case 1- No Contract Discrimination

The expected utility of a user who does not invest is self-defense in Scenario 2 is given as

$$E[U^2_{ndef}] = E[U^2_{ndef}(l(x^{m_2}))] = p_d U(w_0 - r + r - P) + (1 - p_d)Q_2,$$

where Q_2 is the probability of the user facing indirect loss in Scenario 2, and is given as

$$Q_2 = q(l(x^{m_2}))U(w_0 - r + r - P) + (1 - q(l(x^{m_2}))U(w_0 - P^2_{11}).$$

Here $P(p, r) = (1 + \lambda)p \cdot r = P^2_{11}$ is the insurance premium that a user in Scenario 2, Case 1, and not investing in security (hence denoted as P^2_{11}), pays to his cyber-insurer in return for full coverage of his loss (hence the ‘$-r+r$’ term in U), and $R = r$ is the risk faced by the user. x^{m_2} is the marginal cost of investment in Scenario 2. The expected utility of the same user when he invests in self-defense mechanisms is given as

$$E[U^2_{def}] = E[U^2_{def}(l(x^{m_2}), x)] = U(w_0 - x - P^2_{12}),$$

where $P^2_{12} = P(q(l(x^m), r) = (1 + \lambda)q(l(x^m)) \cdot r$ is the insurance premium a user in Scenario 2, Case 1, and investing in security pays to his insurer. A user would want to invest in loss prevention only if $E[U^2_{def}] \geq E[U^2_{ndef}]$.

Define $\Psi_2(l(x^{m_2}), X = x)$ as

$$\Psi_2(l(x^{m_2}), x) = E[U^2_{def}(l(x^{m_2}), x)] - E[U^2_{ndef}(l(x^{m_2}))]. \quad (10)$$

When $X = 0$, we have

$$\Psi_2(l(x^{m_2}), 0) = U(w_0 - P^2_{12}) - U(w_0 - P^2_{11}) > 0, \quad (11)$$

and at $X = r$ we have

$$\Psi_2(l(x^{m_2}), r) = U(w_0 - r) - U(w_0 - p_d r) < 0. \quad (12)$$

In most practical cases, Equations 11 and 12 jointly indicate the monotonicity of $\Psi_2(\cdot)$ and imply that $\Psi_2(\cdot)$ is decreasing in x and there exists $x^{eq2} \,\epsilon\, (0, r)$, such that

$$\Psi_2(l(x^{m_2}), x^{eq_2}) = E[U^2_{def}(l(x^{m_2}), x^{eq_2})] - E[U^2_{ndef}(l(x^{eq_2}))] = 0. \quad (13)$$

Nash Equilibrium: The solution, x^{eq_2}, to $E[U^2_{def}] \geq E[U^2_{ndef}]$ is the Nash equilibrium (NE) cost of protection investment, and equals x^{m_2}, the marginal cost of making self-defense investments in Scenario 2. This implies the fact that users whose cost of self-defense is less than x^{eq_2} find it profitable to invest in self-defense and cyber-insurance, whereas the others invest only in cyber-insurance.

Mathematically, the expression for the Nash equilibrium can be derived from the following equation arising due to [19].

$$U(w_0 - x^{eq_2}) = U(w_0 - p(x^{eq_2}) \cdot r), \quad (14)$$

which leads to a NE value given by

$$x^{eq_2} = p(x^{eq_2}) \cdot r. \quad (15)$$

Social Welfare Maximization: We define the social welfare of a network of users as the sum of the expected utility of all the users. Mathematically, we denote social welfare in Scenario 2 as $SW_2(x^{m_2})$ and is evaluated to

$$\int_0^\infty \int_0^{x^{m_2}} E[U^2_{def}(l(x^{m_2}, x)]f(x)dxd\lambda + E[U^2_{ndef}(x^{m_2})]l(x^{m_2}).$$

The first term of $SW_2(x^{m_2})$ denotes the sum of the expected utility of all agents adopting self-defense, the second term denotes the sum of the expected utilities of all agents not investing in self-defense and buying only cyber-insurance. Equating the first order condition for $SW_2(x^{m_2})$ results in finding x^{sopt_2}, the cost of investment that maximizes social welfare.

The first order condition (FOC) for an interior maximum is

$$\frac{dSW_2(x^{m_2})}{dx} = A_{21} + B_{21} + C_{21} + D_{21}, \quad (16)$$

where

$$A_{21} = \int_0^\infty E[U^2_{def}(l(x^{m_2}), x^{m_2})]f(x^{m_2})d\lambda,$$

$$B_{21} = E[U^2_{ndef}(l(x^{m_2}))]\frac{dl(x^{m_2})}{dx^{m_1}},$$

$$C_{21} = \frac{dE[U^2_{ndef}(l(x^{m_2}))]}{dx^{m_2}}l(x^{m_2}),$$

and

$$D_{21} = \int_0^\infty \int_0^{x^{m_2}} \frac{dE[U^2_{def}(x^{m_2})]}{dx^{m_2}}f(x)dxd\lambda.$$

In the light of Equation 1, Equation 16 can be written as

$$\frac{dSW_2(x^{m_2})}{dx^{m_2}} = G + C_{21} + D_{21}, \quad (17)$$

where

$$G = \{E[U^2_{def}(l(x^{m_2}), x^{m_2})] - EU^2_{ndef}(l(x^{m_2}))\}f(x^{m_2})$$

Here, the first term of G in brackets is the excess of expected utility, $\Psi_2(l(x^{m_2}), x^{m_2})$, C_{21} and D_{21} are non-negative and non-decreasing in x. Since the excess of expected utility is positive at $x = 0$ and negative at $x = r$, there exists $x = x^{sopt_2}$ such $\frac{dSW_2(x)}{dx}$ is zero, and the social welfare in the network is maximized. We represent this mathematically as

$$x^{sopt_2} = argmax_x SW_2(x). \quad (18)$$

Substituting x^{eq_2} for x^{m_2} in Equation 17, and using Equation 13 we get

$$\frac{dSW_2(x)}{dx}|_{x=x^{eq_2}} > 0. \quad (19)$$

This implies that $x^{sopt_2} > x^{eq_2}$ and $l(x^{sopt_2}) < l(x^{eq_2})$. i.e., the proportion of users not resorting to self-defense mechanisms is higher in the Nash equilibrium than in the welfare optimum. **The analysis above proves the following theorem for Scenario 2, Case 1.**

Theorem 2. *Under compulsory monopolistic cyber-insurance, there exists a unique Nash equilibrium (NE) cost to invest in self-defense, x^{eq_2}. Users facing protection costs below x^{eq_2} invest in self-defense mechanisms, whereas other users only buy cyber-insurance. This NE cost of self-defense does not result in maximizing user social welfare in the network (i.e., the proportion of users not resorting to self-defense mechanisms is higher in the Nash equilibrium than in the welfare optimum.), and cyber-insurance does not incentivize users to invest in self-defense mechanisms.*

Theorem Intuition and Practical Implications: The intuition behind Theorem 2 is that externalities caused due to individual user investment in security mechanisms are not internalized by the users, and as a result social welfare is not maximized at Nash equilibrium.

The implications of the theorem are (i) cyber-insurance does not incentivize network users to invest in self-defense mechanisms[6], (ii) cyber-insurance exacerbates the moral hazard problem, i.e., once users buy insurance they do not spend as much in self-defense as they would without it. This makes sense from an economic viewpoint as users would loath to bear excessive cost in self-defense if there is an alternative to canceling out risk albeit at an unfair premium, i.e., premium greater than the fair amount, and (iii) cyber-insurance might increase individual user utilities (as users get full coverage of their losses) but does not positively contribute to the increase of overall network security. As a result a regulator interested in improving network security is not satisfied. These implications are also mentioned by the authors in [15] for a competitive market setting. Also note that since $\lambda \geq 0$, the cyber-insurer makes non-negative expected profits. A security vendor does not satisfy its interests from an existing cyber-insurance market, i.e., compared to Scenario 1, as the sales of its products are going to go down.

Central Point: In the monopolistic cyber-insurance scenario with no client contract discrimination, there exists an inefficient market, i.e., the social welfare of users is not maximized at NE. This does not help satisfy the interests of all the market stakeholders.

B. Case 2 - Contract Discrimination

In the previous section we saw and investigated why inspite of mandating cyber-insurance on network users, a social welfare maximum could not be reached. In this section we aim to improve upon this drawback by allowing the insurer to premium discriminate its clients, and keeping all other factors the same as in the case without premium discrimination[7]. The rationale for client discrimination is that users who take (do not take) appropriate self-defense actions reduce (increase) their chances of getting attacked as well as reduce (increase) other network users' chances of facing a loss. In order to differentiate between clients, the cyber-insurer imposes a fine of amount a per user of high risk type, and provides a rebate of amount b per user of low risk type. A user is considered of high risk type if he does not invest in self-defense mechanisms, and is considered of low risk type when he does invest in the same. A user decides whether it wants to invest in self-protection depending on the cost of investment and the provided fine/rebate. The sequence of the protocol between the insurer and the clients can be seen as follows: ***Stage 1*** - the insurer advertises appropriate contracts to its clients that include the fine/rebate values. ***Stage 2*** - the users simultaneously decide whether or not to invest in self-defense based on the cost of investment and their signed contract information, and ***Stage 3*** - when a coverage claim is filed by clients, the cyber-insurer examines the claims and charges the suitable rebate/fine to each client based on whether his investment amounts were above or below a particular threshold. Here we assume that the cyber-insurer can observe or stochastically learn the investment amounts of its clients *after* a claim is made.

Note that the premium differentiation approach is feasible only in the case of monopolistic cyber-insurance markets or imperfect competitive markets. In the case of perfectly competitive markets, price competition will not allow insurers to discriminate amongst their clients for commercial demand purposes and insurers will have to sell contracts at absolute fair premiums making zero expected profits. We now proceed with the analysis of the case when users are premium discriminated in monopoly markets.

A user not willing to invest in self-defense investments will pay a fine a over his premium. At equilibrium the following result needs to hold for the cyber-insurer to treat equally (fairly), a user who invests in self-defense investments, as well as a user who does not invest in self-defense investments.

$$U(w_0 - x - P_{22}^2) = U(w_0 - (P_{21}^2 + a)), \quad (20)$$

where P_{21}^2 and P_{22}^2 are user premiums in the case of investment and no investment respectively in Scenario 2 Case 2, i.e., with contract discrimination. *Our goal here is to find the optimal self-defense cost $x^{sopt_{2'}}$ that achieves maximum social welfare.* Let

$$A_{22} = U(w_0 - P_{21}^2) - C_{22},$$

where

$$C_{22} = \int_0^\infty U(w_0 - x^{sopt_{2'}} - P_{22}^2) \cdot f(x^{sopt_{2'}}) d\lambda.$$

Let

$$B_{22} = \frac{d(U(w_0 - P_{21}^2)}{dx} l(x^{sopt_{2'}}) + D_{22},$$

where

$$D_{22} = \int_0^\infty \int_0^{x^{sopt_{2'}}} \frac{\delta U(w_0 - x - P_{22}^2)}{\delta x} f(x) dx d\lambda.$$

Here P_{21}^2 and P_{22}^2 are the premiums evaluated at $x^{sopt_{2'}}$, and A_{22} and B_{22} are the expected utilities of users investing and not investing in self-defense, respectively. The condition for achieving maximum

[6] As an exception, cyber-insurance incentivizes self-defense investments of users in the case when insurable and non-insurable risk co-exist together and it is not easy for a user to distinguish between the two [18]. For example, a hardware failure can be caused due to either a security lapse, or hardware defect, and it is difficult for a naive user to figure out the right reason for the failure.

[7] In a recent paper [17], the authors have proposed cooperation amongst users on their self-defense investment information, as a way to ensure social welfare maximization of network users under a cyber-insurance setting. The authors use the well known Coase Bargaining Theorem [20] to arrive at their result. However, user cooperation can only be sustained only under restricted network settings where all users work towards a common goal, e.g., system performance maximization in a multicasting scenario.

social welfare is given as $A_{22} = B_{22}$. Substituting $x = x^{sopt_{2'}}$, and $a = a^{sopt_{2'}}$ in Equation 20, we get

$$U(w_0 - x^{sopt_{2'}} - P_{22}^2) = U(w_0 - (P_{21}^2 + a^{sopt_{2'}})), \qquad (21)$$

where $a^{sopt_{2'}}$ satisfies $E = B_{22}$, where

$$E = U(w_0 - P_{21}^2) - \int_0^\infty U(w_0 - (P_{21}^2 + a^{sopt_{2'}}))f(x^{sopt_{2'}})d\lambda.$$

Thus the optimal self-defense investment cost $x^{sopt_{2'}}$ to achieve social welfare maximization is obtained by charging high risk type users a fine of a on top of their premiums.

A user willing to invest in self-defense investments will receive a rebate of b on his premium. At equilibrium the following result needs to hold for the cyber-insurer to treat equally (fairly), a user who invests in self-defense investments, as well as a user who does not invest in self-defense investments:

$$U(w_0 - x - (P_{22}^2 - b)) = U(w_0 - P_{21}^2). \qquad (22)$$

Our goal here again is to find the optimal self-defense cost $x^{sopt_{2'}}$ that achieves maximum social welfare. Substituting $x = x^{sopt_{2'}}$, and $b = b^{sopt_{2'}}$ in Equation 22, we get

$$U(w_0 - x^{sopt_{2'}} - P_{22}^2 - b^{sopt_{2'}}) = U(w_0 - P_{21}^2), \qquad (23)$$

where P_{12}^2 and P_{22}^2 are evaluated at $x^{sopt_{2'}}$. Let

$$M = U(w_0 - x^{sopt_{2'}} - (P_{22}^2 - b^{sopt_{2'}})) - C_{22}.$$

Then $b^{sopt_{2'}}$ is such that it satisfies the following condition (derived by combining Equations 20 and 22.):

$$M = B_{22}.$$

Thus, the optimal self-defense investment cost $x^{sopt2'}$ to achieve social welfare maximization is obtained by providing low risk type users with a rebate of b on their premiums.

The net minimum profit made by a cyber-insurer per contract (without any loading, λ, with loading the net profit is even more.) in a monopoly market with contract discrimination is given as

$$\Pi_{monopoly} = a \cdot l(x^{sopt_{2'}} - b \cdot (1 - l(x^{sopt_{2'}})) \geq 0. \qquad (24)$$

The analysis above proves the following theorem on Scenario 2, Case 2.

Theorem 3. *Under conditions of compulsory monopolistic cyber-insurance, a cyber-insurer can help achieve social welfare maximization by premium discriminating clients. In turn, it makes non-negative expected profits, and also incentivizes users to invest in self-defense investments.*

Theorem Intuition and Practical Implications: By premium discriminating clients in the form of fines and rebates, cyber-insurers guide risk-averse users to internalize the externalities caused by user peers, and as a result help users invest in optimal self-defense amounts that lead to social welfare maximization. The problem of moral hazard in mitigated and as a result the overall network security is optimal, which would please security regulatory bodies. Regarding profits, cyber-insurers make non-negative expected profits[8], and security product vendors would see an increase in their product sales (and subsequently profits) due to users being incentivized to invest appropriate amounts in self-defense mechanisms.

Central Point: In the monopolistic cyber-insurance scenario with client contract discrimination, there may exist an efficient market (always exists if $\lambda > 0$) that helps satisfy the interests of all the market stakeholders.

V. Scenario 3: Competitive Markets

We assume a perfectly competitive cyber-insurance market[9] where multiple cyber-insurers provide their clients with full coverage at fair premiums[10]. Due to imperfect prevention, we also assume that a risk-averse user resorts to insurance solutions whenever he invests in self-defense mechanisms. The expected utility of a user who does not invest in self-defense mechanisms in Scenario 3 and only buys insurance is given as

$$E[U_{ndef}^3] = E[U_{ndef}^3(l(x^{m_3})] = p_d U(w_0 - r + r - P_1^3) + (1 - p_d)Q_3,$$

where Q_3 is the probability of the user facing indirect loss in Scenario 3 and is given as

$$Q_3 = q(l(x^{m_3})U(w_0 - r + r - P_1^3) + (1 - q(l(x^{m_3}))U(w_0 - P_1^3),$$

where $q = q(l(x^{m_3}))$. $P_1^3 = P(p \neq q, r) = p \cdot r$ is the actuarially fair insurance premium that a user in Scenario 3 not investing in self-defense, pays to his cyber-insurer in return for full coverage of his loss. Here x^{m_3} is the marginal cost of investment in Scenario 3.

The expected utility of the same user when he invests in self-defense mechanisms is given as

$$E[U_{def}^3] = E[U_{def}^3(l(x^{m_3}), x)] = U(w_0 - x - P_2^3),$$

where $P_2^3 = P(p = q, r) = q \cdot r$ is the actuarially fair insurance premium that a user in Scenario 3 not investing in self-defense, pays to his cyber-insurer in return for full coverage of his loss. We note that $P_2^3 < P_1^3$. A user would want to invest in loss prevention only if $E[U_{def}^3] \geq E[U_{ndef}^3]$.

$$\Psi_3(l(x^{m_3}), x) = E[U_{def}(l(x^{m_3}), x)] - E[U_{ndef}(l(x^{m_3}))]. \qquad (25)$$

When $X = P_1^3$, we have

$$\Psi_3(l(x^{m_3}), P_1^3) = U(w_0 - (P_1^3 + P_2^3) - U(w_0 - P_1^3) < 0, \qquad (26)$$

and at $X = 0$ we have

$$\Psi_3(l(x^{m_3}), 0) = p\{U(w_0 - P_2^3) - U(w_0 - P_1^3)\} > 0. \qquad (27)$$

In most practical cases, Equations 26 and 27 jointly indicate the monotonicity of $\Psi_3(\cdot)$ and imply that there exists an interior solution x^{eq_3}, where $0 < x^{eq_3} < P_1^3$, such that

$$\Psi_3(l(x^{m_3}), x^{eq_3}) = E[U_{def}^3(l(x^{eq_3}), x^{eq_3})] - E[U_{ndef}^3(l(x^{eq_3}))] = 0. \qquad (28)$$

Walrasian Equilibrium: The interior solutions, x^{eq_3}, to $E[U_{def}^3] = E[U_{ndef}^3]$ is the competitive market equilibrium (also named as Walrasian equilibrium [13] for perfectly competitive markets) cost of protection investment, and equals x^{m_3}, the marginal cost of making self-defense investments in Scenario 3, i.e., the cost of investment to a user indifferent between making and not making self-defense investments. This implies the fact that users whose cost of self-defense is less than x^{eq_3} find it profitable to invest in self-defense and cyber-insurance, whereas the others invest only in cyber-insurance. Mathematically, the expression for the Walrasian equilibrium can be derived from the following equation arising due to [19].

$$U(w_0 - x^{eq_3}) = U(w_0 - p(x^{eq_3} \cdot r),$$

which leads to a Walrasian equilibrium value given by

$$x^{eq_3} = p(x^{eq_3}) \cdot r.$$

[8] Note that in most cases the cyber-insurer would set λ values to be positive, which implies strictly positive expected profits.

[9] Later in this section, we will comment on contract pricing in non-perfect competitive (oligopolistic) markets.

[10] Note that under perfect competition, the equilibrium strategy for all firms in a market is to charge fair premiums [13]. Charging unfair premiums will result in a firm having zero demand.

Social Welfare Maximization: We define the social welfare of a network of users as the sum of the expected utility of all the users. Mathematically, we denote social welfare in Scenario 3 as $SW_3(x^{m_3})$ and it is evaluated to

$$\int_0^{x^{m_3}} E[U^3_{def}(l(x^{m_3}), x)]f(x)dx + E[U^3_{ndef}(x^{m_3})] \cdot l(x^{m_3}).$$

The first term of $SW_3(x^{m_3})$ denotes the sum of the expected utility of all agents with adopting self-defense, the second term denotes the sum of the expected utilities of all agents not investing in self-defense and buying cyber-insurance. Equating the first order condition for $SW_3(x^{m_3})$ results in finding x^{sopt_3}, the cost of investment that maximizes social welfare.

The first order condition (FOC) for an interior maximum is

$$\frac{dSW_3(x^{m_3})}{dx} = A_3 + B_3 + C_3 + D_3, \tag{29}$$

where

$$A_3 = E[U^3_{def}(l(x^{m_3}), x^{m_3})]f(x^{m_3}),$$

$$B_3 = E[U^3_{ndef}(l(x^{m_3}))]\frac{dl(x^{m_3})}{dx^{m_3}},$$

$$C_3 = \frac{dE[U^3_{ndef}(l(x^{m_3}))]}{dx^{m_3}} l(x^{m_3}),$$

and

$$D_3 = \int_0^x \frac{\delta E[U^3_{def}(l(x^{m_3}), x)}{\delta x^{m_3}} f(x)dx.$$

In light of Equation 1, Equation 29 can be written as

$$\frac{dSW_3(x^{m_3})}{dx^{m_3}} = N + C_3 + D_3, \tag{30}$$

where

$$N = \{E[U^3_{def}(l(x^{m_3}), x^{m_3})] - E[U^3_{ndef}(x^{m_3})]\}f(x^{m_3}).$$

Here, the first term in brackets in N is the excess of expected utility, $\Psi_3(l(x^{m_3}), x^{m_3})$, C_3 and D_3 are non-negative and non-decreasing in x. Since excess of expected utility is positive at $x = 0$ and negative at $x = P^3_1$, there exists $x = x^{sopt_3}$ such $\frac{dSW_3(x)}{dx}$ is zero, and the social welfare in the network is maximized. We represent this mathematically as

$$x^{sopt_3} = argmax_{x^m} SW_3(x^{m_3}). \tag{31}$$

Substituting x^{eq_3} in Equation 31, and using Equation 28 we get

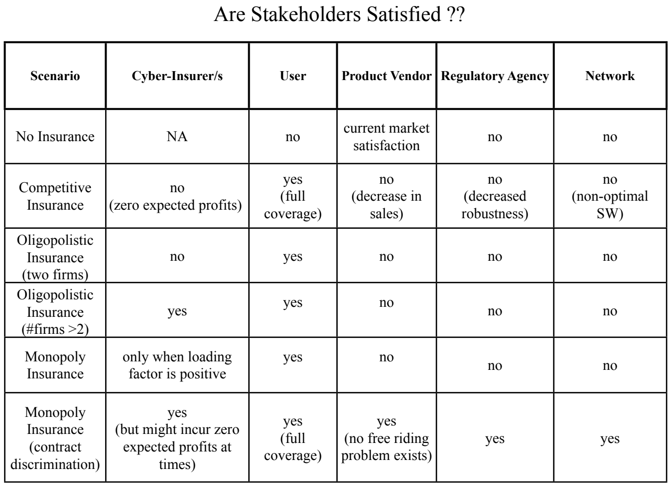
$$\frac{dSW_3(x)}{dx}|_{x=x^{eq_3}} > 0. \tag{32}$$

This implies that $x^{sopt_3} > x^{eq_3}$ and $l(x^{sopt_3}) < l(x^{eq_3})$. i.e., the proportion of users not resorting to self-defense mechanisms is higher in the Nash equilibrium than in the welfare optimum. **The analysis above proves the following theorem on Scenario 3.**

Theorem 4. *When network users have the option of cyber-insurance protection, there exists a unique Walrasian equilibrium cost to invest in self-defense, x^{eq_3}. Users facing protection costs below x^{eq_3} jointly invest in self-defense mechanisms and insurance, whereas other users only buy cyber-insurance. This Walrasian equilibrium cost of self-defense does not result in maximizing user social welfare in the network and cyber-insurance does not incentivize users into making self-defense investments. In addition, the insurers make zero expected profits.*

Theorem Intuition and Practical Implications: The intuition and implications behind Theorem 4 are exactly similar to that of Theorem 2. The intuition for a cyber-insurer in the perfectly competitive setting to charge actuarially fair premiums is that adverse selection cannot induce users to pay a premium loading as other insurers can undercut the demanded price by ignoring externalities. Thus, the externalities in a competitive cyber-insurance market cannot be internalized. So it makes sense that the greater the amount of externalities in a network, the more it makes sense to enforce a monopolistic cyber-insurance market with client contract discrimination.

Central Point: Like in Scenario 2, in a competitive (perfect or oligopolistic) cyber-insurance scenario with no client contract discrimination, there exists an inefficient market, i.e., the social welfare is not maximized at market equilibrium, and this does not help satisfy the interests of all the market stakeholders.



Are Stakeholders Satisfied ??

Scenario	Cyber-Insurer/s	User	Product Vendor	Regulatory Agency	Network
No Insurance	NA	no	current market satisfaction	no	no
Competitive Insurance	no (zero expected profits)	yes (full coverage)	no (decrease in sales)	no (decreased robustness)	no (non-optimal SW)
Oligopolistic Insurance (two firms)	no	yes	no	no	no
Oligopolistic Insurance (#firms >2)	yes	yes	no	no	no
Monopoly Insurance	only when loading factor is positive	yes	no	no	no
Monopoly Insurance (contract discrimination)	yes (but might incur zero expected profits at times)	yes (full coverage)	yes (no free riding problem exists)	yes	yes

Fig. 1. Comparative Study of Scenarios

A Note on Oligopolistic Markets: Oligopolistic markets resemble imperfect (not perfectly competitive) competition between firms in a market. In these markets, for a cyber-insurance setting, the insurers have market power to set prices unlike in the perfect competition case, where each insurer is price taking (has no market power to charge actuarially unfair premiums) and can only charge actuarially fair premiums to its clients. However, due to Bertrand's paradox [13], for number of insurers equal to two, the insurers find it optimal to charge fair premiums to their clients. So does that mean that in competitive settings, cyber-insurers will always make zero expected profits (due to charging actuarially fair premiums to clients) ? The answer is *no* because in reality factors such as firm popularity and customer lock-in will result in some insurers charging unfair premiums to their clients and making strictly positive expected profits, without having to worry about their client demands decreasing. In the case when the number of cyber-insurance firms in a market are greater than two, the authors in [15] show there exists a market Nash equilibrium which does not maximize social welfare.

A comparative study of the three scenarios analyzed in the paper is shown in Figure 1.

VI. Related Work

In this section, we give an overview of related work on cyber-insurance as applicable to this paper.

The field of cyber-insurance in networked environments has been triggered by recent results on the amount of self-defense investments users should expend in the presence of network externalities in order to ensure a robust cyber-space. The authors in [6][7][10] [11][14][16] mathematically show that Internet users invest too little in self-defense mechanisms relative to the socially efficient level, due to the presence of network externalities. These works highlight the role of positive externalities in preventing users from investing optimally in self-defense investments. Thus, the challenge to improving overall network security lies in incentivizing end-users to invest in sufficient amount of self-defense investments inspite of the positive externalities they experience from other users investing in the network.

In response to the challenge, the works in [10][11] modeled network externalities and showed that a tipping phenomenon is possible, i.e., in a situation of low level of self-defense, if a certain fraction of population decides to invest in self-defense mechanisms, it could trigger a large cascade of adoption in security features, thereby strengthening the overall Internet security. However, they did not state how the tipping phenomenon could be realized in practice.

In another set of recent works [9][12], Lelarge and Bolot have stated that under conditions of no *information asymmetry* [1] between the insurer and the insured, cyber-insurance *incentivizes* Internet user investments in self-defense mechanisms, thereby paving the path to trigger a cascade of adoption. They also show that investments in both self-defense mechanisms and insurance schemes are quite inter-related in maintaining a socially efficient level of security on the Internet. The authors in [21] follow up on the framework of Lelarge et.al and mathematically show that insurance is an incentive to self-defense investments only if the quality of self-defense is not very good, and the initial security level of a user is poor. In a recent work [17], the authors show that in a cyber-insurance framework similar to the one proposed by Lelarge and Bolot, cooperation amongst network users results in the latter making better (more) self-defense investments than the case in which they would not cooperate. Thus, the authors' results reflect that cooperation amongst network users will result in a more robust cyberspace. However, not all applications in cyberspace can be cooperative and as a result we consider the general case of non-cooperative application environments and to ensure optimal insurance-driven self-defense amongst users in such environments.

In another recent work [18], the authors derive *Aegis*, a novel optimal insurance contract type based on the traditional cyber-insurance model, in order to address the realistic scenario when both, insurable and non-insurable risks co-exist in practice. They mathematically show that (i) for any type of single-insurer cyber-insurance market (whether offering Aegis type or traditional type contracts) to exist, a *necessary condition* is to make insurance mandatory for all risk-averse network users, (ii) Aegis contracts *mandatorily* shift more liability on to network users to self-defend their own computing systems, when compared to traditional cyber-insurance contracts, and (iii) it is rational to prefer Aegis contracts to traditional cyber-insurance contracts when an option is available. However, the authors do not analyze markets for cyber-insurance, where one needs to consider as important goals, maximizing social welfare, and satisfying multiple stake-holders. Without such considerations, simply shifting liability on users to invest more may not be enough for a successful cyber-insurance market.

Drawbacks: All of the above mentioned works conduct analysis under the assumption of ideal insurance environments, i.e., when there is no information asymmetry between the insurer and the insured. These works also do not address the problem of ways for cyber-insurers to always make strictly expected positive profits, without which the cyber-insurance business would not survive in the long run. In addition the above works assume a risk-neutral cyber-insurer. As mentioned previously, in a correlated risk environment such as the Internet, the assumption of insurers being risk-neutral is not a good one as the latter could become bankrupt. Thus, modeling the insurer as being risk-averse is appropriate.

VII. Conclusion and Future Work

In this paper we analyzed the existence and success of potential cyber-insurance markets. We showed that without client contract discrimination, cyber-insurers offering full insurance coverage can entail the existence of markets, i.e., existence of a market equilibrium, but cannot guarantee themselves of making strictly positive profits. These markets do not maximize the social welfare in a network, cannot help alleviate the moral hazard problem, and result in sub-optimal network security. Surely these markets will not be successful and stable in the long run as it makes multiple stakeholders unsatisfied. In order to overcome these issues we proposed client contract discrimination on behalf of monopolistic insurers that alleviates the moral hazard problem and entail markets that result in optimal network security. However, the insurer is still not guaranteed to make strictly positive profits in these markets.

To alleviate this issue a security vendor 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 profits keeping the social welfare state identical. As a special case the security vendor could be the cyber-insurer itself. We plan to investigate the symbiotic relationship between security vendors and cyber-insurers as part of future work.

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. Another problem we want to explore is to find ways to satisfy all market stakeholders under non-compulsory cyber-insurance.

References

[1] *Information Asymmetry*. Internet Wikipedia Source.

[2] G. A. Akerlof. The market for lemons - quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 84(3), 1970.

[3] R. Anderson and T. Moore. Information security economics and beyond. In *Information Security Summit*, 2008.

[4] R. Bohme. Personal communication.

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

[6] J. Grossklags, N. Christin, and J. Chuang. Security and insurance management in networks with heterogenous agents. In *ACM EC*, 2008.

[7] L. Jiang, V. Ananthram, and J. Walrand. How bad are selfish inverstments in network security. *To Appear in IEEE/ACM Transactions on Networking*, 2010.

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

[9] M. Lelarge and J. Bolot. Cyber insurance as an incentive for internet security. In *WEIS*, 2008.

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

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

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

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

[14] R. A. Miura-Ko, B. Yolken, N. Bambos, and J. Mitchell. Security investment games of interdependent organizations. In *Allerton*, 2008.

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

[16] J. Omic, A. Orda, and P. V. Mieghem. Protecting against network infections: A game theoretic perspective. In *IEEE INFOCOM*, 2009.

[17] R. Pal and L. Golubchik. Analyzing self-defense investments in the internet under cyber-insurance coverage. In *IEEE ICDCS*, 2010.

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

[19] J. W. Pratt. Risk aversion in the small and in the large. *Econometrica*, 32, 1964.

[20] R.H.Coase. The problem of social cost. *Journal of Law and Economics*, 3, 1960.

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