Improving Network Security Via Cyber-Insurance
A Market Analysis

RANJAN PAL, LEANA GOLUBCHIK, Konstantinos Psounis
University of Southern California
PAN HUI
Hong Kong University of Science and Technology

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 the incentives of security vendors (e.g., Symantec, Microsoft), cyber-insurers (e.g., ISPs, cloud providers, security vendors), 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 profit. 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. In this regard, we propose a non-regulatory mechanism to allow monopoly cyber-insurers to make strictly positive profit.


General Terms: Performance, Security, Economics

Additional Key Words and Phrases: security, cyber-insurance, market, equilibrium

1. 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 these threats, network users have traditionally resorted to antivirus and anti-spam software, 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 resulting 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 perfect/near-perfect cyber-security protection [Anderson and Moore 2008][Lelarge and Bolot 2009]. 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 protecting the network, (iv) network users taking advantage of the positive security effects generated by other users’ 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 [Akerlof 1970], 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 for 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, 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 and specialized - large to medium/scale business being the sole insurance clients. There are currently over 30 insurance companies offering cyber-insurance contracts in the United States. Many insurers have reported growths of 10-25% in premiums in a 2012 survey of the market, with some companies even reporting higher rates [Naghizadeh and Liu 2014]. We refer the interested reader to [Romanovsky 2013][Betterly 2012][Arimic 2013] 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 US$ 2 billion, whereas the total cost of security breaches to the global economy amounts to a whopping US$ 445 billion [Thompson 2014].

The inability to bridge this huge financial gap and form a successful 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 [Bohme and Schwartz 2010], 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-risks2. We refer the reader

---

1To highlight the importance of improving the current state of cyber-security, US President Barack Obama has passed a security bill in 2013 that emphasizes the need to reduce cyber-threats and be resilient to them.

2In this work we use the terms ‘risk’ and ‘expected loss’ interchangeably.
Improving Network Security Via Cyber-Insurance: A Market Analysis

1. Research Contributions
We make the following primary research contributions in this paper.

—We show that under regulation, a risk-averse monopoly cyber-insurer providing full or partial coverage to its clients without contract discrimination, 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 profit. Through our contributions we (i) prove qualitative statements made in previous work on the benefits of premium discrimination for achieving efficient cyber-insurance markets, and (ii) consider risk-averse cyber-insurers compared to risk-neutral ones modeled in literature. (See Sections 4 and 5.)

—We show that in perfectly competitive and general oligopolistic cyber-insurance settings with risk-averse cyber-insurers, full/partial loss coverage, and under the presence of a regulatory agency, there exists an inefficient insurance market that does not improve network security. (See Section 6.)

—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. 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 7.)

The rest of the paper is structured as follows. We propose a supply-demand model of cyber-insurance markets in Section 2. In Sections 3-7, we analyse different types of cyber-insurance markets. We discuss related work in Section 8. In Section 9, we briefly look into some practical aspects of realizing cyber-insurance markets. We conclude our paper in Section 10.

2. Supply-Demand Model
In this section we propose a 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 a supply (cyber-insurer) perspective. Important notation used in the paper is summarized in Table 1. Relevant economic terms are briefly described in the Appendix.

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 (Bohme...
and Schwartz 2010]. 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)\text{[Mas-Collol et al. 1995]}. 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 $x_i^m$ 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 $x_i^m$. 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 [Kunreuther and Heal 2002], 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 affected 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 $p_{i}^{i,r}$ 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 $p_{i}^{i,r}$ is a function of $x_i^r$, i.e., $p_{i}^{i,r} = p_{i}^{x_i^r}$ if user $i$ invests does not invest in self-defense solutions and $p_{i}^{i,r} = 0$ 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 $p_{i}^{i,m}(l)$ 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 $x_i^m$, i.e., the marginal cost to a user indifferent to investing in self-defense investments. $x_i^m$ 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, \( p_{ind}^{i,r}(l) = p_{ind}^{i,r}(l(x_m^r)) \). Note that the proportion of individuals without self-defense investments is strictly decreasing in \( x_m^r \); 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 \( l(x_m^r) \), the higher the value of \( l(x_m^r) \), the greater is the value of \( p_{ind}^{i,r}(l) \). Therefore, \( p_{ind}^{i,r}(l(x_m^r)) > 0 \), and \( 0 \leq p_{ind}^{i,r}(l(x_m^r)) \leq p_{ind}^{max} \). 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 \( x_m^r \) 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

\[
p_i^r = p_{ind}^{i,r}(l(x_m^r)).
\]

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

\[
p_i^r = p_d^i + (1 - p_d^i)p_{ind}^{i,r}(l(x_m^r)).
\]

We note that one particular way of computing the value of \( p_i^r \) as a function of parameters \( p_d^i \) and \( p_{ind}^{i,r} \) in a network graph, is using Local Mean Field Analysis (LMFA) [Lelarge and Bolot 2008b][Lelarge and Bolot 2008c][Yang and Lui 2012].

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 and competitive (both perfect competition and oligopolistic competition) 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 widely 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 [Dionne and Harrington 1992]). 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 [Pal et al. 2011][Naghizadeh and Liu 2014] 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 [Khouzani et al. 2013], 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 [Bohme and Schwartz 2010], 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. We assume 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 \(p_r \cdot r\), 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. 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\(^3\), and effective computational tools (e.g., the local mean field method), thereby resolving the adverse selection problem to an extent\(^4\). In a series of recent works, [Johnson et al. 2014][Lazska et al. 2014] 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 [Mukhopadhyay et al. 2013][Herath and Herath 2011] 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,

\(^3\)Precedents include the Information and Readiness Disclosure Act (1998), and Electronic Freedom of Information Act (1996).

\(^4\)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 achieve 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. [Odlyzko 2003]
cyber-insurers can resort to a mixture of actuarial, normative, and emotional considerations proposed in [Baddeley 2011] 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 [Toregas and Zahn 2014], 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/voluntarily buy insurance.

3. MARKET TYPE 1: NO INSURANCE SOLUTIONS OFFERED

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

For a given threat type having a potential to incur a loss of amount \( r \) on any user \( i \), let \( U_{i_{\text{ndef}}}(l(x^m_r)) \) be the utility to a user \( i \) in Market Type 1 when he does not invest in self-defense. \( x^m_r \) is the marginal cost of self-defense for this market. The expected utility of user \( i \), when he does not invest in self-defense mechanisms is thus given by

\[
E[U_{i_{\text{ndef}}}(l(x^m_r))] = p^s_{id} U_i(w_0 - r) + (1 - p^s_{id})Q_{\text{ind}}^l,
\]

where \( Q_{\text{ind}}^l \) is the probability of user \( i \) facing indirect loss, and is given\(^5\) by

\[
Q_{\text{ind}}^l = p^s_{ind}(l(x^m_r))U_i(w_0 - r) + (1 - p^s_{ind}(l(x^m_r)))U_i(w_0),
\]

Similarly, the expected utility of a user who does invest in self-defense mechanisms is given by

\[
E[U_{def}(l(x^m_r), x^*_r)] = p^s_{ind}(l(x^m_r))U_i(w_0 - x^*_r - r) + (1 - p^s_{ind}(l(x^m_r)))U_i(w_0 - x^*_r).
\]

Binary Investment Model. Throughout this paper we will use the binary investment model, i.e., a user either does not invest in security mechanisms or invests an appropriate amount he thinks fit given his latent security profile. In this work, the crux of our analysis deals with the cost of security investment to a marginal user. Thus, one of our main goals is to prove the existence of a marginal user (see Section 2.1.3) for all market settings. Once we are able to find a marginal user, we can deduce market properties from the class of high and low investing users. In this regard, a binary investment model is sufficient. A non-binary model will also lead to the existence of a marginal user, but without changing the nature of the results.

Social Welfare. 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 network users. We denote social welfare of the ‘no insurance’ case by \( SW_{NI}(x^m_r) \) and express it as

\[
SW_{NI}(x^m_r) = \int_0^{x^m_r} E[U_{def}(l(x^m_r), x)]f(x)dx + E[U_{ndef}(l(x^m_r))]l(x^m).
\]

The first term in \( SW_{NI}(x^m_r) \) 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 users not investing in self-defense. \( f(\cdot) \) denotes the probability density function of \( X \), the random variable representing the self-defense investment costs of users. \( X \) takes on values in the range \([0, r] \).

We have the following theorem regarding market properties when no insurance solutions are available. The proof of the theorem is in the Appendix.

\(^5\)In order to have more condensed equations, we somewhat abuse the expression for expected utility, and use ‘\( Q_{\text{ind}}^l \)’ instead of the entire expression denoting \( Q_{\text{ind}}^l \).
Theorem 3.1. For a given threat type, when network users do not have cyber-insurance protection, there exists a unique market equilibrium (ME) cost to invest in self-defense, $x_m^{eq}$. Users facing self-defense costs below $x_m^{eq}$ invest in self-defense mechanisms, whereas other users do not. This ME 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 market equilibrium than in the welfare optimum, the network security is sub-optimal, and the moral hazard problem persists.

Proof Sketch. The main proof intuition behind the existence of unique equilibria is showing the monotonicity of a potential function relating $E[U_{ndef}(l(x_m))]$ and $E[U_{def}(l(x_m), x^*_m)]$, for any arbitrary user $i$. The monotonic property of the potential function leads us to a unique market equilibrium cost of self-defense investment, $x_m^{eq}$. We show that $x_m^{eq}$ equals $x_m^{opt}$. Regarding testing for social welfare maximum at market equilibrium, we equate the first order condition for $SW_{N1}(x_m)$ to zero to find $x_m^{opt}$ - the cost of self-defense investment that maximizes social welfare, and then test whether this cost equals the market equilibrium cost of self-defense, i.e., $x_m^{eq}$.

Theorem Intuition and Practical Implications. The theorem result is not novel and has been also been arrived at by [N.Shetty et al. 2009],[Lelarge and Bolot 2009],[Omic et al. 2009],[Miura-Ko et al. 2008]. The intuition behind Theorem 3.1 is based on the first fundamental theorem in welfare economics [Mas-Collel et al. 1995] 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 user risk probabilities (denoted as $p_{avg}(x_m)$), is not minimized at market equilibrium, for a given threat type. In [N.Shetty et al. 2009], the authors state that $p_{avg}(x_m)$ is minimized if and only if social welfare is maximized. At market equilibrium we intuitively have two categories of the network user population - (i) the class of users who face a cost of investment above the ME cost, do not buy security products, and face a loss on being attacked, and (ii) the other class consisting of users who invest in security measures, do not face direct risks but are still susceptible to indirect risks.

4. Market Type 2: Monopoly Markets (No Client Discrimination)

In the previous section, we observed the non-optimality of network security when insurance solutions are not available. In this and subsequent sections, we analyse the state of network security improvement under various insurance environments. 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 a governmental agency to (i) ensure each Internet user buys voluntary/compulsory cyber-insurance, and (ii) allow basic monitoring of user security behavior by insurance agencies in order to estimate risks better and price premiums effectively. In this section we analyze the case when there is no contract discrimination amongst clients, i.e., $\lambda$ - the insurance loading factor charged per user is the same for every user.

For a given threat type with the potential to inflict a loss of $r$ on any user, the expected utility of a user $i$ who does not invest is self-defense is given by

$$E[U_{ndef}^{i}(l(x_m))] = p_{d}^{i}U_{i}(w_{0} - r + r - (1 + \lambda)p_{i}^{d} \cdot r) + (1 - p_{d})Q_{ind}^{i}.$$

where $Q_{ind}^{i}$ is the probability of the user facing indirect loss, and is given by

$$Q_{ind}^{i} = p_{ind}^{i}(l(x_m))U_{i}(w_{0} - r + r - (1 + \lambda)p_{ind}^{i} \cdot r) + (1 - p_{ind})U_{i}(w_{0} - (1 + \lambda)p_{ind}^{i} \cdot r).$$
Here \((1 + \lambda)p^*_r \cdot r\), and \((1 + \lambda)p^*_{ind}(l(x^m_n)) \cdot r\) are insurance premiums that a user in Market Type 2 not investing in security, pays to his cyber-insurer in return for full/partial coverage of his loss (hence the ‘\(-r + r\)’ term in \(U_i\)). \(x^m_n\) is the marginal cost of investment in this market type.

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

\[
E[U_{def}^i(l(x^m_n), x^m_i)] = U_i(w_0 - x^m_i - (1 + \lambda)p^*_{ind}(l(x^m_n)) \cdot r),
\]

where \((1 + \lambda)p^*_{ind}(l(x^m_n)) \cdot r\) is the insurance premium a user in this market type, and investing in security, pays to his insurer.

Partial Coverage. We emphasize here that \(r\) in the above equations can be replaced by any \(k \epsilon [0, r]\) for the case of partial coverage. Here partial coverage implies the decision of the network users to not transfer his entire risk to a cyber-insurer. The residual risk could either be absorbed by him, or be transferred to a self-insurance mechanism [Johnson et al. 2011].

Social Welfare Maximization. We define the social welfare of a network of users as the sum of the expected utilities of all the users. We denote social welfare in the monopoly setting of Market Type 2 as \(SW_{M_{ncd}}(x^m_{eq})\) (Here, \(M_{ncd}\) denoting ‘monopoly with no client discrimination’), which evaluates to

\[
SW_{M_{ncd}}(x^m_{eq}) = \int_0^\infty \int_0^{x^m_{eq}} E[U_{def}^i(l(x^m_n), x)] dx \, dl + E[U_{ndef}^i(x^m_n)]l(x^m_n).
\]

The first term of \(SW_{M_{ncd}}(x^m_{eq})\) 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 cyber-insurance only (be it full coverage or partial coverage). \(f(.)\) denotes the probability density function of \(X\), the random variable representing the self-defense investment costs of users. \(X\) takes on values in the range \([0, r]\). We assume here that cyber-insurers have knowledge of the distribution, \(f\), from actuarial studies of user security behavior.

We have the following theorem regarding market properties for Market Type 2. The proof of the theorem is in the Appendix.

**Theorem 4.1.** For a given threat type, there exists a unique monopoly market equilibrium (MME) cost, \(x^m_{eq}\), of investing in self-defense in a monopolistic cyber-insurance setting with no client discrimination. Users facing protection costs below \(x^m_{eq}\) invest in self-defense mechanisms, whereas other users buy cyber-insurance only (be it full coverage or partial coverage). This MME 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 market equilibrium than in the welfare optimum.), cyber-insurance does not incentivize users to invest in self-defense mechanisms, the network security is sub-optimal, and the moral hazard problem persists.

**Proof Sketch.** The main proof intuition behind the existence of unique equilibria is similar to that of Theorem 3.1. We show the monotonicity of a potential function relating \(E[U_{ndef}^i(l(x^m_n))]\) and \(E[U_{def}^i(l(x^m_n), x^m_i)]\), for any arbitrary user \(i\). The monotonicity property of the potential function leads us to a unique market equilibrium cost of self-defense investment, \(x^m_{eq}\). We show that \(x^m_{eq}\) equals \(x^m\). Regarding testing for social welfare maximum at market equilibria, we equate the first order condition for \(SW_{M_{ncd}}(x^m_{eq})\) to zero to find \(x^m_{eq}\) - the cost of self-defense investment that maximizes social welfare, and then test whether this cost equals the market equilibrium cost of self-defense, i.e., \(x^m_{eq}\).

**Theorem Intuition and Practical Implications:** The intuition behind Theorem 4.1 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 market equilibrium. The implications of the theorem are (i) cyber-insurance does not incentivize network users to invest in self-defense mech-
anisms, (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. Also note, since $\lambda \geq 0$, the cyber-insurer makes non-negative expected profits. In context of a security vendor, it does not satisfy its interests from an existing cyber-insurance market, i.e., compared to Market Type 1, as the sales of its products are going to go down with users relying on cyber-insurance for risk mitigation. From a network perspective, users with high network degree will tend to under-invest in security investments and free-ride on their neighbors’ investments, whereas users with low network degree cannot afford to free ride (due to lesser number of neighbors), and being risk-averse, they will invest properly in self-defense mechanisms. Also, the low degree users would be the ones more inclined towards investing in cyber-insurance than high-degree users.

5. MARKET TYPE 3: MONOPOLY WITH CLIENT DISCRIMINATION

In the previous section we observed why despite 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. 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 appropriately invests in the same. Analytical mechanisms to decide which users get fines and which users get rebates are proposed in [Pal and Hui 2013][Pal and Hui 2012][Pal et al. 2013]. 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

---

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 [Pal et al. 2011]. 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 [Pal and Golubchik 2010a], 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 [R.H.Coase 1960] 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.

ACM Transactions on Performance Evaluation of Computer Systems, Vol. V, No. N, Article 1, Publication date: January YY.
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 (refer to Section 6.), 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.

For a given threat type capable of inflicting a potential loss of $r$ on any user, a user not willing to invest in self-defense investments will pay a fine $a$ over his premium. At market equilibrium the following result needs to hold for the cyber-insurer to treat equally (fairly), a user $i$ who invests in self-defense investments, as well as a user $j$ who does not invest in self-defense investments.

$$U_{\text{def}}^{i}(w_0 - x_i^r - (1 + \lambda)p_r \cdot r) = U_{\text{ndef}}^{j}(w_0 - (1 + \lambda)p_r \cdot r + a).$$

(1)

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

$$U_{\text{def}}^{i}(w_0 - x_i^r - ((1 + \lambda)p_r \cdot r) = U_{\text{ndef}}^{j}(w_0 - (1 + \lambda)p_r \cdot r - b).$$

(2)

We emphasize here that $r$ in the above equations can be replaced by any $k \in [0, r]$ for the case of partial coverage. Via equations (1) and (2), our goal is to find the optimal self-defense cost $x_r^{\text{opt}}$ that achieves maximum social welfare, and one that equals the market equilibrium self-defense cost, $x_r^{eq}$. In this work, we have assumed two classes of users: the high risk users, and the low risk users. However, our analysis easily extend to the case of multiple user classes. We now have the following theorem stating the properties of Market Type 3. The proof of the theorem is the Appendix.

**Theorem 5.1.** Under conditions of monopolistic cyber-insurance, a risk-averse cyber-insurer can help achieve social welfare maximization by premium discriminating clients. In turn, it makes non-negative expected profit, and also incentivizes users to invest in self-defense investments. The network security is optimal, the moral hazard problem is resolved, and the cyber-insurance market is efficient.

**Proof Sketch.** The proof method is similar to those of Theorems 3.1 and 5.1.

**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 (though not completely) 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 is 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, and also incentivizes users to invest in self-defense investments. The network security is optimal, the moral hazard problem is resolved, and the cyber-insurance market is efficient.

---

8Note that in most cases the cyber-insurer would set $\lambda$ values to be positive, which implies strictly positive expected profit, unless there is a huge catastrophe and all the revenue + safety capital get expended on insuring users.

ACM Transactions on Performance Evaluation of Computer Systems, Vol. V, No. N, Article 1, Publication date: January YY.
6. MARKET TYPE 4: COMPETITIVE MARKETS

In practice, there may be multiple cyber-insurance companies existing in a market scenario. In this section, we assume perfect and imperfect competitive cyber-insurance markets. In competitive markets, multiple cyber-insurers provide their clients with full/partial coverage at fair or unfair premiums. Under perfect competition, the equilibrium strategy for all firms in a market is to charge fair premiums [Dionne and Harrington 1992]. This is because in the presence of adverse selection, individual insurers cannot induce agents without prevention to pay a premium loading due to the fact that other insurers can undercut the demanded premium by ignoring externalities. Charging unfair premiums will result in a firm having zero demand. In the case of imperfect or oligopolistic competition, a firm can afford to premium discriminate, one of the main reasons being insurers locking-in their clients (with high costs of moving to other insurance vendors) with certain product features that attract different types of clients in the market to different insurers. In this work we will primarily analyse the case of perfectly competitive markets. Later in this section, we will comment on contract pricing in non-perfect competitive (oligopolistic) markets. Due to imperfect nature of security mechanisms, we assume that a risk-averse user resorts to insurance solutions whenever he invests in self-defense mechanisms.

For a given threat type capable of inflicting a loss of \( r \) on any user, the expected utility of user \( i \) who does not invest in self-defense mechanisms in Market Type 4, and only buys insurance is given by

\[
E[U_{ndef}^i(l(x_r^m))] = p_d U_i(w_0 - r + r - p_r^i \cdot r) + (1 - p_d) Q_{ind}^i, \]

where \( Q_{ind}^i \) is the probability of the user \( i \) facing indirect loss in this market type, and is given as

\[
Q_{ind}^i = p_{ind}^{i,r}(l(x_r^m)) U_i(w_0 - r + r - p_{ind}^{i,r}(l(x_r^m)) \cdot r) + (1 - p_{ind}^{i,r}(l(x_r^m))) U_i(w_0 - p_{ind}^{i,r}(l(x_r^m)) \cdot r),
\]

Here \( p_r^i \cdot r \), and \( p_{ind}^{i,r}(l(x_r^m)) \cdot r \) are insurance premiums that a user in Market Type 4 not investing in security, pays to his cyber-insurer in return for full/partial coverage of his loss. \( x_r^m \) is the marginal cost of investment in this market type.

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

\[
E[U_{def}^i(l(x_r^m), x_i^r)] = U_i(w_0 - x_i^r - p_{ind}^{i,r}(l(x_r^m)) \cdot r),
\]

where \( p_{ind}^{i,r}(l(x_r^m)) \cdot r \) is the actuarially fair insurance premium that a user in this market type not investing in self-defense, pays to his cyber-insurer in return for full/partial coverage of his loss. We emphasize here that \( r \) in the above equations can be replaced by any \( k \epsilon [0, r] \) for the case of partial coverage.

**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 a competitive market setting as \( SW_C(x_r^m) \) and it is evaluated as

\[
SW_C(x_r^m) = \int_0^{x_r^m} E[U_{def}^i(l(x_r^m), x)] f(x) dx + E[U_{ndef}^i(l(x_r^m))] \cdot l(x_r^m).
\]

The first term of \( SW_C(x_r^m) \) 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. \( f(.) \) denotes the probability density function of \( X \), the random variable representing the self-defense investment costs of users. \( X \) takes on values in the range \([0, r]\). We assume here that cyber-insurers have knowledge of the distribution, \( f \), from actuarial studies of user security behavior.

We have the following theorem regarding market properties for Market Type 4. The proof of the theorem is in the Appendix.
THEOREM 6.1. When network users have the option of cyber-insurance protection, there exists a unique competitive market equilibrium cost of investing in self-defense, \( x_{eq} \). Users facing protection costs below \( x_{eq} \) jointly invest in self-defense mechanisms and insurance, whereas other users only buy cyber-insurance. This market 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 profit. The network security is sub-optimal, problem of moral hazard persists, and cyber-insurance markets are inefficient.

Proof Sketch: The proof method is similar to that of Theorems 3.1, 4.1, and 5.1.

Theorem Intuition and Practical Implications: The intuition and implications behind Theorem 6.1 are very similar to that of Theorem 4.1. 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 greater the amount of externalities in a network, the more it makes sense to enforce a monopolistic cyber-insurance market with client contract discrimination. In terms of profits since \( \lambda = 0 \), the expected profit a insurer makes is zero. One more important point regarding internalizing externalities comes from the ‘compulsory’ nature of cyber-insurance contracts. If there exists a mechanism such that all users voluntarily buy cyber-insurance, the situation is exactly similar to the case when insurance is made compulsory, and in both these cases the network externalities are not internalized. If it is the case that some users buy cyber-insurance and the others do not then it is more the case that externalities will not be internalized. As a result with no voluntary/compulsory insurance, even perfectly competitive cyber-insurance markets are likely to be inefficient.

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. We have already mentioned that security being a public good is the main culprit behind externalities not completely being internalized, even if the markets are perfectly competitive. Thus, in an oligopoly with a fixed number of insurers, product non-discrimination will not result in an efficient market. Product discrimination will lead to customer lock-in, but has the potential to ensure efficient markets only if insurance can be made compulsory, something which is debatable at this point from a policy implementation viewpoint. With non-compulsory insurance it will become very hard to ensure efficient markets, soley because of the public nature of security products. In the case when the number of cyber-insurance firms in a market are greater than two, the authors in [N.Shetty et al. 2009] show there exists a market equilibrium which does not maximize social welfare.

7. MAKING STRICTLY POSITIVE PROFIT
In Section 5, 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 between investing in self-defense and not investing if

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

(3)

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

\[ a \cdot l(x_r^{m,i}) - b \cdot (1 - l(x_r^{m,i})) = k. \]

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 corresponding optimal and rebate values. The proof of the lemma is in the Appendix.

**Lemma 7.1.** For a given threat type, the lower bound of profit \( k \) made by a monopoly cyber-insurer at market equilibrium is given by

\[ k \geq (x_r^{s,\text{opt}} - p_d(1 - p_i^{r,i}(l(x_r^{s,\text{opt}})))r)l(x_r^{s,\text{opt}}) - p_i^{r,r}(x_r^{s,\text{opt}})r, \]

and corresponding fine and rebate values are respectively given by

\[ a = x_r^{s,\text{opt}} - p_d(1 - p_i^{r,i}(l(x_r^{s,\text{opt}})))r - b; \text{ where } b = \{x_r^{s,\text{opt}} - p_d(1 - p_i^{r,i}(x_r^{s,\text{opt}}))r\}l(x_r^{s,\text{opt}}) - k, \]

and \( x_r^{s,\text{opt}} = x_r^{e,\text{opt}} = x_r^{m,i}, \) 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 both 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 7.1. The proof of the theorem is in the Appendix.

**Theorem 7.2.** With (i) a premium fine \( \alpha \) for users without self-defense such that \( \alpha \) 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 \( \alpha \) must satisfy

\[ k \geq \alpha \cdot l(x_r^{s,\text{opt}}) - (1 - l(x_r^{s,\text{opt}}))p_i^{r,i}(l(x_r^{s,\text{opt}}))r > 0. \]

**Proof Sketch.** The proof method is similar to that of Theorems 2.1, 3.1, and 4.1, i.e., 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 7.1 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 externalities, 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 7.1 and Theorem 7.2: 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 graph, and their relationship with user investment patterns.

8. RELATED WORK

In this section, we review related work pertaining to this paper. We structure this section into parts and comment on how our contributions relate to each part.

8.1 Triggering the Field of Cyber-Insurance

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, for ensuring a robust cyber-space. The authors in [Grossklags et al. 2008][Jiang et al. 2010][Lelarge and Bolot 2008b][Lelarge and Bolot 2008c][Miura-Ko et al. 2008][Omic et al. 2009] 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 [Lelarge and Bolot 2008b][Lelarge and Bolot 2008c] 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, the authors state that the tipping phenomenon is possible only when the quality of security protection manufactured by a monopolist is weak, and also does not result in market efficiency. In addition, the authors did not state how the tipping phenomenon could be realized in practice from selling high quality protection techniques.

In another set of recent works [Lelarge and Bolot 2008a][Lelarge and Bolot 2009], Lelarge and Bolot have stated that under conditions of no information asymmetry [wik ] 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. In this regard, the authors in [Johnson et al. 2011] provide a framework to appropriately decide on the amount of investments in self-insurance (e.g., backup mechanisms), cyber-insurance, and self-protection in an environment when cyber-insurance need not be mandatory. They
show that cyber-insurance is a substitute for expensive self-insurance mechanisms but a complement to low quality and cheap self-defense mechanisms. However, this work does not account for information asymmetries. The authors in [Yang and Lui 2012] account for information asymmetries and 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 [Pal and Golubchik 2010a], 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 one needs to consider (i) the general case of non-cooperative application environments, and (ii) how to ensure optimal self-defense investments from users in such environments.

In another recent work [Pal et al. 2011], 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 - a result also substantiated by the authors in [Naghizadeh and Liu 2014] for ensuring social welfare in insurance-driven risk management environments, (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.

In this work, we alleviate the drawbacks of the above mentioned works by endogenizing the cyber-insurance market structure, and analyzing general markets for cyber-insurance by relaxing assumptions related to the risk-propensity of cyber-insurers and their coverage amounts. In the process we address important system goals such as maximizing social welfare, and satisfying multiple stake-holders.

8.2 Security Metrics and Risk Estimation

Regarding the practical implementability of cyber-insurance in networked environments, designing security metrics and estimating risks is of utmost importance to channelize cyber-insurers into pricing their products appropriately. In this regard, [Bohme and Kataria 2006] proposed models and measures for risk correlation in cyber-insurance environments, but ignored interdependent security amongst network users - a salient property in networked environments. In [Lazska et al. 2014], the authors propose an effective sampling technique to estimate systematic risks in real-world networks in a tractable manner using techniques proposed in [Johnson et al. 2014]. In [Bohme 2010], the author states various security metrics to measure the security effectiveness of a system, and an insurer can use these metrics to decide on the coverage and premium values of contracts. In [Mukhopadhyay et al. 2013], the authors propose a Copula-aided Bayesian Belief Network (CBBN) for cyber-vulnerability assessment (C-VA), and expected loss computation. Taking these as an input and using the concepts of collective risk modeling theory, they also compute the premium that a cyber risk insurer can charge to indemnify cyber losses. In computing the premiums, the authors also account for the risk profile and wealth of the firm under consideration. Picking up on the copula-based approaches in [Mukhopadhyay et al. 2013], the authors in [Herath and Herath 2011] propose copula-based models to capture the non-linear dependencies between parameters responsible for pricing cyber-insurance premiums, and in turn use.
Monte-Carlo simulation to appropriately price premiums for various classes of cyber-insurance policies.

The relevance of this section for our work is the knowledge of practical ways to estimate loss probabilities and measure losses approximately, which are inputs to our modeling framework.

8.3 On Efficiency of Cyber-Insurance Markets

Recent research works on cyber-insurance [Hoffman 2007][Lelarge and Bolot 2009][N.Shetty et al. 2009] have mathematically shown the existence of inefficient insurance markets. Intuitively, an efficient market (see Appendix.) is one where all stakeholders (market elements) mutually satisfy their interests. These works state that cyber-insurance satisfies every stakeholder (see Appendix.) 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 [Lelarge and Bolot 2009] 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 [Yang and Lui 2012][Yang and Lui 2014], 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 [Pal et al. 2014], we overcome the drawbacks of the mentioned existing works, and propose ways to form provably efficient monopolistic 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 [Pal and Golubchik 2010b] and [Pal and Hui 2011] that account for market stakeholders and information asymmetry respectively, in a weak manner. However, a drawback of the work in [Pal et al. 2014] 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.

The above mentioned works in the respective sub-sections primarily target the interdependent role of user security investments, insurance coverage, and information asymmetry in making cyber-insurance widely adoptable. However, from these works we observe that a primary bottleneck to have successful and widely adopted cyber-insurance markets lies in insurers making strictly positive profit at all times. In this paper, we make a theoretical effort to address this problem using non-regulatory mechanisms.

9. DISCUSSION - PRACTICAL ASPECTS

In this section, we briefly describe practical aspects of realizing cyber-insurance. We divide this section into the following categories: (i) evaluating and metricizing loss, (ii) achieving efficient market equilibria, (iii) attack types, (iv) tackling information asymmetry, (v) liability assignment, and (vi) application domains.

Measuring Loss. It is quite a challenge in practice to quantify the loss a user accrues when successfully attacked by malicious entities [Pfleeger and Cunningham 2010]. An improper estimate of a loss by the insurer will cause difficulties in charging the appropriate premium and providing the right amount of coverage. Practically realizable loss(loss probability estimation techniques have been pro-
posed in [Lelarge and Bolot 2008b][Lelarge and Bolot 2008c][Yang and Lui 2012] (using Local Mean Field Analysis (LMFA)), [Johnson et al. 2014][Lazska et al. 2014] (using sampling), and [Baddeley 2011] (using behavioral economic considerations combined with actuarial and normative mechanisms). Copula-based techniques for estimating loss probabilities in corporate network settings have been proposed in [Mukhopadhyay et al. 2013][Herath and Herath 2011][Bohme and Kataria 2006]. Losses can either be tangible or non-tangible. Tangible losses are those that can be quantified, even if not with perfect accuracy, e.g., monetary losses due to credit card fraud, data loss, etc. Non-tangible losses are those that are hard to or cannot be quantified, e.g., loss of organizational reputation, loss of a digital item causing emotional/psychological low. Tangible losses can be statistical estimated via techniques proposed above, whereas certain non-tangible losses (e.g., loss of reputation in the eyes of its customers for a bank on being attacked), might be hard to estimate. Policies and practical guidelines to implement loss estimation related parameters are proposed in [Toregas and Zahn 2014].

**Efficiency of Market Equilibria.** In this paper, we mathematically demonstrate efficient cyber-insurance markets satisfying all stakeholders. Our model was based on the assumption of perfect rationality of stakeholders. However, in reality stakeholders are either irrational or boundedly rational. Thus, efficient equilibria from our model might not be a true reflection of strategic human behavior in practice. In addition, due to the presence of externalities, complementarities of security goods, and various market heterogeneities, multiple equilibria might exist [Baddeley 2011]. Finding and operating at the best market equilibria might be difficult, both in theory and in practice. Also, from an insurer perspective, there are transaction costs proportional to the premiums or expected losses for underwriting insurance, which need to be included in the insurer’s profit equation. This makes the analysis of equilibria very challenging. The requirement of compulsory cyber-insurance in our work to achieve market efficiency might also raise some eyebrows regarding implementation. In [Naghizadeh and Liu 2014], the authors state that voluntary participation by network users to buy insurance might not work in practice. In order to make participation voluntary, the authors suggested steps like (i) a relaxation in the economic objective of achieving market efficiency, (ii) relaxing the insurer’s budget balance condition, and (iii) injecting external resources in the system (resulting in Kaldor-Hicks efficiency [Mas-Collel et al. 1995]). In reality, given the current state of cyber-security, it is a big enough leap towards the improvement of global security even if all stakeholders are happy with their net utility, and not the happiest (the state of market efficiency) [Odlyzko 2003]. Cyber-insurance is a great tool to achieve this ‘happy’ ecosystem state and might lead to the ‘happiest’ ecosystem state in the future.

**Attack Types.** Our model in this paper is based on direct and non-direct attack scenarios, and these scenarios cover the main features of most cyber-space threats including viruses, worms, social engineering attacks, and botnets. To just highlight how our model fits these attack categories, we choose botnets as a representative example. A bot is an end-user machine containing software that allows it to be controlled by a remote administrator called the bot herder via a command and control network. Bots are generally created by finding vulnerabilities in computer systems, exploiting these vulnerabilities with malware and inserting malware into those systems. The bots are then programmed and instructed by the bot herder to perform a variety of cyber-attacks. Recall that we defined two types of losses a user faces in a network: direct losses could model the attack of the bot herder who infects machines when he detects it lacks a security feature and then indirect losses would model the contagion process taking place without the direct control of the bot herder. Note that the underlying network would model the propagation mechanism as file sharing executables or email attachment. In particular, it does not necessary correspond to a physical network but it can also be a social network. Clearly, our model is a simplified model of threats observed on the Internet. However, they capture the main features, i.e., the direct and indirect nature of threats, which are common to most threats.

**Tackling Information Asymmetry.** Information asymmetry between the insurer and the insured on
various insurance parameters is a big barrier to realizing cyber-insurance markets and tackling it is a huge challenge, specially in networked environments of interdependent and correlated risks. It has long been known that we simply do not have good statistics on online crime, attacks, and vulnerabilities. Companies are hesitant to discuss their weakness with competitors even though a coordinated view of attacks could allow faster mitigation to everyone's benefit and also help the insurer in estimating losses better. In this regard, information sharing associations, security breach disclosure laws, vulnerability markets, and user monitoring might prove to be useful in mitigating the information asymmetry problem [R.Anderson et al. 2008]. In regard to breach disclosure laws, competent firms should welcome a situation where incompetent firms who cut corners to save money will be exposed, incur costs, and lose customers. Security breach laws should also be extended to the case individual users, whereby the latter should be able to notify the breaches and the potential causes. To enable better premium pricing by insurers, we feel the strong need for information sharing associations as part of a regulatory step to ensure the publication of robust loss statistics for online crime. For example, security companies will have an incentive to over-report crime for better selling of their products, whereas ISPs would have an incentive to undercount the amount of wickedness emanating from their customers, particularly if they are held accountable for it. Vulnerability markets can be a way to estimate the value of different types of threats that arise due to faulty software. While some researchers have argued against the implementation of such markets [Resorla 2004], others feel that public disclosure will increase the number of attacks but decrease the number of reported vulnerabilities over time [Arora et al. 2004][Kannan and Telang 2004].

In reality, one way in which the information gap amongst insurers and individual users might be bridged or at least shortened to a considerable extent is via proper user monitoring. As an example, a cyber-insurer (like an ISP) could have a policy that each client would (a) be required to give and pass a written test on the adoption of safe Internet practices (like the automobile driving tests) to demonstrate how educated and aware he is on good security measures, (b) need to sign up an insurance form before buying Internet connection that consists of questions that would reflect the client's security mindset in addition to knowing his protection methodologies (antivirus, etc.) and Internet environment (related to type and number of social connections, etc.). The answers to the questions (may not be truthfully revealed by the clients) are recorded, and on the report of a security breach by clients, a team of ISP officials examine the causes of the loss and decide on the premium and coverage amounts. Reports on a number of breaches above a certain threshold in a given period would imply a high risk and careless user and his premiums would rise (irrespective of what the answers are on the form), and also potentially reduce his coverage. In the worst case, the Internet connection of a client might be temporarily or permanently withdrawn [R.Anderson et al. 2008]. On the contrary, good behavior by users would reward them with reduced premiums and increased coverage. This would incentivize clients to adopt secure Internet practices, and motivate them to be truthful in answering ISP questionnaires. On the other hand, laws should be framed to make the insurance contract underwriting process as transparent as possible.

**Liability Assignment.** Our civilisation is becoming ever more dependent on software, and yet the liability for failure is largely disclaimed and certainly misallocated, both by individuals and organizations. It is only going to be easier for a cyber-insurer to design its contracts if the liability assignment process is made more efficient. We take the pragmatic view that liability is too large an issue to be dealt with a single legal directive, because of (i) the large and growing variety of applications, goods, and services in which software plays a critical role, (ii) the fact that proper functioning of several services rely jointly on multiple software/hardware components manufactured by independent vendors (e.g., as in the case of Square), (iii) threats can originate from any where on the planet, and (iv) consumers transferring liability on other parties for security blemishes for which the former are primarily responsible.
A good starting point to efficient liability assignment could be to require vendors of PCs and other network connected programmable devices to certify that their products are secure by default. It is illegal to sell a care without a seatbeat, so why should network products be allowed to be sold without strong latent security features? On a similar note why should users be allowed to have Internet access when they do not take proper security measures? There should be laws in place to harmonise procedures for the resolution of disputes between (a) customers and service providers, (b) cyber-insurers and the insureds, and (c) service providers and independent software/hardware manufacturers contributing to the business of the service provider, over liability issues regarding security breaches. Regarding inter-continental online crimes, it is hard for cyber-insurance companies to catch criminals and bring them to justice due to the fragmentation of law enforcement efforts across continents. In addition, cooperation among several national jurisdictions is an extremely slow process. Thus, to make cyber-insurers' job easier, proper legal directives should be in place to enforce smooth cyber-policing and cooperation among international governments.

**Application Domains.** Cyber-insurance is an elastic risk management tool that seems promising to be widely applied to various networking domains such as organizational and enterprise networks, data centers, the Internet, and social networks. However, there are certain questions that are interesting and important to answer. For example, who buys insurance in the case when a user has data on the cloud and cloud security is breached? In our opinion, the cloud provider is the entity that should buy cyber-insurance. For example, there could be a trusted third-party security agent (e.g., a security vendor like Symantec) who would be responsible for assessing the cloud infrastructure for potential threats, security flaws, and risk probabilities. The cloud customers could evaluate the impact they face from various losses and report it to the cloud provider. On a security breach in the cloud, the cloud provider gets covered from an insurance agency in return for premiums. The coverage gets transferred to the cloud customer. Now suppose a user goes to a public coffee store/university and starts using the WiFi, and he gets hacked. The relevant question here is how does the user get covered, and by whom? If he uses his data plan, then his mobile service provider might take up the responsibility of covering him, but what if he uses WiFi. Policies regarding loss coverage need to be designed for Internet access in such public settings. Similarly, how does one design coverage policies for a corporate employee using his company laptop in a non-corporate environment and getting hacked? How does the company get covered for losses due to such a hack? We feel the need to design a practical cyber-insurance framework to tackle such scenarios.

10. 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/partial insurance coverage can entail the existence of markets, i.e., existence of a market equilibrium, but cannot guarantee themselves of making strictly positive profit. 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 profit in these markets. We alleviate this problem in theory 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. 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 insight here is to find a way to internalize all network externalities.
The problem of making strictly positive profit can also be addressed using a symbiotic relationship between a market entity and a cyber-insurer. 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 between 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 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. We plan to investigate in detail the symbiotic relationship between security vendors and cyber-insurers as well as the effects a network has on cyber-insurance parameters, 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. We strongly feel that the theory of mechanism 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 is to find ways to satisfy all market stakeholders under non-compulsory cyber-insurance in an oligopolistic setting.

REFERENCES
Information Asymmetry. Internet Wikipedia Source.


APPENDIX

In this section, (i) we briefly describe basic economics concepts relevant to the paper, and (ii) provide complete proofs to the theorems stated in our work. Regarding basic economics concepts, additional details can be found in a standard economics text such as [Mas-Collel et al. 1995].

A.1 Basic Economics Concepts

**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 positive, i.e., improvements in individual security of network users who are connected to heterogeneous users investing in different amounts of self-defense investments.

**user risk propensity:** Risk propensity reflects the psychological mindset of a user to deal with risk. A risk-neutral investor (either the insurer or the insured in our work) 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:** A market is a group of buyers and sellers, where buyers determine the demand and sellers determine the supply, together with the means whereby they exchange their goods or services. With regards to our work, a market is a regulated 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 a monopolistic market, the single insurer has the power to set client premiums to its liking. An oligopolistic insurance market is a special type of a competitive market where multiple insurance firms exist in a manner so that each insurer can set client premiums to its liking. In this paper, we consider a monopolistic market where a regulated cyber-insurer has the power to price its clients.

**market equilibrium:** An equilibrium in a market game refers to a situation when both, buyers, as well as the sellers end up playing strategies from which no side has any incentive to deviate. In our work, this concept implies the situation when cyber-insurers make their satisfying choice of user premiums, and the network users are satisfied with their net utilities after investing in self-defense mechanisms and insurance policies. Note here that a market can have multiple equilibria, some better than the others. In this case, the satisfaction level of market players vary from equilibrium to equilibrium.

**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 the insurance companies, network users, a regulatory agency such as the government, and security vendors (also acting as the cyber-insurers) such as Symantec and Microsoft. When all stakeholders in a market are jointly happy with respect to their interests, it results in a market success. It might be the case that a particular market equilibrium might make the stakeholders jointly satisfied but not necessarily jointly happy, e.g., in our work when the insurer makes non-negative expected profit but wants to make
positive profit to have long-term interests in the cyber-insurance market. In this situation we are not guaranteed a market success.

**market efficiency**: A cyber-insurance market is called efficient if the social welfare of all insured 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 insured network users after investing in self-defense and/or cyber-insurance. At the maximum social welfare state, the moral hazard problem\(^9\) in cyber-insurance is alleviated, i.e., network users adopt safe Internet browsing habits even after getting insured, knowing that they would be covered by their insurers. However, market efficiency does not imply market success, i.e., might make stakeholders jointly satisfied, but not necessarily to a level to ensure long-term market participation.

### A.2 Theorem Proofs

In this section, we provide proofs of the lemmas and theorems proposed in this paper.

**Proof of Theorem 3.1.** A user \(i\) would want to invest in loss prevention only if \(E[U^i_{def}(l(x^m), x^i_t)] \geq E[U^i_{nde}(l(x^m))].\)

Define \(\Psi(l(x^m), x)\) to be the difference in utilities for user \(i\) when he decides to invest or goes against investing in self-protection, and it is given by

\[
\Psi(l(x^m), x_t) = E[U^i_{def}(l(x^m), x_t)] - E[U^i_{nde}(l(x^m))].
\]  

(4)

As special case, when \(x^i_t = r\), we have

\[
\Psi(l(x^m), r) = (1 - p^i_d)\{U_i(w_0 - r) - U_i(w_0)\} < 0,
\]  

(5)

and at \(x^i_t = 0\) we have

\[
\Psi(l(x^m), 0) = p^i_d(1 - p^{max})\{U_i(w_0) - U_i(w_0 - r)\} > 0.
\]  

(6)

In most practical cases, Equations 5 and 6 jointly indicate the monotonicity of \(\Psi(\cdot)\) (due to \(\Psi\) being often strictly decreasing in practice) and imply that (i) if no user invests in self-defense 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 \(x^{eq}_r\), where \(0 < x^{eq}_r < r\), such that

\[
\Psi(l(x^m), x^{eq}_r) = E[U^i_{def}(l(x^m), x^{eq}_r)] - E[U^i_{nde}(l(x^m))] = 0.
\]  

(7)

Basically, the implications of (5) and (6) indicate that there exists a state where some network users invest in self-defense and others do not.

The solution to \(E[U^i_{def}(l(x^m), x^{eq}_r)] = E[U^i_{nde}(l(x^m))]\) gives us the investment cost to a user who is indifferent between investing and not investing in self-defense. Thus \(x^{eq}_r = x^m\), the marginal cost of making self-defense investments in Market Type 1. The interior solution, \(x^{eq}_r\), in Equation 7 is the market equilibrium (ME) cost of protection investment. It implies that users whose cost of self-defense is less than \(x^{eq}_r\) 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.

Regarding reaching social welfare maximum, equating the first order condition for \(SW_{N1}(x^m)\) results in finding \(x^{opt}_r\), the cost of investment that maximizes social welfare. The first order condition (FOC)

\[^9\text{Moral hazard is a well known problem in insurance literature where an insured could behave recklessly after getting insured, knowing that he could get coverage from his insurance company for the losses faced.}\]
We represent this mathematically as

\[
\frac{dSW_{NI}(x_r^m)}{dx_r^m} = F + C + D,
\]

where

\[
A = E[U_{i,def}^i(l(x_r^m), x_r^m)]f(x_r^m), \quad B = E[U_{n,def}^i(l(x_r^m))]\frac{dl_r(x_r^m)}{dx_r^m},
\]

\[
C = \frac{dE[U_{n,def}^i(l(x_r^m))]}{dx_r^m}l(x_r^m), \quad D = \int_0^{x_r^m} \frac{dE[U_{i,def}^i(l(x_r^m), x)]}{dx_r^m}f(x)dx.
\]

Using Equation 4, Equation 8 can be written as

\[
\frac{dSW_{NI}(x_r^m)}{dx_r^m} = F + C + D,
\]

where

\[
F = \{E[U_{i,def}^i(l(x_r^m), x_r^m)] - E[U_{n,def}^i(l(x_r^m))]\}f(x_r^m).
\]

The term inside brackets of \( F \) is the excess of expected utility, \( \Psi(l(x_r^m), x_r^m) \). \( C \) and \( D \) are non-negative and non-decreasing in \( x \). Since the excess of expected utility is positive at \( x_r^i = 0 \) and negative at \( x_r^i = r \), there exists \( x_r^{opt} \) such that \( \frac{dSW_{NI}(x_r^m)}{dx_r^m} \) is zero, and the social welfare in the network is maximized. We represent this mathematically as

\[
x_r^{opt} = \arg\max_{x_r^m} SW_{NI}(x_r^m).
\]

Substituting \( x_r^{opt} \) in Equation 9, and using Equation 7 we get

\[
\frac{dSW_{NI}(x_r^m)}{dx_r^m}|_{x_r^m=x_r^{opt}} > 0.
\]

The first derivate of \( SW_{NI} \) being positive at \( x_r^{opt} \) clearly indicates that \( x_r^{opt} > x_r^{eq} \), thus implying \( l(x_r^{opt}) < l(x_r^{eq}) \), i.e., the proportion of users not resorting to self-defense mechanisms is higher in the market equilibrium than in the welfare optimum. Thus, we have proved Theorem 3.1. \( \textbf{Q.E.D.} \)

**Proof of Theorem 4.1.** A user \( i \) would want to invest in loss prevention only if \( E[U_{i,def}^i(l(x_r^m), x_r^i)] \geq E[U_{i,def}^i(l(x_r^m))] \).

Define \( \Psi(l(x_r^m), x_r^i) \) to be the difference in utilities for user \( i \) when he decides to invest or goes against investing in self-protection, and it is given by

\[
\Psi(l(x_r^m), x_r^i) = E[U_{i,def}^i(l(x_r^m), x_r^i)] - E[U_{i,def}^i(l(x_r^m))].
\]

When \( x_r^i = 0 \), we have

\[
\Psi((x_r^m), 0) = U_i(w_0 - (1 + \lambda)p_{ind}^i r) - U_i(w_0 - (1 + \lambda)p_{ind}^i r) > 0,
\]

and at \( x_r^i = r \) we have

\[
\Psi(l(x_r^m), r) = U_i(w_0 - r) - U_i(w_0 - (1 + \lambda)p_{ind}^i r) < 0.
\]

In most practical cases, Equations 13 and 14 jointly indicate the monotonicity of \( \Psi(\cdot) \) and imply that \( \Psi(\cdot) \) is decreasing in \( x_r^i \) and there exists \( x_r^{eq} \in (0, r) \), such that

\[
\Psi(l(x_r^m), x_r^{eq}) = E[U_{i,def}^i(l(x_r^m), x_r^{eq})] - E[U_{i,def}^i(l(x_r^m))] = 0.
\]
The solution, \( x_r^{eq} \), to \( E[U_{def}^r(l(x), x^n_r)] \geq E[U_{ndef}^r(l(x^n_r))] \) is the monopoly market equilibrium (MME) cost of protection investment, and equals \( x_r^{eq} \), the marginal cost of making self-defense investments in Market Type 2. This implies that users whose cost of self-defense is less than \( x_r^{eq} \) find it profitable to invest in self-defense and cyber-insurance, whereas the others invest only in cyber-insurance.

Regarding reaching social welfare maximum, Equating the first order condition for \( SW_{Macc}(x_r^{eq}) \) results in finding \( x_r^{opt} \), the cost of investment that maximizes social welfare.

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

\[
\frac{dSW_{Macc}(x_r^{eq})}{dx} = A + B + C + D,
\]

where

\[
A = \int_0^\infty E[U_{def}^r(l(x_r^{eq}), x^n_r)]f(x^n_r)d\lambda,
\]

\[
B = E[U_{ndef}^r(l(x^n_r))]\frac{d(l(x^n_r))}{dx^n_r},
\]

\[
C = \frac{dE[U_{ndef}^r(l(x^n_r))]}{dx^n_r}l(x^n_r),
\]

\[
D = \int_0^\infty \int_0^{x_r^{eq}} dE[U_{def}^r(x^n_r)]f(x)dxd\lambda.
\]

In the light of Equation 12, Equation 16 can be written as

\[
\frac{dSW_2(x_r^{eq})}{dx_r^{eq}} = G + C + D,
\]

where

\[
G = \{E[U_{def}^r(l(x_r^{eq}), x^n_r)] - EU_{ndef}^r(l(x^n_r))]\}f(x^n_r)
\]

Here, the first term of \( G \) in brackets is the excess of expected utility, \( \Psi(l_r(x_r^{eq}), x_r^{eq}) \), \( C \) and \( D \) are non-negative and non-decreasing in \( x_r^{eq} \). Since the excess of expected utility is positive at \( x_r^{eq} = 0 \) and negative at \( x_r^{eq} = r \), there exists \( x_r^{eq} = x_r^{opt} \) such \( \frac{dSW_{Macc}(x_r^{eq})}{dx} \) is zero, and the social welfare in the network is maximized. We represent this mathematically as

\[
x_r^{opt} = \text{argmax}_{x_r^{eq}} SW_{Macc}(x_r^{eq}).
\]

Substituting \( x_r^{eq} \) for \( x_r^{eq} \) in Equation 17, and using Equation 15 we get

\[
\frac{dSW_{Macc}(x_r^{eq})}{dx} \bigg|_{x = x_r^{eq}} > 0.
\]

This implies that \( x_r^{opt} > x_r^{eq} \) and \( l(x_r^{opt}) < l(x_r^{eq}) \), i.e., the proportion of users not resorting to self-defense mechanisms is higher in the market equilibrium than in the welfare optimum. Thus, we have proved Theorem 3.2. Q.E.D.

**Proof of Theorem 5.1.** Taking off from the social welfare implications of Theorem 4.1, our goal here is to find the optimal self-defense cost \( x_r^{opt} \) that achieves maximum social welfare in the case when monopoly cyber-insurers can adopt client discrimination. Let

\[
A = U_i(w_0 - (1 + \lambda)p^r_{ind} \cdot r) - C,
\]

where

\[
C = \int_0^\infty U_i(w_0 - x_r^{opt} - (1 + \lambda)p^r_{ind} \cdot r) \cdot f(x_r^{opt})d\lambda.
\]

Let

\[
B = \frac{d(U_i(w_0 - (1 + \lambda)p^r_{ind} \cdot r))}{dx}l(x_r^{opt}) + D.
\]
where

\[ D = \int_0^\infty \int_0^{x_{r_{\text{opt}}}} \frac{\delta U_i(w_0 - x - (1 + \lambda)p_{\text{ind}}^{i,r} \cdot r)}{\delta x} f(x) dx d\lambda. \]

Here, \( A \) and \( B \) are the expected utilities of users investing and not investing in self-defense, respectively. The condition for achieving maximum social welfare is given as \( A = B \). Substituting \( x = x_{r_{\text{opt}}} \), and \( a = a_{r_{\text{opt}}} \) in Equation 1, we get

\[ U_i(w_0 - x_{r_{\text{opt}}} - (1 + \lambda)p_{\text{ind}}^{i,r} \cdot r) = U_i(w_0 - ((1 + \lambda)p_i^r \cdot r + a_{r_{\text{opt}}}) \), \]

where \( a_{r_{\text{opt}}} \) satisfies \( E = B \), where

\[ E = U_i(w_0 - (1 + \lambda)p_i^r \cdot r) - \int_0^\infty U_i(w_0 - ((1 + \lambda)p_i^r \cdot r + a_{r_{\text{opt}}})) f(x_{r_{\text{opt}}} \) d\( \lambda \).

Thus the optimal self-defense investment cost \( x_{r_{\text{opt}}} \) to achieve social welfare maximization is obtained by charging high risk type users a fine of \( a \) on top of their premiums.

In the case of rebates, our goal here again is to find the optimal self-defense cost \( x_{r_{\text{opt}}} \) that achieves maximum social welfare. Substituting \( x = x_{r_{\text{opt}}} \), and \( b = b_{r_{\text{opt}}} \) in Equation 2, we get

\[ U_i(w_0 - x_{r_{\text{opt}}} - (1 + \lambda)p_{\text{ind}}^{i,r} \cdot r - b_{r_{\text{opt}}}) = U_i(w_0 - (1 + \lambda)p_i^r \cdot r). \]

Let

\[ M = U_i(w_0 - x_{r_{\text{opt}}} - ((1 + \lambda)p_{\text{ind}}^{i,r} \cdot r - b_{r_{\text{opt}}}) - C. \]

Then \( b_{r_{\text{opt}}} \) is such that it satisfies the following condition (derived by combining Equations 1 and 2.):

\[ M = B. \]

Thus, the optimal self-defense investment cost \( x_{r_{\text{opt}}} \) 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, \( \Pi_{\text{monopoly}} \), made by a monopoly cyber-insurer per contract (without any loading, \( \lambda \), with loading, the net profit is even more.) in a monopoly market with contract discrimination is given by

\[ \Pi_{\text{monopoly}} = a \cdot l(x_{r_{\text{opt}}} - b \cdot (1 - l(x_{r_{\text{opt}}}) \geq 0. \]

Thus, we have proved Theorem 5.1. Q.E.D.

**Proof of Theorem 6.1.** A user \( i \) would want to invest in loss prevention only if \( E[U_{\text{def}f}(l(x_{r_{\text{opt}}}), x_i^r]) \geq E[U_{\text{ndef}f}(l_r(x_{r_{\text{opt}}}))] \). Define \( \Psi(l(x_{r_{\text{opt}}}), x_i^r) \) as the difference in utilities for user \( i \) when he decides to invest or goes against investing in self-protection, and it is given by

\[ \Psi(l(x_{r_{\text{opt}}}), x_i^r) = E[U_{\text{def}f}(l(x_{r_{\text{opt}}}), x_i^r)] - E[U_{\text{ndef}f}(l_r(x_{r_{\text{opt}}})]. \]

When \( x_i^r = p_i^r \cdot r \), we have

\[ \Psi(l(x_{r_{\text{opt}}}), p_i^r \cdot r) = U_i(w_0 - (p_i^r \cdot r + p_{\text{ind}}^{i,r} \cdot r) - U_i(w_0 - p_i^r \cdot r) < 0, \]

and at \( x_i^r = 0 \) we have

\[ \Psi(l(x_{r_{\text{opt}}}), 0) = \{U_i(w_0 - p_{\text{ind}}^{i,r} \cdot r) - U_i(w_0 - p_i^r \cdot r)\} > 0. \]

In most practical cases, Equations 24 and 25 jointly indicate the monotonicity of \( \Psi(\cdot) \) and imply that there exists an interior solution \( x_{r_{\text{opt}}} \), where \( 0 < x_{r_{\text{opt}}} < p_i^r \cdot r \), such that

\[ \Psi(l(x_{r_{\text{opt}}}), x_{r_{\text{opt}}}) = E[U_{\text{def}f}(l(x_{r_{\text{opt}}}), x_{r_{\text{opt}}})] - E[U_{\text{ndef}f}(l(x_{r_{\text{opt}}}))] = 0. \]
The interior solutions, $x_r^{eq}$, to $E[U_{def}(l(x_r^m), x_r')] = E[U_{ndef}(l(x_r^m))]$ is the competitive market equilibrium cost of protection investment, and equals $x_r^m$, the marginal cost of making self-defense investments in Market Type 4, 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 $x_r^{eq}$ find it profitable to invest in self-defense and cyber-insurance, whereas the others invest only in cyber-insurance.

Regarding reaching social welfare maximum, equating the first order condition for $SW_C(x_r^m)$ results in finding $x_r^{opt}$, the cost of investment that maximizes social welfare.

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

$$
\frac{dSW_C(x_r^m)}{dx} = A + B + C + D,
$$

(27)

where

$$
A = E[U_{def}(l(x_r^m), x_r^m)]f(x_r^m), \quad B = E[U_{ndef}(l(x_r^m))] \frac{dl(x_r^m)}{dx_r^m},
$$

$$
C = \frac{dE[U_{ndef}(l(x_r^m))]}{dx_r^m}l(x_r^m), \quad D = \int_0^x \frac{\delta E[U_{def}(l(x_r^m), x)]}{\delta x_r}f(x)dx.
$$

In light of Equation 23, Equation 27 can be written as

$$
\frac{dSW_C(x_r^m)}{dx_r} = N + C + D,
$$

(28)

where

$$
N = \{E[U_{def}(l(x_r^m), x_r^m)] - E[U_{ndef}(x_r^m)]\}f(x_r^m).
$$

Here, the first term in brackets in $N$ is the excess of expected utility, $\Psi_r(l(x_r^m), x_r^m)$, $C$ and $D$ are non-negative and non-decreasing in $x_r'$. Since excess of expected utility is positive at $x_r' = 0$ and negative at $x_r' = p_r' \cdot r$, there exists $x_r' = x_r^{opt}$ such $\frac{dSW_C(x_r^m)}{dx_r}$ is zero, and the social welfare in the network is maximized. We represent this mathematically as

$$
x_r^{opt} = \text{argmax}_{x_r^m} SW_C(x_r^m).
$$

(29)

Substituting $x_r^{eq}$ in Equation 29, and using Equation 26 we get

$$
\frac{dSW_C(x)}{dx} \bigg|_{x=x_r^{eq}} > 0.
$$

(30)

This implies that $x_r^{opt} > x_r^{eq}$ and $l(x_r^{opt}) < l(x_r^{eq})$, i.e., the proportion of users not resorting to self-defense mechanisms is higher in the Nash equilibrium than in the welfare optimum. Thus, we have proved Theorem 6.1. **Q.E.D.**

**Proof of Lemma 7.1.** Consider $\lambda = 0$. In such a case, because premiums are marginally fair, risk-averse users act as if they were risk neutral [Dionne and Harrington 1992]. 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

$$
SW_{M_{ncd}} = \int_0^{x_r^m} (w_0 - x - (p_r^{ind}(l(x_r^m)) \cdot r - b))f(x)dx + (w_0 - (p_r^i \cdot r + a))l(x_r^m) + k.
$$

Now, we know that

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

ACM Transactions on Performance Evaluation of Computer Systems, Vol. V, No. N, Article 1, Publication date: January YY.
Thus, using the relation, $a l(x_m^r) - b (1 - l(x_m^r)) = k$, $SW_{Mncd}(x_m^r)$ can be expressed as

$$SW_{Mncd}(x_m^r) = \int_0^{x_m^r} (w_0 - x - p_{ind}^i(l(x_m^r)) \cdot r) f(x) dx + (w_0 - p_i^r \cdot r) l(x_m^r).$$

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

$$p_d^r (1 - p_{ind}^i(l(x_m^r))) r - x_m^r + \frac{a}{1 - l(x_m^r)} - \frac{k}{1 - l(x_m^r)} = 0. \quad (31)$$

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

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

where

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

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

$$\frac{\delta \mathcal{L}(a, x_m^r)}{\delta a} = L \cdot \left\{ \frac{1}{1 - l(x_m^r)} \right\} = 0. \quad (33)$$

Since the term inside braces of Equation (33) is positive, we have $L = 0$. Thus, the optimal self-defense investment cost is $x_m^{opt}$ at market equilibrium. Correspondingly, the values of $a$ (fine) and $b$ (rebate) for a given $k$, are given by

$$a = x_m^{opt} - p_d^r (1 - p_{ind}^i(l(x_m^{opt}))) r - b,$$

where

$$b = \{x_m^{opt} - p_d^r (1 - p_{ind}^i(l(x_m^{opt}))) r\} - k.$$

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

$$k \geq \{x_m^{opt} - p_d^r (1 - p_{ind}^i(l(x_m^{opt}))) r\} - l(x_m^{opt}) r.$$

Thus, we have proved Lemma 7.1. Q.E.D.

**Proof of Theorem 7.2.** Without a premium fine, the expected utility of network users who invest in self-defense is $U_i(w_0 - x_0^r)$, 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

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

We also have $\frac{d\Psi}{dx_m^r}$ evaluate to

$$-U_i(w_0 - x_m^r) + U(w_0 - p_i^r - (1 - p_i^r) p_{ind}^i(l(x_m^r)) r) (1 - p_d^r) \frac{dp_{ind}^i(l(x_m^r))}{dx_m^r} r,$$

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

$$\Psi(l(x_m^r), x_m^{opt}) = U_i(w_0 - x_m^{opt}) - U_i(w_0 - p_i^r \cdot r) = 0,$$

ACM Transactions on Performance Evaluation of Computer Systems, Vol. V, No. N, Article 1, Publication date: January YY.
where \( p_i^r \cdot r \) is evaluated at \( x^{s_{opt}}_r \). Introducing a premium fine of \( \alpha \) for users who do not invest in self-defense, the following two must hold:

\[
U_i(w_0 - x^m_r) = U_i(w_0 - p_i^r \cdot r + \alpha).
\]

and

\[
U_i(w_0 - p_i^r \cdot r) - U_i(w_0 - x^{s_{opt}}_r) = \frac{dU_i(w_0 - p_i^r \cdot r)}{dx^m_r} l(x^m_r),
\]

where \( x^m_r = x^{s_{opt}}_r \). In order to attain the optimal self-defense cost value, \( x^{s_{opt}}_r \), Equation (34) can be written as

\[
U_i(w_0 - x^{s_{opt}}_r) = U_i(w_0 - p_i^r \cdot r + \alpha),
\]

where \( p_i^r \cdot r \) is evaluated at \( x^{s_{opt}}_r \). Thus, there exists an \( \alpha \) that satisfies

\[
U_i(w_0 - x^{s_{opt}}_r) = U_i(w_0 - (p_i^r \cdot r + \alpha)),
\]

where \( x^m_r = x^{s_{opt}}_r \). The latter expression is greater than zero and thus the socially optimal level of self-defense, \( x^{s_{opt}}_r \) is achievable by a fine of \( \alpha \), and for the insurer-desired profit margin, \( k \), the following must hold:

\[
k \geq \alpha \cdot l(x^{s_{opt}}_r) - (1 - l(x^{s_{opt}}_r)) p_{ind}^i l(x^{s_{opt}}_r) r > 0.
\]

Here \( p_{ind}^i l(x^{s_{opt}}_r) r \) denotes the expected loss of users whose self-defense investment cost level is \( x^{s_{opt}}_r \). Equation (37) results because the quantity, \( p_{ind}^i l(x^{s_{opt}}_r) r \), 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 l(x^{s_{opt}}_r)) \cdot \text{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 7.2. Q.E.D.}