IMPROVING NETWORK SECURITY THROUGH CYBER-INSURANCE

by

Ranjan Pal

A Dissertation Presented to the
FACULTY OF THE USC GRADUATE SCHOOL
UNIVERSITY OF SOUTHERN CALIFORNIA
In Partial Fulfillment of the
Requirements for the Degree
DOCTOR OF PHILOSOPHY
(COMPUTER SCIENCE)

December 2014

to my late father who wanted to see his son graduate

Acknowledgements

I am grateful to my advisors Professors Leana Golubchik and Konstantinos Psounis for their continued guidance and the numerous stimulating discussions. Leana and Kostas's providing me freedom to independently work on novel and practically important problems shaped me as a researcher. I am also grateful to the Provost Fellowship program at USC for awarding me the Provost Fellowship to conduct independent and high quality research.

I would also like to thank Professor Pan Hui of Hong Kong University of Science and Technology for collaborating with me on my thesis and providing me valuable inputs. Further, I would like to thank Professors Viktor Prasanna, Minlan Yu, Ramesh Govindan, Sergey Lototsky, and Cauligi Raghavendra for serving on my qualification and defense commitees, and providing me with relevant inputs to improve my thesis.

I would like to thank Professor Pan Hui, Professor Mung Chiang, and Dr. Xin Huang for giving me the opportunity to do summer internships at Deutsch Telekom Research Laboratories, Princeton University, and Cyan Inc. respectively during my tenure as a Ph.D student. Through my internships, I got the scope to work on industrially important research problems parallel to my Ph.D work. In this regard, I would like to thank Felix Wong, Sangtae Ha, and Christopher Leberknight of Princeton University and Darren Dowker of Cyan Inc. with whom I had fruitful discussions related to research and industry. At USC, I would like to thank Lizsl - the graduate advisor of the CS PhD program, who made my research life a lot easier than it could have been.

I had the privilege to share office space and discuss research topics with many talented people. In this regard I would like to thank Antonios Michaloliakos, Vlad Balan, Nachiketas Ananthakrishnan Jagadeesan, Bochun Wang, Kai Song, Michael Hung, Sung-Han Lin, and Suvil Deora.

My life at USC would have been a lot less exciting without my Indian friends. For a long project like a Ph.D., this is absolutely essential. I had great fun with Amit, Aditya, Adarsh, Nachiketas, Zoheb, Gursimran, and Pragya.

These acknowledgements would not be complete without mentioning the great pleasure that I have had in exploring different countries in Europe during my PhD with my friends in Europe - Ardhy, Gautam, Bayu, Tahir, and Bodhisattwa.

Finally, I would like to express my deepest appreciation for my parents for being a constant source of loving support, patience, and encouragement througout the years. My late father always wanted to see his son graduate with flying colors. It is to him I dedicate this thesis.

Table of Contents

List of Tables

List of Figures

Abstract

In recent years, security researchers have well established the fact that technical security solutions alone will not result in a robust cyberspace due to several issues jointly related to the economics and technology of computer security. In this regard some of them proposed cyber-insurance as a suitable risk management technique that has the potential to jointly align with the various incentives of security vendors (e.g., Symantec, Microsoft, etc.), cyber-insurers (e.g., security vendors, ISPs, cloud providers, etc.), regulatory agencies (e.g., government), and network users (individuals and organizations), in turn paving the way for robust cyber-security. In this work, we theoretically investigate the following important question: can cyber-insurance really improve the security in a network? To answer our question we adopt a market-based approach. We analyze regulated monopolistic and competitive cyber-insurance markets in our work, where the market elements consist of risk-averse cyber-insurers, risk-averse network users, a regulatory agency, and security vendors (SVs). Our analysis proves that technical solutions will alone not result in optimal network security, and leads to two important results: (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 and results in improvement of network security - however, the cyber-insurer can make zero expected profit. The latter fact is often sufficient to de-incentivize the formation or practical realization of successful and stable cyber-insurance markets.

To alleviate the insurers problem of potentially making zero profits, we suggest two mechanisms: (a) the SV could enter into a business relationship with the insurer and lock the latters clients in using security products manufactured by the SV. In return for the increased sale of its products, the SV could split the average profit per consumer with the insurer, and (b) the SV could itself be the insurer and account for logical/social network information of its clients to price them. In this regard, we study homogenous, heterogeneous, and binary pricing mechanisms designed via a common Stackelberg pricing game framework. The binary pricing game turns out to be NP-hard, for which we develop an efficient randomized approximation algorithm that achieves insurer profits up to 0.878 of the optimal solution. Our game analysis combined with simulation results on practical networking topologies illustrate increased maximum profits for the insurer (SV) at market equilibrium and always generate strictly positive profits for the latter, when compared to current SV pricing mechanisms in practice. In addition, the state of improved network security remains intact.

Chapter 1

Introduction

1.1 Chapter 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 [4][24]. 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 [2], whereby security vendors have no incentive to release robust products in the market, (viii) liability shell games played by product vendors, and (ix) user naiveness in optimally exploiting feature benefits of technical solutions. In view of the above mentioned inevitable barriers to near 100% risk mitigation, the need arises for alternative methods 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] To 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.

1.2 Research Motivation

Despite all promises, current cyber-insurance markets are moderately competitive and specialized. As of 2010, there are approximately 18 insurance organizations in the United states insuring $800 million worth of organizational IT resources [6], and there is little information as to whether the current cyber-insurance market improves network security by incentivizing organizations to invest aptly in security solutions. The inability of cyber-insurance to become a common reality (i.e., to form a successful market) amongst non-organizational individual users is due to a number of unresolved research challenges as well as practical considerations. The most prominent amongst them is *information asymmetry* (see Section 1.3) between the insurer and the insured, and the *interdependent and correlated* nature of cyber-risks [8].

In this dissertation, we investigate the following two important questions, given the above mentioned challenges: (i) *can cyber-insurance solutions induce efficient markets (See 6.2) that improve the security of a network?*, and (ii) *how can cyber-insurance markets be realized in practice?* Before we state our research contributions, we review some basic economics concepts used throughout the dissertation. In the process of studying improvement of network security, we are interested in analyzing the welfare of elements (stakeholders) that form a cyber-insurance market (if one exists).

1.3 Basic Economics Concepts

In this section we briefly review some basic economics concepts as applicable to this work in order to establish terminology for the remainder of the dissertation. Additional details could be found in a standard economics textbooks such as [25].

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

risk probability: It is the probability of a network user being successfully attacked by a cyber-threat.

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

user risk propensity: A risk-neutral investor (either the insurer or the insured) is more concerned about the expected return on their investment, not 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, and 50% of receiving nothing. A 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, a risk-averse investor would generally settle for the ”sure thing” or 100% certain $100, while the risk-seeking investor will opt for the 50% chance of getting $200.

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

equilibrium: An equilibrium refers to a market situation when both, buyers and sellers are satisfied with their net utilities and no one has any incentive to deviate from their strategies.

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

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

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

safety capital: A safety capital is the additional amount over the expected aggregate loss in a period such that the probability of an insurer incurring a loss of value greater than the sum of the capital and expected aggregate loss in that period does not exceed a particular threshold. The threshold value is defined by a regulator.

1.4 Research Contributions

We make the following primary research contributions in this dissertation.

- We propose a supply-demand model of regulated cyber-insurance markets that accounts for inter-dependent risks in a networked environment as well as the externalities generated by user security investments. (See Sections 3.2 and 3.3.)
- We first show that purely technical solutions alone will not result in optimal network security. We then show using an insurance framework for risk management that even a monopoly cyber-insurer providing full coverage to its clients without contract discrimination cannot enable the existence of an efficient cyber-insurance market, thereby not improving network security. In addition we also show that perfectly competitive and oligopolistic cyber-insurance settings, leads to inefficient insurance markets that does not improve network security. (See Sections 3.4 and 3.6.)
- We show that with client contract discrimination, the cyber-insurer is successful in enabling an efficient cyber-insurance market that alleviates the moral hazard problem and improves network security. In the process the insurer makes non-negative expected profits. As a result, we derive unregulated 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 investments, and at the same time maximize social welfare at market equilibrium. (See Section 3.7.)

- The important question that thus arises from previous chapters is *is there a practical way for a cyber-insurer to make strictly positive profits at all times, under regulation, and at the same time ensure optimal network robustness?* A positive answer to this question would imply cyber-insurance market success on a larger than moderate scale. In addition, in a correlated risk environment such as the Internet, insurers cannot afford to be risk-neutral as there are chances it might go bankrupt due to expected aggregate losses in a period being more than what it could afford to compensate. As a result it might hold a safety capital for a certain cost in order to prevent itself from going bankrupt [8]. The question that arises here is *how can the cyber-insurers recover costs of buying safety capital from the consumers of their products?* The above two questions motivate us to investigate a way in which cyber-insurers can always make profits and recover their costs (includes safety capital) to provide insurance coverage to clients, and at the same time ensure optimal network robustness.

  In this regard, we model risk-averse security vendors as cyber-insurers and propose a one-period static and heterogenous product pricing scheme for their consumers based on the consumers' logical network and their security investment amounts. Our proposed approach (i) potentially increases the current profit margins of SVs upto approximately 25% (relative to our model) and allows an SV to make strictly positive profits at all times, solely as an insurer, (ii) ensures the state of optimal network robustness, and (iii) allows risk-averse SV insurers to recover costs such as ones related to buying safety capital. Our proposed static pricing mechanism also incorporates the case of uniform and binary pricing, when the SV might be constrained from adopting heterogenous pricing schemes. (See Chapter 4.)

- We conduct an extensive numerical evaluation highlighting the effects of consumer overlay network on SV heterogenous pricing outcomes. Specifically, for practical real world topologies like scale free graphs and trees, we show that (i) the per-unit product price charged by an SV to consumers is proportional to the Bonacich centrality of consumers in their overlay network, and (ii) the total cost incurred by a consumer (network user) in security investments is nearly a constant, and is independent of the underlying network topology. The latter point implies consumer fairness because no matter how a consumer is placed in an overlay network, he pays the same total amount in security investments as any other consumer in the network, even though his per-unit security investment price charged by an SV is proportional to the amount of positive externalities he generates via his investments, which in turn is a function of his network centrality. (See Section 4.11 .)

- In reality, an Internet user faces risks due to security attacks as well as risks due to non-security related failures (e.g., reliability faults in the form of hardware crash, buffer overflow, etc.). These risk types are often indistinguishable by a naive user. However, a cyber-insurance agency would most likely insure risks only due to security attacks. In this case, it becomes a challenge for an Internet user to choose the right type of cyber-insurance contract as traditional optimal contracts, i.e., contracts for security attacks only, might prove to be sub-optimal for himself.

  In this regard we propose an alternative and novel[2] model of cyber-insurance, Aegis, in which Internet users need not transfer the total loss recovery liability to a cyber-

[2] Our cyber-insurance model is novel because we model partial insurance, whereas existing works related to traditional cyber-insurance model full and partial insurance coverage but not partial insurance. The notion of partial insurance can be explained as follows: in traditional cyber-insurance models, only the cyber-insurer has the say on the amount of coverage it would provide to its clients and in turn the premiums it would charge, whereas in the Aegis model, the clients get to decide on the fraction of the total amount of advertised insurance coverage it wants and in turn the proportional premiums it would pay, given an advertised contract. Thus, in traditional cyber-insurance, it is mandatory for users to accept the insurance policy in full, whereas in the Aegis model users have the option of accepting the insurance policy in partial.

insurer, and may keep some liability to themselves, i.e., an Internet user may not transfer the entire risk to an insurance company. Thus, as an example, an Internet user may rest 80% of his loss recovery liability to a cyber-insurer and may want to bear the remaining 20% on his own. Our model captures the realistic scenario that Internet users could face risks from security attacks as well as from non-security related failures. It is based on the concept of co-insurance in the traditional insurance domain.

We mathematically show that when Internet users are risk-averse, Aegis contracts are *always* the user preferred policies when compared to traditional cyber-insurance contracts. In this regard, the latter result de-establishes a market for traditional cyber-insurance. The availability of Aegis contracts also *incentivizes* risk-averse Internet users to rest some loss coverage liability upon themselves rather than shifting it all to a cyber-insurer, but does not achieve market efficiency. In addition we show that a risk-averse Internet user would prefer cyber-insurance of some type (Aegis or traditional) *only* if it is mandatory for him to buy some kind of insurance, given that he faces risks due to both, security as well as non-security failures. We also mathematically show the following counterintuitive results: (i) an increase in the premium of an Aegis contract *may not* always lead to a decrease in its user demand and (ii) a decrease in the premium of an Aegis contract may not always lead to an increase in its user demand. In the process, we also state the conditions under which these trends emerge. The conditions give a guideline to cyber-insurers on how to increase or decrease their premiums in order to increase user demands for cyber-insurance. (See Sections 6.2, 5.3, and 5.4)

- Under full insurance coverage, we perform a mathematical comparative study to show that co-operation amongst Internet users results in optimal self-defense investments that maximizes social welfare, when the risks faced by the users in the Internet are inter-dependent (see Section 6.4). We use basic concepts from both, co-operative and non-co-operative game theory to support the claims we make in Sections 6.3 and 6.4. Our results are applicable to co-operative (e.g., distributed file sharing) and non-cooperative Internet applications where a user has the option to be either co-operative or non-cooperative with respect to security parameters.

Chapter 2

Literature Survey

In this section, we give an overview of related work on cyber-insurance as applicable to this paper. We first state existing work and its drawbacks, which is then followed by stating our contributions in this dissertation.

2.1 Existing Work and its Drawbacks

The field of cyber-insurance in networked environments has been triggered by recent results on the amount of self-defense investments users should expend in the presence of network externalities in order to ensure a robust cyber-space. The authors in [14][20][22] [23][27][29] 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 [22][23] 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 [21][24], Lelarge and Bolot have stated that under conditions of no *information asymmetry* [1] between the insurer and the insured, cyber-insurance *incentivizes* Internet user investments in self-defense mechanisms, thereby paving the path to trigger a cascade of adoption. They also show that investments in both self-defense mechanisms and insurance schemes are quite inter-related in maintaining a socially efficient level of security on the Internet. The authors in [44] 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 [31], the authors show that in a cyber-insurance framework similar to the one proposed by Lelarge and Bolot, cooperation amongst network users results in the latter making better (more) self-defense investments than the case in which they would not cooperate. Thus, the authors' results reflect that cooperation amongst network users will result in a more robust cyberspace. However, not all applications in cyberspace can be cooperative and as a result we consider the general case of non-cooperative application environments and to ensure optimal insurance-driven self-defense amongst users in such environments.

In another recent work [33], the authors derive *Aegis*, a novel optimal insurance contract type based on the traditional cyber-insurance model, in order to address the realistic scenario when both, insurable and non-insurable risks co-exist in practice. They mathematically show that (i) for any type of single-insurer cyber-insurance market (whether offering Aegis type or traditional type contracts) to exist, a *necessary condition* is to make insurance mandatory for all risk-averse network users, (ii) Aegis contracts *mandatorily* shift more liability on to network users to self-defend their own computing systems, when compared to traditional cyber-insurance contracts, and (iii) it is rational to prefer Aegis contracts to traditional cyber-insurance contracts when an option is available. However, the authors do not analyze markets for cyber-insurance, where one needs to consider as important goals, maximizing social welfare, and satisfying multiple stake-holders. Without such considerations, simply shifting liability on users to invest more may not be enough for a successful cyber-insurance market.

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

2.2 Alleviating Existing Drawbacks

In this dissertation, we overcome the drawbacks of the mentioned existing works through our works in [35][34]. We propose ways to form efficient monopolisitc cyber-insurance markets by satisfying market stakeholders including a risk-averse cyber-insurer, in environments of interdependent risk. We also account for information asymmetry and correlated risks in a partial manner. In doing so we also extend and strengthen our own works in [32] and [36] that account for market stakeholders and information asymmetry respectively, in a weak manner. However, a drawback of the work in [35] is that there is no strict guarantee provided to the monopolistic cyber-insurer that it would always make positive profits. This is strong enough a disincentive for the cyber-insurer to opt out of the market in the long run. To alleviate this issue we extend our work in [35] to design premium discriminating contracts that enable the monopolistic insurer to make strictly positive profits of its choice and at the same time maximize social welfare. *Through our work, we also contradict the results cited in [21][24] that cyber-insurance will enable network users to optimally invest in network security via a cascading effect.* In fact, we show that only under specific monopoly scenarios can an efficient cyber-insurance market exist that satisfies all market stakeholders. This also justifies the specialized cyber-insurance markets that exists in practice today. The authors in [7] use Student t-copulas in statistics to model global and local correlation for information and communications technology (ICT) organizations and show through simulations that a cyber-insurance market exists for risks with high internal and low global correlation. However, their work does not consider interdependent risks.

To the best of our knowledge, existing research on how the structure of application networks affects the computation of cyber-insurance elements that leads to market success is scarce and non-significant. We study the network effect problem in significant detail and highlight the role of consumer overlay (application) networks on security product and cyber-insurance element pricing, and their discriminative allocation amongst consumers. Our proposed discriminative pricing mechanism in turn enables the formation of efficient cyber-insurance markets with the cyber-insurer making strictly positive profits. The term 'cyber-insurance elements' mentioned above include fines, rebates, and safety capital. In our work we vouch for the idea that these elements be allocated amongst clients based on their network centrality and security investment amounts in order to achieve efficient cyber-insurance markets. Throughout the rest of this dissertation we use the terms, 'client', and 'consumer', and 'network user' interchangeably to imply entities buying security products. We will also use the terms 'investment' 'self-defense investment' and 'security' investment interchangeably to denote the number of units of security product purchased by each client.

Chapter 3

Analyzing Cyber-Insurance Markets

3.1 Chapter Introduction

In this chapter we analyze cyber-insurance markets. We deal with perfectly competitive markets, oligopolistic markets, and monopoly markets. For each of these markets we study equilibrium existence, uniqueness, and efficiency. We now briefly describe each market type.

3.1.1 Perfectly Competitive Markets

In economic theory, perfect competition (sometimes called pure competition) describes markets such that no participants are large enough to have the market power to set the price of a homogeneous product. Because the conditions for perfect competition are strict, there are few if any perfectly competitive markets. Generally, a perfectly competitive market exists when every participant is a ”price taker”, and no participant influences the price of the product it buys or sells. Specific characteristics may include:

- *A large number buyers and sellers:* A large number of consumers with the willingness and ability to buy the product at a certain price, and a large number of producers with the willingness and ability to supply the product at a certain price.

- *No barriers of entry and exit:* No entry and exit barriers makes it extremely easy to enter or exit a perfectly competitive market.

- *Perfect factor mobility:* In the long run factors of production are perfectly mobile, allowing free long term adjustments to changing market conditions.

- *Perfect information:* All consumers and producers are assumed to have perfect knowledge of price, utility, quality and production methods of products.

- *Zero transaction costs:* Buyers and sellers do not incur costs in making an exchange of goods in a perfectly competitive market.

- *Profit maximization:* Firms are assumed to sell where marginal costs meet marginal revenue, where the most profit is generated.

- *Homogenous products:* The qualities and characteristics of a market good or service do not vary between different suppliers.

- *Non-increasing returns to scale:* The lack of increasing returns to scale (or economies of scale) ensures that there will always be a sufficient number of firms in the industry.

- *Rational buyers:* buyers capable of making rational purchases based on information given

- *No externalities:* costs or benefits of an activity do not affect third parties.

3.1.2 Oligopolistic Markets

An oligopoly is a market form in which a market or industry is dominated by a small number of sellers (oligopolists). Oligopolies can result from various forms of collusion which reduce competition and lead to higher prices for consumers. With few sellers, each oligopolist is likely to be aware of the actions of the others. The decisions of one firm therefore influence and are influenced by the decisions of other firms. Specific characteristics of oligopolistic markets include:

- *Profit maximization conditions:* An oligopoly maximizes profits.
- *Ability to set price:* Oligopolies are price setters rather than price takers.
- *Entry and exit:* Barriers to entry are high. The most important barriers are economies of scale, patents, access to expensive and complex technology, and strategic actions by incumbent firms designed to discourage or destroy nascent firms. Additional sources of barriers to entry often result from government regulation favoring existing firms making it difficult for new firms to enter the market.
- *Number of firms:* ”Few” - a ”handful” of sellers. There are so few firms that the actions of one firm can influence the actions of the other firms.
- *Long run profits:* Oligopolies can retain long run abnormal profits. High barriers of entry prevent sideline firms from entering market to capture excess profits.
- *Product differentiation:* Product may be homogeneous (steel) or differentiated (automobiles).
- *Perfect knowledge:* Assumptions about perfect knowledge vary but the knowledge of various economic factors can be generally described as selective. Oligopolies have perfect knowledge of their own cost and demand functions but their inter-firm information may be incomplete. Buyers have only imperfect knowledge as to price, cost and product quality.
- *Interdependence:* The distinctive feature of an oligopoly is interdependence. Oligopolies are typically composed of a few large firms. Each firm is so large that its

actions affect market conditions. Therefore the competing firms will be aware of a firm's market actions and will respond appropriately. This means that in contemplating a market action, a firm must take into consideration the possible reactions of all competing firms and the firm's countermoves. It is very much like a game of chess or pool in which a player must anticipate a whole sequence of moves and countermoves in determining how to achieve his or her objectives. For example, an oligopoly considering a price reduction may wish to estimate the likelihood that competing firms would also lower their prices and possibly trigger a ruinous price war. Or if the firm is considering a price increase, it may want to know whether other firms will also increase prices or hold existing prices constant. This high degree of interdependence and need to be aware of what other firms are doing or might do is to be contrasted with lack of interdependence in other market structures. In a perfectly competitive (PC) market there is zero interdependence because no firm is large enough to affect market price. All firms in a PC market are price takers, as current market selling price can be followed predictably to maximize short-term profits. In a monopoly, there are no competitors to be concerned about. In a monopolistically-competitive market, each firm's effects on market conditions is so negligible as to be safely ignored by competitors.

- *Non-Price Competition:* Oligopolies tend to compete on terms other than price. Loyalty schemes, advertisement, and product differentiation are all examples of non-price competition.

3.1.3 Monopoly Markets

A monopoly market exists when a specific person or enterprise is the only supplier of a particular commodity. Monopolies are thus characterized by a lack of economic competition to produce the good or service and a lack of viable substitute goods. The verb ”monopolize” refers to the process by which a company gains the ability to raise prices or exclude competitors. In economics, a monopoly is a single seller. Although monopolies may be big businesses, size is not a characteristic of a monopoly. A small business may still have the power to raise prices in a small industry (or market). Specific characteristics of monopoly markets include:

- *Profit Maximizer:* Maximizes profits.
- *Price Maker:* Decides the price of the good or product to be sold, but does so by determining the quantity in order to demand the price desired by the firm.
- *High Barriers to Entry:* Other sellers are unable to enter the market of the monopoly.
- *Single Seller:* In a monopoly, there is one seller of the good that produces all the output. Therefore, the whole market is being served by a single company, and for practical purposes, the company is the same as the industry.
- *Price Discrimination:* A monopolist can change the price and quality of the product. He or She sells more quantities charging less price for the product in a very elastic market and sells less quantities charging high price in a less elastic market.

The rest of the chapter 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 chapter is summarized in Table 1.

3.2 Model from a Demand Perspective

We consider a communication network comprised of a continuum of *risk-averse* users. Here we use the notion of ‘users’ as defined in [8], where users are considered as atomic nodes (individuals, organizations, enterprise, data center elements, etc.) in the network, each controlling a possible collection of devices. The links between the nodes need not necessarily be physical connections and could also represent logical or social ties amongst the nodes. For example, social engineering attacks are conducted on overlay networks. Each user i has initial wealth w_0 and faces a risk of size $r < w_0$ with probability p_i^r. Here p_i^r is a function of i's efforts in self-protection, and the proportion of users not investing in security measures. Each risk-averse user has the standard *von Neumann-Morgenstern (VNM)* utility, $U(\cdot)$[25]. VNM utilities are a function of a user's final wealth, and is twice continuously differentiable, increasing, and strictly concave. For a particular risk of size r, each user i also incurs a cost x_i^r to invest in self-defense mechanisms, which is an instance of a random variable X_r having distribution function F_r and density function f_r, each defined over the support $[0, r]$. As a practical example, we can think of x_i^r as the sum of the cost of buying anti-virus software and the cost of expending efforts in keeping one's computer secure. Thus, users are heterogenous in their cost of self-defense investments. We define x_r^m (a particular instantiation of X_r) to be the marginal cost of investing in self-defense mechanisms, i.e., it is the cost to a user who is indifferent between investing and not investing in self-defense. Such a user's net utility on investment is the same as his net utility on non-investment. In the remainder of the dissertatio, we assume that such a user always invests in self-defense. All other risk-averse users either decide to invest or not invest in self-defense mechanisms, depending on whether their cost of investment is lower or higher than x_r^m. Throughout the chapter we let r and x_i^r's have the same units.

We assume that a user does not completely avoid loss on self-protection, i.e., self-protection is not perfect, and is subject to two types of losses: *direct* and *indirect*. A direct loss to a user is caused when it is directly attacked by a malicious entity (threat). An indirect loss to a user is caused when it is indirectly affected by direct threats to other users in the network. A brief description of examples of direct and indirect threats is given in

Section VII. Let $p_d^{i,r}$ denote the probability of a direct loss to a user, where $p_d^{i,r}$ is a function of x_i^r, i.e., $p_d^{i,r} = p_d^r$ if user i invests an amount x_i^r in self-protection, and zero if it does not. Let $p_{ind}^i(l)$ denote the probability of a user getting indirectly affected by other network users, where l is the *proportion of users in the network not adopting self-defense (self-protection) mechanisms*, which in turn is a function of x_r^m, i.e., the marginal cost to a user indifferent to investing in self-defense investments. x_r^m is a function of the vector of user investments, the network topology, and the number of users who are affected by a threat. Thus, $p_{ind}^r(l) = p_{ind}^r(l(x_r^m))$. We have the following relationship between l and x_r^m:

$$l = l(X = x_r^m) = \int_{x_r^m}^{r} f(\theta)d\theta = 1 - F(x_r^m). \tag{3.1}$$

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

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

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

Table 3.1: Summary of Important Symbols in Chapter 3

is given as

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

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

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

We note that one particular way of computing the value of p_i^r as a function of parameters $p_d^{i,r}$ and p_{ind}^r in a network graph, is using *Local Mean Field Analysis* (LMFA) [22][23].

3.3 Model from a Supply Perspective

In this chapter we consider regulated monopolistic and competitive (both perfect and oligopolistic) cyber-insurance markets. A cyber-insurer could be any combination of an ISP, security product vendor, traditional insurance companies, and security third parties. We assume that insurers are *risk-averse* and provide full coverage to their clients (users), who must buy cyber-insurance in the monopolistic case (not necessarily in the competitive case). Mandatory insurance is considered as a regulator's tool to improve cyber-security[1]. Another reason why compulsory insurance could be mandated is to prevent high-risk users from adopting unsafe protection measures. In a non-compulsory system, high risk users might opt out of buying cyber-insurance knowing that they would have to pay high premiums. This would imply that these users could adopt unsafe security measures that negatively affect cyber-security. With insurance being made compulsory, high risk users would take steps to protect their systems more in order to pay lesser premiums, and hence positively affect cyber-security. We ensure full coverage from the insurer side in return for clients committing to buying cyber-insurance.

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

[1] As a matter of fact, in [33], the authors show that when insurable and non-insurable risks (for example those caused by hardware/software reliability faults) co-exist together, even under conditions of no information asymmetry between the monopolistic insurer and the insured, cyber-insurance needs to be made mandatory for a market to exist. From a policy viewpoint, this seems tough to implement, but as mentioned above, in the interest of cyber-security, such measures might be adopted in the near future.

$E(R)$ is the expected loss value of the client. 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 $E(R)$.

3.4 Scenario 1: No Insurance Case

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.

Let $U^{1,i}_{ndef}(l(x^{m_1}_r))$ be the utility to a user i in Scenario 1 when he does not invest in self-defense. $x^{m_1}_r$ is the marginal cost of self-defense in Scenario 1. The expected utility of a user i in Scenario 1 who does not invest in self-defense mechanisms is thus given as

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

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

$$Q_1 = p^r_{ind}(l(x^{m_1}_r))U(w_0 - r) + (1 - p^r_{ind}(l(x^{m_1}_r))U(w_0),$$

In order to have more condensed equations, we somewhat abuse notation and use Q_1 instead directly using the expression denoting Q_1. Similarly, the expected utility of a user who invests in self-defense mechanisms is given as

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

or

$$E[U^{1,i}_{def}] = p^r_{ind}(l(x^{m_1}_r))U(w_0 - x^r_i - r) + (1 - p^r_{ind}(l(x^{m_1}_r))U(w_0 - x^r_i).$$

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

$$\Psi_1(l(x^{m_1}_r), x^r_i) = E[U^{1,i}_{def}(l(x^{m_1}_r), x^r_i)] - E[U^{1,i}_{ndef}(l_r(x^{m_1}_r)]. \tag{3.2}$$

As special case, when $x^r_i = r$, we have

$$\Psi_1(l(x^{m_1}_r), r) = (1 - p^r_d)\{U(w_0 - r) - U(w_0)\} < 0, \tag{3.3}$$

and at $x^r_i = 0$ we have

$$\Psi_1(l(x^{m_1}_r), 0) = p^r_d(1 - p^{max}_{ind})\{U(w_0) - U(w_0 - r)\} > 0. \tag{3.4}$$

In most practical cases, Equations 3.3 and 3.4 jointly indicate the monotonicity of $\Psi_1(\cdot)$ (due to Ψ being often strictly decreasing) and imply that (i) if no user invests in self-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 $x^{eq_1}_r$, where $0 < x^{eq_1}_r < r$, such that

$$\Psi_1(l(x^{m_1}_r), x^{eq_1}_r) = E[U^{1,i}_{def}(l(x^{m_1}_r), x^{eq_1})] - E[U^{1,i}_{ndef}(l(x^{eq_1}_r))] = 0. \tag{3.5}$$

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

Market Equilibrium: The solution to $E[U^{1,i}_{def}] = E[U^{1,i}_{ndef}(l(x^{m_1}_r))]$ gives us the investment cost to a user who is indifferent between investing and not investing in self-defense. Thus $x^{eq_1}_r = x^{m_1}_r$, the marginal cost of making self-defense investments in Scenario 1. The interior solution, $x^{eq_1}_r$, in Equation 3.5 is the competitive market equilibrium (CME) cost of protection investment. It implies that users whose cost of self-defense is less than $x^{eq_1}_r$ 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. Mathematically, the expression for the CME can be derived from the following equation in [40].

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

The CME value given by

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

Here $\pi[p^r_i]$ is the risk premium.

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

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

The first term in $SW_1(x^{m_1}_r)$ 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 users not investing in self-defense. Equating the first order condition for $SW_1(x^{m_1}_r)$ results in finding $x^{sopt_1}_r$, the cost of investment that maximizes social welfare. The first order condition

(FOC) for an interior maximum is

$$\frac{dSW_1(x_r^{m_1})}{dx_r^{m_1}} = A_1 + B_1 + C_1 + D_1, \tag{3.6}$$

where

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

$$B_1 = E[U^1_{ndef}(l(x_r^{m_1}))]\frac{dl_r(x_r^{m_1})}{dx_r^{m_1}},$$

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

and

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

Using Equation 3.1, Equation 3.6 can be written as

$$\frac{dSW_1(x_r^{m_1})}{dx^{m_1}} = F + C_1 + D_1, \tag{3.7}$$

where

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

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

$$x_r^{sopt_1} = argmax_{x_r^{m_1}} SW_1(x_r^{m_1}). \tag{3.8}$$

Substituting $x_r^{eq_1}$ in Equation 3.7, and using Equation 3.5 we get

$$\frac{dSW_1(x_r^{m_1})}{dx_r^{m_1}}|_{x_r^{m_1}=x_r^{eq_1}} > 0. \tag{3.9}$$

The first derivate of SW_1 being positive at $x_r^{eq_1}$ clearly indicates that $x_r^{sopt_1} > x_r^{eq_1}$, thus implying $l(x_r^{sopt_1}) < l(x_r^{eq_1})$. i.e., the proportion of users not resorting to self-defense mechanisms is higher in the market equilibrium than in the welfare optimum. **The analysis above proves the following theorem.**

Theorem 1. *In the case of imperfect prevention, when network users do not have cyber-insurance protection, there exists a unique market equilibrium cost to invest in self-defense,* $x_r^{eq_1}$*. Users facing protection costs below* $x_r^{eq_1}$ *invest in self-defense mechanisms, whereas other users do not. This CME 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.*

Theorem Intuition and Practical Implications: The intuition behind Theorem 1 is based on the *first fundamental theorem in welfare economics* [25] 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 $p(x^m)$), is not minimized. With respect to the welfare of users, the ones who face a cost of investment above the CME cost do not buy security products and face a loss on being attacked. The ones who do invest in security measures are better off but are still susceptible to indirect risks. The case of no insurance is currently the situation in Internet security, apart from a few organizations that are insured.

3.5 Scenario 2: Monopoly Markets

In this section we analyze a regulated monopolistic cyber-insurance market under conditions of imperfect prevention (self-protection does not guarantee risk removal) and premium indiscrimination amongst the insured. Here the term ‘regulated’ implies the role of the government to (i) ensure Internet users buy compulsory cyber-insurance, (ii) enable insurers to adopt premium discrimination amongst clients based on the user risk types, and (iii) allow basic user security behavior monitoring by insurance agencies.

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

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

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

$$Q_2 = q(l(x^{m_2}_r))U(w_0 - r + r - (1+\lambda)p^r_i \cdot r) + (1 - p^r_{ind}(l(x^{m_2}_r))U(w_0 - P^2_{11}).$$

Here $P^2_{11} = (1+\lambda)p^r_i \cdot r)$ is the insurance premium that a user in Scenario 2, Case 1 (no contract discrimination)[2]and not investing in security (hence denoted as P^2_{11}), pays to his cyber-insurer in return for full coverage of his loss (hence the ‘$-r + r$’ term in U). $x^{m_2}_r$ is the marginal cost of investment in Scenario 2.

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

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

where $P^2_{12} = P(p^r_{ind}(l(x^m_r)) = (1+\lambda)p^r_{ind}(l(x^m_r)) \cdot r$ is the insurance premium a user in Scenario 2, Case 1, and investing in security pays to his insurer. A user would want to

[2] Case 2 is the setting where the monopoly insurer premium discriminates its clients, and will be discussed in chapter 3.7.

invest in loss prevention only if $E[U^{2,i}_{def}] \geq E[U^{2,i}_{ndef}]$.

Define $\Psi_2(l(x^{m_2}_r), x^r_i)$ 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

$$\Psi_2(l(x^{m_2}_r), x^r_i) = E[U^{2,i}_{def}(l(x^{m_2}_r), x^r_i)] - E[U^{2,i}_{ndef}(l(x^{m_2}_r))]. \tag{3.10}$$

When $x^r_i = 0$, we have

$$\Psi_2((x^{m_2}_r), 0) = U(w_0 - P^2_{12}) - U(w_0 - P^2_{11}) > 0, \tag{3.11}$$

and at $x^r_i = r$ we have

$$\Psi_2(l(x^{m_2}_r), r) = U(w_0 - r) - U(w_0 - p_d r) < 0. \tag{3.12}$$

In most practical cases, Equations 3.11 and 3.12 jointly indicate the monotonicity of $\Psi_2(\cdot)$ and imply that $\Psi_2(\cdot)$ is decreasing in x^r_i and there exists $x^{eq2}_r \,\epsilon\, (0, r)$, such that

$$\Psi_2(l(x^{m_2}_r), x^{eq_2}_r) = E[U^{2,i}_{def}(l(x^{m_2}_r), x^{eq_2}_r)] - E[U^{2,i}_{ndef}(l(x^{eq_2}_r))] = 0. \tag{3.13}$$

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

Mathematically, the expression for the Nash equilibrium can be derived from the following equation in [40].

$$U(w_0 - x^{eq_2}_r) = U(w_0 - p^r_i(x^{eq_2}_r) \cdot r), \tag{3.14}$$

which leads to a MME value given by

$$x^{eq_2} = p_i^r(x_r^{eq_2}) \cdot r. \tag{3.15}$$

Social Welfare Maximization: We define the social welfare of a network of users as the sum of the expected utility of all the users. We denote social welfare in Scenario 2 as $SW_2(x_r^{m_2})$, which evaluates to

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

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

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

$$\frac{dSW_2(x_r^{m_2})}{dx} = A_{21} + B_{21} + C_{21} + D_{21}, \tag{3.16}$$

where

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

$$B_{21} = E[U_{ndef}^2(l(x_r^{m_2}))]\frac{dl(x_r^{m_2})}{dx_r^{m_2}},$$

$$C_{21} = \frac{dE[U_{ndef}^2(l(x_r^{m_2}))]}{dx_r^{m_2}}l(x_r^{m_2}),$$

and

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

In the light of Equation 3.1, Equation 3.16 can be written as

$$\frac{dSW_2(x_r^{m_2})}{dx_r^{m_2}} = G + C_{21} + D_{21}, \tag{3.17}$$

where

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

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

$$x_r^{sopt_2} = argmax_{x_i^r} SW_2(x_i^r). \tag{3.18}$$

Substituting $x_r^{eq_2}$ for $x_r^{m_2}$ in Equation 3.17, and using Equation 3.13 we get

$$\frac{dSW_2(x_r^{m_2})}{dx}|_{x=x_r^{eq_2}} > 0. \tag{3.19}$$

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

Theorem 2. *Under compulsory monopolistic cyber-insurance, there exists a unique monopoly market equilibrium (MME) cost to invest in self-defense, $x_r^{eq_2}$. Users facing protection costs below $x_r^{eq_2}$ invest in self-defense mechanisms, whereas other users only buy cyber-insurance. 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 Nash equilibrium than in the welfare optimum.), and cyber-insurance does not incentivize users to invest in self-defense mechanisms.*

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

The implications of the theorem are (i) cyber-insurance does not incentivize network users to invest in self-defense mechanisms[3], (ii) cyber-insurance exacerbates the moral hazard problem, i.e., once users buy insurance they do not spend as much in self-defense as they would without it. This makes sense from an economic viewpoint as users would loath to bear excessive cost in self-defense if there is an alternative to canceling out risk albeit at an unfair premium, i.e., premium greater than the fair amount, and (iii) cyber-insurance might increase individual user utilities (as users get full coverage of their losses) but does not positively contribute to the increase of overall network security. As a result a regulator interested in improving network security is not satisfied. These implications are also mentioned by the authors in [28] for a competitive market setting. Also note that since $\lambda \geq 0$, the cyber-insurer makes non-negative expected profits. A security vendor does not satisfy its interests from an existing cyber-insurance market, i.e., compared to Scenario 1, as the sales of its products are going to go down.

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

[3] 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 [33]. 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.

3.6 Scenario 3: Competitive Markets

We assume a perfectly competitive cyber-insurance market[4] where multiple cyber-insurers provide their clients with full coverage at fair premiums[5]. Due to imperfect prevention, we also assume that a risk-averse user resorts to insurance solutions whenever he invests in self-defense mechanisms. The expected utility of a user who does not invest in self-defense mechanisms in Scenario 3 and only buys insurance is given as

$$E[U^{3,i}_{ndef}] = E[U^{3,i}_{ndef}(l(x^{m_3}_r)] = p_d U(w_0 - r + r - P^3_1) + (1 - p_d)Q_3,$$

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

$$Q_3 = p^r_{ind}(l(x^{m_3}_r)U(w_0 - r + r - P^3_1) + (1 - p^r_{ind}(l(x^{m_3}_r))U(w_0 - P^3_1),$$

where $p^r_{ind} = p^r_{ind}(l(x^{m_3}_r))$. $P^3_1 = P(p^r_i \neq p^r_{ind}, r) = p^r_i \cdot r$ is the actuarially fair insurance premium that a user in Scenario 3 not investing in self-defense, pays to his cyber-insurer in return for full coverage of his loss. Here $x^{m_3}_r$ is the marginal cost of investment in Scenario 3.

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

$$E[U^{3,r}_{def}(l(x^{m_3}_r), x^r_i)] = U(w_0 - x^r_i - P^3_2),$$

where $P^3_2 = p^r_{ind} \cdot r$ is the actuarially fair insurance premium that a user in Scenario 3 not investing in self-defense, pays to his cyber-insurer in return for full coverage of his loss. We note that $P^3_2 < P^3_1$. A user i would want to invest in loss prevention only if

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

[5] Note that under perfect competition, the equilibrium strategy for all firms in a market is to charge fair premiums [25]. Charging unfair premiums will result in a firm having zero demand.

$E[U^{3,i}_{def}] \geq E[U^{3,i}_{ndef}]$.

$$\Psi_3(l(x_r^{m_3}), x_i^r) = E[U_{def}(l(x_r^{m_3}), x_i^r)] - E[U_{ndef}(l_r(x_r^{m_3}))]. \tag{3.20}$$

When $x_i^r = P_1^3$, we have

$$\Psi_3(l_r(x_r^{m_3}), P_1^3) = U(w_0 - (P_1^3 + P_2^3) - U(w_0 - P_1^3) < 0, \tag{3.21}$$

and at $x_i^r = 0$ we have

$$\Psi_3(l_r(x_r^{m_3}), 0) = p\{U(w_0 - P_2^3) - U(w_0 - P_1^3)\} > 0. \tag{3.22}$$

In most practical cases, Equations 3.21 and 3.22 jointly indicate the monotonicity of $\Psi_3(\cdot)$ and imply that there exists an interior solution $x_r^{eq_3}$, where $0 < x^{eq_3} < P_1^3$, such that

$$\Psi_3(l(x_r^{m_3}), x_r^{eq_3}) = E[U^{3,r}_{def}(l(x_r^{eq_3}), x_r^{eq_3})] - E[U^{3,r}_{ndef}(l(x_r^{eq_3}))] = 0. \tag{3.23}$$

Walrasian Equilibrium: The interior solutions, $x_r^{eq_3}$, to $E[U^{3,r}_{def}] = E[U^{3,r}_{ndef}]$ is the competitive market equilibrium (also named as Walrasian equilibrium [25] for perfectly competitive markets) cost of protection investment, and equals $x_r^{m_3}$, the marginal cost of making self-defense investments in Scenario 3, i.e., the cost of investment to a user indifferent between making and not making self-defense investments. This implies the fact that users whose cost of self-defense is less than $x_r^{eq_3}$ find it profitable to invest in self-defense and cyber-insurance, whereas the others invest only in cyber-insurance. Mathematically, the expression for the Walrasian equilibrium can be derived from the following equation arising due to [40].

$$U(w_0 - x_r^{eq_3}) = U(w_0 - p_i^r(x_r^{eq_3} \cdot r),$$

which leads to a Walrasian equilibrium value given by

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

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

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

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

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

$$\frac{dSW_3(x_r^{m_3})}{dx} = A_3 + B_3 + C_3 + D_3, \tag{3.24}$$

where

$$A_3 = E[U_{def}^{3,r}(l(x_r^{m_3}), x_r^{m_3})]f(x_r^{m_3}),$$

$$B_3 = E[U_{ndef}^{3,r}(l(x_r^{m_3}))]\frac{dl(x_r^{m_3})}{dx_r^{m_3}},$$

$$C_3 = \frac{dE[U_{ndef}^{3,r}(l(x_r^{m_3}))]}{dx_r^{m_3}} l(x_r^{m_3}),$$

and

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

In light of Equation 3.1, Equation 3.24 can be written as

$$\frac{dSW_3(x_r^{m_3})}{dx_r^{m_3}} = N + C_3 + D_3, \tag{3.25}$$

where

$$N = \{E[U_{def}^3(l(x_r^{m_3}), x_r^{m_3})] - E[U_{ndef}^{3,r}(x_r^{m_3})]\}f(x_r^{m_3}).$$

Here, the first term in brackets in N is the excess of expected utility, $\Psi_{3,r}(l(x_r^{m_3}), x_r^{m_3})$, C_3 and D_3 are non-negative and non-decreasing in x_i^r. Since excess of expected utility is positive at $x_i^r = 0$ and negative at $x_i^r = P_1^3$, there exists $x_i^r = x_r^{sopt_3}$ such $\frac{dSW_3(x_i^r)}{dx_i^r}$ is zero, and the social welfare in the network is maximized. We represent this mathematically as

$$x_r^{sopt_3} = argmax_{x_r^m} SW_3(x_r^{m_3}). \tag{3.26}$$

Substituting $x_r^{eq_3}$ in Equation 3.26, and using Equation 3.23 we get

$$\frac{dSW_3(x)}{dx}|_{x=x_r^{eq_3}} > 0. \tag{3.27}$$

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

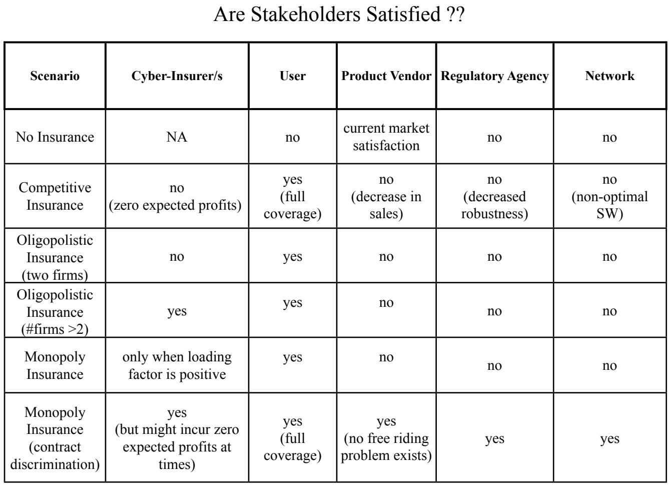
Theorem 3. *When network users have the option of cyber-insurance protection, there exists a unique Walrasian equilibrium cost to invest in self-defense, $x_r^{eq_3}$. Users facing protection costs below $x_r^{eq_3}$ jointly invest in self-defense mechanisms and insurance, whereas other users only buy cyber-insurance. This Walrasian equilibrium cost of self-defense does not result in maximizing user social welfare in the network and cyber-insurance does not incentivize users into making self-defense investments. In addition, the insurers make zero expected profits.*

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

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

A Note on Oligopolistic Markets: Oligopolistic markets resemble imperfect (not perfectly competitive) competition between firms in a market. In these markets, for a cyber-insurance setting, the insurers have market power to set prices unlike in the perfect competition case, where each insurer is price taking (has no market power to charge actuarially unfair premiums) and can only charge actuarially fair premiums to its clients. However, due to Bertrand's paradox [25], for number of insurers equal to two, the insurers find it optimal to charge fair premiums to their clients. So does that mean that in competitive settings, cyber-insurers will always make zero expected profits (due to charging actuarially fair premiums to clients) ? The answer is *no* because in reality factors such as firm popularity and customer lock-in will result in some insurers charging unfair premiums to their clients and making strictly positive expected profits, without having to worry about their client demands decreasing. In the case when the number of cyber-insurance firms in a market are greater than two, the authors in [28] show there exists a market Nash equilibrium which does not maximize social welfare.

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



Are Stakeholders Satisfied ??

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

Figure 3.1: Comparative Study of Scenarios

3.7 Achieving Market Efficiency

We saw and investigated why inspite of mandating cyber-insurance on network users, a social welfare maximum could not be reached. In this chapter 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[6]. 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

[6] In a recent paper [31], 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 [41] 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.

a fine of amount a per user of high risk type, and provides a rebate of amount b per user of low risk type. A user is considered of high risk type if he does not invest in self-defense mechanisms, and is considered of low risk type when he does invest in the same. A user decides whether it wants to invest in self-protection depending on the cost of investment and the provided fine/rebate. The sequence of the protocol between the insurer and the clients can be seen as follows: ***Stage 1*** - the insurer advertises appropriate contracts to its clients that include the fine/rebate values. ***Stage 2*** - the users simultaneously decide whether or not to invest in self-defense based on the cost of investment and their signed contract information, and ***Stage 3*** - when a coverage claim is filed by clients, the cyber-insurer examines the claims and charges the suitable rebate/fine to each client based on whether his investment amounts were above or below a particular threshold. Here we assume that the cyber-insurer can observe or stochastically learn the investment amounts of its clients *after* a claim is made.

Note that the premium differentiation approach is feasible only in the case of monopolistic cyber-insurance markets or imperfect competitive markets. In the case of perfectly competitive markets, price competition will not allow insurers to discriminate amongst their clients for commercial demand purposes and insurers will have to sell contracts at absolute fair premiums making zero expected profits. We now proceed with the analysis of the case when users are premium discriminated in monopoly markets. The analysis can be structured in two parts: one where the insurer might not make positive expected profit, and the other where the insurer makes positive expected profit.

3.7.1 Insurer Might not Make Positive Expected Profit

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

$$U(w_0 - x_i^r - P_{22}^2) = U(w_0 - (P_{21}^2 + a)), \tag{3.28}$$

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

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

where

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

Let

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

where

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

Here $P_{21}^{2,r}$ and $P_{22}^{2,r}$ are the premiums evaluated at $x_r^{sopt_{2'}}$, and A_{22} and B_{22} are the expected utilities of users investing and not investing in self-defense, respectively. The condition for achieving maximum social welfare is given as $A_{22} = B_{22}$. Substituting $x = x_r^{sopt_{2'}}$, and $a = a_r^{sopt_{2'}}$ in Equation 3.28, we get

$$U(w_0 - x_r^{sopt_{2'}} - P_{22}^2) = U(w_0 - (P_{21}^2 + a_r^{sopt_{2'}})), \tag{3.29}$$

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

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

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

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

$$U(w_0 - x_i^r - (P_{22}^2 - b)) = U(w_0 - P_{21}^2). \tag{3.30}$$

Our goal here again is to find the optimal self-defense cost $x_r^{sopt_{2'}}$ that achieves maximum social welfare. Substituting $x = x_r^{sopt_{2'}}$, and $b = b_r^{sopt_{2'}}$ in Equation 3.30, we get

$$U(w_0 - x_r^{sopt_{2'}} - P_{22}^2 - b_r^{sopt_{2'}}) = U(w_0 - P_{21}^2), \tag{3.31}$$

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

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

Then $b_r^{sopt_{2'}}$ is such that it satisfies the following condition (derived by combining Equations 3.28 and 3.30.):

$$M = B_{22}.$$

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

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

$$\Pi_{monopoly} = a \cdot l(x_r^{sopt_{2'}} - b \cdot (1 - l(x_r^{sopt_{2'}})) \geq 0. \tag{3.32}$$

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

Theorem 4. *Under conditions of compulsory monopolistic cyber-insurance, a cyber-insurer can help achieve social welfare maximization by premium discriminating clients. In turn, it makes non-negative expected profits, and also incentivizes users to invest in self-defense investments.*

Theorem Intuition and Practical Implications: By premium discriminating clients in the form of fines and rebates, cyber-insurers guide risk-averse users to internalize the externalities (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 in mitigated and as a result the overall network security is optimal, which would please security regulatory bodies. Regarding profits, cyber-insurers make non-negative expected profits[7], and security product vendors would see an increase in their product sales (and subsequently profits) due to users being incentivized to invest appropriate amounts in self-defense mechanisms.
Central Point: In the monopolistic cyber-insurance scenario with client contract discrimination, there may exist an efficient market (always exists if $\lambda > 0$) that helps satisfy the interests of all the market stakeholders.

3.7.2 Insurer Always Makes Positive Expected Profit

We just showed that premium discrimination in a monopoly setting leads to social welfare maximization, but does not necessarily guarantee a strictly positive expected profits for the cyber-insurer. This fact in turn is strong enough a disincentive for the cyber-insurer to drop out of the market. We now aim to alleviate this problem by designing contracts that allow

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

the monopolistic insurer to make strictly positive profits and at the same time ensure social welfare maximization. We start off with the concept that marginal users will be indifferent beween investing in self-defense and not investing if

$$U(w_0 - x_r^{m_2} - (P_{22}^{2,r} - b)) = U(w_0 - P_{21}^2 + a)). \tag{3.33}$$

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

$$a \cdot l(x_r^{m_2}) - b \cdot (1 - l(x_r^{m_2}) = k.$$

Consider $\lambda = 0$. In such a case, because premiums are marginally fair, risk-averse users act as if they were risk neutral [25]. The social welfare expression, $SW_2(x_r^{m_2})$, in the monopoly scenario (when insurer wants a profit of k) is then given by

$$\int_0^{x_r^{m_2}} (w_0 - x - (P_{22}^2 - b))f(x)dx + (w_0 - (P_{21}^2 + a))l(x_r^{m_2}) + k.$$

Now, we know that

$$\int_0^{x_r^{m_2}} bf(x)dx - al(x_r^{m_2}) = b(1 - l(x_r^{m_2})) - al(x_r^{m_2}) = -k.$$

Thus, using Equation (33), $SW_2(x_r^{m_2})$ can be expressed as

$$SW_2(x_r^{m_2}) = \int_0^{x_r^{m_2}} (w_0 - x - P_{22}^2)f(x)dx + (w_0 - (P_{21}^2)l(x_r^{m_2}).$$

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

$$p_d(1 - p_{ind}^i(l(x_r^{m_2}))r - x_r^{m_2} + \frac{a}{1 - l(x_r^{m_2})} - \frac{k}{1 - l(x_r^{m_2})} = 0. \tag{3.34}$$

The Lagrangian function, $\mathcal{L}(a, x_r^{m_2}, L, k)$ subject to Equation (34) is given by

$$\mathcal{L}(a, x_r^{m_2}, L, k) = \int_0^{x_r^{m_2}} (w_0 - x - P_{22}^2) f(x) dx + L \cdot C, \tag{3.35}$$

where

$$C = p_d(1 - p_{ind}^i(l(x_r^{m_2}))R - x_r^{m_2} + \frac{a}{1 - l(x_r^{m_2})} - \frac{k}{1 - l(x_r^{m_2})},$$

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

$$\frac{\delta \mathcal{L}(a, x_r^{m_2})}{\delta a} = L \cdot \left\{ \frac{1}{1 - l(x_r^{m_2})} \right\} = 0. \tag{3.36}$$

Since the term inside braces of Equation (36) is positive, we have $L = 0$. Thus, the optimal self-defense investmen cost is $x_r^{sopt_2}$ at market equilibrium. Correspondingly, the values of a (fine) and b (rebate) for a given k, are given by

$$a = x^{sopt_2} - p_d(1 - p_{ind}^i(l(x_r^{sopt_2}))r - b,$$

where

$$b = \{x_r^{sopt_2} - p_d(1 - p_{ind}^i(x_r^{sopt_2}))r\} - k.$$

Since the rebate, b, does not exceed the fair premium value, we have $k \geq \{x_r^{sopt_2} - p_d(1 - l(x_r^{sopt_2}))r\} - p_{ind}^i(x_r^{sopt_2})r$.

Practical Implications:The above analysis show that an efficient market equilibrium can be reached by ensuring a strictly positive profit of k for the cyber-insurer. Note that we performed our analysis constraining $\lambda = 0$. This is useful from both a theory perspective, as it makes analysis easier (need only deal with utility arguments and not the utilities themselves), and also from a practical perspective, as it saves the insurance company the hassle of computing the optimal 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.

Without a premium fine, the expected utility of network users who invest in self-defense is $U(w_0 - x)$, and $U(w_0 - P_{21}^2)$ for users who do not invest in self-defense mechanisms. In that case we have

$$\Psi_2(l(x_r^{m_2}), x_r^{m_2}) = U(w_0 - x_r^{m_2}) - U(w_0 - P_{21}^2).$$

We also have $\frac{d\Psi_2}{dx_r^{m_2}}$ evaluate to

$$-U(w_0 - x_r^{m_2}) + U(w_0 - p_d r - (1-p_d)p_{ind}^i(l(x_r^{m_2}))r)(1-p_d)\frac{dp_{ind}^i(l(x_r^{m_2}))}{dx_r^{m_2}}r,$$

which is less than zero, and thus $\frac{d\Psi_2}{dx_r^{m_2}}$ is strictly decreasing in $x_r^{m_2}$. Again, $\Psi_2(l(x_r^{m_2}), 0) > 0$, and $\Psi_2(l(x_r^{m_2}), r) < 0$. Thus in most practical cases, there is a unique interior solution (according to monotonicity properties), $x_r^{sopt2_2}$ such that

$$\Psi_2(l(x_r^{m_2}), x_r^{sopt2_2}) = U(w_0 - x_r^{sopt2_2}) - U(w_0 - P_{21}^2) = 0,$$

where P_{21}^2 is evaluated at $x_r^{sopt2_2}$. Introducing a premium fine of α for users who do not invest in self-defense, the following two must hold:

$$U(w_0 - x_r^{m_2}) = U(w_0 - P_{21}^2 + \alpha). \tag{3.37}$$

and

$$U(w_0 - P_{21}^2) - U(w_0 - x_r^{sopt2_2}) = \frac{dU(w_0 - P_{21}^2)}{dx_r^{m_2}} l(x_r^{m_2}), \tag{3.38}$$

where $x_r^{m_2} = x_r^{sopt2_2}$. In order to attain the optimal self-defense cost value, $x_r^{sopt2_2}$, Equation (37) can be written as

$$U(w_0 - x_r^{sopt2_2}) = U(w_0 - P_{21}^2 + \alpha),$$

where P_{21}^2 is evaluated at x^{sopt2_2}. Thus, there exists an α that satisfies

$$U(w_0 - P_{21}^2) - U(w_0 - (P_{21}^2 + \alpha)) = \frac{dU(w_0 - P_{21}^2 - \alpha)}{dx_r^{m_2}} l(x_r^{m_2}), \tag{3.39}$$

where $x_r^{m_2} = x_r^{sopt2_2}$. The latter expression is greater than zero and thus the socially optimal level of self-defense, $x_r^{sopt2_2}$ is achievable by a fine of α, and for the insurer-desired profit margin, k, the following must hold:

$$k \geq \alpha \cdot l(x_r^{sopt2_2}) - (1 - l(x_r^{sopt2_2}))q(l(x_r^{sopt2_2}))r > 0. \tag{3.40}$$

Here $p_{ind}^i(l(x_r^{sopt2_2})r$ denotes the expected loss of users whose self-defense investment cost level is x^{sopt2_2}. Equation (39) results because the quantity, $p_{ind}^i(x_r^{sopt2_2})r$, 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 $\alpha(p_{ind}^i(x_r^{sopt2_2}))$ - 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 shown that for a given k, network external-*

ities can indeed be completely internalized by designing monopoly contracts, where users are premium discriminated in a manner such that users investing in self-defense pay a premium of zero cost, and users not investing in self-defense pay a premium fine of α*.* However, we also note that for such contracts, there might be barriers imposed by a regulatory agency on the cyber-insurer for selling such contracts because the insurer can take advantage of its monopoly power to generate profits.

3.8 Practical Aspects of Realizing Cyber-Insurance

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

3.8.1 Measuring Loss

It is quite a challenge in practice to quantify the loss a user accrues when successfully attacked by malicious entities [39]. An improper estimate of a loss by the insurer will cause difficulties in charging the appropriate premium and providing the right amount of coverage. 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. We believe that it is very important that the cyber-insurer conducts/refers to statistical estimates of the values of different types of stated per client losses caused due to several cyber-crime types as cited in [3], and at the same time judge the current loss situation at hand, in order to get the best estimate of loss. However, in case of certain non-tangible losses (e.g., loss of reputation in thr eyes of its customers for a bank on being attacked), it is very hard to estimate an appropriate loss value. One additional important issue is the metricizing of different loss types to a common coverage unit. It is easier for any cyber-insurance company to perform a cost-benefit analysis on a common unit of coverage as done in this dissertation, and in turn analyze market equilibrium. However, the downside to this approach in practice is that all losses cannot be quantified to a single metric. On the other side, if different coverage units are designed for different loss types, the mathematical models may not be that easy to analyze for the existence and uniqueness of market equilibria.

3.8.2 Efficiency of Market Equilibria

In this dissertation, we mathematically demonstrate efficient cyber-insurance markets satisfying all stakeholders. However, in practice markets may not converge fast to a market equilibria due to uncertainties and heterogeneity of insurance parameters amongst clients, or might result in multiple equilibria. In this dissertation we have assumed heterogeneity of users with respect to investment costs only. In reality heterogeneity amongst users also arises due to the initial wealth and the type of utility functions. In addition, 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. 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. Cyber-insurance is a great tool to achieve this 'happy' ecosystem state and might even lead to the 'happiest' ecosystem state in the future.

3.8.3 Attack Types

The question we ask here is *losses from what types of attacks are insurable?* Our model in this dissertation is based on direct and non-direct attack scenarios and this covers the main features of 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 very 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 many threats.

3.8.4 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. The author in [30] makes an attempt to resolve the information asymmetry problem but without explicitly taking into account the interdependent and correlated risks inherent in networks. Using concepts from mechanism design and principal-agent theory in micro-economics, he shows that partial coverage by a monopoly cyber-insurer is the solution that will enable users to take more responsibility of their security behavior. In practice, partial insurance coverage may not go down well with users for internetworked environments with considerable externalities floating around, unless all the externalities are precisely internalized - a hard problem indeed. As a result, users may opt out of buying cyber-insurance (if not made compulsory) and a market might fail to exist. However, in practice, partial coverage is a very popular solution in insurance environments that do not have much externalities. In another attempt to resolve the information asymmetry problem, now between network users, the authors in [36] propose techniques using Bayesian game theory to enable users take appropriate investment decisions in equilibrium, even if they have partial knowledge of both the investments of other users in the network as well as the underlying communication network structure. This in turn would make the cyber-space more secure and lead towards efficient cyber-insurance markets. However, the dissertation assumes global knowledge of the distribution of users investments, which in practice might be hard to get hold of. Thus, it is difficult to have a theoretically sound solution and at the same time that solution being practically implementable. However, we emphasize that sound theoretical solutions will give us the all important insight and intuition of how things would behave in practice.

In reality, a way in which the information gap might be bridged or at least shortened to a considerable extent is via proper regulation and 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. 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. However, a strong regulation (e.g., by the government) is necessary to make buying insurance compulsory, as well as to prevent monopolists to misuse their power. The monopoly scenario (with premium discrimination) described in this dissertation could be realized in practice using ideas in this paragraph.

3.8.5 Application Domains

Cyber-insurance is an elastic risk management tool that can be widely applied to various networking domains such as organizational and enterprise networks, data centers, and to some extent the Internet and social networks. A major practical challenge to Internet-scale adoption is tracking down culprits in different geographical regions and in turn them taking responsibility for malicious behavior. Due to differences in international policies of various countries, insurance agencies like ISPs may not get the required cooperation from other country ISPs to track down culprits. Another practical challenge that arises in cloud and data center networks is figuring out who should buy insurance. Should a network user who stores data on the cloud buy insurance, and/or the data storage entity buy cyber-insurance? Such questions should have well-defined answers in order for cyber-insurance markets becoming more popular. Finally, the cyber-insurer in a correlated environment might become bankrupt as well, and either needs to invest in safety capital, or adopt high levels of risk transfer like cyber-reinusrance and catastrophe bonds [8].

Chapter 4

Realizing Efficient Markets in Practice

4.1 Chapter Introduction

Security vendors (SVs) are an important component in the analysis of security ecosystems. From the cyber-insurance viewpoint, research in the recent past has considered the market analysis of ecosystems that primarily comprise of cyber-insurer/s, network users[1], and the regulatory agency. However, network users adopt self-protection mechanisms that are manufactured by the SVs, who are inherently doing business with a profit making philosophy. Unfortunately, the profit mindset of SVs and its corresponding effects on security ecosystem components have not been studied so far with respect to cyber-insurance research. We now look at three ways in which SV profits fit into an insurance-driven security ecosystem.

- **Enhancing Cyber-Insurer profits**: In perfectly competitive and monopolistic markets without premium discrimination, the insurer/s gain zero expected profits by charging clients fair premiums [24], [35]. Thus, one way for the insurer/s to gain positive expected profits is to share profits made by SVs, in return for some favors offered to the SVs to increase current SV profits. Similarly in the case of (i) regulated and imperfectly competitive cyber-insurance markets [28] and (ii) monopolistic cyber-insurance markets with loading and premium discrimination, the insurers make non-negative expected profits and could boost their profits even further by sharing

[1] We use the notion of 'users' as mentioned in [8], where users are considered as atomic nodes (individuals or organizations) in the network, each controlling a possible collection of devices. The links between the nodes need not necessarily be physical connections and could also represent logical or social ties amongst the nodes.

valuable client information with SVs that increase their current profits.

- **Covering Insurer Costs of Holding Safety Capital**: In a correlated risk environment such as the Internet, an insurers cannot afford to be risk-neutral as there are chances it might go bankrupt due to expected aggregate losses in a period being more than what it could afford to compensate. As a result it might hold a safety capital for a certain cost in order to prevent itself from going bankrupt. One avenue for the insurer to recover full/partial costs of holding safety capital is to extract a fraction of SV profits in return for some benefits provided to the latter.

- **Role in Increase of Network Security**: In recent works, Pal et.al. [35] and Lelarge and Bolot [24] have proposed the concept of a cyber-insurer allocating fines and rebates amongst its clients in order to enable social welfare maximization in a network, with respect to individual user investments in security. Under this notion of maximum social welfare, users invest in optimal security, moral hazard problem is resolved, the sum of the utilities of all users in the network is maximized, and network security is optimal. However, in such scenarios a monopolistic cyber-insurer could make zero expected profits. Given the latter's profit making mindset, it would want to find a source of always making strictly positive profits so that it is incentivized to sell cyber-insurance contracts with premium discrimination, and contribute to optimal network security. An SV could be the profit-making source that the insurer could be looking for.

Thus, we observe that a symbiotic give and take relationship between cyber-insurers and SVs can prove beneficial to both. It is precisely for this reason in the dissertation that we want to investigate an appropriate way to fruitify the symbiotic relationship.

In this chapter we look to design ways to achieve market efficiency and at the same time allow insurers to make expected positive profit at all times. We model a security vendor (e.g., *Symantec*) as a cyber-insurer, and propose a novel consumer differentiated pricing mechanism for a monopoly SV based on its consumers' logical network locations and their security investment amounts, with the goal to improve profits. First, we qualitatively describe the insurance environment under which our proposed SV pricing mechanisms could operate. We then follow it up with a description of the SV pricing environment. Finally, we define our system model. A list of important symbols relevant to the chapter is shown in Table II.

4.2 Issues with Achieving Market Efficiency

Our work here is a thematic extension of our work in the previous chapter. There we had come to the conclusion that (i) in the presence of a monopoly cyber-insurer performing price discrimination amongst its clients, market efficiency is achieved but with no guarantee that the cyber-insurer will make strictly positive profits, and (ii) in the presence of no regulation, the monopoly insurer can premium discriminate in a way so as to make positive profits at all times. However, none of these conclusions will lead to practically realizable cyber-insurance markets, simply because the cyber-insurer who is profit-motivated, is not guaranteed to make profits at all times. Even when it does, the process might not be regulated, which is not a realistic scenario. In this chapter, we propose a method for cyber-insurers to make strictly positive profits under regulation. The rationale is for the cyber-insurer to increase profits by gaining additional profits through an entity such as an ISP, or generating additional profits for itself through a side business. For example, an ISP can bundle its Internet service packages with compulsory insurance and make a particular cyber-insurer its official insurer. In this case due to the lock-in effect, a cyber-insurer is likely to make additional profits due to increases sales. As another example, a security vendor itself could be a cyber-insurer and can transfer a part of its profits from its security product business to the insurance business. In this chapter, we primarily focus on how the external profit-making process can be realized in practice by a cyber-insurer in a manner so as to maximize his additional profits, apart from the expected profits it makes from its cyber-insurance business. *Thus, due to the external nature of the profit improvement process, we do not model specific cyber-insurance elements like premiums and coverage in this chapter.*

4.3 Insurance Setting (Environment)

We consider a system where a single monopolistic security vendor exists in a market and offers cyber-insurance solutions to its clients as the vendor's secondary business. Security vendors are a good choice as insurance agents because they have data regarding types, nature, and magnitude of attacks, and as a result can analyze client attack complaints. We assume that clients are subject to social engineering attacks and form a logical network between themselves (e.g., via Gmail, Facebook, Twitter, etc.)[2]. We consider social attack situations in this chapter because they are currently amongst the most common cyberattack methods in practice.

Each client is locked with his SV with respect to using security products manufactured by the SV, i.e., in this chapter each network user is the client of the insuring SV and mandated (e.g., by the government for global security improvement) to buy at least a threshold amount of security product manufactured by the SV. We model a single SV for two reasons: (i) the work in [35] talks about achieving efficient markets in monopolistic insurance scenarios, and (ii) a single SV easens tractable model analysis. However, in practice there will be multiple SVs, where a client may lock-in with a particular security vendor due to various aspects such as reputation, service quality, etc. A brief explanation of how an insurance

[2] Security vendors could act as insurance agents in enterprise and data center environments as well. However, corporations and enterprises are often self-insured.

market could function amongst multiple competitive SVs as insurers in provided in Section V. In view of recent recommendations made by an FCC advisory committee[3], ISPs have committed to taking steps to combat cyber-security threats (e.g., enforcing antibot conduct code, executing the ability to monitor, trace, analyse, and block traffic without violating privacy rules, and educating Internet users to access the web safely. Thus, we envision a future where SVs can work in collaboration with ISPs to make cyber-space secure. In this regard, SVs (and or ISPs) can act as cyber-insurers, where clients lock-in with a particular SV (cyber-insurer) thorough an ISP providing service to the client. This could happen if while signing an Internet agreement with the ISP, the client is required to buy security products by a particular vendor. As part of a business relationship, ISPs and SVs can finally trade incentives (profits, etc.,) with one another.

We assume that each consumer (network user) of security products buys cyber-insurance from a monopoly SV when he purchases an Internet connection. *We emphasize here that the cyber-insurance purchase by network users is different from and independent of them buying the security product from the SV.* We justify this assumption in the light of the fact that the government will encourage ISPs to take steps to protect cyber-security and similar to the case of car insurance, ISPs can potentially make insurance mandatory for clients buying an Internet connection. If it is identified (e.g., through tracking mechanisms conducted by the SV) that a client does not adopt proper security measures, his premiums would increase (and eventually leading to potential disconnection), and would drive him towards a direction of safe Internet practice. A consumer buying cyber-insurance is provided full coverage by his SV on facing a loss and is charged a premium which is not necessarily fair, i.e., the expected value of the loss. Each SV also premium discriminates its clients in the form of charging fines/rebates atop premiums. Based on works

[3] FCC chairman Julius Genachowski recently (2012) spoke at the Cybersecurity Bipartisan Policy Center on the role of ISPs in improving cybersecurity.

Symbol	Meaning
$u_i(\cdot)$	utility of user (consumer) i in consumer-seller model
N	number of consumers of an SV
h_{ij}	externality effect of user j on user i
x_i	amount of self-defense good consumed by user i
G	matrix representing externality values between user pairs
$\overrightarrow{x_{-i}}$	vector of self-defense amounts of users apart from i
$B(\cdot)$	Bonacich centrality vector of users in a logical network
c	constant marginal manufacturing cost to SV
p_i	price per unit of self-defense good consumed by i

Table 4.1: Summary of Important Symbols in Chapter 4

in [16][24][35], premium discriminating cyber-insurance clients is one way to alleviate the moral hazard problem, enables the insured's to optimally invest in self-defense investments, and maximizes the social welfare of the insured's in the network. We assume in light of [35] that the monopoly cyber-insurer in the market wants to maximize social welfare of its clients as a regulatory constraint imposed upon it by a regulator such as the government, and therefore premium discriminates its clients.

4.4 Security Vendor Pricing Environment

We consider SVs adopting a heterogenous product pricing mechanism that is based on the logical/overlay/application network of its consumers and their corresponding security investments, e.g., Gmail networks, Facebook networks, etc., The purpose of an SV to price clients in an heterogenous manner way is (i) to make additional profits from its security products, (ii) to cover up for the costs of providing insurance to clients, and (iii) to make strictly positive profits at all times as an insurer. We note here that price discrimination in general will not go down well with consumers. However, in the presence of a regulatory agency trying to improve global security, there might be incentives provided to a security vendor to transfer increased profits to its cyber-insurance business, and for consumers to adopt a differentiated pricing scheme. However, it is best for the security vendor to ensure some sort of fairness in its pricing mechanism so that despite government mandates to impose differentiated pricing, consumers feel satisfied. An important question that arises here is: *apart from regulatory agency interests, is there any incentive for an SV to price differently based on consumer logical network and his security investment amount when it could transfer a part of his current profits to the insurance business and always make strictly positive profits?* The answer to this question is an yes and the reason is three fold: (i) a rational firm would not mind finding a way to make more profits than their current scenario, and from principles of basic economics, pricing based on increased client information results in more profits [25], (ii) the amount of security investments of users results in unpaid positive externalities for other users in the logical network and these externalities need to be accounted for in some manner to ensure a certain price fairness amongst consumers[4], and (iii) specifically when an SV is the cyber-insurer, our proposed pricing philosophy would allow appropriate contracts (with fines/rebates) to be handed out to consumers buying insurance. For example, a consumer who generates a high amount of externality would be priced less for SV products than a consumer generating a low amount of externality, and as a result the latter might end up paying a fine, whereas the former consumer might get a rebate on his premium.

4.5 Defining The Pricing Model

We assume that each SV (seller) has a set of clients, N, (consumers) connected via a logical network and using self-defense products manufactured by the SV. *For simplicity of analysis, we assume that a single SV has monopoly and serves all clients in a logical*

[4] A SV can get investment related information from its insurance clients (and hence estimate externalities) through disclosure agreements signed between the client and the SV as part of some mandate imposed by the government [8].

network. Each consumer $i \epsilon N$ has an utility function, $u_i(\cdot)$, which is given as

$$u_i(x_i, \overrightarrow{x_{-i}}, p_i) = \alpha_i x_i - \beta_i x_i^2 + x_i \cdot \sum_j h_{ij} x_j - p_i x_i, \tag{4.1}$$

where x_i, a continuous variable, is the amount of self-defense/self-protection features consumed or invested in by user i, $\overrightarrow{x_{-i}}$ is the vector of self-defense investments of users other than i, and p_i is the price charged by the SV to user i per unit of self-defense investment consumed by i. In reality, SV products are bundled in a package which is priced as a single item. However, every bundled package has a number of features which different users use differently, and the effectiveness of a user's security protection would depend on how he uses those features (personal communication with Symantec employee). In that light, we assume that x_i is continuous. Here p_i is the equilibrium market price set by the SV (in case of a competitive setting, the equilibrium price is set after competing with other SVs in the security product business.). $\alpha_i, \beta_i, h_{ij}$ are constants. h_{ij} is the amount of externality user j exerts on user i through his per unit investments. Here $h_{ij} \geq 0$ and $h_{ii} = 0, \forall i$. x_i is assumed to be continuous for analysis tractability reasons. The first and second term in the utility function denotes the utility to a user solely dependent on his own investments, the third term is the positive externality effects of investments made by other users in the network on user i, and the fourth term is the price user i pays for consuming x_i units of self-defense goods manufactured by the SV. We assume here that x_i is bounded. The quadratic nature of the utility function allows for a tractable analysis and a nice second-order approximation of concave payoffs.

The SV accounts for the strategic investment behavior (after it would have set its prices) of users it provides service to, and decides on an optimal pricing scheme that arises from the solution to the following optimization problem.

$$max_{\overrightarrow{p}} \sum_i p_i x_i - c x_i,$$

where $\overrightarrow{p}$ are the vectors of prices charged by the SV to its consumers, and x_i is the amount of self-defense good consumed by consumer i after the SV sets its prices. c is the constant marginal cost to the SV to manufacture a unit of any of its products. For the analysis that follows in the dissertation, we will assume for all i, (i) $2\beta_i > \sum_{j\,\epsilon\,N} h_{ij}$ and (ii) $\alpha_i > c$. Assumption (i) implies that the optimal investment level of network users is bounded and assumption (ii) implies that all network users purchase a positive amount of security product manufactured by the SV.

4.6 Security Product Pricing Strategies

In this section we describe our two-stage static pricing game between an SV and its consumers and state state the different pricing scenarios we deal in the chapter.

4.6.1 Two-Stage Pricing Game Definition

The game has the following two steps.

1. The SV chooses a price vector $\overrightarrow{p}$ so as to maximize its profits via the following optimization problem.

   $$max_{\overrightarrow{p}} \sum_i p_i x_i - c x_i,$$

   where $\overrightarrow{p}$ is price vector charged by the SV to its consumers, per unit of investment, and x_i is the amount of self-defense good consumed (invested) by user i after the SV sets its prices.

4.6.2 The Different Pricing Scenarios

We consider three types of consumer pricing scenarios in the chapter:

- ***Scenario 1*** - here, the SV does not price discriminate amongst its consumers and all elements of $\overrightarrow{p}$ are identical, i.e., $p_i = p$, $\forall i$.
- ***Scenario 2*** (binary pricing) - here, the SV charges two types of prices per unit of user investment: a regular price denoted as p_{reg} for each user in a particular category, and a discounted price, denoted as p_{dsc} for other users, and
- ***Scenario 3*** - here, the SV charges different prices to different consumers and the elements of $\overrightarrow{p}$ are non-identical. c is the constant marginal cost to the SV to manufacture a unit of any of its products.

2. Consumer i chooses to consume x_i units of self-defense products, so as to maximize his utility $u_i(x_i, , \overrightarrow{x_{-i}}, p_i)$ given the prices chosen by the SV.

Since the game consists of two stages, we will analyze the subgame perfect Nash equilibria of this game, instead of just focussing on simple Nash equilibria.

4.7 Results for Homogenous and Heterogenous Pricing Schemes

In this section we state the results related to our static pricing strategy. We first comment on the equilibrium of the second stage of the two-stage pricing game, *given* a vector of prices $\overrightarrow{p}$ (not specific to the scenarios mentioned above). Given $\overrightarrow{p}$, the second stage of our pricing game is a subgame and we denote it as G^{sub}. We the have the following theorem.

Theorem 5. *G^{sub} has a unique Nash equilibrium and is represented in closed form as*

$$x_i = BR(\overrightarrow{x_{-i}}) = \frac{\alpha_i - p_i}{2\beta_i} + \frac{1}{2\beta_i}\sum_{j \epsilon N} h_{ij}x_j, \tag{4.2}$$

where $BR(\overrightarrow{x_{-i}})$ is the strategic best response of user i when other users in the network consume $\overrightarrow{x_{-i}}$. In the case when SV does not price discriminate its consumers, the Nash equilibrium vector of user investments is given by

$$\overrightarrow{x} = (Q - G)^{-1}(\overrightarrow{\alpha} - p\,\overrightarrow{1}), \tag{4.3}$$

where p is the optimal uniform per unit investment price charged by the SV to all its consumers, and Q is a matrix that takes values $2\beta_i$ at location (i, j) if $i = j$ and zero otherwise.

Proof: The proof relies on the results on the following lemmas. We first state and prove the relevant lemmas required for the proof of Theorem 5 and follow it up with the proof of the main theorem.

Lemma 1. *The game G^{sub} is supermodular*[5]*.*

Proof. The payoff/utility functions are continuous, the strategy sets are compact subsets of real space, and for any two consumers $i, j\, \epsilon N$, $\frac{\partial^2 u_i}{\partial x_i \partial x_j} \geq 0$. Hence G^{sub} is supermodular. ■

Lemma 2. The spectral radius of $Q^{-1}G$ is smaller than 1, and the matrix $I - Q^{-1}G$ is invertible.

Proof. Let $\overrightarrow{v}$ be an eigenvector of $Q^{-1}G$ with λ being the corresponding eigenvalue, with $|v_i| > |v_j|$ for all $j\,\epsilon\,N$. We have the following equation due to the fact that $(Q^{-1}G)\overrightarrow{v} = \lambda\overrightarrow{v}$.

$$|\lambda v_i| = |(Q^{-1}G_i)\overrightarrow{v}| \leq \sum_{j\,\epsilon\,N}(Q^{-1}G)_{ij}|v_j| \leq \frac{1}{2\beta_i}|v_i|\sum_{j\,\epsilon\,N} h_{ij} < \frac{v_i}{2}. \tag{4.4}$$

[5] In supermodular games, the marginal utility of increasing a player's strategy increases with the increases in the other players' strategies.

Here $(Q^{-1}G)_i$ denotes the $i-th$ row of $(Q^{-1}G)$. Since the equation holds for any eigenvalue-eigenvector pair, the spectral radius of $(Q^{-1}G)$ is strictly smaller than 1. Now observe that each eigenvalue of $I - Q^{-1}G$ can be written as $1 - \lambda$. Since the spectral radius of $Q^{-1}G$ is strictly smaller than 1, none of the eigenvalues of $I - Q^{1}G$ is zero, and thus the matrix is invertible. ■

Now we continue with the proof of Theorem 5. Since G^{sub} is a supermodular game, the equilibrium set has a minimum and a maximum element [43]. Let $\overrightarrow{x}$ denote the maximum of the equilibrium set and let S be such that $x_i > 0$ only if $i \in S$. If $S = \phi$ there cannot be another equilibrium point, since $\overrightarrow{x} = 0$ is the maximum of the equilibrium set. Assume for a contradictory purpose that $S \neq \phi$ and there is another equilibrium $\overrightarrow{\tilde{x}}$, of the game. By the supermodularity property of G^{sub}, $x_i \geq \tilde{x}_i, \forall i \in N$. Allow k to equal $argmax_{i \in N} x_i - \tilde{x}_i$. Since $\overrightarrow{x}$ and $\overrightarrow{\tilde{x}}$ are not equal, we have $x_k - \tilde{x_k} > 0$. Since at NE no consumer has an incentive to increase or decrease his consumption, we have

$$x_k - \tilde{x}_k \leq \frac{1}{2\beta_k} G_k(\overrightarrow{x} - \overrightarrow{\tilde{x}}) = \frac{1}{2\beta_k} \sum_j h_{kj}(x_j - \tilde{x_j}), \tag{4.5}$$

where G_k is the $k-th$ row of G. But we have

$$\frac{1}{2\beta_k} \sum_j h_{kj}(x_j - \tilde{x_j}) \leq \frac{x_k - \tilde{x}_k}{2\beta_k} \sum_j h_{kj} < x_k - \tilde{x_k} \tag{4.6}$$

Thus, we reach a contradiction and G^{sub} has a unique Nash equilibrium. ■

Theorem Intuition and Implications: The intuition behind a unique Nash equilibrium is the fact that increasing one's consumption incurs a positive externality on his peers, which further implies that the game involves *strategic complementarities*[6] [25], and therefore the equilibria are ordered. This monotonic ordering results in a unique NE. The unique equi-

[6] In economics and game theory, the decisions of two or more players are called strategic complements if they mutually reinforce one another.

librium implies that the SV just needs to be concerned about the single equilibrium vector of user consumption amounts and base its optimal strategy on that equilibrium vector. If there would be multiple equilibria to G^{sub}, it would be cumbersome for the SV to decide on its optimal strategy. Why? because it would be difficult for non-cooperative users to decide in the first place which equilibrium is the best and then jointly play the best equilibria. As a result the SV might not be sure that the best equilibrium would be played by the users. However, if the SV is able to compute the best equilibria, it could base its pricing strategy on that one irrespective of the equilibria played by the users.

We now discuss the optimal pricing strategy for the SV given that the users self-protect according to the Nash equilibrium of G^{sub}. Before going into the details we first define the concept of a Bonacich centrality in a network of heterogenous users. The Bonacich centrality measure [9] is a sociological graph-theoretic measure of network influence. It assigns relative influence scores to all nodes in the network based on the concept that connections to high-scoring nodes contribute more to the score of the node in question than equal connections to low-scoring nodes. In our work, the Bonacich measure of a user reflects his influence on other users of the network via the externalities generated by him through his self-defense investments[7]. Formally, let G be a matrix defining the logical network of N users (consumers), and having in its entries the h_{ij} values. Let D be a diagonal matrix, and $\overrightarrow{w}$ be a weight vector. The weighted Bonacich centrality vector is given by

$$B(G, D, \overrightarrow{w}) = (I - GD)^{-1}\overrightarrow{w}, \tag{4.7}$$

where $(I - GD)^{-1}$ is well-defined and non-negative.

We now have our first result regarding the optimal prices charged by the SV to its consumers.

[7] The use of the concept of Bonacich centrality in externality driven networks is explained in [10]

Theorem 6. *The optimal price vector $\overrightarrow{p}$ charged by the SV is given by*

$$\overrightarrow{p} = \frac{\overrightarrow{\alpha} + c \cdot \overrightarrow{1}}{2} + GQ^{-1}B(G', Q^{-1}, \overrightarrow{w'}) - G^TQ^{-1}B(G', Q^{-1}, \overrightarrow{w'}), \tag{4.8}$$

where $G' = \frac{G+G^T}{2}$ and $\overrightarrow{w'} = \frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}$.

In the case when the SV does not price discriminate its consumers, the optimal price (same for every consumer) charged per consumer is given by

$$p = \frac{1}{2}\frac{\overrightarrow{1}^T(Q-G)^{-1}(\overrightarrow{\alpha} + c\,\overrightarrow{1})}{\overrightarrow{1}^T(Q-G)^{-1}\overrightarrow{1}}. \tag{4.9}$$

Proof. We have from Lemma 1 that $Q - G$ is non-singular and as a result the following equation holds.

$$\overrightarrow{p} = \overrightarrow{\alpha} - (Q-G)\left(Q - G - \frac{G^T - G}{2}\right)^{-1}\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2} \tag{4.10}$$

Equation (4.10) can we rewritten as

$$\overrightarrow{p} = \overrightarrow{\alpha} - \left(I - \frac{G^T - G}{2}(Q-G)^{-1}\right)^{-1}\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2} \tag{4.11}$$

By the *matrix inversion lemma* [26], we have

$$\left(I - \frac{G^T - G}{2}(Q-G)^{-1}\right)^{-1} = I + \frac{G^T - G}{2}\left(Q - \frac{G^T + G}{2}\right)^{-1} \tag{4.12}$$

Thus, from Equation (4.11) it follows that

$$\overrightarrow{p} = \frac{\alpha + c\,\overrightarrow{1}}{2} - \frac{G^T - G}{2}\left(Q - \frac{G^T + G}{2}\right)^{-1}\frac{\overrightarrow{\alpha} - c\,\overrightarrow{1}}{2} \tag{4.13}$$

Applying Equation(4.13) and using the definition of weighted Bonacich centrality, we get

$$\overrightarrow{p} = \frac{\overrightarrow{\alpha} + c \cdot \overrightarrow{1}}{2} + GQ^{-1}B(G', Q^{-1}, \overrightarrow{w'}) - G^{T}Q^{-1}B(G', Q^{-1}, \overrightarrow{w'})$$

and thus prove Theorem 6. ■

Theorem Intuition and Implications: The optimal price vector in the no price discrimination case is independent of individual node centralities, whereas in the price discrimination case the optimal price vector depends on the Bonacich centrality of individual users. The intuition behind the result is the fact that users tend to invest in security mechanisms proportional to their Bonacich centrality (and in turn generate proportional amount of network externalities) in the Nash Equilibrium [37][38]. Therefore it makes sense for the SV to charge users based on their Bonacich centralities when price discrimination is possible.

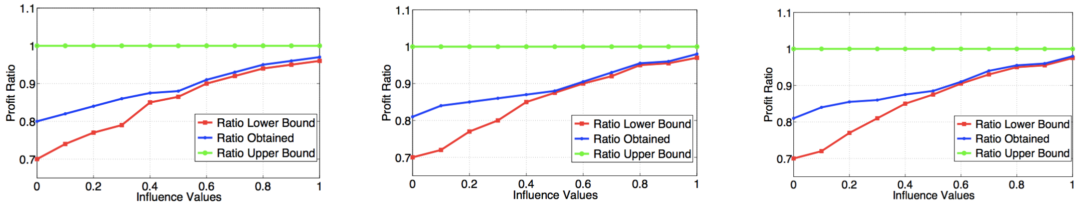


Figure 4.1: 100 Node Profit Ratio Plots for (a) $\beta = 3$ (left), (b) $\beta = 2.5$ (middle), and (c) $\beta = 2$ (right) [PA Graphs]

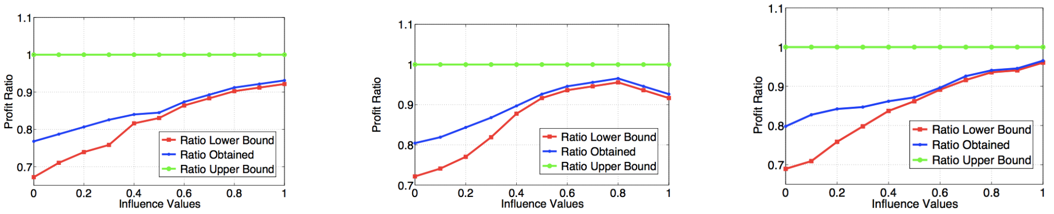


Figure 4.2: 500 Node Profit Ratio Plots for (a) $\beta = 3$ (left), (b) $\beta = 2.5$ (middle), and (c) $\beta = 2$ (right) [PA Graphs]

We now state the following result regarding profit amounts made by a SV from its cyber-insurance business for pricing scenarios 1 and 3.

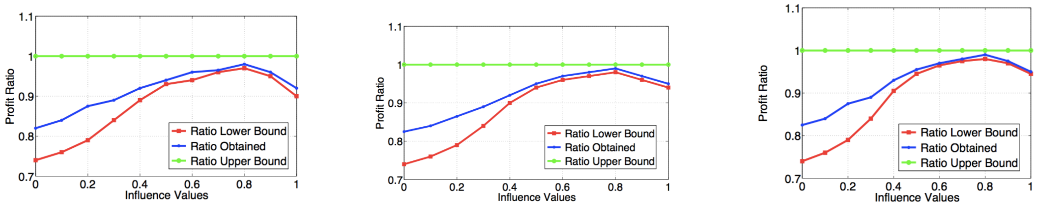


Figure 4.3: 100 Node Profit Ratio Plots for (a) $\gamma = 1$ (left), (b) $\gamma = 3$ (middle), and (c) $\gamma = 5$ (right) [Tree Topology]

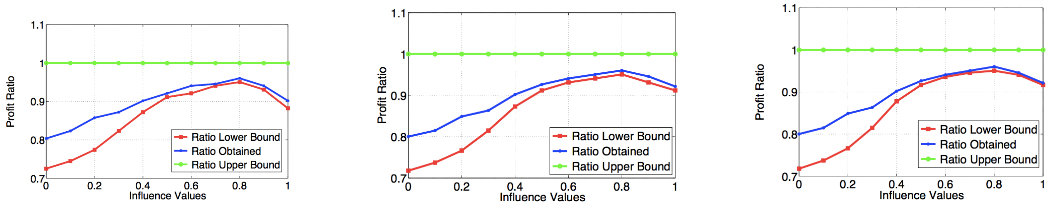


Figure 4.4: 500 Node Profit Ratio Plots for (a) $\gamma = 1$ (left), (b) $\gamma = 3$ (middle), and (c) $\gamma = 5$ (right) [Tree Topology]

Theorem 7. *The profits, P_0 and P_1, made by an SV from its cyber-insurance business when the latter does not (does) account for user investment externalities respectively are given by*

$$P_0 = \left\{ \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2} \right)^T (Q - G)^{-1} \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2} \right) \right\} \tag{4.14}$$

and

$$P_1 = \left\{ \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2} \right)^T (Q - G')^{-1} \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2} \right) \right\}, \tag{4.15}$$

. Assuming $Q - G$ to be positive definite, the bounds of the ratio of profits in these two cases is given by

$$0 \leq \frac{1}{2} + \lambda_{min}(K) \leq \frac{P_0}{P_1} \leq \frac{1}{2} + \lambda_{max}(K) \leq 1, \tag{4.16}$$

where $R = Q - G$ and $\lambda_{min}(\cdot)$, $\lambda_{max}(\cdot)$ denote the minimum and maximum eigenvalues of their arguments respectively, and K equals $\left(\frac{RR^{-T} + R^T R^{-1}}{4}\right)$.

Proof: The optimal price vector of the SV without and with the consideration of externality effects are given by the following equations.

$$\overrightarrow{p_0} = \frac{\overrightarrow{\alpha} + c \cdot \overrightarrow{1}}{2}. \tag{4.17}$$

and

$$\overrightarrow{p_1} = \overrightarrow{\alpha} - (Q - G)\left(Q - \frac{G + G^T}{2}\right)^{-1} \frac{\alpha - c \cdot \overrightarrow{1}}{2}. \tag{4.18}$$

The corresponding consumption vectors are given by

$$\overrightarrow{x_0} = (Q - G)^{-1} \frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}. \tag{4.19}$$

and

$$\overrightarrow{x_1} = (Q - G')^{-1} \frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}. \tag{4.20}$$

It then follows that

$$P_0 = (\overrightarrow{p_0} - c \cdot \overrightarrow{1})^T \overrightarrow{x_0} = \frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2} (Q - G)^{-1} \frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}. \tag{4.21}$$

and

$$P_1 = (\overrightarrow{p_1} - c \cdot \overrightarrow{1})^T \overrightarrow{x_1}, \tag{4.22}$$

P_1 can be re-written as

$$P_1 = X - Y,$$

where

$$X = 2\left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}\right)^T \left(\frac{R + R^T}{2}\right)^{-1} \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}\right),$$

and

$$Y = \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}\right)^T \left(\frac{R + R^T}{2}\right)^{-1} \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}\right).$$

Thus, we have

$$P_1 = \left\{ \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}\right)^T (Q - G')^{-1} \left(\frac{\overrightarrow{\alpha} - c \cdot \overrightarrow{1}}{2}\right) \right\},$$

Now let $\overrightarrow{v} = \frac{\alpha - c \cdot \overrightarrow{1}}{2}$. We have

$$\frac{P_1}{P_0} = \frac{\overrightarrow{v}^T (Q - G')^{-1} \overrightarrow{v}}{\overrightarrow{v}^T (Q - G)^{-1} \overrightarrow{v}} \leq max_{||\overrightarrow{x}=1||} \frac{\overrightarrow{x}^T \left(\frac{R+R'}{2}\right)^{-1} \overrightarrow{x}}{\overrightarrow{x}^T \frac{R^{-1}+R^{-T}}{2} \overrightarrow{x}}. \tag{4.23}$$

Since $\frac{R^{-T}+R^{-1}}{2}$ and $\frac{R^T+R}{2}$ are symmetric positive definite matrices, we have from the Rayleigh-Ritz Theorem [18] the following.

$$K = \lambda_{max} \left(\left(\frac{R^{-1} + R^{-T}}{2}\right)^{-0.5} \left(\frac{R + R^T}{2}\right)^{-1} \left(\frac{R^{-1} + R^{-T}}{2}\right)^{-0.5} \right), \tag{4.24}$$

where $K = max_{||\overrightarrow{x}=1||} \frac{\overrightarrow{x}^T \left(\frac{R+R'}{2}\right)^{-1} \overrightarrow{x}}{\overrightarrow{x}^T \frac{R^{-1}+R^{-T}}{2} \overrightarrow{x}}$. Note that for any real matrix A and invertible matrix B, the eigenvalues of A and $B^{-1}AB$ are identical. Thus, it follows that

$$K = \lambda_{max} \left(\frac{2I + RR^T + R^T R^{-1}}{4}\right)^{-1}. \tag{4.25}$$

Now since the eigenvalues of $RR^{-T} + R^T R^{-1}$ are real and belong to $[-2, 2]$, the eigenvalues of $\left(\frac{2I+RR^T+R^TR^{-1}}{4}\right)$ are positive, and we have

$$\lambda_{max} \left(\frac{2I + RR^T + R^T R^{-1}}{4}\right)^{-1} = \frac{1}{\lambda_{min}} \left(\frac{2I + RR^T + R^T R^{-1}}{4}\right). \tag{4.26}$$

Similarly we obtain

$$max_{||\overrightarrow{x}=1||}\frac{\overrightarrow{x}^T \frac{R^{-1}+R^{-T}}{2} \overrightarrow{x}}{\overrightarrow{x}^T \left(\frac{R+R'}{2}\right)^{-1} \overrightarrow{x}} = \lambda_{max}\left(\frac{2I + RR^T + R^T R^{-1}}{4}\right). \tag{4.27}$$

From the above two equations it follows that

$$\frac{1}{2} + \lambda_{min}\left(\frac{2I + RR^T + R^T R^{-1}}{4}\right)^{-1} \leq \frac{P_0}{P_1}, \tag{4.28}$$

and

$$\frac{P_0}{P_1} \leq \frac{1}{2} + \lambda_{max}\left(\frac{2I + RR^T + R^T R^{-1}}{4}\right)^{-1}. \tag{4.29}$$

We have thus proved our theorem. ■.

Before we explain the theorem intuitions and its implications, we plot the ratio of $\frac{P_0}{P_1}$ for *preferential attachment* (PA) graphs in Figures 4.1 and 4.2 and tree graphs in Figures 4.3 and 4.4, respectively, as they help us understand the theorem implications better. The following section briefly explains the formation of graphs using the preferential attachment process and how tree topologies are formed. The theorem intuitions and its implications will also be explained in the following section.

4.8 Generating Practical Networking Topologies

In this section we briefly describe the process of generating practical networking topologies for the purposes of simulation. We deal with two graph types: (i) random graphs generated via the preferential attachment mechanism, and (ii) random trees generated via a Poisson process.

We choose preferential attachment graphs as they represent real world social/logical network interactions [5]. A random graph formed by the PA process can have two extremes: (i) a new born user can influence users born earlier, i.e., $G^1_{ij} > 0$ for all i, j and j born after i, and (ii) only older users influence new users, i.e., $G^1_{ij} > 0$ for all i, j and j born before i. We can thus form a family of PA graphs parameterized by $\mu \epsilon [0, 1]$, which we call the 'influence value', such that G^μ is a linear combination of G^1 and G^2, i.e., $G^\mu = \mu G^1 + (1 - \mu)G^2$. Here μ is a parameter that controls the influencing nature of a user in a PA graph w.r.t. the positive externality effects of his security investments made on users born before and after him. A μ value of 1 generates random graph G^1, whereas a μ value of 0 generates random graph G^2. For networks of size 100, we generate 50 PA graphs for each different value of μ ranging from 0 to 1 in steps of 0.1. Each point in a sub-plot in Figure 4.1 is the average of the 50 $\frac{P_0}{P_1}$ values obtained per value of μ (the x-axis). Each sub-plot is the average of 50 graphs for a particular value of γ, the scale-free exponent parameter for PA graphs, β (in many papers also denoted as γ) is known to generally lie between $[2, 3]$, and for our plots we choose three values of β: 2, 2.5, and 3. For the purposes of simulation we assume for all i that $\beta_i = 1$ and $\alpha_i - c = 1$. We also assume that for each i the h_{ij} values are equal to $\frac{1}{d_i}$, where d_i is the number of non-negative entries in row i of G. We repeat the above process for networks of size 500, and the results are shown in Figure 4.2.

We choose tree topologies as they often represent corporate and enterprise social networks. In this work, we consider random trees of specific types. Given a constant $\lambda > 0$, a depth-d Poisson tree $T(\lambda, d)$ with parameter λ and depth d is constructed as follows: the root node has degree which is a random variable distributed according to a Poisson distribution with parameter λ. All the children of the root have outdegrees which are also random, distributed according to a Poisson λ distribution. We continue this process until either the process stops at some depth $d' < d$, where no nodes in level d' has any children or until we reach level d. In this case, all the children of nodes in level d are deleted and the nodes in level d becomes leaves. In this paper, we fix $d = \infty$. Note that star topologies are formed as a special case of tree topologies. We generate $\frac{P_0}{P_1}$ plots for tree graphs of size 100 and 500 nodes in Figures 4.3 and 4.4 respectively, in the same manner as we generate

PA graphs in the previous paragraph, i.e., based on influence values. Each point in the sub-plots is the average of 50 instances for a fixed value of λ. For our work we fix λ to lie in the set $\{1, 3, 5\}$. For the purposes of simulation we assume for all i that $\beta_i = \frac{|G|}{20}$ and $\alpha_i - c = 1$. We also assume that for each i the h_{ij} values are equal to $\frac{1}{d_i}$, where d_i is the number of non-negative entries in row i of G.

Plot Results: Our plot results from both the preferential attachment and tree topology graphs show that (i) the provable *profit ratio bounds are not reasonably tight enough, and are less than 1*[8], implying the fact that an SV can do better in terms of profit when it has full information compared to the case when it is not informed about consumer externality values and their network location properties, and (ii) the gap between the ratio obtained from simulations and its lower bound decreases with increase in μ (influence) values. The reason for the trend in (ii) can be explained as follows: note that the gap between the ratio obtained by simulations and its lower bound denotes the profit loss of the security vendor from ignoring the network externalities during the pricing process. This gap will be larger for lower values of μ as it implies that nodes with higher centrality values are affecting nodes with low centrality values and the insurer is not taking this externality into account while charging its clients, thereby reducing profits. When μ values are high, the insurer does not take into account the externality effects of low centrality users on high centrality users, which does not affect the profits as much.

Theorem Intuition and Implications: As observed from the plot in Figures 4.1 and 4.2, for preferential attachment graphs, the profits to the SV are greater when it accounts for externalities than when it does not, and an SV could make up to approximately 25% extra profits (relative to our model) with complete information. This is intuitive in the sense that the SV has more user information when knowing about the externalities and can price optimally to

[8] Here '1' is the trivial upper bound. However, for the simulations in this work, the non-trivial upper bound obtained is very close to 1.

increase its profits. However, in reality it is difficult to measure/observe the externalities. Thus, in spite of getting topological information from the insurer, an SV might have to price its products without taking externalities into account. The profits for the non price discrimination scenario is encapsulated as a special case of P_1 when G has all entries equal except the zero diagonal entries. *We also emphasize here that even in the absence of complete information, partial information will boost SV profits in a proportional manner.* We also observe from Figures 4.1 and 4.2 that (i) the plot trends are invariant of the graph topology, i.e., with different β values, the sub-plots look very nearly the same, and (ii) increasing the network size does not affect the plot trends as well.

4.9 Plot Results for Profit Ratios

In this section, we describe the plot results for SV profit ratios between the case when network externalities are accounted for in the pricing mechanism and the case when they are not.

Our plot results for tree graphs are very similar to those of preferential attachment graphs and due to the same reasons mentioned in the previous paragraph, except that for influence values between 0.7 and 1.0, the profit ratio curve increases towards values in the range [.95 .99] and then decreases. This trend is due to the fact that at an influence value of around 0.8, the graph topology and investment externalities have little effect on the optimal prices charged by the SV, and as a result the difference between P_0 and P_1 is minimal. Intuitively, this happens because when deciding what price to offer to a user, the monopolist considers the trade-off between profit loss due to (potentially) subsidizing the user and increase in profits due to the user's externality influence over his peers. The profit loss is proportional to the security investment of the user, and it increases with the influence of the network on this user. The profit increase term, on the other hand relates to the influence of the agent on the rest of the network. At an influence value of 0.8, the profit loss nearly equals profit gain and network and externality effects does not affect the profit ratio by a significant margin. For all other influence values, the effects of the network and investment externalities are more than non-signifcant. We emphasize here that the rationale proposed in this paragraph also applies to the trends observed on preferential attachment graphs, but there the peak point is achieved for an influence value of 1.

Implementation Remarks and Practical Challenges: Here, we discuss a little on how measuring network externalities is difficult, and why we only model a monopoly SV scenario. In practice, it is really difficult to compute the h_{ij} values. One can at best approximate or stochastically estimate it. Realistically speaking, the entire networking space can hardly be monopolized by a single SV cyber-insurer. In case of corporate settings, it is relatively easier to estimate externalities as the corporate network is administered by one entity. In case of non-corporate settings, it may be really hard to estimate externalities because of two reasons: (i) there might be users of SV X who may be connected to users of SV Y and X may not have relevant details of clients of Y to measure externalities, unless X and Y form an alliance with the same ISP and trade externalities, and (ii) if insurance is not made compulsory (as the current scenario in the Internet) some users who generate high amount of externalities may not be held accountable and externalities due to them might not be estimable. Because of the difficulty to measure network externalities even in the case of a single SV domain, and the challenges to allocate externality liabilities amongst consumers of different co-existing SVs with overlapping consumer overlay networks, we only model a monopoly SV scenario in this work. The Bonacich centrality measure can however be exactly computed given the logical network structure of consumers. However, in practice multiple SVs will co-exist in a market, and as mentioned before, even partial information on consumer investments and related externalities will improve profit margins for individual SVs. In the case a logical network consists of disjoint large subnetworks or sparsely overlapping networks, insurance sellers (SVs) would segment the market at equilibrium and exercise monopoly pricing power in their respective localities. When networks are considerably overlapping it would be difficult for any SV to exercise monopoly pricing of its products. However, in reality there is some heterogeneity between product types of sellers which leads to one being more popular than others, and as a result sellers could have a slight pricing power over their consumers.

4.10 The Case for Binary Pricing

In reality, charging multiple different prices to various consumers may not be very practical to implement. To make things simpler, a SV can opt to charge two types of prices for two different classes of consumers: (i) a discounted price, p_{dsc}, for consumers who have significant positive influence on the security of a network based on their network location and the amount of investments made, (ii) and a regular price, p_{reg} for the other consumers. Thus, the first goal of an SV is to determine the subset of consumers that should be offered the discounted price so as to maximize its own profits.

Given that p_{reg} and p_{dsc} are exogenously specified, the profit optimization problem for an SV is given by

$$Maximize\ (\overrightarrow{p} - c\,\overrightarrow{1})^T(Q - G)^{-1}(\overrightarrow{\alpha} - \overrightarrow{p})$$

$$s.t.\ p_i \,\epsilon\, \{p_{reg}, p_{dsc}\},\ \forall i \,\epsilon\, N.$$

Note here that the expression, $(Q - G)^{-1}(\overrightarrow{\alpha} - \overrightarrow{p})$, in the objective function is the NE investment amount of users in self-defense mechanisms. Thus, we have a combinatorial optimization problem for maximizing the profits of an SV. In order to investigate the tractability of the problem, we formulate it in the following manner:

$$OPT: \ Maximize \ (\delta\overrightarrow{y} + c'\overrightarrow{1})^T(Q-G)^{-1}(\overrightarrow{\alpha'} - \delta\overrightarrow{y})$$

$$s.t. \ y_i \,\epsilon\, \{-1, 1\}, \ \forall i \,\epsilon\, N.$$

Here $\delta = p_{reg} - p_T$, where $p_T = \frac{p_{reg}+p_{dsc}}{2}$, $\overrightarrow{a'} = \overrightarrow{a} - p_T$, and $c' = p_T - c \geq \delta$. Note that using these variables, the feasible price allocation can be expressed as $\overrightarrow{p} = \delta\overrightarrow{y} + p_T$. Our next result comments on the intractability of solving OPT. The proof of the result is based on the reduction of OPT from the well-known MAX-CUT problem [12].

Theorem 8. *Given that p_{reg} and p_{dsc} are exogenously specified in the binary pricing case, an SV's profit optimization problem, OPT, is NP-Hard.*

Proof: The well known MAX-CUT problem [12] is as follows:

$$max \sum_{(i,j)\,\epsilon\, E} W_{ij}(1 - x_i x_j)$$

$$s.t. \, x_i \,\epsilon\, \{-1, +1\}, \ \forall i \,\epsilon\, V,$$

where W denotes a matrix of binary weights consisting of 0s and 1s. The solution to this problem corresponds to a cut as follows: let S be the agents who were assigned value 1 in the optimal solution. Then it is straightforward to see that the value of the objective function corresponds to the size of the cut defined by S and $V - S$. The problem can also be re-wriiten as

$$P0: \ min \, \overrightarrow{x}^T W \overrightarrow{x}$$

$$s.t. \, x_i \,\epsilon\, \{-1, +1\}, \ \forall i \,\epsilon\, V.$$

Now consider the following related problem:

$$P1: \ min \, \overrightarrow{x}^T W \overrightarrow{x}$$

$$s.t. \, x_i \, \epsilon \, \{-1, +1\}, \, \forall i \, \epsilon \, V,$$

where W is a symmetric matrix with rational entries that satisfy $0 < W^T = W < 1$. In the proof of Theorem 8, we will first show that $P1$ is NP-Hard by reducing from MAX-CUT. We will then reduce P1 to OPT to claim the correctness of our theorem.

Lemma 3. *P1 is NP-Hard.*

Proof. We prove our claim by reducing P1 from P0. Let W be the weight matrix in an instance of P0. Let $W_\epsilon = \frac{1}{2}(\epsilon + W)$, where ϵ is a rational number between 0 and $\frac{1}{2n^2}$ and $|V| = n$. Observe that for any feasible $\overrightarrow{x}$ in P0 or P1, it follows that

$$2\overrightarrow{x}^T W_\epsilon(\overrightarrow{x}) - n2\epsilon \leq \overrightarrow{x}^T W \overrightarrow{x} \leq 2\overrightarrow{x}^T W_\epsilon(\overrightarrow{x}) + n2\epsilon.$$

Because the objective of P0 is always an integer and $n^2\epsilon < \frac{1}{2}$, the cost of P0 for any feasible vector $\overrightarrow{x}$ can be obtained from the cost of P1 by scaling and rounding. Therefore, since P0 is NP-Hard, it follows that P1 is also NP-Hard. ■.

Having proved P1 to be NP-Hard, we now prove Theorem 4 by reducing OPT from P1. We consider special instances of OPT where $G = G^T$, $c = 0$, and $\overrightarrow{\alpha} = [\alpha, ..., \alpha]$, and $\alpha = p_{reg} + p_{dsc}$. OPT can then be re-casted as

$$OPT2: \ min \, \overrightarrow{x}^T (Q - G) \overrightarrow{x}$$

$$s.t. \, x_i \, \epsilon \, \{-1, +1\}, \, \forall i \, \epsilon \, N.$$

Now consider an instance of P1 with $W > 0$. Note that because $x_i^2 = 1$, P1 is equivalent to

$$min\,\overrightarrow{x}^T(W + \gamma I)\overrightarrow{x}$$

$$s.t.\, x_i \,\epsilon\, \{-1, +1\},\; \forall i \,\epsilon\, V,$$

where we choose γ as an integer such that

$$\gamma > 4 \cdot max\{\rho(W), \sum_{i,j} \frac{W_{i,j}}{min_{i,j} W_{ij}}\}$$

and $\rho(\cdot)$ is the spectral radius of its argument. The definition of γ implies that the spectral radius of $\frac{W}{\gamma}$ is less than 1. Therefore we have

$$(W + \gamma I)^{-1} = \frac{1}{\gamma}\left(I - \frac{1}{\gamma}(W - \frac{W^2}{\gamma}) - \frac{W^2}{\gamma^3}(W - \frac{W^2}{\gamma}).....\right). \tag{4.30}$$

Since all entries of W and $\left(W - (\frac{W^2}{\gamma})\right)$ are positive, the above equality implies that the off-diagonal entries of $(W + \gamma I)^{-1}$ are negative. Therefore $(W + \gamma I)^{-1} = (Q - G)$ for some diagonal matrix Q and some $G \geq 0$. Thus, it follows that

$$((Q - G)\overrightarrow{1})_k = \left(\frac{1}{\gamma}\left(I - \frac{W}{\gamma} + \frac{W^2}{\gamma^2}....\right)\overrightarrow{1}\right)_k. \tag{4.31}$$

Since $W > 0$, we have

$$((Q - G)\overrightarrow{1})_k \geq \frac{1}{\gamma}\left(1 + \left(-\frac{W\overrightarrow{1}}{\gamma}) - \frac{W^2\overrightarrow{1}}{\gamma^2}....\right)_k \overrightarrow{1}\right).$$

From the definition of γ it follows that $\frac{W\overrightarrow{1}}{\gamma} \leq (\frac{(\sum_{i.j} W_{ij})}{\gamma})\overrightarrow{1} \leq \frac{1}{4}\overrightarrow{1}$. The above inequality implies that

$$((Q-G)\overrightarrow{1})_k \geq \frac{1}{\gamma}\left(1-\frac{1}{4}\left(\sum_{l=0}^{\infty}\left(\frac{1}{4}\right)^l\right)\right) = \frac{1}{\gamma}\left(\frac{2}{3}\right) > 0. \tag{4.32}$$

Thus, P1 can be reduced to an instance of OPT2 by defining Q and G according to $(W + \gamma I)^{-1} = (Q - G)$. Therefore it follows that OPT2, and hence OPT, are NP-Hard. ■.

Theorem Intuitions and Implications: The i, jth entry of $(Q - G)^{-1}$ gives a measure of how much the edge between i and j contributes to the centrality of agent i. Therefore, the MAX-CUT interpretation roughly suggests that the optimal solution of the pricing problem is achieved when the monopolist tries to price discriminate agents that influence each other significantly, however, at the same time takes into account the agents' value of consumption in the absence of network effects. The NP-Hard nature of the pricing problem implies the impracticality of computing optimal prices in practice and thus drives the need to design schemes to computing optimal binary prices up to a certain acceptable approximation. The following theorem states the result of approximating the optimal prices charged in the binary pricing case. The theorem exploits the relation of OPT to the MAX-CUT problem, and establishes that there exists an algorithm that provides a solution with a provable approximation guarantee.

Theorem 9. *Let W_{OPT} be the optimal value for problem OPT. Then, there exists a randomized polynomial-time algorithm that outputs a solution with objective value W_{alg} such that $E[W_{alg}] + r > 0.878(W_{OPT} + r)$, where*

$$r = \delta^2 \overrightarrow{1}^T A \overrightarrow{1} + \delta \overrightarrow{1}^T |A\overrightarrow{a'} - A^T c' \overrightarrow{1}| - c' \overrightarrow{1}^T A \overrightarrow{a'} - 2\delta^2 Trace(A),$$

and

$$A = (Q - G)^{-1}$$

Proof. First, we describe a semidefinite programming (SDP) relaxation for the following optimization problem:

$$max\frac{1}{4}\sum_{i,j} w_{ij}(1 - x_i x_j))$$

subject to

$$x_i \,\epsilon\, \{-1, +1\}\, \forall i \,\epsilon\, V$$

This optimization problem can be reduced to

$$max\frac{1}{4}\sum_{i,j} w_{ij}(1 - \nu_i \nu_j)$$

subject to

$$\nu_i \,\epsilon\, S_n \,\forall i \,\epsilon\, V$$

where $\nu_i \cdot \nu_j$ denotes the regular inner product of vectors $\nu_i, \nu_j \,\epsilon\, \mathbb{R}^n$, and S_n denotes the n-dimensional unit sphere, i.e., $S_n = \{\overrightarrow{x} \,\epsilon\, \mathbb{R}^n | \overrightarrow{x} \cdot \overrightarrow{x} = 1\}$.. We next show that this optimization problem leads to a semidefinite program.

Consider the collection of vectors $\{\nu_1, ..., \nu_n\}$ such that $\nu_i \,\epsilon\, S_n$. Define a symmetric matrix $Y \,\epsilon\, \mathbb{R}^{n \times n}$ such that $Y_{ij} = \nu_i \nu_j$ and $Y_{ii} = 1$. It can be seen that $Y = F^T F$. where $F \,\epsilon\, R^{n \times n}$ is such that $F = [\nu_1, ..., \nu_n]$. This implies that $Y \geq 0$. Conversely, consider a positive semidefinite matrix $Y \,\epsilon\, \mathbb{R}^n$ such that $Y_{ii} = 1$. Since Y is positive semidefinite, there exists $F \,\epsilon\, \mathbb{R}^{n \times n}$ (which can be obtained from Cholesky factorization of the original matrix) such that $Y = F^T F$, it follows that $\nu_i \cdot \nu_i = 1$. These arguments imply that the feasible set in

$$max\frac{1}{4}\sum_{i,j} w_{ij}(1 - \nu_i \nu_j)$$

subject to

$$\nu_i \,\epsilon\, S_n \,\forall i \,\epsilon\, V$$

can be equivalently written as

$$max\frac{1}{4}\sum_{i,j} w_{ij}(1 - \nu_i\nu_j)$$

subject to

$$Y_{i,i} = 1\, \forall i\, \epsilon\, V,\, Y \geq 0$$

We now show a way to obtain a provable approximation guarantee for binary quadratic optimization problems of the form:

$$max\,\overrightarrow{x}^T Q \overrightarrow{x} + 2\,\overrightarrow{d}^T \overrightarrow{x} + z$$

subject to

$$x_i\,\epsilon\,\{-1, 1\},\; i\,\epsilon\,\{1, ..., n\},$$

where Q, $\overrightarrow{d}$, and $\overrightarrow{z}$ have rational entries. We observe that $\overrightarrow{x}^T Q \overrightarrow{x} = Trace(Q) + \overrightarrow{x}^T \tilde{Q} \overrightarrow{x}$, where $\tilde{Q} = Q - diag(Q)$ and $x_i\,\epsilon\,\{-1, +1\}$. Thus, the diagonal entries of the Q matrix as part of the constant term, and we can assume that $diag(Q) = 0$ without any loss of generality. We can also assume that Q is symmetric. Now consider the following optimization problem:

$$max[\overrightarrow{x}; y]^T Q'[\overrightarrow{x}; y] + z$$

subject to

$$x_i\,\epsilon\,\{-1, +1\},\; i\,\epsilon\,\{1, ..., n\},$$

$$y_i\,\epsilon\,\{-1, +1\},$$

where Q' is given by the following matrix:

$$Q' = \begin{pmatrix} Q & \overrightarrow{d} \\ \overrightarrow{d}^T & 0 \end{pmatrix}.$$

Since $[\overrightarrow{x}; y]^T Q' [\overrightarrow{x}; y] = \overrightarrow{x}^T Q \overrightarrow{x} + 2y \overrightarrow{d}^T \overrightarrow{x}$, it follows that the optimal $\overrightarrow{x}$ and the optimal objective values of the previous two optimization problems are equal. Relaxing the previous optimization problem we get

$$max \sum_{ij} \nu_i \cdot \nu_j Q'_{ij} + z$$

subject to

$$\nu_i \, \epsilon \, S_{n+1}, \; i \, \epsilon \, \{1, ..., n, n+1\},$$

and obtain an equivalent semidefinite program (SDP) by defining $Y_{ij} = \nu_i \nu_j$ as follows:

$$max \sum_{ij} Y_{ij} Q'_{ij} + z\}$$

subject to

$$Y_{ii} = 1, \; i \, \epsilon \, \{1, ..., n, n+1\},$$

$$Y \geq 0.$$

Using this semidefinite relaxation one can obtain an approximate solution to the original problem. We adopt an approach used by the authors in [13] to achieve this goal. We have the following lemma to characterize the approximate solution to our semi-definite program.

Lemma 4. *Let $z \geq \sum_{i,j} |Q'_{ij}|$. The solution to the following optimization problem:*

$$max \overrightarrow{x}^T Q \overrightarrow{x} + 2 \overrightarrow{d}^T \overrightarrow{x} + z$$

subject to

$$x_i \,\epsilon\, \{-1, 1\},\; i \,\epsilon\, \{1, ..., n\},$$

using the randomized algorithm in [13] achieves at least 0.878 times the optimal objective value of the problem.

Proof. Let W denote the objective value of a solution the algorithm provides. W_M denote the optimal solution of the underlying quadratic optimization mentioned in the lemma, and W_P denote the optimal value of the SDP relaxation, then the corresponding optimal value can be given as

$$W_P = \sum_{i,j} Q'_{ij} \nu_i \cdot \nu_j + z.$$

The solutions of the problem provided by the randomized algorithm in [13] gives us the expected contribution of given agents i and j to the objective function as $Q'_{ij}\left(1 - 2\frac{arccos(\nu_i,\nu_j)}{\pi}\right)$. Hence, the expected value of a solution is given as

$$E[W] = \sum_{ij}\left(1 - 2\frac{arccos(\nu_i, \nu_j)}{\pi}\right) Q'_{i,j} + z.$$

Now since $z \geq \sum_{i,j} |Q'_{ij}|$, it follows that both W_M and $E[W]$ are non-negative, also since W_P corresponds to the optimal solution of the relaxation, it follows that $W_P \geq W_M$. Using these it follows that

$$W_P = \sum_{i,j:Q'_{ij}>0} Q'_{ij}(1 + \nu_i \cdot \nu_j) + \sum_{i,j:Q'_{ij}<0} |Q'_{ij}(1 - \nu_i \cdot \nu_j) + z_2$$

and

$$E[W] = W_1 + W_2.$$

where

$$W_1 = \sum_{i:jQ'_{ij}>0} Q'_{ij}\left(2 - 2\frac{arccos(\nu_i,\nu_j)}{\pi}\right)$$

and

$$W_2 = \sum_{i,j:Q'_{ij}<0} |Q_{ij}|2\frac{arccos(\nu_i,\nu_j)}{\pi} + z_2.$$

Here $z_2 = z - \sum_{i,j}|Q'_{ij}| > 0$. Since $\frac{arccosx}{\pi} \geq \frac{\alpha}{2}(1-x)$ and $1 - \frac{arccosx}{\pi} \geq \frac{\alpha}{2}(1+x)$ for all $x \,\epsilon\, [-1,+1]$, it follows that $E[W] > 0.878W_P \geq 0.878W_M$, where $\alpha = 0.878$. ■
A corollary of this result is

$$E[W] + \sum_{ij}|Q'_{ij}| - z > 0.878(W_M + \sum_{ij}|Q'_{ij}| - z).$$

Applying this corollary, the solution to the pricing problem of the monopolist leads to satisfying the claims in Theorem 8. ■

Theorem Implications: Clearly, if $m \leq 0$, which, for instance, is the case when is δ is small, this algorithm provides at least an 0.878-optimal solution of the problem. On the other hand, if $m > 0$, we obtain 0.878 optimality after a constant (m) addition to the objective function. This suggests that for small $m > 0$, the algorithm still provides near-optimal solutions.

4.11 Performance Evaluation

In the previous sections in this chapter, we looked at how network externalities can affect the profit ratios of secuity vendors. We performed simulations on practical networking topologies to validate our theory. In this section, we study how the different pricing methodologies are affected by the client location in a network, and how the resulting prices affect the security investment amounts of the clients, and the fairness of their charged prices. We compare the pricing rules developed in the previous chapter and obtain qualitative insights by applying them to examples generated via simulations. In particular, we consider random networks that consist of 50 and 100 nodes, and generated via the same preferential attachment and Poisson tree mechanisms mentioned in previous chapter post the definition of Theorem 7.

4.11.1 Questions We Address

Through our simulations we aim to address the following questions.

- In case of the heterogenous pricing scenario , how does the unit price charged by the SV per client at market equilibrium vary with client centrality in the consumer logical network ?
- For any given pricing scenario, how does the network location of a consumer relate with his total security investment amount ?
- For the three pricing scenarios, does the total cost incurred by a client (the product of the unit price charged to him by the SV, and his net investment) in security investments vary from client to client based on their network location?

4.11.2 Simulation Setup

In this section, we describe our simulation setup. The parameters of the problem for our example networks of 50 and 100 nodes are given as follows: $c = 0.5, \alpha_i = 2$, $\beta_i = 2.5$ (for the preferential attachment mechanism), and $\beta_i = \frac{|G|}{20}$ (for random trees), for all $i \,\epsilon\, N$. The parameters α_i and β_i are chosen to make sure that the utility function of each client is twice differentiable and strictly increasing. We assume that the influence matrix G is such that for all i, h_{ij} equals $\frac{1}{d_i}$, where d_i is the number of non-negative entries in row i of G.

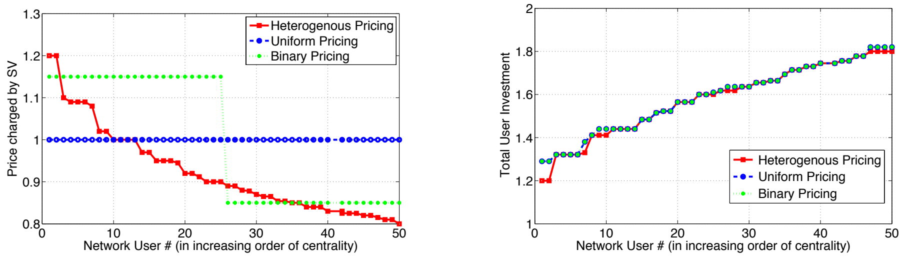


Figure 4.5: 50-Node Plots for (a) Per-Unit SV Prices (left) and (b) Total User Investment when $\beta = 3$ (right) (PA Graph Topology)

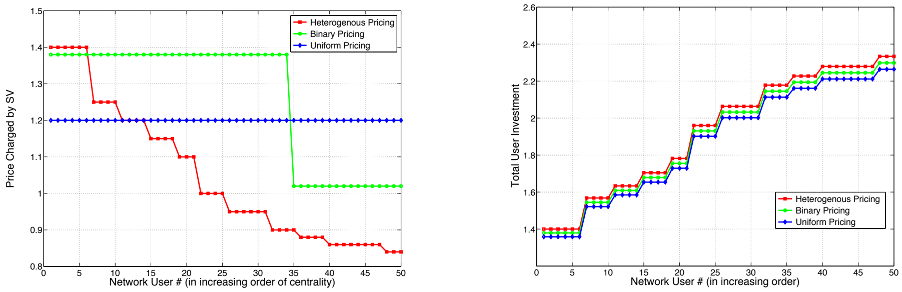


Figure 4.6: 50-Node Plots for (a) Per-Unit SV Prices (left) and (b) Total User Investment when $\lambda = 3$ (right) (Tree Topology)

In this setting, we first consider a 50-node scenario for graphs generated using the PA and random tree approaches. If the monopolist is only allowed to charge a uniform per-unit price to all its clients, the optimal such price is computed to be $p_0 = 1$ per-unit of investment, for one instance of a 50-node (user) PA generated network with $\beta = 3$. For the same network instance we plot the heterogenous prices charged to users, in Figure 4.5(a). We observe that the per-unit prices decrease with the increase in the centrality of nodes.

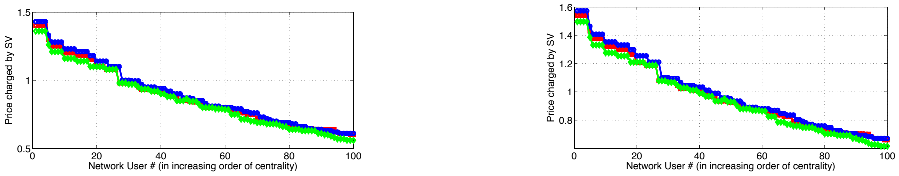


Figure 4.7: [Heterogenous Pricing] 100-Node Plots for Per-Unit SV Prices when (a) $\beta = 3$ (left) and (b) $\beta = 2.5$ (right)

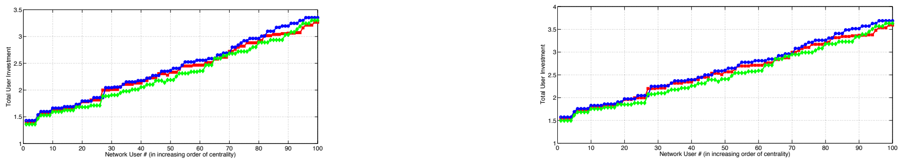


Figure 4.8: [Heterogenous Pricing] 100-Node Plots for Total User Investment when (a) $\beta = 3$ (left) and (b) $\beta = 2.5$ (right)

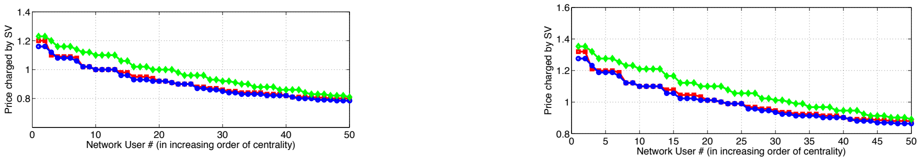


Figure 4.9: [Heterogenous Pricing] 50-Node Plots for Per-Unit SV Prices when (a) $\beta = 3$ (left) and (b) $\beta = 2.5$ (right)

For the two-prices case, we assume that the prices are given exogenously and are equal to $p_L = 0.85$, and $p_H = 1.15$, i.e., 15 percent deviation from the optimal single price. We emphasize here that our value of 15% is arbitrarily chosen. We just make sure that $p_L < p_H$ and that these prices differ by practical industry margins. Next, we compute the optimal user investment for that same 50-node network instance, when (i) the monopolist can only use the binary pricing scheme, and (ii) when it can perfectly price discriminate.

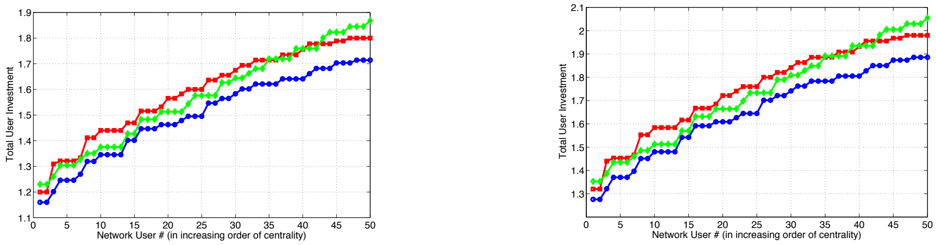


Figure 4.10: [Heterogenous Pricing] 50-Node Plots for Total User Investment when (a) $\beta = 3$ (left) and (b) $\beta = 2.5$ (right)

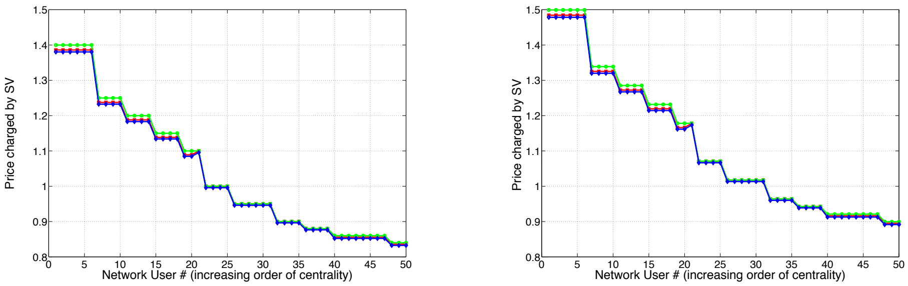


Figure 4.11: [Heterogenous Pricing] 50-Node Plots for Per-Unit SV Prices when (a) $\lambda = 3$ (left) and (b) $\lambda = 5$ (right)

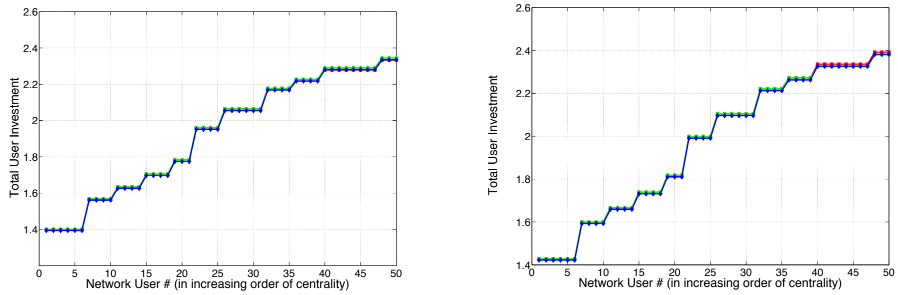


Figure 4.12: [Heterogenous Pricing] 50-Node Plots for Total User Investment when (a) $\lambda = 3$ (left) and (b) $\lambda = 5$ (right)

4.11.3 Results

The corresponding total consumption levels for all users for the three different pricing scenarios are given in Figure 4.5(b). We repeat the same process mentioned in this paragraph for an instance of a 50-node graph formed using the random tree generation process. We report the results in Figure 4.6. The results suggest that for each of the three pricing scenarios, the resulting consumption (amount in security investments) profiles are very similar. We observe that the agents who are the most influential, i.e., influence the rest of the agents more than they are influenced, consume the largest amounts of the good. This observation supports the result in [37][38]. Moreover, as predicted by our analysis, it is precisely these agents that are offered the most favorable prices (in the heterogenous pricing case) by the monopolist (as seen from Figures 4.5(a) and 4.6(a).). Finally, even when the monopolist is

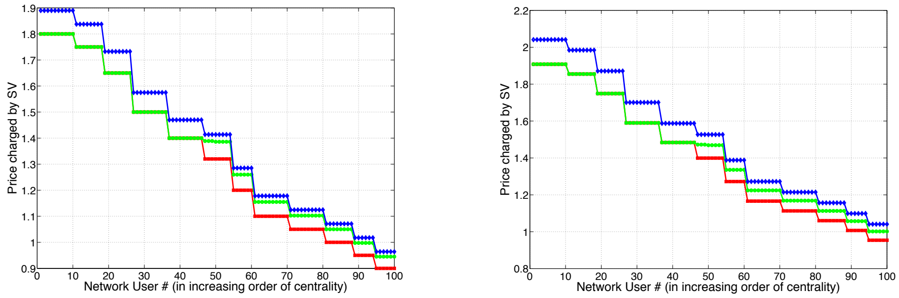


Figure 4.13: [Heterogenous Pricing] 100-Node Plots for Per-Unit SV Prices when (a) $\lambda = 3$ (left) and (b) $\lambda = 5$ (right)

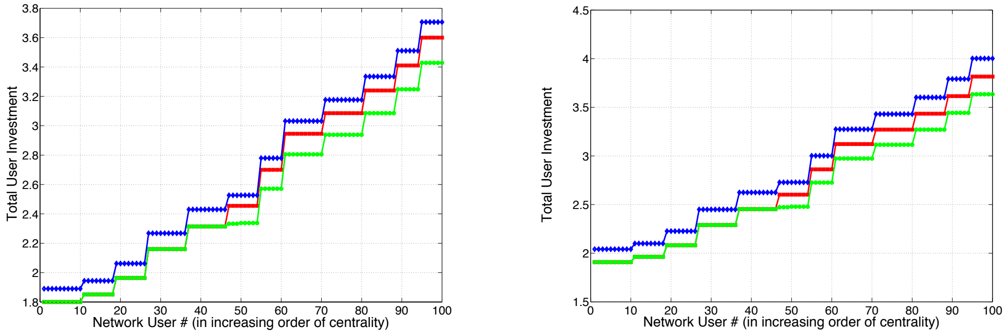


Figure 4.14: [Heterogenous Pricing] 100-Node Plots for Total User Investment when (a) $\lambda = 3$ (left) and (b) $\lambda = 5$ (right)

constrained to charging two prices, it tries again to favor those central agents, who end up getting the discounted price (see Figures 4.5()a and 4.6(a).).

After generating single instances of a 50 node network for both the PA and tree topology types, we try different sets of 50-node and 100-node networks with different values of β (for PA graphs) and γ (for random trees) to observe network effects on the per-unit SV prices and individual total investment amounts. From Figures 4.7.-4.10 (for PA graphs), and Figures 4.11-4.14 (for random tree graphs), we observe the same trends as in Figures 7.1 and 7.2 for the heterogenous pricing scheme, i.e., the per-unit price charged by the SV to its clients decreases with user Bonacich centrality, and total user investments per user increase with the user centralities in the network. Each of the sub-plots in Figures 4.7 to

4.10 and 4.11 to 4.14 plot results on three network instances for given (number of users, β), (number of users, γ) pairs.

For the heterogenous pricing case, we note from Figures 4.7- 4.10 that the product of the price charged per client with his total corresponding security investment is nearly the same constant for every user. This observation is favorable from a implementation viewpoint because a user would not prefer to pay a total cost of security investment that is more than any of the other users in the network, given that different network users are charged different prices. On the other hand, in the case of uniform and binary pricing, the product of price charged per client and their corresponding security investment is not a value that is same for every user. This is because of the fact that the users invest according to their Bonacich centrality in the network irrespective of the prices charged to them. In addition, from a psychological viewpoint users would not think too much on the variance in the net expenditure when SVs advertize at most two prices in the market compared to the case when the SV charges multiple per-unit prices.

A Note on Model Assumptions and Simulation Output: We made a few important assumptions for modeling purposes which we relax during our simulation setup to verify the strength and necessity of the assumptions. For simulation purposes we have not assumed $Q - G$ to necessarily be positive definite, and still we observe trends of profit ratio, $\frac{P_0}{P_1}$, to follow results in Theorem 7. This implies that Equation (4.14) does not strictly require $Q-G$ to be positive definite for it to hold, even though from an analysis perspective, positive definiteness of the matrix $Q - G$ ensures closed form expressions of $\frac{P_0}{P_1}$ bounds. We also do not enforce $2\beta_i > \sum_{j \epsilon N} h_{ij}$ for simulation purposes and observe that optimal user investments are bounded for many random samples of PA and Poisson tree topologies.

Takeaway Message in Relation to Network Effects: We have shown that pricing consumers based on their location and consumption amounts in a consumer overlay network is fair for each consumer (since the product of the consumption amount and the per unit price is nearly a constant for every user), and at the same time allows the SV to make more profits than it would make in case of uniform pricing (as in the current market scenario). The extra profits in turn allows the cyber-insurer to make strictly positive profits. In terms of differentiating cyber-insurance elements (e.g., fine, rebate, and safety capital amounts) from client to client, network centrality information is vital to proportion appropriate amounts of elements amongst clients based on the externality they generate due to their investments.

Chapter 5

Insurance Amidst Non-Insurable Risks

5.1 Chapter Introduction

The concept of cyber-insurance as proposed in the security literature covers losses only due to security attacks. However, in reality, security losses are not the only form of losses. Non-security losses (e.g., reliability losses) form a major loss type, where a user suffers, either because of hardware malfunction due to a manufacturing defect or a software failure (e.g., buffer overflow caused by non-malicious programming or operational errors[1])[17]. A naive Internet user would not be able to distinguish between a security or a non-security failure and might be at a disadvantage w.r.t. buying traditional cyber-insurance contracts. That is, on facing a risk, the user would not know whether the cause of the risk is a security attack or a non-security related failure[2]. The disadvantage is due to the fact that traditional cyber-insurance would only cover those losses due to security attacks, whereas an Internet user may incur a loss that occurs due to a non-security problem and not get covered for it[3]. In such cases, it is an interesting problem to investigate the demand for traditional cyber-insurance as it seems logical to believe that an Internet user might not be in favor of

[1] A buffer overflow can also be caused by a malicious attack by hackers. Example of such attacks include the Morris worm, Slapper worm, and Blaster worm attacks on Windows PCs.

[2] Irrespective of whether a loss due to a risk is because of a security attack or a non-security failure, the effects felt by a user are the same in both cases.

[3] We assume here that the loss covering agency can distinguish between both types of losses and it does not find it suitable to cover losses due to hardware or software malfunctions, as it feels that they should be the responsibility of the hardware and software vendors (e.g., some computer service agencies in India employ experts who could distinguish between the two loss types, and these experts may be hired by the loss recovery agency also.).

transferring complete loss recovery liability to a cyber-insurer as the former would would have to pay the premium and at the same time bear the valuation of the loss on being affected by non-security related losses. In this chapter, we analyze the situation of Internet users buying cyber-insurance when they face risks that may arise due to non-security failures or security attacks.

We propose an alternative and novel[4] model of cyber-insurance, Aegis, in which Internet users need not transfer the total loss recovery liability to a cyber-insurer, and may keep some liability to themselves, i.e., an Internet user may not transfer the entire risk to an insurance company. Thus, as an example, an Internet user may rest 80% of his loss recovery liability to a cyber-insurer and may want to bear the remaining 20% on his own. Our model captures the realistic scenario that Internet users could face risks from security attacks as well as from non-security related failures. It is based on the concept of co-insurance in the traditional insurance domain. We mathematically show that when Internet users are risk-averse, Aegis contracts are *always* the user preferred policies when compared to traditional cyber-insurance contracts. In this regard, the latter result de-establishes a market for traditional cyber-insurance. The availability of Aegis contracts also *incentivizes* risk-averse Internet users to rest some loss coverage liability upon themselves rather than shifting it all to a cyber-insurer. In addition we show that a risk-averse Internet user would prefer cyber-insurance of some type (Aegis or traditional) *only* if it is mandatory for him to buy some kind of insurance, given that he faces risks due to both, security as well as non-security failures. We also mathematically show the following counterintuitive results: (i) an increase

[4] Our cyber-insurance model is novel because we model partial insurance, whereas existing works related to traditional cyber-insurance model full and partial insurance coverage but not partial insurance. The notion of partial insurance can be explained as follows: in traditional cyber-insurance models, only the cyber-insurer has the say on the amount of coverage it would provide to its clients and in turn the premiums it would charge, whereas in the Aegis model, the clients get to decide on the fraction of the total amount of advertised insurance coverage it wants and in turn the proportional premiums it would pay, given an advertised contract. Thus, in traditional cyber-insurance, it is mandatory for users to accept the insurance policy in full, whereas in the Aegis model users have the option of accepting the insurance policy in partial.

in the premium of an Aegis contract *may not* always lead to a decrease in its user demand and (ii) a decrease in the premium of an Aegis contract may not always lead to an increase in its user demand. In the process, we also state the conditions under which these trends emerge. The conditions give a guideline to cyber-insurers on how to increase or decrease their premiums in order to increase user demands for cyber-insurance.

5.2 The Aegis Cyber-Insurance Model

We consider the scenario where an Internet user faces risks[5] that arise due to security attacks from worms, viruses, etc., as well as due to non-security related failures. One example of non-security related problems arises due to reliability faults. In a seminal paper [17], the authors identified operational and programming errors, manufacturing problems of software and hardware vendors, and buffer overflow as some examples of system reliability faults, which have effects on Internet users that are identical to the effects when they are affected by certain security threats (e.g., buffer overflow due to a malicious attack). On facing the negative effects, an Internet user in general cannot distinguish between the loss type. In this paper, we assume that a loss occurs either due to a security attack or a non-security related failure and not both, i.e., a unit of damage cannot occur simultaneously due to a security and a non-security failure. For example, a file or a part of it that has been damaged by a security attack cannot be damaged by a non-security fault at the same time.

We assume that cyber-insurers[6] offer Aegis contracts to their clients, Aegis contracts unlike traditional insurance contracts allow the user to rest some fraction of loss recovery liability upon itself. For example, if the value[7] of a loss incurred by an Internet user equals

[5] A risk is defined as the chance that a user faces a certain amount of loss.

[6] A cyber-insurer could be an ISP, a third-party agency, or the government.

[7] In this paper, like in all of existing cyber-insurance literature, we assume that loss and coverage have the same scalar unit. In reality, this may not be true. As an example, losing a valuable file may not be compensated

L, and the insurance coverage advertised by an insurer equals $L-d$, where $d \geq 0$, an Aegis contract would allow its client to rest a fraction, $1-\theta$, of the coverage on itself and the remaining θ part on the cyber-insurer, whereas a traditional contract would fix the value of θ to 1. Our concept of Aegis contracts are based on the theory of *co-insurance* in general insurance literature. It is logical to believe that a user will not prefer a $1-\theta$ value that is large as it would mean that it wants to rest a substantial loss recovery liability on itself, thereby diminishing the importance of buying cyber-insurance. We assume that the value of θ is fixed between the user and the cyber-insurer prior to contract operation.

Most of our analysis in the paper will revolve around the final wealth of a risk-averse Internet user who may be subject to risks due to both security attacks and non-security related failures. We have the following equation regarding its final wealth according to the Aegis concept:

$$W = w_0 + v - L_S - L_{NS} + \theta(I(L_S) - P), \tag{5.1}$$

where W is a random variable representing the final wealth of a user, $w_0 + v$ is his constant initial wealth, with v[8] being the constant total value of the object subject to loss as a result of a security attack or a non-security attack, L_S is a random variable denoting loss due to security attacks, L_{NS} is the random variable denoting loss due to non security related failures, and$I(L_S)$ is the cyber-insurance function that decides the amount of coverage to be provided in the event of a security-related loss, where $0 \leq I(L_S) \leq L_S$. We assume that both L_S and L_{NS} lie in the interval $[0, v]$. As mentioned previously, a given amount of loss can be caused either by a security attack or a by a non-security fault and not by both. In this sense the loss types are *not independent* but are *negatively correlated*. P is the

by replacing the same file. In return, monetary compensation may result. Considering appropriate units of loss and coverage is an area of future work.

[8] We divide the fixed initial wealth of a user into two parts for modeling simplicity.

premium[9] charged to users in insurable losses and is defined as $P = (1+\lambda)E(I(L_S))$. λ is the loading factor and is zero for fair premiums and greater than zero for unfair premiums. We define $\theta \,\epsilon\, [0, 1]$ as the *level of cyber-insurance liability* opted for by a user. For example, a value of $\theta = 0.6$, implies that the user transfers 60% of its insurance coverage liability to the cyber-insurer and keeps the rest 40% of the coverage liability on himself, where the insurance coverage could be either full or partial. We observe from Equation (1) that depending on the liability level, a user pays proportional premiums to the cyber-insurer.

We define the expected utility of final wealth[10] of an Internet user as

$$E(W) = A + B + C + D, \tag{5.2}$$

where

$$A = \int\int_{0<L_S\leq v, L_{NS}=0} u(w_0 + v - L_S - L_{NS} + \theta(I(L_S) - P)) \cdot g(L_S, L_{NS})dL_1 \cdot dL_{NS},$$

$$B = \int\int_{0<L_{NS}\leq V, L_S=0} u(w_0 + v - L_S - L_{NS} + \theta(I(L_S) - P)) \cdot g(L_S, L_{NS})dL_S \cdot dL_{NS},$$

$$C = \int\int_{0<L_S, 0<L_{NS}} u(w_0 + v - L_S - L_{NS} + \theta(I(L_S) - P)) \cdot g(L_S, L_{NS})dL_S \cdot dL_{NS},$$

and

$$D = \beta \cdot u(w_0 + v - \theta \cdot P),$$

with A, B, C, and D being the components of expected utility of final wealth when there is a loss due to a security attack only, a non-security related failure only, a security attack as well as a non-security related failure, and no failure of any kind, respectively. u is a twice

[9] P is the premium corresponding to a θ value of 1, where θ is the level of cyber-insurance liability opted by a user.

[10] In economic and risk analyses, dealing with the expected utility of final wealth is a standard approach and it arises from the von Neumann-Morgenstern model of expected utility [**?**].

continuously differentiable risk-averse concave utility function of wealth of a user.

We define the joint probability density function, $g()$, of L_S and L_{NS} as

$$g(L_S, L_{NS}) = \begin{cases} \alpha \cdot f_S(L_S) & 0 < L_S \leq v, L_{NS} = 0 \\ (1 - \alpha - \beta) \cdot f_{NS}(L_{NS}) & 0 < L_{NS} \leq v, L_S = 0, \\ 0 & 0 < L_S \leq v, 0 < L_{NS} \leq v \end{cases} \tag{5.3}$$

where α is the probability[11] of loss occurring due to a security attack, and β is the probability of no attack due to either a security or a non security attack. $f_S(L_S)$ and $f_{NS}(L_{NS})$ are the univariate density functions of losses due to a security attack and non security attack respectively. The joint probability density function has three components: 1) the case where there is a loss only due to a security attack, 2) the case when there is a loss only due to a non-security related failure, and 3) the case when a loss occurs due to both types of risks.

Based on $g()$, Equation (5.1) can be re-written as

$$E(W) = A1 + B1 + C1, \tag{5.4}$$

where

$$A1 = \int_0^v u(w_0 + v - L_S + \theta(I(L_S) - P))\alpha \cdot f_S(L_S) dL_S,$$

$$B1 = \int_0^v u(v_0 + v - L_{NS} - \theta(P))(1 - \alpha - \beta) \cdot f_{NS}(L_{NS}) dL_{NS},$$

and

$$C1 = \beta \cdot u(w_0 + v - \theta \cdot P),$$

with $A1$, $B1$, and $C1$ being the components of expected utility of final wealth when there is a loss due to a security attack only, a non-security related failure only, and no failure of

[11] We plan to estimate α using correlation models.

any kind, respectively.

5.3 Efficacy of Aegis Contracts

In this section, we investigate whether Aegis contracts are preferred by Internet users over traditional cyber-insurance contracts, and if yes, then under what conditions. In this regard, we state the following theorems that establish results regarding the user demand for Aegis contracts when compared to traditional cyber-insurance contracts.

Theorem 10. *Risk-averse Internet users always prefer Aegis contracts to traditional cyber-insurance contracts when non-insurable losses exist, irrespective of whether the cyber-insurance premium charged in an Aegis contract is fair* $(\lambda = 0)$ *or unfair* $(\lambda > 0)$ [12]

Proof. Taking the first derivative of $E(W)$ w.r.t. θ, and equating it to zero, we get the first order condition as

$$\frac{dE(W)}{d\theta} = A2 + B2 + C2 = 0, \tag{5.5}$$

where

$$A2 = \int_0^v u'(w_0 + v - L_S + \theta(I_{L_S} - P))(I(L_S) - P)\alpha \cdot f_S(L_S) dL_S,$$

$$B2 = \int_0^v u'(w_0 + v - L_{NS} - \theta(P))(-P)(1 - \alpha - \beta) \cdot f_{NS}(L_{NS}) dL_{NS},$$

and

$$C2 = \beta \cdot u'(w_0 + v - \theta \cdot P)(-P).$$

[12] The comparison is based on *equal* degrees of fairness or unfairness between an Aegis contract and a traditional cyber-insurance contract.

Now substituting $I(L_S) = L_S$ (indicating full coverage) and $\theta = 1$ (indicating no co-insurance) into the first order condition, we get

$$\frac{dE(W)}{d\theta} = A3 + B3 + C3 = 0, \tag{5.6}$$

where

$$A3 = \int_0^v u'(w_0 + v - P)(L_S - P)\alpha \cdot f_S(L_S)dL_S,$$

$$B3 = \int_0^v u'(w_0 + v - L_S - P)(-P)(1 - \alpha - \beta) \cdot f_{NS}(L_{NS})dL_{NS},$$

and

$$C3 = \beta \cdot u'(w_0 + v - P)(-P).$$

Re-arranging the integrals we get

$$A3 = u'(w_0 + v - P) \cdot \alpha \int_0^v (L_S - P)f_S(L_S)dL_S,$$

and

$$B3 = (-P)(1 - \alpha - \beta) \int_0^v u'(w_0 + v - L_{NS} - P)f_{NS}(L_{NS})dL_{NS},$$

Now using the fact that $E(I(L_S)) = \alpha \cdot \int_0^v L_S \cdot f_S(L_S)dL_S = P$ (fair premiums), we have the following equation

$$\frac{dE(W)}{d\theta} = A4 + B4, \tag{5.7}$$

where

$$A4 = u'(w_0 + v - P)(1 - \alpha - \beta)P$$

and

$$B4 = (-P)(1 - \alpha - \beta) \int_0^v u'(w_0 + v - L_{NS} - P)f_{NS}(L_{NS})dL_{NS}.$$

Since a user has a risk-averse utility function, we have $u'(w_0 + v - L_{NS} - P) > u'(w_0 + v - P) \forall L_{NS} > 0$. Thus, $\frac{dE(W)}{d\theta} < 0$ at $\theta = 1$. This indicates that the optimal value of θ is less than 1 for fair insurance premiums. On the other hand, even if we consider unfair premiums with a load factor $\lambda > 0$, we get $\frac{dE(W)}{d\theta} < 0$. Therefore in this case also the optimal value of θ is less than 1. ■

Implications of Theorem 10. The theorem implies that risk-averse users would always choose Aegis cyber-insurance contracts over traditional cyber-insurance contracts, when given an option.

Intuition Behind Theorem 10. In situations where a risk-averse user cannot distinguish between losses due to a security attack or a non-security failure, he would be conservative in his investments in insurance (as he could pay premiums and still not get covered due to a non-insurable loss) and would prefer to invest more in self-effort for taking care of his own system so as to minimize the chances of a loss. *Thus, in a sense the Aegis model incentivizes risk-averse Internet users to invest more in taking care of their own systems than simply rest the entire coverage liability upon a cyber-insurer.*

Theorem 11. *When risks due to non-insurable losses are increased in a first order stochastic dominant*[13] *sense, the demand for traditional cyber-insurance amongst all risk-averse Internet users decreases.*

Proof. Again consider the first order condition

$$\frac{dE(W)}{d\theta} = A2 + B2 + C2 = 0, \tag{5.8}$$

[13] Let X and Y be two random variables representing risks. Then X is said to be smaller than Y in first order stochastic dominance, denoted as $X \leq_{ST} Y$ if the inequality $VaR[X;p] \leq VaR[Y;p]$ is satisfied for all $p \,\epsilon\, [0,1]$, where $VaR[X;p]$ is the value at risk and is equal to $F_X^{-1}(p)$. First order stochastic dominance implies dominance of higher orders. We adopt the stochastic dominant approach to comparing risks because a simple comparison between various moments of two distributions may not be enough for a correct prediction about the dominance of one distribution over another.

where

$$A2 = \int_0^v u'(w_0 + v - L_S + \theta(I_{L_S} - P))(I(L_S) - P)\alpha \cdot f_S(L_S)dL_S,$$

$$B2 = \int_0^v u'(w_0 + v - L_{NS} - \theta(P))(-P)(1 - \alpha - \beta) \cdot f_{NS}(L_{NS})dL_{NS},$$

and

$$C2 = \beta \cdot u'(w_0 + v - \theta \cdot P)(-P).$$

We observe that when L_{NS} is increased in a first order stochastic dominant sense[14] and $f_S(L_S)$ and β remain unchanged, the premium for insurance does not change. An increase in L_{NS} in the first order stochastic dominant sense increases the magnitude of $\int_0^v u'(w_0 + v - L_{NS} - \theta(P))(-P)(1 - \alpha - \beta) \cdot f_{NS}(L_{NS})dL_{NS}$, whenever $u'(w_0 + v - L_{NS} - \theta(P))$ is increasing in L_{NS}. This happens when $u(W)$ is concave, which is the exactly the case in our definition of u. Thus, an increase in L_{NS} in a first order stochastic dominant sense leads to the first order expression, $\frac{dE(W)}{d\theta}$, to become increasingly negative and results in reductions in θ, implying the lowering of demand for cyber-insurance. ■

Implications of Theorem 11. The theorem simply implies the intuitive fact that an increase in the risk due to non-insurable losses leads to a decrease in the demand of traditional cyber-insurance contracts, irrespective of the degree of risk-averseness of a user.

Intuition Behind Theorem 11. The implications of Theorem 11 hold as the user would think that there are greater chances of it being affected by a loss and not being covered at the same time. An increase in the risk due to non-insurable losses also decreases the demand for Aegis contracts. However, according to Theorem 10, for the same amount of

[14] Let X and Y be two random variables representing risks. Then X is said to be smaller than Y in first order stochastic dominance, denoted as $X \leq_{ST} Y$ if the inequality $VaR[X;p] \leq VaR[Y;p]$ is satisfied for all $p \,\epsilon\, [0,1]$, where $VaR[X;p]$ is the value at risk and is equal to $F_X^{-1}(p)$. First order stochastic dominance implies dominance of higher orders. We adopt the stochastic dominant approach to comparing risks because a simple comparison between various moments of two distributions may not be enough for a correct prediction about the dominance of one distribution over another.

risk, Aegis contracts are preferred to traditional cyber-insurance contracts.

Theorem 12. When the risk due to non-insurable losses increases in the first order stochastic dominant sense, the expected utility of final wealth for any cyber-insurance contract (Aegis and traditional) falls when compared to the alternative of no cyber-insurance, for risk averse Internet users.

Proof. The expected utility of any cyber-insurance contract is given by the following

$$E(W) = A1 + B1 + C1, \tag{5.9}$$

where

$$A1 = \int_0^v u(w_0 + v - L_S + \theta(I(L_S) - P))\alpha \cdot f_S(L_S)dL_S,$$

$$B1 = \int_0^v u(w_0 + v - L_{NS} - \theta(P))(1 - \alpha - \beta) \cdot f_{NS}(L_{NS})dL_{NS},$$

and

$$C1 = \beta \cdot u(w_0 + v - \theta \cdot P).$$

When $\theta = 0$ (the case for no cyber-insurance), $E(W)$ reduces to

$$E(W) = A1' + B1' + C1', \tag{5.10}$$

where

$$A1' = \int_0^v u(w_0 + v - L_S)\alpha \cdot f_S(L_S)dL_S,$$

$$B1' = \int_0^v u(w_0 + v - L_{NS})(1 - \alpha - \beta) \cdot f_2(L_{NS})dL_{NS},$$

and

$$C1' = \beta \cdot u(w_0 + v).$$

Increases in L_{NS} affect only the second terms in each of these utility expressions. Thus, we need to consider the change in the second order terms in the two utility expressions to observe the impact of the increase in L_{NS}. The difference in the second order terms is given as

$$R1 - R2,$$

where

$$R1 = \int_0^v u(w_0 + v - L_{NS} - \theta(P))(1 - \alpha - \beta) \cdot f_{NS}(L_{NS})dL_{NS}$$

and

$$R2 = \int_0^v u(w_0 + v - L_{NS})(1 - \alpha - \beta) \cdot f_{NS}(L_{NS})dL_{NS}.$$

Thus, $R1 - R2$ evaluates to

$$\int_0^v [u(w_0 + v - L_{NS} - \theta(P)) - u(w_0 + v - L_{NS})](1 - \alpha - \beta) \cdot f_{NS}(L_{NS})dL_{NS},$$

where $[u(w_0+v-L_{NS}-\theta(P))-u(w_0+v-L_{NS})]$ is decreasing in L_{NS} under risk aversion and concave under user prudence. Thus, increases in L_{NS} in the first order stochastic dominant sense reduces the expected utility of cyber-insurance relative to no cyber-insurance. ■

Implications of Theorem 12. Theorem 12 provides us with an explanation of why risk-averse Internet users would be reluctant to buy cyber-insurance of any kind given an option between choosing and not choosing insurance, when risks due to non-security related losses are present along with risks due to security attacks.

Intuition Behind Theorem 12. Theorem 12 holds because the expected utility to a risk-averse Internet user opting for a zero level of cyber-insurance liability is greater than that obtained when he opts for a positive level of cyber-insurance liability.

Combining the results in Theorems 10, 11, and 12, we conclude the following:

- In the presence of non-insurable losses, the market for traditional cyber-insurance may not exist.

- When risk-averse Internet users have an option between traditional cyber-insurance, Aegis contracts, and no cyber-insurance, they may prefer the last option. Thus, Aegis contracts might be preferred by Internet users over traditional cyber-insurance contracts *only* if it is mandatory for them to buy some kind of insurance. In general, Internet service providers (ISPs) or cyber-insurance agencies might force its clients on regulatory grounds to sign up for some positive amount of cyber-insurance to ensure a more secure and robust Internet.

5.4 Sensitivity Analysis of User Demands

In this section we conduct a sensitivity analysis of user demands for Aegis contracts. We investigate whether an increase in the premium charged by a contract results in an increase/decrease in user demand for the contract. The user demand is reflected in the θ value, i.e., user demand indicates the fraction of loss coverage liability a risk-averse user is willing to rest on the cyber-insurance agency. In an Aegis contract, to avoid insurance costs not related to a security attack, a risk-averse user takes up a fraction of loss coverage liability on himself as it does not know beforehand whether he is affected by a security or a non security threat. Thus, intuitively, a decrease in a contract premium may not always lead to a user increasing his demand and analogously an increase in the premium may not always lead to a decrease in the user demands. The exact nature of the relationship between the premiums and user demand in this case depends on the degree of risk averseness of a user. To make the latter statement clear, consider an Internet user who is very risk averse. It would not matter to that user if there is a slight decrease in the premium amount because he might still not transfer additional loss coverage liability to the cyber-insurer, given that he is unsure about whether the risk he faces is due to a security attack or a non security related issue. On the other hand a not so risk averse user may not decrease the amount of loss coverage liability rested upon a cyber-insurer, even if there is a slight increase in the cyber-insurance premiums. In this section we study the conditions under which there is an increase/decrease of user demand for Aegis contracts with change in contract premiums. We first provide the basic setup for sensitivity analysis, which is then followed by the study of the analysis results.

5.4.1 Analysis Setup

Let a user's realized final wealth be represented as

$$W = w - L + \theta(L - P). \tag{5.11}$$

Substituting $P = \lambda' E(L)$, we get

$$W = w - L + \theta(L - \lambda' E(L)), \tag{5.12}$$

where λ' equals $(1 + \lambda)$, w is equal to $w_0 + v$, θ lies in the interval $[0, 1]$, $\lambda \geq 1$ is the gross loading factor of insurance, $L = L_S + L_{NS}$, and $\lambda E(L) = \alpha \int_0^v L \cdot f_S(L) dL$ is the premium payment for full insurance[15] with E being the expectation operator. The user is interested in maximizing his expected utility of final wealth in the von Neumann-Morgenstern expected utility sense and chooses a corresponding θ to achieve the purpose. Thus, we have the following optimization problem.

$$argmax_\theta E(U(W)) = E[U(w - L + \theta(L - \lambda' E(L))],$$

[15] By the term 'full insurance', we imply a user resting its complete loss liability on the cyber-insurer, i.e., $\theta = 1$. Full insurance here does not indicate full insurance coverage.

where $0 \leq \theta \leq 1$. The first order condition for an optimum θ is given by

$$E'_\theta(U(W)) = E[U'(W)(L - \lambda' E(L))] = 0, \tag{5.13}$$

which occurs at an optimal $\theta = \theta^*$. Integrating by parts the LHS of the first order condition and equating it to zero, we get

$$M1 + M2 = 0, \tag{5.14}$$

where

$$M1 = U'(W(0)) \int_0^v (L - \lambda' E(L)) dF_S(L)$$

and

$$M2 = \int_0^v U''(W(L))W'(L) \left(\int_L^v (t - \lambda' E(L)) dF_S(t) \right) dL.$$

Here $W(x)$ is the value of W at $L = x$ and $W'(L) = -(1 - \theta) \leq 0$. The second order condition is given by

$$E''_\theta(U(W)) = E[U''(W)(L - \lambda' E(L))^2] < 0, \tag{5.16}$$

which is always satisfied for $U'' < 0$. We now consider the following condition C, which we assume to hold for the rest of the paper.

Condition C - *The utility function U for a user is twice continuously differentiable, thrice piecewise continuously differentiable*[16] *and exhibits* $U' > 0$, $U'' < 0$ *with the coefficient of risk aversion,* A*, being bounded from above.*

The condition states the nature of the user utility function U, which is in accordance with the standard user utility function used in the insurance literature, with the additional restriction of thrice piecewise continuous differentiability of U to make the coefficient of

[16] We consider the thrice piecewise continuously differentiable property of U so that $A'(W)$ becomes piecewise continuous and is thus defined for all W.

risk aversion well-defined for all W. We adopt the standard *Arrow-Pratt* risk aversion measure [25], according to which the coefficient of risk aversion is expressed as (i) $A = A(W) = -\frac{U''(W)}{U'(W)}$ for an *absolute* risk averse measure and (ii) $R = R(W) = -\frac{WU''(W)}{U'(W)}$ for a *relative* risk averse measure.

5.4.2 Sensitivity Analysis Study

In this section we study the change in user demands for Aegis contracts with variations in cyber-insurance premiums, under two standard risk-averse measures: (1) the decreasing absolute risk averse measure and (2) the decreasing relative risk averse measure. The term 'decreasing' in both the risk measures implies that the risk averse mentality of users decrease with the increase in their wealth, which is intuitive from a user perspective. We are interested in investigating the sign of the quantity, $\frac{d\theta^*}{d\lambda'}$. The nature of the sign drives the conditions for an Aegis contract to be either more or less preferred by Internet users when there is an increase in the premiums, i.e., if $\frac{d\theta^*}{d\lambda'} \leq 0$, an increase in cyber-insurance premium implies decrease in user demand, and $\frac{d\theta^*}{d\lambda'} \geq 0$ implies an increase in user demand with increase in premiums.

We have the following theorem and its corresponding proposition related to the conditions under which Internet users increase or decrease their demands for Aegis contracts, when the users are risk-averse in an *absolute* sense.

Theorem 13. *For any arbitrary w, λ', F, and any U satisfying condition C, (i) $\frac{d\theta^*}{d\lambda'} \geq 0$ if and only if there exists $\rho \,\epsilon\, \mathbb{R}$ such that*

$$\int_L^w [A(W(x))\theta^*(x - \lambda' E(L)) - 1]dF(x) \geq \rho \int_L^w \theta^*(x - \lambda' E(L))dF(x), \qquad (5.17)$$

and (ii) $\frac{d\theta^*}{d\lambda'} < 0$ *if and only if there exists* $\rho \,\epsilon\, \mathbb{R}$ *such that*

$$\int_L^w [A(W(x))\theta^*(x - \lambda' E(L)) - 1]dF(x) < \rho \int_L^w \theta^*(x - \lambda' E(L))dF(x), \qquad (5.18)$$

where $L \,\epsilon\, [0, w]$ *and* $F(\cdot)$ *is the distribution function of loss* L*.*

Proof. We know that $\frac{d\theta^*}{d\lambda'} = -\frac{E'_{\theta\lambda'}}{E''_{\theta}}$. Now $\frac{d\theta^*}{d\lambda} \leq 0$ if and only if the following relationship holds because $E''_\theta < 0$.

$$E'_{\theta\lambda'}(U(W(L))) = E[-U''(W(L))\theta^* E(L)(L - \lambda' E(L)) - U'(W(L))E(L)] \leq 0 \quad (5.19)$$

or

$$E\left\{\left(A(W(L)) - \frac{1}{\theta(L - \lambda' E(L))}\right) U'(W(L))(L - \lambda' E(L)\right\} \leq 0 \qquad (5.20)$$

The LHS of Equation (5.19) can be expressed via integration by parts as

$$\int_0^w [A(W(L))\theta^*(L - \lambda' E(L)) - 1]U'(W(L))dF(L)$$

which evaluates to

$$X + Y,$$

where

$$X = U'(W(0)) \int_0^w [A(W(L))\theta^*(L - \lambda' E(L)) - 1]dF(L)$$

and

$$Y = \int_0^w U''(W(L))W'(L) \left\{ \int_L^w [A(W(t))\theta^*(x - \lambda' E(L)) - 1]dF(x) \right\} dL.$$

Now $X + Y \geq M + N$, where

$$M = U'(W(0)) \int_0^w \rho(L - \lambda' E(L)) dF(L)$$

and

$$N = \int_0^w U''(W(L))W'(L) \cdot \left(\rho \int_L^w (x - \lambda' E(L)) dF(x) \right) dL.$$

Thus, $\frac{d\theta^*}{d\lambda'} \geq 0$, and the sufficient condition is proved. The proof of the necessary condition follows from Proposition 1' in [15]. Reversing Equation (5.16) we get the necessary and sufficient conditions for $\frac{d\theta^*}{d\lambda'} \leq 0$, which is condition (ii) in Theorem 13. ■

Proposition 1. *There exists a $\rho \,\epsilon\, \mathbb{R} - \{0\}$ such that Theorem 4 holds if the following two conditions are satisfied.*

$$\frac{(1-\theta^*)A'}{A} \leq \theta^* A \tag{5.21}$$

and

$$\int_0^w A(W(L)) \left\{ L - \lambda' E(L) - \frac{1}{\theta^* A(W(L))} \right\} dF(L) > 0 \tag{5.22}$$

Proof. We observe the following relation

$$E1 < E2, \tag{5.23}$$

where

$$E1 = \int_0^w A(W(L)) \left\{ L - \lambda' E(L) - \frac{1}{\theta^* A(W(L))} \right\} dF(L)$$

and

$$E2 = \int_0^w A(W(L))(L - \lambda' E(L)) dF(L).$$

Thus, from Equation 21 in the theorem statement, we have

$$\int_0^w A(W(L))(L - \lambda' E(L))dF(L) > 0 \tag{5.25}$$

According to Lemma 2 in [15], there exists $\rho^* \,\epsilon\, \mathbb{R} - \{0\}$ such that the following relation holds for all $L \,\epsilon\, [0, w]$.

$$\int_L^w A(W(x))(x - \lambda' E(L))dF(x) \geq \rho^* \int_L^w (x - \lambda' E(L))dF(x) \tag{5.26}$$

Now, $\frac{d[L - \lambda' E(L) - (\theta^* A(W(L)))^{-1}]}{dL} \geq 0$ if and only if $(1 - \theta^* \frac{A'}{A} \leq \theta^* A$. Since both $L - \lambda' E(L))d(F(x)$ and $L - \lambda' E(L) - (\theta^* A(W(L)))^{-1}$ are increasing and become negative when L is sufficiently small, and using arguments presented in Lemma 2 in [15], we can show that Equations (5.21) and (5.22) imply

$$\int_L^w A(W(t))(t - \lambda' E(L))d(F(t) > 0 \tag{5.27}$$

and

$$\int_L^w A(W(t))[t - \lambda' E(L) - (\theta^* A(W(t)))^{-1}]dF(t) > 0. \tag{5.28}$$

for all $L \,\epsilon\, [0, w]$. Now choosing a $\delta > 0$ sufficiently small gives

$$P1 > P2 > 0, \tag{5.29}$$

where

$$P1 = \int_L^w A(W(t))[t - \lambda' E(L) - (\theta^* A(W(t)))^{-1}]dF(t)$$

and

$$P2 = \delta \int_L^w A(W(t))(t - \lambda' E(L))d(F(t),$$

for all $L \,\epsilon\, [0, w]$. Now, setting $\rho = \rho^* \delta$, we get for all $L \,\epsilon\, [0, w]$, the following relation

$$\int_L^w A(W(t))[t - \lambda' E(L) - (\theta^* A(W(t)))^{-1}]dF(t) \geq \rho \int_L^w (t - \lambda' E(L))dF(t) \quad (5.30)$$

This proves the proposition. ■

Notes on Theorem 13 and Proposition 1. Theorem 13 and Proposition 1 are related to each other in the sense that Theorem 13 provides the necessary and sufficient conditions under which Internet users increase/decrease demands of Aegis contracts. The intuition behind the result in Theorem 13 is based on expected utility comparisons. For an increase in the λ value, the expected utilities of a user are compared with and without a corresponding increase in θ value. We say that user demands for Aegis contracts increase (decrease) if there is an increase (decrease) in expected utility with an increase in the θ value, and we find the conditions for such situations to arise. Proposition 1 states that Theorem 13 always holds provided certain conditions are met.

We have the following theorem that states the conditions under which Internet users increase or decrease their demands for Aegis contracts, when the users are risk averse in a *relative* sense.

Theorem 14. *For any arbitrary w, λ', F,* and any *U satisfying condition C, (i)* $\frac{d\theta^*}{d\lambda'} \geq 0$ only if $R(W) > 1$ *and (ii)* $\frac{d\theta^*}{d\lambda'} < 0$ only if $R(W) \leq 1$, *where* $W \,\epsilon\, [W(w), W(0)]$.

Proof. We can rewrite Equation (5.16) as follows

$$\int_L^w \{\theta^*[A(W(x)) - \rho](x - \lambda' E(L)) - 1\}dF(x) \geq 0, \quad (5.31)$$

which can be further rewritten as

$$\int_L^w \{(R(W(x)) - 1) - A(W(x))(w_0 - x) - \rho(x - \lambda' E(L))\}dF(x) \geq 0. \quad (5.32)$$

The integral in Equation (5.23) is non-negative for all $L \epsilon [0, w]$ only if $R(W) > 1$ for some W. To see this it suffices to realize that $-A(W(L))(w_0 - L) < 0$ for all $L \epsilon [0, w)$ as $L \leq w_0$ and there exists $L \epsilon [0, w]$ at which $-\int_L^w \rho(L - \lambda' E(L))dF(x) < 0$ as $\int_L^w (x - \lambda' E(L))dF(x))$ alternates in sign on $(0, w)$. Now suppose by contradiction that $R(W) \leq 1$ for all W. Substituting this into Equation (5.23) violates the condition stated in Equation 22 for some $L \epsilon [0, w]$. Again by Theorem 13, we have that there exists utility function U satisfying condition C such that $\frac{d\theta^*}{d\lambda'} \geq 0$ - a contradiction. Since F is arbitrary, the result (i) in the theorem follows. By reversing the sign of the condition on $R(W)$ the result (ii) in the theorem follows. ■

Implications of Theorem 14. The theorem implies that above a certain level of the degree of relative risk averseness, a user prefers Aegis contracts even if there is an increase in contract premiums.

Intuition Behind Theorem 14. The coefficient of relative risk aversion is measured relative to the wealth of a user and thus more his wealth, lesser would be his concerns about losing money due to paying more cyber-insurance premiums, and not getting coverage on being affected by a non-security failure. The intuition is similar for the case when below a certain threshold of relative risk averseness, users reduce their demand for Aegis contracts.

Chapter 6

Insurance Under User Cooperation

6.1 Chapter Introduction

In none our previous chapters as well as in [24][21][42][28], the authors do not consider the *co-operative and the non-cooperative* nature of network users and the *effect* this has on the overall level of security and appropriate user self-defense investments. We note that the case of co-operating users is important for the following reasons: (1) It invites an opportunity for a user to benefit from the positive externality that its investment poses on the other users in the network, and (2) Although, the majority of Internet users today are non co-operative and selfish in nature, i.e., they are primarily interested in maximizing their own performance without caring for the overall system performance, there exist Internet applications where co-operation amongst users is encouraged (e.g., distributed file sharing in peer-to-peer environments, multicasting, and efficient network resource sharing). Although, in such applications Internet users co-operate to improve performance, it is *not evident* that the same users are incentivized to co-operate on their security parameters (e.g., self-defense investment) as well.

Hence in this chapter, we investigate the problem of appropriate self-defense investments under insurance regulation[1], *given* that Internet users are *fully* or *partially* covered by Internet insurance and that Internet users can be both, co-operative and non-co-operative *with respect* to their self-defense investment amounts.

[1] The term ‘insurance regulation’ refers to the act of making sure that insurance contracts are enforced by concerned parties in a proper and legal manner.

6.2 Economic Model

In this section, we give a brief description of a representative application, namely for ease of presentation we focus the discussion on botnet risks. We also give a description of our proposed model.

6.2.1 Representative applications

There are a number of applications where our model is useful. In this chapter, we describe ‘botnets’ as a representative example of Internet threats. That is, we use botnets here as a real and useful application; however our approach can be applied to other applications with direct/indirect risk scenarios (e.g., worms and viruses). A bot is an end-user machine containing code that can be controlled by a remote administrator (bot herder) via a command and control network. Bots are created by finding vulnerabilities in computer systems. The vulnerabilities are exploited with malware and the malware is then inserted into the systems. A bot herder can subsequently program the bots and instruct them to perform various types of cyber-attacks. A malware infected computing device is susceptible to information theft from it. The infected device can become part of a botnet and in turn can be used to scan for vulnerabilities in other computer systems connected to the Internet, thus creating a cycle that rapidly infects vulnerable computer systems. Hence, bots result in both direct and indirect losses. Direct losses result when the bot herder infects machines that lack a security feature, whereas indirect losses result due to the contagion process of one machine getting infected by its neighbors.

Risks posed by bots are extremely common and spread rapidly. In a recent study, Symantec corporation observed approximately five million distinct bot-infected computers within a period of just six months between July, 2007 and December, 2007[24]. We also assume that Internet users could buy insurance from their Internet service providers

(ISPs) to cover the risks posed by botnets. For instance, the coverage could be in the form of money or protection against lost data.

6.2.2 Model

We consider n identical[2] rational risk-averse users in a network. The users could be (1) entirely non co-operative in nature, i.e., the network supports Internet applications where users are not incentivized to co-operate with other users in any capacity (e.g., web surfing) or (2) co-operative to a variable degree, i.e, the network supports Internet applications where users co-operate with other users in some capacity to improve overall system performance but may or may not co-operate entirely. The users could either voluntarily co-operate by sharing information with other network users about their intentions to invest in self-defense, or be bound to co-operate due to a network regulation which requires participating users to share self-defense investment information. Each user has initial wealth w_0 and is exposed to a substantial risk of size R with a certain probability p_0. (Here, risk represents the negative wealth accumulated by a user when it is affected by botnet threats.) We also assume there exist markets for self-defense and cyber-insurance.

A user investing in self-defense mechanisms reduces its risk probability. For an amount x, invested in self-defense, a user faces a risk probability of $p(x)$, which is a continuous and twice differentiable decreasing function of investment, i.e., $p'(x) < 0$, $p''(x) > 0$, $lim_{x\to\infty}p(x) = 0$, and $lim_{x\to\infty}p'(x) = 0$.

The investment x is a function of the amount of security software the user buys and the effort it spends on maintaining security settings on its computing device. In addition to investing in self-defense mechanisms, a user may also buy *full* or *partial* cyber-insurance coverage at a particular premium to eliminate its residual risk. A user *does not* buy insur-

[2] In general, Internet users are not identical. However, our aim in this chapter is to study certain general investment trends which we show, remain intact even if users are heterogenous.

ance for high probability low risk events because 1)these events are extremely common and does not cause sufficient damage to demand insurance solutions and 2) the insurance company also has reservations in insuring every kind of risk for profit purposes. We assume that the insurance market is perfectly competitive with no barriers to entry and exit, which results in actuarially fair premiums. We also account for the fact that the system does not face the moral hazard problem, i.e., a user insulated from risk does not behave differently from the way it would behave if it were fully exposed to the risk.

An Internet user apart from being directly affected by threats may be indirectly infected by the other Internet users. We denote the indirect risk facing probability of a user i as $q(\overrightarrow{x}_{-i}, n)$, where $\overrightarrow{x}_{-i} = (x_1, ..., x_{i-1}, x_{i+1}, ..., x_n)$ is the vector of self-defense investments of users other than i. An indirect infection spread is either 'perfect' or 'imperfect' in nature. In a perfect spread, infection spreads from a user to other users in the network with probability 1, whereas in case of imperfect spread, infection spreads from a user to others with probability less than 1. For a perfect information spread $q(\overrightarrow{x}_{-i}, n) = 1 - \prod_{j=1,j\neq i}^{n}(1 - p(x_j))$, whereas in the case of imperfect spread, $q(\overrightarrow{x}_{-i}, n) < 1 - \prod_{j=1,j\neq i}^{n}(1 - p(x_j))$. In this chapter, we consider perfect spread only, without loss of generality because the probability of getting infected by others in the case of imperfect spread is less than that in the case of perfect spread, and as a result this case is subsumed by the results of the perfect spread case. Under perfect spread, the risk probability of a user i is given as

$$p(x_i) + (1 - p(x_i))q(\overrightarrow{x}_{-i}, n) = 1 - \prod_{j=1}^{n}(1 - p(x_j))$$

and its expected final wealth upon facing risk is denoted as $w_0 - x_i - (1 - \prod_{j=1}^{n}(1 - p(x_j)) \cdot IC) - R + IC$, where $(1 - \prod_{j=1}^{n}(1 - p(x_j)) \cdot IC$ is the fair premium and IC denotes the insurance coverage. In this chapter, we use the terms 'final wealth' and 'expected final wealth' interchangeably. The aim of a network user is to invest in self-defense mechanisms in such a manner so as to maximize its expected utility of final wealth.

6.3 Framework for Full Insurance Coverage

In this section, we assume full cyber-insurance coverage and propose a general mathematical framework for deciding on the appropriate self-defense investment of an Internet user. We model the following risk management scenarios: (1) users do not co-operate and do not get infected by other users in the network, (2) users co-operate and may get infected by other users in the network, (3) users do not co-operate but may get infected by other users in the network, and (4) users co-operate but do not get infected by other users in the network. We note that Case 4 is a special case of Case 2 and thus is subsumed in the results of Section 6.3.2.

6.3.1 Case 1: No Co-operation, No Infection Spread

Under full insurance, the risk is equal to the insurance coverage, and users determine their optimal amount of self-defense investment by maximizing their level of final wealth, which in turn is equivalent to maximizing their expected utility of wealth [19]. We can determine the optimal amount of self-defense investment for each user i by solving for the value of p that maximizes the following constrained optimization problem:

$$argmax_{x_i} FW_i(x_i) = w_0 - x_i - p(x_i)R - R + IC$$

or

$$argmax_{x_i} FW_i(x_i) = w_0 - x_i - p(x_i)R$$

subject to

$$0 \leq p(x_i) \leq p_0,$$

where FW_i is the final wealth of user i and $p(x_i)R$ is the actuarially fair premium for full insurance coverage. Taking the first and second derivatives of FW_i with respect to x_i, we obtain

$$FW_i'(x_i) = -1 - p'(x_i)R$$

$$FW_i''(x_i) = -p''(x_i)R < 0$$

Thus, our objective function is globally concave. Let x_i^{opt} be the optimal x_i obtained by equating the first derivative to 0. Thus, we have:

$$p'(x_i^{opt})R = -1. \tag{6.1}$$

Economic Interpretation: The left hand side (LHS) of Equation (6.1) is the marginal benefit of investing an additional dollar in self-protection mechanisms, whereas the right hand side (RHS) denotes the marginal cost of the investment. A user equates the LHS with the RHS to determine its self-defense investment.

Conditions for Investment: We first investigate the boundary costs. The user will not consider investing in self-defense if $p'(0)R \geq -1$ because its marginal cost of investing in any defense mechanism, i.e., -1, will be relatively equal to or lower than the marginal benefit when no investment occurs. In this case, $x_i^{opt} = 0$. If the user invests such that it has no exposure to risk, $x_i^{opt} = \infty$. When $p'(0)R < -1$, the costs do not lie on the boundary, i.e., $0 < x_i^{opt} < \infty$, and the user invests to partially eliminate risk (see Equation (6.1)).

6.3.2 Case 2: Co-operation, Infection spread

Under full insurance coverage, user i's expected final wealth is given by

$$FW_i = FW(x_i, \overrightarrow{x}_{-i}) = w_0 - x_i - (1 - \prod_{j=1}^{n}(1 - p(x_j)))R$$

When Internet users co-operate, they jointly determine their optimal self-defense investments. We assume that co-operation and bargaining costs are nil. In such a case, according to Coase theorem [41], the optimal investments for users are determined by solving for the socially optimal investment values that maximize the aggregate final wealth (AFW) of all users. Thus, we have the following constrained optimization problem:

$$argmax_{x_i, \overrightarrow{x}_{-i}} AFW = nw_0 - \sum_{i=1}^{n} x_i - n(1 - \prod_{j=1}^{n}(1 - p(x_j)))R$$

$$0 \leq p_i(x_i) \leq p_0, \, \forall i$$

Taking the first and the second partial derivatives of the aggregate final wealth with respect to x_i, we obtain

$$\frac{\partial}{\partial x_i}(AFW) = -1 - np'(x_i) \prod_{j=1, j \neq i}^{n} (1 - p(x_j))R$$

$$\frac{\partial^2}{\partial x_i^2}(AFW) = -np''(x_i) \prod_{j=1, j \neq i}^{n} (1 - p(x_j))R < 0$$

The objective function is globally concave, which implies the existence of a unique solution $x_i^{opt}(\overrightarrow{x}_{-i})$, for each $\overrightarrow{x}_{-i}$. Our maximization problem is symmetric for all i, and thus the optimal solution is given by $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) = x_j^{opt}(\overrightarrow{x_{-j}^{opt}})$ for all $j = 2, ..., n$. We obtain the optimal solution by equating the first derivative to zero, which gives us the following equation

$$np'(x_i^{opt}(\overrightarrow{x}_{-i})) \prod_{j=1,j\neq i} (1 - p(x_i))R = -1 \tag{6.2}$$

Economic Interpretation: The left hand side (LHS) of Equation (6.2) is the marginal benefit of investing in self-defense. The right hand side (RHS) of Equation (6.2) is the marginal cost of investing in self-defense, i.e., -1. We obtain the former term of the marginal benefit by internalizing the positive externality[3], i.e., by accounting for the self-defense investments of other users in the network. The external well-being posed to other users by user i when it invests an additional dollar in self-defense is $-p'(x_i)\prod_{j=1,j\neq i}^{n}(1 - p(x_i))$. This is the amount by which the likelihood of each of the other users getting infected is reduced, when user i invests an additional dollar.

Conditions for Investment: If $np'(0)\prod_{j=1,j\neq i}^{n}(1 - p(x_j))R \geq -1$, it is not optimal to invest any amount in self-defense because the marginal cost of investing in defense mechanisms is relatively equal to or less than the marginal benefit of the joint reduction in risks to individuals when no investment occurs. In this case, the optimal value is a boundary investment, i.e., $x_i^{opt}(\overrightarrow{x}_{-i}) = 0$. If the user invests such that it has no exposure to risk, $x_i^{opt} = \infty$. In cases where $np'(0)\prod_{j=1,j\neq i}^{n}(1 - p(x_j))R < -1$, the optimal probabilities do not lie on the boundary and the user invests to partially eliminate risk (see Equation (6.2)).

6.3.3 Case 3: No Co-operation, Infection Spread

We assume that users do not co-operate with each other on the level of investment, i.e., users are selfish. In such a case, the optimal level of self-defense investment is the pure strategy Nash equilibria of the normal form game, $G = (N, A, u_i(s))$, played by the users

[3] Internalizing a positive externality refers to rewarding a user, who contributes positively and without compensation, to the well-being of other users, through its actions.

[11]. The game consists of two players, i.e., $|N|$ = n; the action set of G is $A = \prod_{i=1}^{n} \times A_i$, where $A_i \,\epsilon\, [0, \infty]$, and the utility/payoff function $u_i(s)$ for each player i is their individual final wealth, where $s \,\epsilon\, \prod_{i=1}^{n} \times A_i$. The pure strategy Nash equilibria of a normal form game is the intersection of the best response functions of each user [11].

We define the best response function of user i, $x_i^{best}(\overrightarrow{x}_{-i})$, as

$$x_i^{best}(\overrightarrow{x}_{-i}) \,\epsilon\, argmax_{x_i} FW_i(x_i, \overrightarrow{x}_{-i}),$$

where

$$FW_i(x_i, \overrightarrow{x}_{-i}) = w_0 - x_i - (1 - \prod_{j=1}^{n}(1 - p(x_j)))R$$

Taking the first and second partial derivative of $FW_i(x_i, \overrightarrow{x}_{-i})$with respect to x_i and equating it to zero, we obtain

$$\frac{\partial}{\partial x_i}(FW_i(x_i, \overrightarrow{x}_{-i})) = -1 - p'(x_i) \prod_{j=1, j \neq i}^{n} (1 - p(x_j))R$$

$$\frac{\partial^2}{\partial x_i^2}(FW_i(x_i, \overrightarrow{x}_{-i})) = -p''(x_i) \prod_{j=1, j \neq i}^{n} (1 - p(x_j))R < 0$$

Thus, our objective function is globally concave, which implies a unique solution $x_i^{best}(\overrightarrow{x}_{-i})$ for each $\overrightarrow{x}_{-i}$. We also observe that a particular user i's strategy complements user j's strategy for all j, which implies that only *symmetric* pure strategy Nash equilibria exist. The optimal investment for user i is determined by the following equation:

$$\begin{aligned} &\frac{\partial}{\partial x_i}(FW_i(x_i, \overrightarrow{x}_{-i})) = \\ &-1 - p'(x_i) \prod_{j=1, j \neq i}^{n} (1 - p(x_j))R = 0 \end{aligned} \tag{6.3}$$

Economic Interpretation: The left hand side (LHS) of Equation (6.3) is the marginal benefit of investing in self-defense. The right hand side (RHS) of Equation (6.3) is the marginal cost of investing in self-defense, i.e., -1. Since the users cannot co-operate on the level of investment in self-defense mechanisms, it is not possible for them to benefit from the positive externality that their investments pose to each other.

Conditions for Investment: If $p'(0)\prod_{j=1,j\neq i}^{n}(1-p(x_j))R \geq -1$, it is not optimal to invest any amount in self-defense because the marginal cost of investing in defense mechanisms is greater than the marginal benefit of the joint reduction in risks to individuals when no investment occurs. In this case, the optimal value is a boundary investment, i.e., $x_i^{best}(\overrightarrow{x}_{-i}) = 0$. If the user invests such that it has no exposure to risk, $x_i^{opt} = \infty$. In cases where $p'(0)\prod_{j=1,j\neq i}^{n}(1-p(x_j))R < -1$, the optimal probabilities do not lie on the boundary and the user invests to partially eliminate risk (see Equation (6.3)).

Multiplicity of Nash Equilibria: Due to the symmetry of our pure strategy Nash equilibria and the increasing nature of the best response functions, there always exists an odd number of pure-strategy Nash equilibria, i.e., $x_i^{best}(\overrightarrow{x}_{-i}^{best})$ = $x_j^{best}(\overrightarrow{x}_{-j}^{best})$ for all $j = 2, \ldots, n$.

6.4 Comparative Study

In this section, we compare the optimal level of investments in the context of various cases discussed in the previous section. Our results are applicable to Internet applications where a user has the option to be either co-operative (e.g., distributed file sharing applications) or non-cooperative with respect to security parameters.

6.4.1 Case 3 versus Case 1

(6.3) The following lemma gives the result of comparing Case 3 and Case 1.

Lemma 1. *If Internet users do not co-operate on their self-defense investments (i.e., do not account for the positive externality posed by other Internet users), in any Nash* *equilibrium in Case 3, the users inefficiently under-invest in self-defense as compared to the case where users do not cooperate and there is no infection spread.*

Proof. In Case 1, the condition for any user i not investing in any self-defense is $-p'(0)R \leq 1$. The condition implies that $-1-p'(0)\prod_{j=1,j\neq i}^{n}(1-p(x_j))R < 0$ for all $\overrightarrow{x}_{-i}$. The latter expression is the condition for non-investment in Case 3. Thus, for all users i, $x_i^{opt} = 0$ in Case 1 implies $x_i^{best} = 0$ in Case 3, i.e., $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) = x_i^{best}(\overrightarrow{x_{-i}^{best}}) = 0, \forall i$. The condition for optimal investment of user i in Case 1 is $-1 - p'(x_i)R = 0$. Hence, $-1 - p'(x_i)\prod_{j=1,j\neq i}^{n}(1 - p(x_j))R < 0$, for all x_{-i}. Thus, in situations of self-investment for user i, $x_i^{opt} > 0$ in Case 1 implies $0 \leq x_i^{best} < x_i^{opt}$, for all x_{-i}, in Case 3, i.e., $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) > x_i^{best}(\overrightarrow{x_{-i}^{best}}) \geq 0, \forall i$. Therefore, under non-cooperative settings, a user always under-invests in self-defense mechanisms. ■

6.4.2 Case 3 versus Case 2

The following lemma gives the result of comparing Case 3 and Case 2.

Lemma 2. *Under environments of infection spread, an Internet user co-operating with other users on its self-defense investment (i.e., accounts for the positive externality posed by other Internet users), always invests at least as much as in the case when it does not co-operate.*

Proof. In Case 2, the condition for any user i not investing in any self-defense mechanism is $-1 - np'(0)(1 - p(0))^{n-1}R \leq 0$. The condition also implies that $-1 - np'(0)(1 - p(0))^{n-1}R \leq 0$. The latter expression is the condition in Case 3 for an Internet user not investing in any self-defense mechanism. Thus, for all users i, $x_i^{opt} = 0$ in Case 2 implies $x_i^{best} = 0$, for all Nash equilibrium in Case 3, i.e., $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) = x_i^{best}(\overrightarrow{x_{-i}^{best}}) = 0, \forall i$. The condition for optimal investment of each user i in Case 2 is $-1 - np'(x_i^{opt}(\overrightarrow{x_{-i}^{opt}})(1 - p(x_i^{opt}(\overrightarrow{x_{-i}^{opt}}))^{n-1}R = 0$. The latter expression implies $-1 - p'(x_i^{opt}(\overrightarrow{x_{-i}^{opt}})(1 - p(x_i^{opt}(\overrightarrow{x_{-i}^{opt}}))^{n-1}R < 0$. Hence $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) > x_i^{best}(\overrightarrow{x_{-i}^{best}}) \geq 0, \forall i$.

Therefore, under environments of infection spread, a user in Case 3 always under invests in self-defense mechanisms when compared to a user in Case 2. ■

6.4.3 Case 2 versus Case 1

The following lemma gives the result of comparing Case 2 and Case 1.

Lemma 3. *In any n-agent cyber-insurance model, where $p(0) < 1 - \sqrt[n-1]{\frac{1}{n}}$, it is always better for Internet users to invest more in self-defense in a co-operative setting with infection spread than in a non-co-operative setting with no infection spread.*

Proof. In Case 1, the condition for any user i not investing in any self-defense is $-p'(0)R \leq 1$. The condition implies that $-1 - np'(0)(1-p(0))^{n-1}R \leq 0$ for all $p_0 < 1 - \sqrt[n-1]{\frac{1}{n}}$. Thus, for all i, $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) = 0$ in Case 1 implies $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) \geq 0$ in Case 3 if and only if $p_0 < 1 - \sqrt[n-1]{\frac{1}{n}}$. In situations of non-zero investment

$$\begin{aligned}&-1 - np'(x_i(\overrightarrow{x}_{-i}))(1 - p(x_i(\overrightarrow{x}_{-i}))^{n-1})R > \\ &-1 - p'(x_i(\overrightarrow{x}_{-i})), \forall i,\ \forall x_i(\overrightarrow{x}_{-i}),\end{aligned}$$

if and only if $p(x_i(\overrightarrow{x}_{-i})) < 1 - \sqrt[n-1]{\frac{1}{n}}$. Hence,

$$\begin{aligned}&-1 - np'(x_i^{opt}(\overrightarrow{x_{-i}^{opt}})(1 - p(x_i^{opt}(\overrightarrow{x_{-i}^{opt}}))^{n-1})R > \\ &-1 - p'(x_i^{opt}(\overrightarrow{x_{-i}^{opt}})), \forall i,\end{aligned}$$

where $x_i^{opt}(\overrightarrow{x_{-i}^{opt}})$ is the optimal investment in Case 2. Since the expected final wealth of a user in Case 1 is concave in $x_i(\overrightarrow{x}_{-i})$, $x_i^{opt}(\overrightarrow{x_{-i}^{opt}})$ in Case 2 is greater than $x_i^{opt}(\overrightarrow{x_{-i}^{opt}})$ in Case 1. Thus, we infer that investments made by users in Case 2 are always greater than those made by users in Case 1 when the risk probability is less than a threshold value that decreases with increase in the number of Internet users. Hence, in the limit as the number of users tends towards infinity, the lemma holds for all p_0. ■

The basic intuition behind the results in the above three lemmas is that internalizing the positive effects on other Internet users leads to better and appropriate self-defense investments for users. We also emphasize that our result trends hold true in case of heterogenous network users because irrespective of the type of users, co-operating on investments always leads to users accounting for the positive externality and investing more efficiently. The only difference in case of heterogenous network user scenarios could be the value of probability thresholds i.e., $p(0)$ (this value would be different for each user in the network), under which the above lemmas hold.

Based on the above three lemmas, we have the following theorem.

Theorem 15. *If Internet users cannot contract on the externalities, in any Nash equilibrium, Internet users inefficiently under-invest in self-defense, that is compared to the socially optimal level of investment in self-defense. In addition, in any Nash equilibrium, a user invests less in self-defense than if they did not face the externality. Furthermore, if* $p(0) < 1 - \sqrt[n-1]{\frac{1}{n}}$*, the socially optimal level of investment in self-defense is higher compared to the level if Internet users did not face the externality.*

Proof. The proof follows directly from the results in Lemmas 1, 2, and 3. ■

Chapter 7

Conclusion

7.1 Summary of Contributions

In this dissertation we analyzed the existence and success of potential cyber-insurance markets. We showed that without client contract discrimination, cyber-insurers offering full insurance coverage can entail the existence of markets, i.e., existence of a market equilibrium, but cannot guarantee themselves of making strictly positive profits. These markets do not maximize the social welfare in a network, cannot help alleviate the moral hazard problem, and result in sub-optimal network security. Surely these markets will not be successful and stable in the long run as it makes multiple stakeholders unsatisfied. In order to overcome these issues we proposed client contract discrimination on behalf of monopolistic insurers that alleviates the moral hazard problem and entail markets that result in optimal network security. However, the insurer is still not guaranteed to make strictly positive profits in these markets. We alleviate this problem by fixing a 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 addressed the problem of making strictly positive profits 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 for profit shares of the SV) can increase its profits and subsequently enable the cyber-insurer to always make strictly positive profits keeping the social welfare state identical. As a special case, the security vendor could be the cyber-insurer itself. According to basic micro-economic theory, pricing techniques based on such additional client information (be it perfect or imperfect) generates extra profits for SVs compared to their traditional pricing methods. In the process, an SV could also ensure a lock-in effect amongst its insurance clients (e.g., via an ISP) by enforcing the latter to buy security products only from their SV, in turn increasing the demand for security products. One advantage of this approach is that fines and rebates could be fairly split amongst the network users based on network structure, and the amount of externalities each user generates in the network via his investments, instead of just charging a fixed fine/rebate for high and low risk users In addition, the symbiotic approach would also allow a cyber-insurer to appropriately allocate its safety capital costs amongst clients. In this dissertation we showed via theory and simulations that (i) price discriminating consumers in proportion to the Bonacich centrality of individual users results in maximum profits for an SV and at the same time makes each client incur a constant total cost in self-defense investments, thus ensuring consumer fairness, (ii) an SV could make up to 25% additional profits (relative to our model) with perfect client information, (iii) the problem of price discriminating consumers in order to maximize SV profits when there are only two price categories, i.e., regular and discounted, is NP-Hard, and (iv) there exists an an approximation algorithm to the binary pricing problem that provides an approximation guarantee of 0.878 within the optimal solution of the total profit made by an SV.

We proposed Aegis, a novel cyber-insurance model in which an Internet user accepts a fraction (strictly positive) of loss recovery on himself and transfers the rest of the loss recovery on the cyber-insurance agency. Our model is specifically suited to situations when a user cannot distinguish between similar types of losses that arise due to either a security attack or a non-security related failure. We showed that given an option, Internet users would prefer Aegis contracts to traditional cyber-insurance contracts, under all premium types. The latter result firmly establishes the non-existence of traditional cyber-insurance markets when Aegis contracts are offered to users. Furthermore, the Aegis model incentivizes risk-averse Internet users to invest more in taking care of their own systems than simply rest the entire coverage liability upon a cyber-insurer. We also derived two interesting counterintuitive results related to the Aegis framework, i.e., we showed that an increase (decrease) in the premium of an Aegis contract *may not* always leads to a decrease (increase) in its user demand. *Finally, through a simple model of cyber-insurance we show that only under conditions when buying some type of cyber-insurance is made mandatory, does a market exist, and that too for idealistic situations when information asymmetry is absent.* Thus, it is important that (i) the insuring agency (if it is not the ISP or the government) partners with the regulators to make cyber-insurance mandatory for Internet users, and (ii) information asymmetry be taken into equation to check whether a market for cyber-insurance can be made to exist in its presence.

We investigated the problem of self-defense investments in the Internet, under the *full insurance* and *partial insurance* coverage models. We showed that co-operation amongst users results in efficient self-defense investments than those in a non-cooperative setting, and result in social welfare maximization under a full insurance coverage model.

7.2 Open Challenges

In this section, we look at some important open challenges not addressed in the dissertation.

- One drawback of this dissertation 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 it remains to be investigated whether there would exist 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 an appropriate manner.

- An important problem that remains to be explored is to find ways to satisfy all market stakeholders under non-compulsory cyber-insurance in an oligopolistic setting. Compulsory insurance is still quite a distance from being deployed in practice and thus designing models to decide whether improvement of network security is possible under non-compulsory insurance is an important direction of future research. In addition, there will be multiple insurance companies existing in practice and competing against one another. Therefore, it is an important research challenge to derive models that ensure market efficiency and jointly satisfy market stakeholders.
- An important research question is to analyze the effect of the presence of multiple SVs on consumer pricing. In the case when the SV client set are clustered into sparse pockets for different SVs, each pocket acts as a monopoly zone. However, in reality SV client sets will be overlapped and in such a scenario it is challenging to estimate externality effects for each individual SV client set and implement the pricing mechanisms proposed in this dissertation. One way to approach this problem is to trade externality information between multiple SVs, under a regulator.
- In this work, we characterize attacks as being exogenous in nature rather than strategic. However, in reality a large share of cyber-attacks is strategic, and research in this direction appears overdue. With the view of strategic attackers, increased network security may have a positive externality on aggregate network losses, because with higher security, attacker costs might increase, and gains decrease. Attackers reacting to changed incentives might hence seek for alternative (and hopefully more

benign) activities. We suggest modeling attackers as players, with objective functions, information sets, and actions. Our framework naturally extends to include strategic attackers, but it may be hard to choose reasonable assumptions and parameters for their capability. Attackers could be modeled as an additional class of players or as a special type of users.

- In interdependent and correlated risk environments such as the Internet, the insurer is risk-averse and might resort to a higher chain of risk transfers. Thus, an important challenge is to model higher-order risk transfers and study market efficiency. Although barely modeled explicitly in the cyber-insurance literature so far, we can distinguish two prototype cases:

    - Cyber-reinsurance: Most naturally, the idea of reinsurance for dealing with rare catastrophic events seems applicable to cyber-insurance. Modeling reinsurance markets is straight-forward with ‘insurers’ taking the role of ‘users’ and reinsurers become ‘insurers’. Obviously, reinsurance is more efficient only if reinsurers can pool risks; this assumes the existence of many insurers with independent (or at least loosely correlated) risk pools. For conventional insurance branches, this is usually achieved by regional or international diversification. However, due to the global homogeneity of cyber-risk, often attributed to the homogeneity of installed systems cyber-reinsurance is virtually not existent. In January 2002, reinsurers even excluded cyber-risks explicitly from their contracts with insurers in fear of global catastrophic events.

    - Exploit derivatives: Other financial instruments are tailored more specifically to cyber-risk and avoid such adverse incentives. The concept of exploit derivatives links the payout of the financial instrument to the discovery of vulnerabilities in systems, that is, at a stage before actual losses occur. So even if incentive incom- patibilities cannot be ruled out entirely, selfish actions of of individual players are less likely to cause tremendous social damage. More- over, it is argued that exploit derivatives can form a kind of prediction market to facilitate information sharing about system vulnerabilities, thereby mitigating the information asymmetries prevalent in cyber-security. However, while exploit derivatives might work for threats related to undiscovered vulnerabilities, this type of threat accounts for part of the cyber-risk our society is exposed to.

References

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

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

[3] R. Anderson, C. Barton, R. Bohme, R. Clayton, M. J. G. Eaten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In *WEIS*, 2012.

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

[5] A. L. Barabasi and R. Albert. Emergence of scaling in random networks. *Science*, 286, 1999.

[6] R. Bohme. Personal communication.

[7] R. Bohme and G. Kataria. Models and measures for correlation in cyber-insurance. In *WEIS*, 2006.

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

[9] P. B. Bonacich. Power and centrality: A family of measures. *American Journal of Sociology*, 92, 1987.

[10] O. Candogan, K. BImpikis, and A. Ozdaglar. Optimal pricing in networks with externalities. *INFORMS Operations Research*, 60(4), 2012.

[11] D.Fudenberg and J.Tirole. *Game Theory*. MIT Press, 1991.

[12] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman and Company, 1979.

[13] M. Goemans and D. Williamson. Improved approximation algorithms for maximum cut satisfiability problems using sem-definite programming. *Journal of the ACM*, 42, 1995.

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

[15] A. Hau. When is a co-insurance type insurance policy inferior or even giffen. *Journal of Risk and Insurance*, 75(2), 2008.

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

[17] P. Honeyman and G. Schwarz. Interdependence of reliability and security. In *WEIS*, 2007.

[18] R. A. Horn and D. D. Johnson. *Matrix Analysis*. Cambridge University Press, 2005.

[19] I.Ehrlick and G.S. Becker. Market insurance, self-insurance, and self-protection. *Journal of Political Economy*, 80(4), 1972.

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

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

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

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

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

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

[26] C. D. Meyer. *Matrix Analysis and Applied Linear Algebra*. SIAM Press, 2000.

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

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

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

[30] R. Pal. Cyber-insurance for cyber-security: A solution to the information asymmetry problem. In *SIAM Annual Meeting*, 2012.

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

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

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

[34] R. Pal, L. Golubchik, K. Psounis, and P. Hui. On a way to improve cyber-insurer profits: When a security vendor becomes the cyber-insurer. In *IFIP Networking*, 2013.

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

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

[37] R. Pal and P. Hui. Cyber-insurance for cyber-security: A topological take on modulating insurance premiums. *Performance Evaluation Review*, 40(3), 2012.

[38] R. Pal and P. Hui. On differentiating cyber-insurance contracts: A topological perspective. In *IEEE/IFIP Internet Management Conference*, 2013.

[39] S. L. Pfleeger and R. K. Cunningham. Why measuring security is hard. In *IEEE Symposium on Security and Privacy*, 2010.

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

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

[42] S.Radosavac, J.Kempf, and U.C.Kozat. Using insurance to increase internet security. In *ACM NetEcon*, 2008.

[43] D. M. Topkis. *Supermodularity and Complementarity*. Princeton University Press, 1998.

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