International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600

http://www.ijcsjournal.com Volume 5, Issue 1, No 2, 2017 ISSN: 2348-6600
Reference ID: IJCS-163 PAGE NO: 984-994

Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

WILL CYBER- IMPROVE NETWORK SECURITY? A MARKET ANALYSIS

Ms.V.Saranya, Mrs.S.Sudha
Assistant Professor, Department Of Information Technology
Assistant Professor, Department Of BCA
Sri Vasavi College (Self Finance), Erode
Email-Id: Charubsccs@gmail.Com

ABSTRACT

Ranjan Pal University of Southern California Leana Golubchik and Konstantis Psounis University of Southern California {leana, Pan Hui HKUST, and T-Labs - Germany Abstract Recent work in security has illustrated that solutions aimed at detection and elimination of security threats alone are unlikely to result in a robust cyberspace. As an orthogonal approach to mitigating security problems, some have pursued the use of cyber-insurance as a suitable risk management technique. Such an approach has the potential to jointly align with the incentives of security vendors (e.g., Symantec, Microsoft, etc., cyber-insurers (e.g., ISPs, cloud providers, security vendors, etc., regulatory agencies (e.g., government, and network users (individuals and organizations, in turn paving the way for comprehensive and robust cyber-security mechanisms. To this end, in this work, we are motivated by the following important question: can cyber-insurance really improve the security in a network? To address this question, we adopt a market-based approach. Specifically, we analyze regulated mopolistic and competitive cyber-insurance markets, the market elements consist of risk-averse cyber-insurers, risk-averse network users, a regulatory agency, and security vendors. Our results show that (i without contract discrimination amongst users, there always exists a unique market equilibrium for both market types, but the equilibrium is inefficient and does t improve network security, and (ii in mopoly markets, contract discrimination amongst users results in a unique market equilibrium that is efficient, which in turn results in network security improvement - however, the cyber-insurer can make zero expected profits. The latter fact is often sufficient to de-incentivize the insurer to be a part of a market, and will eventually lead to its collapse. This fact also emphasizes the need for designing mechanisms that incentivize the insurer to permanently be part of the market.

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

INTRODUCTION

The infrastructure, the users, and the services offered on computer networks today are all subject to a wide variety of risks posed by threats that include distributed denial of service attacks, intrusions of various kinds, eavesdropping, hacking, phishing, worms, viruses, spams, etc. In order to counter the risk posed by the threats, network users have traditionally resorted to antivirus and anti-spam software's, 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 amalies in order to protect the cyber infrastructure and its users from the negative impact of the amalies. In spite of improvements in risk protection techniques over the last decade due to hardware, software and cryptographic methodologies, it is impossible to achieve a perfect/near-perfect cyber security protection

The impossibility arises due to a number of reasons: (i scarce existence of sound technical solutions, (ii difficulty in designing solutions catered to varied intentions behind network attacks, (iii misaligned incentives between network users, security product vendors, and regulatory authorities regarding each taking appropriate liabilities to protect the network, (iv network users taking advantage of the positive security effects generated by other user investments in security, in turn themselves t 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], by security vendors have 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 1% risk mitigation, the need arises for alternative methods of risk management in cyberspace 1. In this regard, some security researchers in the recent past have identified cyber-insurance as a potential tool for effective risk management. Cyber-insurance is a risk management technique via which network user risks are transferred to an insurance company (e.g., ISP, cloud provider, traditional insurance organizations, in return for a fee, i.e., the insurance premium. Proponents of cyber-insurance believe that cyber-insurance would lead to the design of insurance contracts that would shift appropriate amounts of self-defense liability on the clients, thereby making the cyberspace more robust. Here the term self-defense implies the efforts by a network user to secure their system through technical solutions such as anti-virus and anti-spam software's, firewalls, using secure operating systems, etc. Cyber-insurance has also the potential to be a market solution that can align with ecomic incentives of cyber-insurers, users (individuals/organizations, policy makers, and security software vendors, i.e., the cyber-insurers will earn profit from appropriately pricing premiums, network users will seek to hedge potential losses by jointly buying insurance and investing in self-defense mechanisms, the policy makers would ensure the increase in overall network security, and the security software vendors could go ahead with their first-mover and lock-in strategies as well as experience an increase in their product sales via forming alliances with cyber-insurers. A. Research Motivation Despite all promises, current cyber-insurance markets are moderately competitive and specialized. As of 21, there are approximately 18 insurance organizations in the United States insuring $8 million worth of organizational IT resources only [4], and there is little information as to whether the current cyber-insurance market improves network security by incentivizing organizations to invest aptly in security solutions. The inability of cyber-insurance to become a common reality (i.e., to form a successful market amongst n-organizational individual users is due to a number of unresolved research challenges as well as practical considerations. 1 To highlight the importance of improving the current state of cyber security, US President Barack Obama has recently passed a security bill that emphasizes the need to reduce cyber-threats and be resilient to them.

In the process of studying improvement and the optimality of network security, we are interested in analyzing the welfare of elements (stakeholders that form a cyber insurance market (if there exists one. B. Research Contributions We makes the following primary research contributions in this paper. We propose a supply-demand model of regulated cyber insurance markets that accounts for inter-dependent risks in a networked environment as well as the externalities generated by user security investments. (See Section II. We show that a mopoly cyber-insurer providing full coverage to its clients without contract discriminating them enables the existence of an inefficient cyber-insurance market that does t improve network security. However, with client contract discrimination, the cyber-insurer is successful in enabling an efficient cyber-insurance market that alleviates the moral hazard problem and improves network security. In the process the insurer makes n-negative expected profits. (See Section IV. We show that in perfectly competitive and oligopolistic cyber insurance settings, there exists an inefficient insurance market that does t improve network security. (See Section V. C. Basic Economics Concepts In this section we briefly review some basic economics concepts as applicable to this work in order to establish terminology for the remainder of the paper. Additional details could be found in a standard economics textbook such as [13]. Basic concepts related to insurance economics will be discussed in Section II. Externality: An externality is an effect (positive or negative of a purchase of self-defense investments by a set of users (individuals or organizations on other users whose interests were t taken into account while making the investments. In this work, the effects are improvements in individual security of network users who are connected to the users investing in self-defense. Risk probability: It is the probability of a network user being successfully attacked by a cyber-threat and incurring a loss of a particular amount. Initial wealth: It is the initial amount of wealth a network user possesses before expending in any self-defense mechanisms and/or insurance solutions. User risk propensity: A risk-neutral investor (either the insurer or the insured is more concerned about the expected return on his investment, t on the risk he may be taking on. A classic experiment to distinguish between risk-taking appetites involves an investor faced with a choice between receiving, say, either $1 with 1% certainty, or a 5% chance of getting $2. The risk-neutral investor in this case would have preference either way, since the expected value of $1 is the same for both outcomes. In contrast, the risk-averse investor would generally settle for the sure thing or 1% certain $1, while the risk-seeking investor will opt for the 5% chance of getting $2. Market: In regard to a cyber-insurance context, it is a platform cyber-insurance products are traded with insurance clients, i.e., the network users. A market may be perfectly competitive, oligopolistic, or mopolistic. In a perfectly competitive market there exist 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 t specified, but a competitive market has eugh buyers and sellers that one buyer or seller can exert any significant influence on premium pricing in the market. On the contrary, in mopolistic and oligopolistic markets, the insurers have the power to set client premiums to a certain liking. Equilibrium: Equilibrium refers to a situation when both, buyers, as well as the sellers are satisfied with their net utilities and one has any incentive to deviate on their strategies. In this paper we consider two equilibrium concepts: (i the Nash equilibrium (for mopoly markets and imperfectly competitive markets, and (ii the Walrasian equilibrium (a standard solution concept for perfectly competitive markets. stakeholders: The stakeholders in a cyber-insurance market refer to entities whose interests are affected by the dynamics of market operation. In our work we assume that the entities are cyber-insurers (e.g., ISPs, cloud providers, security vendors, traditional insurance companies, the network users, a regulatory agency such as the government, and security vendors such as Symantec.

SUPPLY-DEMAND MODEL

In this section we propose a supply-demand model of a cyber insurance market. The section has two parts: in the first part we describe our model from a demand (network user perspective, in the second part we describe our model from the supply (cyber-insurer perspective. Important station 2 used in the paper is summarized in Table 1. Additional station is explained when used in subsequent sections. A. Model from a Demand Perspective We considers a communication network comprised of a continuum of risk-averse users. Here we use the station of users as mentioned in [5], users are considered as atomic des (individuals, organizations, enterprise, data center elements, etc. in the network, each controlling a possible collection of devices. The links between the des need t necessarily be physical connections and could also represent logical or social ties amongst the des. For example, social engineering attacks are conducted on overlay networks. Each 2 Variations of certain stations as applicable to the section at hand are described in the respective sections. User has initial wealth w and faces a risk of size r < w with probability p, i.e., he either faces a risk of size r with probability p or faces risk with probability 1 p. Here p is a function of the proportion of user's t investing in security measures (read on for a more formal description... Each risk-averse user has the standard von Neumann-Morgenstern (VNM utility 3, U ([13], that is a function of his final wealth, is twice continuously differentiable, increasing, and strictly concave. Each user also incurs a cost x to invest in self-defense mechanisms, which is drawn from a random variable X having distribution function F and density function f, each defined over the support [, r]. We define x m to be the marginal cost of investing in self-defense mechanisms, i.e., it is the cost to a user who is indifferent between investing and t investing in self-defense. Such a user s net utility on investment is the same as his net utility on n-investment. From w on in the paper, we assume that such a user always invests in self-defense. All other risk-averse users either decide to invest or t invests in self-defense mechanisms, depending on whether their cost of investment is lower or higher than x m. We assume that a user does t completely avoid loss on self-protection, i.e., self-protection is t perfect, and is subject to two types of losses: direct and indirect. A direct loss to a user is caused when it is directly attacked by a malicious entity (threat. An indirect loss to a user is caused when it is indirectly affected by direct threats to other users in the network. Let p be the probability of a direct loss to a user. Let q(l be the probability of a user getting indirectly affected by other network users, l is the proportion of users in the network t adopting self-defense (self-protection mechanisms, which in turn is a function of x m, i.e., the marginal cost to a user indifferent to investing in self-defense investments. Thus, q = q (l = q (l(x m. We have the following relationship between l and x m: Thus, dl (xm m l = l(x = x m = r x m f (θdθ = 1 F (x m. (1 = f(x m <, implying the proportion of individuals without self-defense investments is strictly decreasing in x m as more users find it preferable to invest in self-defense with increasing marginal costs. Regarding the connection between q and l(x m, the higher the value of l(x m, the greater is the value of q. Therefore we assume q (l(x m >, and q (l(x m q max. Here q max is the value of the function q taken at an argument value of 1, and we assume that q (=. The interpretation behind q is that if body invests in self-defense, a user gets indirectly affected with probability q max, and if everyone invests in self-defense, the probability of indirect loss to a user is zero. Note that x m is dependent on the investment of one s neighbors in the contact graph (our work assumes any general contact graph, which in turn is dependent on the investment of neighbor s neighbors and so on. From a policy viewpoint, this seems tough to implement, but as mentioned above, in the interest of cyber-security, such measures might be adopted in the near future. 5 In practice, for reliability purposes, it is possible to enforce compulsory insurance in data center and enterprise networks the network is generally owned by a single entity providing application services to numerous customers. Get bankrupt if the expected aggregate loss in a period is greater than what it could afford to cover. We assume the risk-averse behavior of the insurer by requiring it to hold safety capital. A safety capital is the additional amount over the expected aggregate loss in a period such that the probability of an insurer incurring of a loss of value greater than the sum of the capital and expected aggregate loss in that period does t exceed a particular threshold. The threshold value is defined by a regulator. The cost of holding safety capital is distributed across the clients through the premiums charged to them. We assume that the share of safety capital cost per client is less than his expected risk value. Each client is charged a premium of (1 + be(r, λ is the loading factor per contract, and E(R is the expected loss value of the client. The loading factor resembles the amount of profit per contract the cyber-insurer is keen on making and/or the share of the safety capital cost of each user. A premium is said to be fair if its value equals E(R, and is unfair if its value is greater than

SCENARIO 1: NO INSURANCE CASE

In this section we analyze the case when network users do t have access to any form of insurance coverage. This case is useful for the comparison of optimal user investments in security between scenarios of insurance coverage and those with coverage. Self-protection and the risk of loss is very high, it is worth to undertake defense measures to reduce expected loss, when cost to invest in self-defense is zero, (ii if every user invests in self defense and the risk is zero, an investment is t worth being undertaken, and indifferent between investing and t investing in self-defense. Thus x eq 1 = x m 1, the marginal cost of making self-defense investments in Scenario 1. The interior solution, x eq 1, in the equation is the competitive Nash equilibrium (NE cost of protection investment. It implies the fact that users whose cost of self-defense is less than x eq 1 invest in self-defense as their expected utilities of investing would be greater than that without it, as the others do t invest in any protection mechanisms as it would t be profitable for them to do so. The analysis above proves the following theorem. Theorem 1. In the case of imperfect prevention, when network users do t have cyber-insurance protection, there exists a unique Nash equilibrium (NE cost to invest in self-defense, x eq 1. Users facing protection costs below x eq 1 invest in self-defense mechanisms, as other users do t. This NE cost of self-defense does t result in maximizing user social welfare in the network, i.e., i.e., the proportion of users t resorting to self-defense mechanisms is higher in the Nash equilibrium than in the welfare optimum. Theorem Intuition and Practical Implications: The intuition behind Theorem 1 follows from the first fundamental theorem in welfare economics [13] which states that the network externalities generated by user investments are t internalized (i.e., users do t 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 t end up putting in optimal self-defense efforts, and this results in sub-optimal network security, i.e., the average of the sum of user risk probabilities (dated as p(x m, is t minimized. With respect to the welfare of users, the ones who face a cost of investment above the NE cost do t buy security products and are t satisfied because they can't defend themselves on being attacked. The ones who do invest in security measures are better off but are still susceptible to indirect risks. Security vendors like Symantec and Microsoft make profits as per their current security product market scenario. The case of insurance is currently the situation in Internet security, apart from a few organizations that are insured.

SCENARIO 2: MONOPOLY MARKETS

In this section we analyze a regulated mopolistic cyber insurance market under conditions of imperfect prevention (self-protection doe's t guarantee risk removal. Here the term regulated implies the role of the government to (i ensure Internet users buy compulsory cyber-insurance, (ii enable insurers to adopt premium discrimination amongst clients based on the user risk types, and (iii allow basic user security behavior monitoring by insurance agencies. We divide this section in two parts: in the first part we analyze the case when there is contract discrimination amongst clients. In the second part we analyze the case with clients being contract discriminated.

The rationale for client discrimination is that users who take (do t take appropriate self-defense actions reduce (increase their chances of getting attacked as well as reduce (increase other network users chances of facing a loss. In order to differentiate between clients, the cyber-insurer imposes a fine of amount a per user of high risk type, and provides a rebate of amount b per user of low risk type. A user is considered of high risk type if he does t invests 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 t 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 mopolistic cyber-insurance markets or imperfect competitive markets. In the case of perfectly competitive markets, price competition will t 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 w proceed with the analysis of the case when users are premium discriminated in mopoly markets. A user willing to invest in self-defense investments will receive a rebate of b on his premium. 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 n-negative expected profits 8, and security product vendors would see an increase in their product sales (and subsequently profits due to users being incentivized to invest appropriate amounts in self-defense mechanisms. Central Point: In the mopolistic cyber-insurance scenario with client contract discrimination, there may exist an efficient market (always exists if λ > that helps satisfy the interests of all the market stakeholders. 8 Note that in most cases the cyber-insurer would set λ values to be positive, which implies strictly positive expected profits.

SCENARIO 3: COMPETITIVE MARKETS

We assume a perfectly competitive cyber-insurance market 9 multiple cyber-insurers provide their clients with full coverage at fair premiums 1. Due to imperfect prevention, we also assume that a risk-averse user resorts to insurance solutions whenever he invests in self-defense mechanisms. Like in Scenario 2, in a competitive (perfect or oligopolistic cyber-insurance scenario with client contract discrimination, there exists an inefficient market, i.e., the social welfare is t maximized at market equilibrium, and this does t help satisfy the interests of all the market stakeholders. A Note on Oligopolistic Markets: Oligopolistic markets resemble imperfect (t 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, each insurer is price taking (has market power to charge actuarially unfair premiums and can only charge actuarially fair premiums to its clients. However, due to Bertrand s paradox [13], for number of insurers equal to two, the insurers find it optimal to charge fair premiums to their clients. So does that mean that in competitive settings, cyber-insurers will always make zero expected profits (due to charging actuarially fair premiums to clients? The answer is because in reality factors such as firm popularity and customer lock-in will result in some insurers charging unfair premiums to their clients and making strictly positive expected profits, without having to worry about their client demands decreasing. In the case when the number of cyber-insurance firms in a market are greater than two, the authors in [15] show there exists a market Nash equilibrium which does t maximize social welfare. A comparative study of the three scenarios analyzed in the paper.

RELATED WORK

In this section, we give an overview of related work on cyber insurance as applicable to this paper. The field of cyber-insurance in networked environments has been triggered by recent results on the amount of self-defense investments users should expend in the presence of network externalities in order to ensure a robust cyber-space Thus, the authors results reflect that cooperation amongst network users will result in a more robust cyberspace. However, t all applications in cyberspace can be cooperative and as a result we consider the general case of n-cooperative application environments and to ensure optimal insurance-driven self-defense amongst users in such environments. In another recent work [18], the authors derive Aegis, a vel optimal insurance contract type based on the traditional cyber-insurance model, in order to address the realistic scenario when both, insurable and n-insurable risks co-exist in practice. Without such considerations, simply shifting liability on users to invest more May t is eugh 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 information asymmetry between the insurer and the insured. These works also do t address the problem of ways for cyber-insurers to always make strictly expected positive profits, without which the cyber-insurance business would t 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 t a good one as the latter could become bankrupt. Thus, modeling the insurer as being risk-averse is appropriate.

CONCLUSION AND FUTURE WORK

In this paper we analyzed the existence and success of potential cyber-insurance markets. We showed that without client contract discrimination, cyber-insurers offering full insurance coverage can entail the existence of markets, i.e., existence of market equilibrium, but can't guarantee themselves of making strictly positive profits. However, the insurer is still t guaranteed to make strictly positive profits in these markets. To alleviate this issue a security vendor can enter the cyber insurance ecosystem and via a symbiotic relationship between the insurer (through exchange of logical/social client topological information and lock-in privileges for profit shares of the SV can increase its profits and subsequently enable the cyber-insurer to always make strictly positive profits keeping the social welfare state identical. As a special case the security vendor could be the cyber-insurer itself. We plan to investigate the symbiotic relationship between security vendors and cyber-insurers as part of future work. One drawback of our work is we assume that an insurer can stochastically observe user investment amounts and infer their risk type. This partially incorporates the adverse selection problem in the model. However, as part of future work we want to investigate the existence of efficient cyber-insurance markets when the insurer can make observations on client investments, or is given false information by the clients. Ather problem we want to explore is to find ways to satisfy all market stakeholders under n-compulsory cyber-insurance.

REFERENCES

1. Information Asymmetry. Internet Wikipedia Source.
2. G. A. Akerlof. The market for lemons - quality uncertainty and the market mechanism. Quarterly Journal of Economics,
3. R. Anderson and T. Moore. Information security economics and beyond. In Information Security Summit, 28. R. Bohme. Personal communication.
4. R. Bohme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. In WEIS, 21.
5. J. Grossklags, N. Christin, and J. Chuang. Security and insurance management in networks with heterogeus agents. In ACM EC, 28.

6. L. Jiang, V. Ananthram, and J. Walrand. How bad are selfish inverstments in network security? To Appear in IEEE/ACM Transactions on Networking, 21. Khouzani, S. Sen., and N. Shroff. An ecomic analysis of regulating security investments in the internet. In IEEE INFOCOM, 213.
7. M.Feleghyazi and J.Walrand. Competitive cyber insurance and internet security. In WEIS, 29. [16] J. Omic, A. Orda, and P. V. Mieghem. Protecting against network infections:
8. A game theoretic perspective. In IEEE INFOCOM, 29. [17] R. Pal and L. Golubchik. Analyzing self-defense investments in the internet under cyber-insurance coverage. In IEEE ICDCS, 21.
9. R. Pal, L. Golubchik, and K. Psounis. Aegis: A vel cyber-insurance model. In IEEE/ACM GameSec.