A Mathematical Theory of Internet Security Investments Under Cyber-Insurance Coverage

Ranjan Pal, Student Member, IEEE, Leana Golubchik, Member, IEEE,

Abstract

Internet users such as individuals and organizations are subject to different types of epidemic risks such as worms, viruses, spams, and botnets. To reduce the probability of risk, an Internet user generally invests in traditional security mechanisms like anti-virus and anti-spam software, sometimes also known as self-defense mechanisms. However, such software does not completely eliminate risk. Recent works have considered the problem of residual risk elimination by proposing the idea of cyber-insurance. In this regard, an important decision for Internet users is their amount of investment in self-defense mechanisms when insurance solutions are offered.

In this paper, we investigate the problem of self-defense investments in the Internet, under optimal cyber-insurance coverage, where optimality is an insurer objective. By the term ‘self-defense investment’, we mean the monetary-cum-precautionary cost that each user needs to invest in employing risk mitigating self-defense mechanisms, given that it is optimally insured by Internet insurance agencies. We propose a general mathematical framework by which co-operative and non-co-operative Internet users can decide whether or not to invest in self-defense for ensuring both, individual and social welfare. Our results show that co-operation amongst users results in more efficient self-defense investments than those in a non-co-operative setting, under full insurance coverage, in a perfect single insurer cyber-insurance market, whereas in imperfect single insurer markets of non-cooperative users, partial insurance driven self-defense investments are optimal.

R. Pal and L. Golubchik are with the Department of Computer Science, University of Southern California, CA, 90089 USA. e-mail: {rpal, leana}@usc.edu.
I. INTRODUCTION

The Internet has become a fundamental and an integral part of our daily lives. Billions of people nowadays are using the Internet for various types of applications. However, all these applications are running on a network, that was built under assumptions, some of which are no longer valid for today’s applications, e.g., that all users on the Internet can be trusted and that there are no malicious elements propagating in the Internet. On the contrary, the infrastructure, the users, and the services offered on the Internet today are all subject to a wide variety of risks. These risks include denial of service attacks, intrusions of various kinds, hacking, phishing, worms, viruses, spams, etc. In order to counter the threats posed by the risks, Internet users\(^1\) have traditionally resorted to antivirus and anti-spam softwares, firewalls, and other add-ons to reduce the likelihood of being affected by threats. In practice, a large industry (companies like Norton, Symantec, McAfee, etc.) as well as considerable research efforts are centered around developing and deploying tools and techniques to detect threats and anomalies in order to protect the Internet infrastructure and its users from the negative impact of the anomalies.

In the past one and half decade, protection techniques from a variety of computer science fields such as cryptography, hardware engineering, and software engineering have continually made improvements. Inspite of such improvements, recent articles by Schneier [29] and Anderson [2][3] have stated that it is impossible to achieve a 100% Internet security protection. The authors attribute this impossibility primarily to four reasons: 1) new viruses, worms, spams, and botnets evolve periodically at a rapid pace and as result it is extremely difficult and expensive to design a security solution that is a panacea for all risks, 2) the Internet is a distributed system, where the system users have divergent security interests and incentives, leading to the problem of ‘misaligned incentives’ amongst users. For example, a rational Internet user might well spend $20 to stop a virus trashing its hard disk, but would hardly have any incentive to invest sufficient amounts in security solutions to prevent a service-denial attack on a wealthy corporation like an Amazon or a Microsoft [32]. Thus, the problem of misaligned incentives can be resolved only if

\(^1\)The term ‘users’ may refer to both, individuals and organizations.
liabilities are assigned to parties (users) that can best manage risk, 3) the risks faced by Internet users are often correlated and interdependent. A user taking protective action in an Internet like distributed system creates positive externalities [14] for other networked users that in turn may discourage them from making appropriate security investments, leading to the ‘free-riding’ problem [7][10][20][22], and 4) network externalities affect the adoption of technology. Katz and Shapiro [12] have analyzed that externalities lead to the classic S-shaped adoption curve, according to which slow early adoption gives way to rapid deployment once the number of users reaches a critical mass. The initial deployment is subject to user benefits exceeding adoption costs, which occurs only if a minimum number of users adopt a technology; so everyone might wait for others to go first, and the technology never gets deployed. For example, DNSSEC, and S-BGP are secure protocols that have been developed to better DNS and BGP in terms of security performance. However, the challenge is getting them deployed by providing sufficient internal benefits to adopting firms.

In view of the above mentioned inevitable barriers to 100% risk mitigation, the need arises for alternative methods of risk management in the Internet. Anderson and Moore [3] state that microeconomics, game theory, and psychology will play as vital a role in effective risk management in the modern and future Internet, as did the mathematics of cryptography a quarter century ago. In this regard, cyber-insurance is a psycho-economic-driven risk-management technique, where risks are transferred to a third party, i.e., an insurance company, in return for a fee, i.e., the insurance premium. The concept of cyber-insurance is growing in importance amongst security engineers. The reason for this is three fold: 1) ideally, cyber-insurance increases Internet safety because the insured increases self-defense as a rational response to the reduction in insurance premium [11][13][31][34]. This fact has also been mathematically proven by the authors in [15][18], 2) in the IT industry, the mindset of ‘absolute protection’ is slowly changing with the realization that absolute security is impossible and too expensive to even approach while adequate security is good enough to enable normal functions - the rest of the risk that cannot be mitigated can be transferred to a third party [19], and 3) cyber-insurance will lead to a market solution that will be aligned with economic incentives of cyber-insurers and users (individuals/organizations).
- the cyber-insurers will earn profit from appropriately pricing premiums, whereas users will seek to hedge potential losses. In practice, users generally employ a simultaneous combination of retaining, mitigating, and insuring risks [30].

The market for cyber-insurance started in the late 90’s when certain security software companies partnered with insurance firms to provide a total risk management solution (risk reduction + residual risk transfer). Some examples of risk management solutions offered include Cigna Secure System Insurance, Counterpane, and AIG NetAdvantage. A more detailed list of cyber-insurance solutions can be found in [19]. However, all these solutions are more like computer insurance and were targeted at users without taking into account the role of connectivity in the Internet or in any large scale distributed system, i.e., they do not explicitly account for correlated and interdependent risks. Correlated risks² make it difficult for cyber-insurers to spread risks across customers, whereas risk interdependency makes a user risk a function of risks faced by other users in the network. In this paper, we address an important problem related to cyber-insurance-driven Internet risk management, in the presence of correlated and interdependent risks.

We analyze user self-defense investments under optimal cyber-insurance coverage in both, non-cooperative as well as cooperative communication scenarios. By the term ‘self-defense’, we imply protection from threats taken by Internet users through anti-virus and anti-spam softwares, firewalls, etc. Our problem is important for two main reasons: 1) investing in self-defense mechanisms reduces a user’s probability of facing risk. Given that a user has cyber-insurance coverage, increase in user self-defense investments reduces its premium charged by the cyber-insurer. Thus, its important to characterize the appropriate amounts of investments by a user in self-defense, as well as in cyber-insurance, such that it maximizes its utility and 2) many distributed Internet applications like peer-to-peer file sharing, multicasting, and network resource sharing encourage co-operation between users to improve overall system performance. In regard to security investments, cooperation invites an opportunity for a user to benefit from

²A considerable fraction of worm and virus attacks tend to propagate rapidly through the Internet and inflict correlated damages [27][35].
the positive externality\textsuperscript{3} that its investment poses on the other users in the network. However, it is not evident that users invest better when they cooperate compared to when they do not, in regard to the network achieving greater overall security. In this paper, we want to study whether security investments are more efficient under cooperation than under non cooperation when it comes to achieving better overall network security.

\textit{Related Work:} Correlated and interdependent risks in the Internet have been addressed by the authors in [4][5][14]. These works handle the decision problem of whether to invest in security mechanisms, but do not analyze the interplay between cyber-insurance and security investments. Recently, the authors in [7][10][16][17][20][22] have mathematically shown that Internet users invest too little in self-defense mechanisms relative to the socially efficient level, due to the presence of network externalities. The works in [16][17] model network externalities and show 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. In a series of recent works [15][18], Lelarge and Bolot have stated that under conditions of no information asymmetry \textsuperscript{1} between the insurer and the insured, cyber-insurance incentivizes user investments in self-defense mechanisms, thereby paving the path to trigger a cascade of adoption. They also show that investments in both self-defense mechanisms and insurance schemes are quite inter-related in maintaining a socially efficient level of security on the Internet. In [21], the authors have investigated risk management using cyber-insurance under different information availability scenarios between the insurer and the user, with respect to user security levels. They show that there is no market for cyber-insurance on the Internet under information asymmetry, i.e., cyber-insurance increases individual user utility but weakens user incentives to improve overall network security\textsuperscript{4}.

None of the cited related works in the above paragraph consider the cooperative and non

\textsuperscript{3}An externality is a positive (external benefit) or negative (external cost) impact on a user not directly involved in an economic transaction.

\textsuperscript{4}The authors define the network security level as the the probability that Internet users are attacked. It is not surprising that the probability of users not being attacked may not be improved using cyber-insurance. The intentions of malicious users to attack the network generally do not change, unless there are mechanisms to track and punish them. Cyber-insurance does not provide a mechanism to track and punish the guilty.
cooperative nature of network users and the effect this has on the overall level of security and appropriate self-defense investments. They also do not consider designing optimal cyber-insurance contracts and alleviating information asymmetry related issues in cyber-insurance. We have already discussed the importance of the problem of investments in cooperative and non cooperative scenarios in a previous paragraph. The problem of optimal cyber-insurance contracts is important for the following two reasons: 1) in general, an insurance contract is first imposed between the insurer and the insured followed by end users deciding on their self-defense investments\(^5\). Previous research efforts assume a given insurance contract in their models and derive the results for incentivizing self-defense and improving network security; they do not compute an optimal cyber-insurance contract that must operate in practice and 2) an optimal insurance contract is important for an insurer to impose, mainly due to commercial profit reasons.

Given an optimal insurance contract, co-operative and non-co-operative Internet users can decide on their optimal amounts of self-defense investments to improve network security [23]. Regarding the importance of addressing informational asymmetry issues, its a well known open problem in network insurance research and to the best of our knowledge, there have been no solutions proposed in the literature [15].

Hence in this paper, we investigate the problem of appropriate self-defense investments under cyber-insurance coverage when Internet users can be both, cooperative as well as non cooperative w.r.t. their self-defense investment amounts. We also devise optimal cyber-insurance contracts in perfect\(^6\) single insurer cyber-insurance markets, and propose a contract-design solution to handle information asymmetry issues in monopolistic cyber-insurance markets. In this regard, we extend our work in [23]. To summarize research advancements, while most related work on cyber-insurance have focussed on proving the role of insurance in incentivizing the adoption self-defense mechanisms, we emphasize our research on the primary elements related to cyber-

\(^5\)Self-defense investments of some kind are also made by a user before it signs a cyber-insurance contract. This is the basic amount of protection an Internet user has before it signs an insurance contract. For commercial profit reasons, a cyber-insurance agency will not insure any user whose basic security protection is below a given threshold. However, if not explicitly specified, we will assume the term ‘self-defense investments’ to be investments made by a user after a cyber-insurance contract is signed.

\(^6\)A perfect insurance market is one where there are no informational asymmetries between the insurer and the insured.
insurance, i.e., insurance parameters and self-defense investments. The contributions of our work are as follows:

1) We quantitatively analyze an $n$-agent model, using botnet risks as a representative application, and propose a general mathematical framework through which Internet users can decide whether to invest in self-defense mechanisms, given that each user is optimally insured w.r.t. insurer objectives in perfect single insurer cyber-insurance markets (see Section II). Our framework is applicable to all risk types that inflict direct and/or indirect losses to users.

2) For perfect single insurer cyber-insurance markets, we perform a mathematical comparative study to show that cooperation amongst Internet users results in better self-defense investments when the risks faced by the users in the Internet are interdependent (see Section III). We use basic concepts from both, cooperative and non cooperative game theory to support the claims we make in Sections II and III. 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.

3) Assuming no informational asymmetry between the cyber-insurer and the insured (for perfect insurance markets), we analytically derive optimal cyber-insurance contracts between a single insurer and its clients (users), where the insurer could have either a social welfare maximizing mindset or a profit maximizing (monopolistic) mindset (see Section IV).

4) We address challenges to implementing cyber-insurance in practical settings, and derive optimal insurance contracts between a monopolistic insurer and non-cooperative insureds under situations of information asymmetry, i.e., under situations of moral hazard and adverse selection [19] (see Section V).

II. MATHEMATICAL FRAMEWORK FOR SELF-DEFENSE INVESTMENTS

In this section, we do the following: 1) to ground the discussion in real systems, we first give a brief description of a representative application of correlated and interdependent risks. That is, for purposes of clarity and ease of presentation, we first describe a representative application,
namely that of ‘botnets’, as this is a reasonably rich and representative example of Internet threats. However, we would like to note that our approach can be applied to other applications with direct/indirect risk scenarios (for instance, such as worms and viruses), 2) we provide a description of our economic model that is relevant to our mathematical framework, and 3) we propose a general mathematical framework for deciding on the appropriate self-defense investment of an Internet user, under optimal cyber-insurance coverage, in perfect single insurer cyber-insurance markets.

A. Representative Application

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 [18]. Here, we 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.
B. Model Description

We consider \( n \) identical\(^7\) rational risk-averse users in a network. We assume the users to be cooperative to a variable degree, i.e, the network supports Internet applications where users cooperate with other users in some capacity to improve overall system performance but may or may not cooperate entirely. The users could either voluntarily cooperate by sharing information with other network users regarding self-defense investments, or be bound to cooperate due to a network regulation, which requires participating users to share self-defense investment information. The users may also decide not to cooperate at all depending on the nature of applications. 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.)

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 buys full\(^8\) cyber-insurance coverage at a particular premium to eliminate its residual risk. A user does not buy insurance 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 also assume for the moment that there exists markets for cyber-insurance, i.e., cyber-insurance strengthens overall network security. For ideal insurance scenarios, i.e., assuming no information asymmetry issues, Lelarge and Bolot [15] have already shown that cyber-insurance improves overall network security. In section V, we design an optimal insurance contract overcoming information asymmetry issues, and thereby

\(^{7}\)We assume identical users to ensure tractable analyses.

\(^{8}\)In section IV, we show that full coverage is the optimal amount of coverage that needs to be advertized by a cyber-insurer in perfect single insurer cyber-insurance markets.
show that cyber-insurance markets exist if there are no information asymmetry problems or if the problems could be overcome.

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 $\overrightarrow{x}_{-i} = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ 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 paper, 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 premium and $IC$ denotes the insurance coverage\(^9\). In this paper, we use the terms ‘final wealth’ and ‘expected final wealth’, ‘user’, ‘Internet user’, and ‘network user’ 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.

C. Mathematical 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 cooperate and do not get infected

\(^9\)For full insurance coverage $R = IC$.
by other users in the network, (2) users cooperate and may get infected by other users in the network, (3) users do not cooperate but may get infected by other users in the network, and (4) users cooperate 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 II-C2.

1) Case 1: No Cooperation, 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 [9]. 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:

\[
\arg\max_{x_i} FW_i(x_i) = w_0 - x_i - p(x_i)R - R + IC
\]

or

\[
\arg\max_{x_i} FW_i(x_i) = w_0 - x_i - p(x_i)R
\]

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 premium for full insurance coverage. Taking the first and second derivatives of \( FW_i \) with respect to \( x_i \), we obtain

\[
FW_i'(x_i) = -1 - p'(x_i)R \tag{2}
\]

and

\[
FW_i''(x_i) = -p''(x_i)R < 0 \tag{3}
\]

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:

\[
p'(x_i^{opt})R = -1. \tag{4}
\]
Economic Interpretation: The left hand side (LHS) of Equation (4) 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 (4)).

2) Case 2: Cooperation, Infection Spread: Under full insurance coverage, user \( i \)'s expected final wealth is given by

\[
FW_i = FW(x_i, \bar{x}_{-i}) = w_0 - x_i - (1 - \prod_{j=1}^{n}(1 - p(x_j)))R \tag{5}
\]

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 [26], 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:

\[
\text{argmax}_{x_i, \bar{x}_{-i}} AFW = nw_0 - \sum_{i=1}^{n} x_i - n(1 - \prod_{j=1}^{n}(1 - p(x_j)))R \\
\text{subject to } 0 \leq p_i(x_i) \leq p_0, \forall i
\]

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

\[
\frac{\partial}{\partial x_i} (AFW) = -1 - np'(x_i) \prod_{j=1, j\neq i}^{n} (1 - p(x_j))R \tag{6}
\]
and
\[
\frac{\partial^2}{\partial x_i^2}(AFW) = -np''(x_i) \prod_{j=1,j\neq i}^{n} (1 - p(x_j))R < 0
\] (7)

The objective function is globally concave, which implies the existence of a unique solution \(x_{i_{opt}}(\vec{x}_{-i})\), for each \(x_{-i}\). Our maximization problem is symmetric for all \(i\), and thus the optimal solution is given by \(x_{i_{opt}}(\vec{x}_{-i}) = x_{j_{opt}}(\vec{x}_{-j})\) for all \(j = 2, ..., n\). We obtain the optimal solution by equating the first derivative to zero, which gives us the following equation
\[
np'(x_{i_{opt}}(\vec{x}_{-i})) \prod_{j=1,j\neq i}^{n} (1 - p(x_i))R = -1
\] (8)

**Economic Interpretation:** The left hand side (LHS) of Equation (8) is the marginal benefit of investing in self-defense. The right hand side (RHS) of Equation (8) 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\(^{10}\), 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., \(x_{i_{opt}}(\vec{x}_{-i}) = 0\). 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 (8)).

3) **Case 3: No Cooperation, 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

\(^{10}\)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.
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 [6]. The game consists of two players, i.e., $|N| = n$; the action set of $G$ is $A = \prod_{i=1}^{n} A_i$, where $A_i \in [0, \infty]$, and the utility/payoff function $u_i(s)$ for each player $i$ is their individual final wealth, where $s \in \prod_{i=1}^{n} A_i$. The pure strategy Nash equilibria of a normal form game is the intersection of the best response functions of each user [6].

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

$$x_{i}^{best}(\overrightarrow{x}_{-i}) \in \arg \max_{x_i} FW_i(x_i, \overrightarrow{x}_{-i}),$$

where

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

(9)

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

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

(10)

and

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

(11)

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:

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

(12)

**Economic Interpretation:** The left hand side (LHS) of Equation (12) is the marginal benefit of investing in self-defense. The right hand side (RHS) of Equation (12) 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., $x_i^{\text{best}}(\overrightarrow{x}_{-i}) = 0$. If the user invests such that it has no exposure to risk, $x_i^{\text{opt}} = \infty$. 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 (12)).

**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., $x_i^{\text{best}}(\overrightarrow{x}_{-i}) = x_j^{\text{best}}(\overrightarrow{x}_{-j})$ for all $j = 2, \ldots, n$.

### III. Comparative Study

In this section, we compare the optimal level of investments in the context of various cases discussed in the previous section. We emphasize here that greater the self-defense investments made by a user, better it is for the security of the whole network. Our results are applicable to Internet applications where a user has the option to be either co-operative or non-cooperative with respect to security parameters.

#### A. Case 3 versus Case 1

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 $i$, $x_i^{\text{opt}} = 0$ in Case 1 implies
In Case 3, i.e., \( x_{i}^{\text{opt}}(x_{-i}^{\text{opt}}) = x_{i}^{\text{best}}(x_{-i}^{\text{best}}) = 0 \), 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 \( i \), \( x_{i}^{\text{opt}} > 0 \) in Case 1 implies \( 0 \leq x_{i}^{\text{best}} < x_{i}^{\text{opt}} \), for all \( x_{-i} \). In Case 3, i.e., \( x_{i}^{\text{opt}}(x_{-i}^{\text{opt}}) > x_{i}^{\text{best}}(x_{-i}^{\text{best}}) \geq 0 \), \( \forall i \). Therefore, under non-cooperative settings, a user always under-invests in self-defense mechanisms.

**B. 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 \( i \), \( x_{i}^{\text{opt}} = 0 \) in Case 2 implies \( x_{i}^{\text{best}} = 0 \), for all Nash equilibrium in Case 3, i.e., \( x_{i}^{\text{opt}}(x_{-i}^{\text{opt}}) = x_{i}^{\text{best}}(x_{-i}^{\text{best}}) = 0 \), \( \forall i \). The condition for optimal investment of each user \( i \) in Case 2 is \(-1 - np'(x_i^{\text{opt}}(x_{-i}^{\text{opt}}))(1 - p(x_i^{\text{opt}}(x_{-i}^{\text{opt}})))^{n-1} R = 0\). The latter expression implies \(-1 - p'(x_i^{\text{opt}}(x_{-i}^{\text{opt}}))(1 - p(x_i^{\text{opt}}(x_{-i}^{\text{opt}})))^{n-1} R < 0\). Hence \( x_{i}^{\text{opt}}(x_{-i}^{\text{opt}}) > x_{i}^{\text{best}}(x_{-i}^{\text{best}}) \geq 0 \), \( \forall i \). 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.

**C. 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 \( p(0) < 1 - n^{-1}\sqrt{\frac{1}{n}} \), 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 \( p_0 < 1 - n^{-1}\sqrt{\frac{1}{n}} \). Thus, for all
In Case 1 implies $x_{i}^{\text{opt}}(\overrightarrow{x_{-i}}) \geq 0$ in Case 3 if and only if $p_0 < 1 - \frac{n-1}{\sqrt{n}}$. In situations of non-zero investment

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

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

$$-1 - np'(x_{i}^{\text{opt}}(\overrightarrow{x_{-i}}))(1 - p(x_{i}^{\text{opt}}(\overrightarrow{x_{-i}}))^{n-1})R > -1 - p'(x_{i}^{\text{opt}}(\overrightarrow{x_{-i}})), \forall i,$$

where $x_{i}^{\text{opt}}(\overrightarrow{x_{-i}})$ is the optimal investment in Case 2. Since the expected final wealth of a user in Case 1 is concave in $x_i(\overrightarrow{x_{-i}})$, $x_{i}^{\text{opt}}(\overrightarrow{x_{-i}})$ in Case 2 is greater than $x_{i}^{\text{opt}}(\overrightarrow{x_{-i}})$ 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 1.** 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 $p(0) < 1 - \frac{n-1}{\sqrt{n}}$, 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. ■

IV. OPTIMAL CYBER-INSURANCE CONTRACTS UNDER NO INFORMATION ASYMMETRY

The main goal of this section is to derive optimal cyber-insurance contracts between the insurer and its clients under conditions of no information asymmetry (for perfect insurance markets), where the insurer could have either a social welfare maximizing mindset or a profit maximizing mindset. When an insurer has a social welfare mindset, it does not care that much about making business profits as it does about insuring people so as to increase the population of users investing in self-defense mechanisms. Its hard to think of any commercial organization in the modern world who would want to provide service without thinking of profits. However, if ISPs would be a cyber-insurance agency, it would want to secure itself, being a computing and networking entity. Given that an ISP is an eyeball and the sink for many end-user flows, it would have a strong reason to ensure high security amongst its clients as a primary objective, in order to strengthen its own security.

A. Model

We consider the scenario where a single cyber-insurance agency provides service to risk-averse Internet users. We assume that the degree of risk averseness of users is 1, i.e., when a user loses an amount of wealth, he does not have any additional pain or negative effect apart from just losing the wealth. We also assume a single cyber-insurer market because Lelarge and Bolot have shown in [15] that insurance targeted towards incentivizing self-defense investments does not entail competitive markets. We model Internet users to be uniformly distributed on the line segment $[0,1]$, i.e., the location $p \in [0, 1]$ of a particular user on the unit interval denotes its probability of facing a substantial risk of size $R$. This is the risk a user faces after some initial investments, which are precautionary efforts both in the monetary, as well as in the non-monetary sense$^{11}$ We assume that the ISP (or any other insurance agency) could have an estimate of this

$^{11}$We emphasize here that these initial investments are not self-defense investments in the sense of the term used in Section II-B. These are investments on security made by a user prior to them signing contracts.
risk probability via the answers to some general questions (e.g., the type of anti-virus protection one uses, the security mindset of a user, and some basic general knowledge on Internet security.) it requires its potential clients to answer before signing up for service, and from the network topology. The network topology gives information about the node degrees, which in turn helps the insurer determine the probability of each user being affected by threats.

Apart from the probability of facing risk, the Internet users are assumed to be homogenous in terms of their initial wealth $w$ and the size $R$ of risk faced, where a risk represents the negative wealth accumulated by a user when it is affected by Internet threats. We assume that the potential risk faced by an Internet user is less than its initial wealth $w$. Each user may buy at most one cyber-insurance policy from the insurer by agreeing to pay a premium $z$ for an insurance coverage amount $c$. The cyber-insurance company advertises only one contract to all its customers. We assume that the level of coverage is not bigger than size $R$ of risk. We also assume that the initial wealth of a user, the size of risk, the cyber-insurance premium, and the level of coverage have the same measurable units$^{12}$. We also account for the fact that the system does not face information asymmetry issues like the moral hazard problem or the adverse selection problem [8].

We apply a risk-averse utility function $U_p(z, c)$ to Internet users, where $U_p(z, c)$ is defined as

$$U_p(z, c) = \begin{cases} w - pR & \text{if it buys no insurance} \\ w - z - p(R - c) & \text{if it buys insurance,} \end{cases}$$

We assume that the cyber-insurance agency is risk-neutral, i.e., it is only concerned with its expected profits. For an insurance policy $(z, c)$ sold to a user, the contract is worth

$$(1 - p)z + p(z - c) = z - pc$$

(13)

to the insurer. Thus, the overall expected profit made by the cyber-insurance agency by providing

$^{12}$Estimating and quantifying risks is an open research problem in cyber-insurance networks [15]. Our model abstracts wealth, coverage, and loss in the same units to ensure modeling simplicity and to promote ease of gaining insights.
the same insurance service to all its clients is

\[ G(z, c) = \int_0^1 (z - pc) dp \]  

(14)

Here, we use ‘contract’ and ‘policy’ interchangeably.

B. Welfare Maximizing Insurance

We now determine an optimal cyber-insurance policy, \((z, c)\), a cyber-insurance agency interested in maximizing social welfare would provide to its customers. We assume here that the insurer values the welfare of each of its customers equally and is not inclined to making negative profit. We also assume that a user can decide whether to buy the policy or not, and that the insurer also has the power to decide whether to provide insurance to a customer, based on its probability of facing risk.

**Problem Formulation.** Let the insurer offer a contract \((z, c)\). An Internet user facing a probability of risk, \(p\), will want to buy cyber-insurance if \(U_p(z, c) \geq U_p(0, 0)\). Thus, the following condition must hold for a user to buy cyber-insurance

\[ w - z - p(R - c) \geq w - pR \]  

(15)

or,

\[ p \geq \frac{z}{c} = p_L(z, c) \]  

(16)

Therefore, a user buys insurance only if its risk probability is higher than some *lower bound* \(p_L\). The lower bound is dependent on \(z\) and \(c\). We observe that lower the value of premium per unit coverage, the higher is the incentive for a user to buy cyber-insurance.

On the other hand, the cyber-insurance agency may not allow every interested user to buy insurance. There exists a particular value, \(p_H\), of the probability of risk, for which \(z = p_Hc\). In such a case, the cyber-insurance company breaks even and the resulting \(z\) is the fair premium. The insurance agency denies insurance service to users whose probability of risk is greater than \(p_H\). Thus, \(p_H\) is the *upper bound* of the risk probability that a user requiring insurance can afford.
if it wants to claim insurance.

A cyber-insurer primarily interested in social welfare advertises a contract \((z, c)\) that maximizes the total welfare of all Internet users in its geographical locality without it making negative profits. Formally, we frame our optimization problem as follows.

\[
\arg\max_{(z, c)} TW = A + B + C
\]

subject to \(D\),

where

\[
A = \int_{p_L}^{p_H} [w - z - p(R - c)]dp,
\]

\[
B = \int_{0}^{p_L} (w - pR)dp,
\]

\[
C = \int_{p_H}^{1} (w - pR)dp,
\]

\[
D = \int_{p_L}^{p_H} (z - pc)dp \geq 0
\]

\(A\) is the expected utility of all Internet users whose risk facing probability, \(p\), lies in the interval \([p_L, p_H]\). \(B\) represents the expected utility of users who have no incentive to buy insurance. The risk probability of these users lies in the interval \([0, p_L]\). \(C\) stands for the expected utility of users who want to purchase cyber-insurance, but are denied by the insurance agency. Their risk probabilities lie in the interval \([p_H, 1]\). Finally, \(D\) represents the constraint of the optimization problem, which states that the expected profits of the cyber-insurer are non-negative.

We state our results through the following theorem. We note that the terms ‘profits’ and ‘total user welfare’ refer to the expected values of profits and social welfare.

**Theorem 2.** For a welfare-maximizing cyber-insurance contract, the optimal (premium, coverage) pair is \((R, R)\); the risk probability lower bound, \(p_L\), equals 1; \(p_H = 1\); total user welfare, \(TW\), is \((w - R\frac{1}{2})\); and the insurer profit, \(P\), equals 0, i.e., the optimal contract is full coverage at a fair premium.
Proof. We first express the risk probability bounds, $p_L$ and $p_H$, as functions of $z$ and $c$. In terms of $z$ and $c$, $p_L$ is equal to $\frac{z}{c}$ and $p_H$ equals $\frac{z}{c}$. Integrating the left hand side of constraint $D$ in our optimization problem, we obtain the cyber-insurer profits as 0. Since the profits are always non-negative, the constraint $D$ is not binding on the optimization problem. Thus, our constrained optimization problem turns into the following unconstrained one.

$$\arg\max_{(z,c)} T - S,$$

where

$$T = w,$$

and

$$S = \frac{1}{2}R$$

Thus, the above unconstrained optimization problem turns out to finding parameters $z$ and $c$ so as to optimize a constant, $w - R/2$. It is evident that the solution to this optimization problem is setting $z$ and $c$ to the maximum values possible, i.e., $R$. The values of $p_L$ and $p_H$ are then easily evaluated to 1.

C. Profit Maximizing Insurance

In this section, we determine the optimal cyber-insurance policy, $(z, c)$, a cyber-insurance agency solely interested in maximizing profits (a monopolist) would provide to its customers. As in Section IV-B, we assume that a user can decide whether to buy the policy or not, and that the insurer also has the power to decide whether to provide insurance to a customer based on its probability of facing risk.

Problem Formulation. A cyber-insurer primarily interested in making business profits chooses a contract $(z, c)$ that maximizes its total profit over all users it services. Formally, we frame our unconstrained optimization problem as follows.

$$\arg\max_{(z,c)} \int_{p_L}^{p_H} (z - pc)dp,$$
where \( p_L \) and \( p_H \) are defined as above.

We state our result through the following theorem.

**Theorem 3.** For a profit-maximizing insurance contract, the optimal (premium, coverage) pair is \((R, R)\); \( p_L = 1 \); \( p_H = 1 \); and the insurer profit, \( P \), equals 0, i.e., the optimal contract is full coverage at a fair premium.

**Proof.** Evaluating the integrand in the objective function, we determine the expression for overall profit as

\[
P = c\left[ \frac{z}{c} \min\{\frac{z}{c}, 1\} - \frac{z}{c} \right] - \frac{1}{2} \left[ (\min\{\frac{z}{c}, 1\})^2 - \left( \frac{z^2}{c^2} \right) \right]
\]

We observe that the expression is increasing in \( c \). Thus, the cyber-insurer maximizes its profit by setting \( c \) equal to \( R \). When the premium per unit of coverage (PPUC) is less than 1, the expected overall profit is 0. When the premium per unit of coverage is greater than 1 and \( c = R \), the optimal premium is determined by equating the partial first derivative of \( P \) to 0, i.e.,

\[
\frac{\partial P}{\partial (PPUC)} = z[1 - \frac{z}{c}] = 0,
\]

which results in a premium \( z \) equal to \( R \). Thus, the insurer profits when PPUC is less than 1 is 0, and also equals 0 when PPUC \( \geq 1 \). Therefore, an insurer never makes profits. Substituting the values of \( z \) and \( c \) in \( p_L \), we get the lower bound of risk probability as 1.

Our result of a monopolistic insurer making zero profits is in accordance with the result by Lelarge and Bolot in [15]. Thus, surprisingly, we observe that a monopolistic cyber-insurance scheme is equivalent to a social welfare motivated insurance scheme. However, this is true because 1) the coverages are provided at a fair premium and 2) the degree of risk averseness of users is 1, i.e., when a user loses an amount of wealth, he does not have any additional pain or negative effect apart from just losing the wealth. The readers are referred to the paper [24] for general results when the degree of risk averseness is greater than 1.

### V. Optimal Cyber-Insurance Contracts Under Information Asymmetry Scenarios

In this section, we model realistic, i.e., imperfect, single insurer cyber-insurance markets and address two informational asymmetry problems arising between the cyber-insurer and the insured,
viz., *adverse selection* and *moral hazard*. In adverse selection, the insurer does not know about the risk category of the user it is insuring, i.e., it does not have knowledge about whether the user is a high risk user or a low risk-user. Moral hazard results in a situation where a user behaves recklessly *after* being insured, knowing the fact that it would be covered. A cyber-insurance agency is most likely to make losses if it does not properly account for information asymmetry in its insurance contract. In this section, we design optimal cyber-insurance contracts under information asymmetry. Our analysis is suitable to scenarios of non-cooperation amongst Internet users, as we firmly believe that it is quite unlikely that users would be cooperative in regard to ensuring social welfare and at the same time behave recklessly themselves.

### A. Model

We assume two classes of users, one which has a high chance of facing risks and the other which has a low chance. We term these classes as ‘LC’ and ‘HC’ respectively. Let $\theta(1-\theta)$ be the proportion of users who run a high chance(low chance) of facing risk of size $R$ respectively. However, on grounds of adverse selection the insurer cannot observe the class of any user. We consider two cases relevant to adverse selection in the Internet: 1) the insurer as well as the insured user have no knowledge about which risk class the user falls in and 2) the insurer has no knowledge of a user’s risk class but the user acquires this knowledge (through third-party agencies) after signing the contract but before it invests in self-defense investments. We assume that each user in class $i \in \{LC, HC\}$ invests an amount $x_i$ in self-defense mechanisms after signing an insurance contract, which reduces its probability $p_i$ of being affected by Internet threats. We list the following mathematical properties related to our risk facing probability function $p$, for users in classes $LC$ and $HC$.

- $p(x)$ is a twice continuously differentiable decreasing function with $0 > p'_{LC}(x) > p'_{HC}(x)$ and $p''_i(x_i) > 0$, i.e., investments by users in class LC are more effective in reducing the loss probability than equivalent investments by users in class HC.

---

13This situation may generally happen when the users do not provide truthful information to insurance agency questionnaires and the insurer cannot estimate the value of correlated and interdependent risks posed to users.
We model moral hazard by assuming that the cyber-insurer cannot observe or have knowledge about the amount of investments made by the insured. Regarding user investments, apart from the self-defense investments made by a user, we assume a certain minimum amount of base investments of value $b_{inv}$ made by an Internet user of class $i$ prior to signing insurance contracts, without which no user can be insured. Thus $p_i(b_{inv})$ is the highest chance of risk a user of class $i$ may face.

The insurance company accounts for adverse selection and moral hazard and designs an insurance contracts of the form $C = (z, c)$, for users in class $j \in \{LC, HC\}$, where $z$ is the premium and $c$ is the net coverage for users. An Internet user adopts the insurance contract and invests in self-defense mechanisms to achieve maximum benefit. We measure the benefit of users of a particular risk class $i$ as a utility, which is expressed as a function of contract $C_k$ and self-defense investments $x_i$. We define the utility function for a users in risk class $i$ and facing a risk of value $R$ as an expected utility of final wealth, and it is expressed as

$$EU_i(C_k, x_i) = p_i(x_i)u(w_0 - R + c_k) + (1 - p_i(x_i))u(w_0 - z_k),$$

where $w_0$ is the initial wealth of user $i$ and $x_i$ is the amount of self-defense investment it makes and $u()$ is a increasing continuously differentiable function ($u'(x_i) > 0, u''(x_i) < 0$) that denotes the utility of wealth. Differentiating Equation 17 w.r.t. $x_i$, we get the first order condition as

$$-p'_i(x_i)[u(w_0 - z_k) - u(w_0 - R + c_k)] = 0$$

The first order condition generates the optimal self-defense investment for user $i$ that maximizes its expected utility of final wealth. In the following sections we analyze optimal cyber-insurance contracts under the presence of moral hazard when 1) neither the insurer nor the insured has any information regarding the risk class of a user and 2) the insurer does not have information regarding user class but the insured acquires information after signing the contract but before
making self-defense investments.

B. Neither the Insurer Nor the Insured Has Information

An Internet user does not know its risk class and therefore it maximizes its expected utility of final wealth by setting its probability of loss equal to an expected probability value of \( p_\alpha(x) = \theta p_{HC}(x) + (1 - \theta)p_{LC}(x) \) and solving Equation 17. We assume that the values of \( p_{LC}(x) \) and \( p_{HC}(x) \) are common knowledge to the insurer and the insured. The cyber-insurer on the other hand, maximizes its profits by offering a contract \( C_{\alpha^*} = (z_{\alpha^*}, c_{\alpha^*}) \). The optimization problem related to an insurer’s profit is given as

\[
\text{argmax}_{z_{\alpha}, c_{\alpha}, \lambda_{\alpha}, \rho_{\alpha}, \rho_0} q_{\alpha} [1 - p_\alpha(x_\alpha) z_\alpha - p_\alpha(x_\alpha) c_\alpha]
\]

subject to

\[
U_{\alpha}(C_{\alpha^*}, x_{\alpha^*}) - U_{\alpha}(0, x_0) \geq 0, \quad (19)
\]

\[
-p'_\alpha(x_\alpha)[u(w_0 - z_\alpha) - u(w_0 - R + c_\alpha)] = 0, \quad (20)
\]

\[
-p'_\alpha(x_0)[u(w_0) - u(w_0 - R)] = 0, \quad (21)
\]

where \( q_{\alpha} \) is the number of cyber-insurance contracts sold by the insurer and \( x_0 \) is the amount of self-defense investments when no insurance is purchased. \( \lambda_{\alpha}, \rho_{\alpha}, \rho_0 \) are the Lagrangian multipliers related to constraints 19, 20, and 21 respectively. \( \alpha \) could be considered as the risk class that each user feels its in, as it does not have perfect information about whether its in class \( LC \) or \( HC \). Constraint 19 is the participation constraint stating that the expected utility of final wealth of a user is atleast as much with cyber-insurance as without cyber-insurance. Constraints 20 and 21 state that Internet users will invest in optimal self-defense investments so as to maximize their utility of final wealth, and this is in exact accordance to what the cyber-insurer wants. We derive the Lagrangian [28] and first order conditions for our optimization problem but omit it in the paper due to lack of space.

The optimization problem presented in this section is an example of a general principal-agent
problem. The Internet users (agents) will act non-cooperatively as utility maximizers, whereas the principal’s problem is to design a mechanism that maximizes its utility by accounting for adverse selection and moral hazard. Thus, the situation represents a Bayesian game of incomplete information [6]. According to Palfrey and Srivastava [25], there exists an incentive-compatible direct revelation mechanism [33] for the problem, where users do what the insurer desires (i.e., invest optimally in self-defense investments), provided the constraints in the optimization problem bind. The solution to the optimization problem in the binding case is full insurance coverage as the utility function becomes more risk averse, and partial insurance coverage otherwise.

C. Insurer Has No Information, Insured Obtains Information

In this scenario, we assume that the insurer does not have information about the risk class of a user and it cannot observe the risk class if the user obtains information from any third party agency. Since, the cyber-insurer is the first mover, it will account for the fact that users will be incentivized to take the help of a third party. We consider the case where the user may acquire information, and based on the information it decides on its self-defense investments.

Let \( U_\alpha(C_k, x) \) be the utility of a user in risk class \( \alpha \) for a contract \( C_k \), when it cannot observe the risk class it is in. Let \( \theta U_{HC}(C_k, x) + (1 - \theta)U_{HC}(C_k, x) \) be the utility of the same user when it can get information about its risk class from a third party agency. Thus, we denote the value of gaining information to a user is \( VI(C_k) \) and its defined as

\[
VI(C_k) = \theta U_{HC}(C_k, x) + (1 - \theta)U_{HC}(C_k, x) - U_\alpha(C_k, x), \quad 0 \leq \theta \leq 1
\]

(22)

We emphasize that \( VI(C_k) \) is zero if there is only type of risk class in the market. Now let \( x_{ik} \) be the solution to Equation 18, for risk class \( i \) and contract \( C_k \). Since \( p'_{LC} < p'_{\alpha} < p'_{HC} \), for contract \( C_k \), we have \( x_{LCk} > x_{\alpha k} > x_{HCk} \). Thus, \( VI(C_k) > 0 \) due to the following relationship

\[
U_i(C_k, x_{ik}) > U_i(C_k, x_{\alpha k}), \quad i = LC, HC
\]

(23)

The cyber-insurer maximizes its profits by offering a contract \( C_d = (z_d, c_d) \). The optimization
problem related to an insurer’s profit is given as

\[
\arg\max_{z_d,c_d,\lambda_d,\rho_d,\rho_0} \sum_{i=LC,HC} q_i [1 - p_i(x_d)z_d - p_i(x_d)c_d]
\]

subject to

\[
U_i(C_d, x_d) - U_i(0, x_0) \geq 0, \ i = LC, HC
\]

\[
-p_i'(x_d)[u(w_0 - z_d) - u(w_0 - R + c_d)] = 0, \quad (25)
\]

\[
-p_\alpha'(x_0)[u(w_0) - u(w_0 - R)] = 0, \ i = LC, HC
\]

where \(q_i\) is the number of cyber-insurance contracts sold by the insurer for class \(i\) and \(x_0\) is the amount of self-defense investments when no insurance is purchased. \(\lambda_d, \rho_d, \rho_0\) are the Lagrangian multipliers related to constraints 24, 25, and 26 respectively. Constraint 24 is the participation constraint stating that the expected utility of final wealth of a user is at least as much with cyber-insurance as without cyber-insurance. Constraints 25 and 26 state that Internet users will invest in optimal self-defense investments so as to maximize their utility of final wealth. We omit the expressions for the Lagrangian and first order conditions due to lack of space. The solution to the optimization problem in the binding case results in full insurance coverage if \(VI(C_k) = 0\) and partial insurance coverage if \(VI(C_k) > 0\). If \(VI(C_k) > 0\), a user would prefer to have information on its risk class and accept contract \(C_d\) rather than accept contract \(C_{\alpha^*}\).

VI. CONCLUSION

In this paper, we developed a general mathematical theory of security investments in the Internet under cyber-insurance coverage for single insurer cyber-insurance markets. We showed that in case of perfect insurance markets with no information asymmetry, full insurance coverage is the optimal coverage offered by the cyber-insurer, and cooperation amongst Internet users leads to better user self-defense investments w.r.t. improving network security. In the case of imperfect cyber-insurance environments where users are generally non-cooperative, we showed that partial insurance is the optimal cyber-insurance coverage offered by a profit-maximizing cyber-insurer.


REFERENCES


