Chinese Traditional Medicine Journal

ISSN : 2693 6356
2019 | Vol 2 | Issue 2

An Analysis of Pre-Screening's Impact on Cyber Insurance Policies and the Role of Security Dependence

G.ANUSHA [1], P.RAMESH BABU [2]

[1] M.C.A Student, Dept of M.C.A, Amrita Sai Institute of Science & Technology, Paritala, A.P., India
[2] Associate Professor, Dept of CSE, Amrita Sai Institute of Science & Technology, Paritala, A.P., India

ABSTRACT

Insuring against cyber attacks is a practical solution for transferring risk. However, it has been shown that the condition of network security may or may not improve, depending on the characteristics of the underlying environment. In this study, we focus on a single, profit-maximizing insurer (principal) working with insureds/clients (agents) who are providing their services willingly. We focus on two specific aspects of cyber security and how they affect the contract design issue. The first is that cyber security is inherently reliant on the actions of other entities within the same ecosystem (i.e. externalities), making it difficult for any one institution to ensure its own security in isolation. The second is that we can now conduct precise quantitative evaluations of an organization's security posture thanks to recent developments in Internet measurement and the use of machine learning methods. It may be used to conduct preliminary security checks on potential customers, sometimes known as "prescreening," to facilitate premium differentiation and the creation of tailored policies. We show that the inefficient effort levels of interdependent agents who do not account for the risk externalities when insurance is not available create a "profit opportunity" for the insurer, in addition to the usual profit that an insurer makes from risk transfer. The insurer can "sell commitment" to interdependent agents in addition to insuring their risks thanks to the results of security pre-screening, which allow the insurer to capitalize on an additional profit opportunity. We determine the circumstances under which this sort of contract results in not only greater principle profit but also enhanced network security.

Search Terms: Framework, Python, Django, MySQL, and WampServer.

INTRODUCTION

Existing studies investigate the impact of insurance on agents' security costs, and take into account competitive insurance markets under compulsory insurance. The authors of demonstrate that when insurance is present, the condition of network security is typically worse than in the no-insurance situation, even when the market is competitive and the agents are all the same. Existing research demonstrate that introducing insurance cannot enhance network security in a network with heterogeneous agents. Analyze how investments change as the degree of dependency between agents changes, and prove that investment drops down sharply as interdependence rises. Examine a competitive market with and without moral hazard, assuming that all agents are acting voluntarily. Without moral hazard, the insurer may see the agents' security investments and charge them a different premium depending on those investments. They demonstrate how agents might be incentivized to expand their investments in self-defense in such a market. They demonstrate, however, that the market does not provide an incentive for upgrading agents' investments when moral hazard is present. In the current system, researchers have examined how insurance affects network security when the insurer is a monopolist that seeks to maximize shareholder value at the expense of policyholders. In these models, agents are motivated by premium discrimination—that is, agents with larger investments in security pay lower premiums—because the insurer's purpose is to maximize societal welfare under the assumption of compulsory insurance. Therefore, these investigations demonstrate that insurance may result in increased network safety. Existing literature examines a market for insurance with a monopolistic profit-maximizing insurer under the premise of voluntary participation, and concludes that insurance cannot enhance network security in the face of moral hazard.

PURPOSE OF THE PROJECT

Cyber insurance contract design for risk-averse and risk-neutral agents by a single profit-maximizing insurer. We demonstrated that although introducing insurance reduces network security amongst unrelated agents, the outcome may change between related agents. In particular, we demonstrated that the inefficient effort levels exerted by free-riding agents when insurance is unavailable but interdependency is present creates a profit opportunity for the insurer, in addition to the typical profit that an insurer earns from risk transfer. We demonstrated that security prescreening provides the insurer with a chance to boost profits by marketing commitment to mutually dependent agents and creating incentives for agents to put in more effort.

EXISTING SYSTEM

In this study, we'll investigate whether or not cyber insurance may be used to motivate better network security practices. Different from the bulk of the previous research, we adopt two model assumptions that we feel better depict the actual status of cyber insurance markets: we will assume a profit-maximizing cyber insurer, and we shall assume that agents may choose not to purchase a contract if they so choose. We highlight the interdependence of security and the availability of risk assessment as two key aspects of cyber-insurance under this paradigm. Because of recent developments in Internet measurements and machine learning methods, we can now conduct precise, quantitative security posture assessments at the enterprise level, which explains the first characteristic. To reduce the risk of moral hazard via premium discrimination and the creation of tailor-made policies, this may be utilized in the preliminary security audit or pre-screening of a new customer. The second distinguishing element is the interdependent nature of security, which is the observation that an entity's security status often relies on the efforts of other entities engaging with it within the eco-system as well as the entity's own efforts towards adopting security measures. Because of this interdependence, the insurer has a contract design challenge in that it must provide protection to each insured against financial loss resulting from both direct and indirect violations.

PROPOSED SYSTEM

Existing studies investigate the impact of insurance on agents' security costs, and take into account competitive insurance markets under compulsory insurance. The authors of demonstrate that when insurance is present, the condition of network security is typically worse than in the no-insurance situation, even when the market is competitive and the agents are all the same. Existing research demonstrate that introducing insurance cannot enhance network security in a network with heterogeneous agents. Analyze how investments change as the degree of dependency between agents changes, and prove that investment reduces as interdependence grows. Examine a competitive market with and without moral hazard, assuming that all agents are acting voluntarily. Without moral hazard, the insurer may see the agents' security investments and charge them a different premium depending on those investments. They demonstrate how agents might be incentivized to expand their investments in self-defense in such a market. They demonstrate, however, that the market does not provide an incentive for upgrading agents' investments when moral hazard is present. In the current system, researchers have examined how insurance affects network security when the insurer is a monopolist that seeks to maximize shareholder value at the expense of policyholders. In these models, agents are motivated by premium discrimination—that is, agents with larger investments in security pay lower premiums—because the insurer's purpose is to maximize societal welfare under the assumption of compulsory insurance. Therefore, these investigations demonstrate that insurance may result in increased network safety. Existing literature examines a market for insurance with a monopolistic profit-maximizing insurer under the premise of voluntary participation, and concludes that insurance cannot enhance network security in the face of moral hazard.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors.

The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

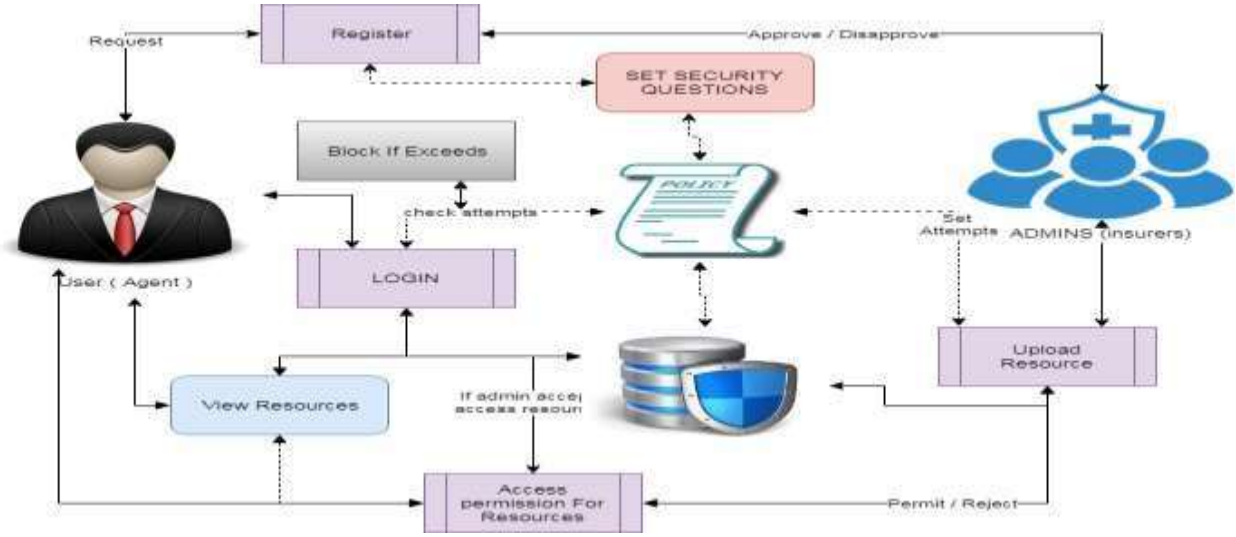
2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by thesystem.
The output form of an information system should accomplish one or more of thefollowing objectives.

- Convey information about past activities, current status or projections oftheFuture.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

SYSTEM ARCHITECTURE

This growing market has motivated an extensive literature which aims to understand the unique characteristics of these emerging contracts, their effect on the insureds' security expenditure, and the possibility of leveraging these contracts to shape users' behavior and improve the state of cybersecurity; see Section II for an overview of the related literature. The conclusions of these studies depend on the assumptions on the insurance market model (profit maker vs. welfare maximizing insurers), the agents' (insured's) participation decisions (compulsory vs. voluntary insurance), and the assumed model of interdependency among the insured.



SCREENS SHOTS

CONCLUSION

We looked at the issue of a single profit-maximizing insurer establishing cyber insurance contracts for both risk-neutral and risk-averse agents. We demonstrated that although introducing insurance reduces network security amongst unrelated agents, the outcome may change between related agents. In particular, we demonstrated that the inefficient effort levels exerted by free-riding agents when insurance is unavailable but interdependency is present creates a profit opportunity for the insurer, in addition to the typical profit that an insurer earns from risk transfer. We demonstrated that security prescreening provides the insurer with a chance to boost profits by marketing commitment to mutually dependent agents and creating incentives for agents to put in more effort. We demonstrate the circumstances under which these contracts lead to not only better network security but also higher profits for the principal and more benefits for the agents.

FUTURE ENHANCEMENTS

Studying the problem with pre-screening under partial information assumptions would be an important direction of future research; this would include imperfect knowledge of the agents' type by the principal as well as imperfect knowledge of the interdependence relationship by the agents and the principal. Other modeling choices such as alternative use of pre-screening assessment (as opposed to linear discounts on premiums), and more general ways of capturing correlated risks (e.g., joint distribution of losses as opposed to average loss being a function of joint effort), would also be of great interest. Finally, a competitive market setting and its effects on network security isalso worth studying.

BIBILOGRAPHY

[1] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: Mitigating moral hazard through security prescreening," in The 7th International EAI Conference on Game Theory fo Networks (Gamenets), 2017.

[2] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies in the presence of security interdependence," in The 12th Workshop on the Economics of Networks, Systems and Computation (NetEcon), 2017.

[3] C. Hemenwa, "ABI Research: Cyber insurance market to reach $10B by 2020," www.advisenltd.com/2015/07/30/abi-researchcyber-insurance-market-to-reach-10b-by-2020/, 2015.

[4] Insurance Information Institute, "U.S. cyber insurance market demonstrates growth, innovation in wake of high profile data breaches," www.iii.org/pressrelease/us-cyber- insurance-marketdemonstrates-growthinnovation-in-wake-of-high-profile-databreaches-102015, 2015.

[5] N. Shetty, G. Schwartz, and J. Walrand, "Can competitive insurers improve network security?," in The Third International Conference on Trust and Trustworthy Computing (TRUST), 2010.

[6] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, "Competitive cyber- insurance and internet security," Economics of Information Security and Privacy, pp. 229–247, 2010.

[7] G. Schwartz, N. Shetty, and J. Walrand, "Cyber-insurance: Missing market driven by user heterogeneity," 2010.

[8] G. A. Schwartz and S. S. Sastry, "Cyber-insurance framework for large scale interdependent networks," in The Third International Conference on High Confidence Networked Systems, 2014.

[9] H. Ogut, N. Menon, and S. Raghunathan, "Cyber insurance and it security investment: Impact of interdependence risk," in The Workshop on the Economics of Information Security, 2005.

[10] Z. Yang and J. C. S. Lui, "Security adoption and influence of cyber-insurance markets in heterogeneous networks," Performance Evaluation, vol. 74, pp. 1–17, Apr. 2014.