Cyber Risk Insurance Pricing Based on Optimized Insured Strategy

by

Yueshan He

A research paper
presented to the University of Waterloo
in partial fulfillment of the
requirement for the degree of
Master of Mathematics
in
Computational Mathematics

Supervisor: Prof. Ken Seng Tan

Waterloo, Ontario, Canada, 2016

I hereby declare that I am the sole author of this report. This is a true copy of the report, including any required final revisions, as accepted by my examiners.

I understand that my report may be made electronically available to the public.

Abstract

This decade has seen a rapidly increasing trend in the demand for cyber risk management strategies. Risk managers and operators of critical organizations are seeking approaches to minimizing cyber risk management budgets and covering exposed value as much as possible. Small business owners used to underestimate cyber risk, and so suffered from cyber accidents. Now even with better understanding of the risks, they hesitate to pay high premiums for cyber protection. The insurance industry is driven to provide standalone contracts for this newly emerged risk with its hard-to-predict losses and deteriorating through information asymmetry. More accurate measurement for analyzing cyber exposure and a model to decide premium loading are imperative to better coverage of the global cyber system.

This paper established a framework of entities for managing cyber accidents and insurance institutions design policies and provides an overview of operations and products. Based on the analysis of the market, the problems of existing adverse selection and limited products for cyber risk are addressed. Designing acceptable contracts is considered to be a key solution. Since there is a problem with lack of loss records, the view of insured is taken to identify transferred risk. An expected cyber loss function is employed and which is the product of the exposure asset, the exposure factor, the probability of being attacked, and the loss given if an attack is successful. An optimized investment decision system is implemented to obtain the transferred risk of the insured (which is also the risk covered by the insurance industry). A Monte Carlo simulation method is used to estimate the premium loading conditioning on the optimized insured strategy. The goal is to better match the demand and supply of insurance contracts. A profit & loss function was used to quantify insurance institutions' profitability. The Monte Carlo method provides a reasonable premium rate and could be utilized with empirical data, as well as with more complicated practical situations. Considering the restrictions and the necessity to control adverse selection and moral hazard, possible ways to hedge the risk of insolvency are also discussed.

Acknowledgment

I cannot express enough thanks to my supervisor : Dr. Kenseng Tan, Canada Research Chair in Quantitative Risk Management at University of Waterloo; I offer my sincere appreciation for his providing me the opportunity being his research assistant, inspiring me with the vision and foresight of insurance industry, supporting me with encouragement and instructions. My project could not have been accomplishment without his help.

I would like to express my gratitude towards all the powerful and supporting professors of University of Waterloo: Dr. Martin Lysy, Dr. Yeying Zhu, Dr. Changbao Wu, Dr. Lilia Krivodonova, Dr. Ali Ghodisi, Dr. Bin Li, Dr. Jeff Orchard, Dr. Paul Marriott, Dr. Peter Forsyth, Dr. Stephen Vavasis, Dr. Wayne Oldford, Dr. Kun Liang, Dr. Shoja'eddin Chenouri. I learned a lot from their courses and they are always providing valuable support and guide. I really enjoy my time learning at University of Waterloo with those wonderful professors. I utilized not only the knowledge they delivered on class, but also the rigorous attitude to academic research I learned from them in my project.

I also appreciate my friends, who make progress and grow with me. Lisa, Alister, Olina, Nathen, Grupreet, Leo, Xinghang, Mike, Disen, Hang, Calcium, Ning. They are willing to share their information about the studies and life. They give me a lot of new ideas about my projects; I will always remember the nights we stay up late working on projects.

I also want to thank Computational Math program, Dr. Arne Storjoann, Dr. Kevin Hare, Stephanie Martin. They provide me best support studying at University of Waterloo. They arrange great academic seminars and activities. They provide useful information and suggestion on school life.

Also a great thanks to school authority for given us students permission to experiment in school labs. And all the martial and data source that we used in library.

Dedication

Every challenging work needs self efforts as will as guidance of elders especially those who were very close to our heart.

I appreciate my parents for supporting me mentally and physically not just finishing the tasks but also my whole studies in order to accomplish my dream one day. I appreciate my teachers and classmates in China who share their informations and always encourage me working harder.

And I would like to appreciate every individual who offered me help during my staying in Canada. I appreciate the first time, the kind stuff of Tim Hortons taught me how to use the self-service machine. I appreciate my first roommate providing a campus tour and giving suggestion on every respect of study life.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

On November 14, 2014, the film studio Sony Pictures Entertainment was attacked by a hacker group called the "Guardians of Peace". Confidential data, including personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films and other information, was released. According to Reuters, this cyber attack would cost Sony studio as much as 100 million dollars. After sonypictures.com was attacked previously in 2011, Sony made a claim of $1.6 million from its insurer, Hiscox. After that, this cyber insurer refused to quote a renewal. Sony Pictures thus purchased a $20 million policy from Lockton, which including $10 million in self-insured retention. In April 2015, Sony's cyber contract was moved to AIG acquiring $10 million in coverage. In May, Sony turned to Marsh, which reached out to Brit Insurance, Liberty International Underwriters, Beazley and other carriers to secure $60 million in coverage. However, compared to the total direct and indirect loss the movie studio confronted, this was apparently not an enough coverage. The costs arose from new software and hardware, employee labor relation repair, investigations, lawsuit fees, as well as reputation damage.

1.1 Overview of Cyber Risk

Since 2010, companies, organizations, and individuals have had to face up to cyber threats, and there is an increasing trend of cyber crimes.

a. Development Risk

The development of information technology has no doubt made a great difference in almost all of the industries in the world, for example, banking, health-care, retail and so on. However, at the same time, the dark side of information and technology has been revealed. Data breaches, business interruptions, unauthorized access, industrial control system (ICS) attacks and many other cyber incidents contribute to high financial and reputation damage. In other words, our dependency on information and technology exposes us to cyber risk.

b. Operational Risk

Cyber risk was first described as Internet-related risk [16], which is a broad definition. Promoted by the awareness of the crucial role of cyber risk, the definition of cyber risk has become more clear and detailed from views of IT and risk management. Biener, Eling and Wirfs [5] discussed several definitions of cyber risk. First, a narrow concept regards cyber risk as the malicious electronic events causing system failure and monetary loss. Second, broader view, generally define cyber risk as information technology security risk. Third, a definition adopted from Cebula and Young [7] considers cyber risk to be operational risks [1]to IT assets that result in damage to confidentiality, availability or integrity of information systems.[2] Categorizing cyber risk as operational risk is widely accepted nowadays. Cyber risk has become the most common operation risk [33].

c. Interdependent Risk

Although cyber threats ate unique based on region, industry, degree and company size, cyber crime is interdependent since the Internet is a shared medium. On the one hand, internal correlation includes collaborations and communications among security layers and systems; on the other hand, global (external) correlation includes entities using standard software facing the same risk of viruses and other vulnerabilities, and firms and their suppliers sharing information. To be more concrete, Bohme and Kataria [6] proposed examples for different kinds of cyber-risk correlation. They claimed that worms and viruses contribute to both high global correlation and high internal correlation; hardware failure has both low global correlation and low internal correlation; spyware/phishing leads to high global correlation and low internal correlation; and insider attacks result in low global correlation and high internal correlation.

d. Top Risk

[1] They categorize cyber risk into four classes based on frameworks in Basel II: (1) actions of people, (2) systems and technology failure, (3) failed internal processes and (4) external events

[2] Confidentiality, availability or integrity: ISO27000

The last decade has seen the astonishing growth of cyber crime industry, which is an escalating threat not only increasing in frequency and spectrum, but also in complexity and severity. To be more specific, the number of detected cyber-attacks skyrocketed during 2014, up 48% from 2004, at roughly 117,339 incidents per day [34]. Although most recorded cyber attacks targeted medium-size entities, there is a growing trend of small enterprise attacks because they can provide a back door to companies with a more robust system [3], [10]. Companies will not only be exposed to direct cyber attacked but also be affected by supply chains and across counterparties. The average annual cost of cyber attacks to affected businesses has grown 17 percent per annum, reaching $9 million per business. Cyber incidents re estimated to cost more than $400 billion a year [9], [10], [36]. Considering that more than 50 billion devices could be connected by 2020[8], along with the increasing interconnectivity, globalization, and commercialization, we can expect increasing numbers of victims,which will enhance both the exposure and the impact of cyber risk and a deteriorating loss in the foreseeable future. According to Global Risks Report of World Economic Forum [13], cyber risk is currently ranked as one of the top 10 risks most likely to cause world crisis.

1.2 Features of Cyber Incidents

a. Regional Variation According to Biener et al.[4], property and liability insurance usually exclude cyber risk, in response to this situation, an exclusive insurance product for cyber risk has emerged, mostly in the United States. This national response can be explained by the regional variation of cyber incidents. North America, Europe, Asia have traditionally spent most on cyber protection and Africa the least, because there is a strong correlation between a region's income level and loss to cyber crime [5], [10]. In Marsh Global Risks Report, 2016, cyber risk is the most likely global risk in North America [13].

b. Victim Size and Sector
Different from Biener et al.'s research [13] which uses employees number to present the size of firms, reports typically use revenue size to describe the size of an entity. Nano-Revenue (<$50M), Micro-Revenue ($50M-$200M) and Small-Revenue ($300M-$2B) companies occupied about 71% of the claims related to data breaches [30], perhaps because they do not have the resources to protect themselves against cyber risk or to absorb its damage. Notice that although the Nano, Micro, and Small organizations account for a significant proportion of the insurance claims, these claims are only for about 20% of the total data exposed worldwide (exposed records). In contract, Mid ($2B-$10B) and

Large-Revenue($10B-$100B) organizations account for 60% of the exposed records. Sectors holding a considerable amount of private information, such as healthcare, retail, and education; sectors storing incentive personal financial information, such as financial institutions, as well as those who depend a lot on digitalized technology processes, such as manufacturing, telecommunications, technology, are most likely to be attacked. However, there is growing impact among the energy, utilities and transport sectors, driven by the increasing perils posed by interconnectivity.

c. Cyber Incidents Types

Data privacy is the key risk at-risk asset, since cyber incidents recorded by Advisien broke down as follows: digital data breach, loss or theft of information (61%); improper disposal/distribution loss or theft (14%); privacy violations 10%; system/network security violation disruption (7%). Other types of accidents, for example, fraudulent use or access and cyber extortion sum up to less than 10% [1]. Personally identifiable information (PII),payment card information (PCI) and private health information (PHI) are the most common types of data included in a claim [30]. The highest average cost cases are digital asset loss or theft, phishing and skimming, and system failure [1].

d. Cause of Loss

The most costly cyber crimes are those attributes to malicious insiders, denial of services and web-based attacks [20], and the most frequent causes of loss are hacking and malware. Notice that in [12], [30], 25% of the claims submitted are attributed to third party vendors, more than 20% of the data breach has insider involvement. A worse finding is that 81.9% of attacks take only minutes to get to in the system, but 67.8% of strikes take days to recover from [12].

1.3 Problem Description

Unlike fire insurance, which has more than 1000 years of history, cyber risk emerged just decades ago and is developing with high technology. Material loss includes property loss, reputation damage and bodily injury, but existing property or liability insurance typically does not cover cyber accidents, moreover, there are few existing policies could make up the coverage gap. Furthermore, many organizations are unaware of the potential loss, underestimate the newly growing threat and their exposure to large risk. Only attacked companies push to seek risk transfer. Finally, the hard-to-predict losses, lack of market participation, adverse selection, and dependent incidents among networks hobble carriers efforts to provide satisfying products. A conservative charge for the cyber insurance contract is higher compared with traditional policies. The limited coverage and high price aggravate the lack of active risk transformation with insurance.

Risk managers and brokers have been eager to introduce and improve quantitative methods to measure expected cyber losses and mitigate the potential loss. Better matching the demand and supply of insurance products is a critical task for the cyber insurance industry. In the first chapter, an overview of cyber risk and cyber incidents are provided. In the next chapter, cyber risk insurance market is analyzed, and we showed that to speed up the procedure covering the global cyber system, the prime process is to design acceptable cyber insurance products. Two main steps of designing insurance contract are identifying insured risk and pricing. A cyber risk management framework was also structured in this chapter to demonstrate that identifying transferred risk based on insured optimized system could be used to quantify risk covered by the insurance industry. Thus, finding out an appropriate method to quantify insureds' risk and establish an insured optimization decision system would accomplish the first step in designing acceptable contracts. In the third chapter, a quantification method is defined based on National Bureau Standard and Gordon's vulnerability function. Four scenarios are discussed to establish an insured optimization system. The quantification function illustrated the cost-effectiveness of cyber insurance and the scenarios explained how the restrictions influence cyber insurance coverage. Thus, this chapter formed the basis for further pricing procedure. In chapter four, Monte Carlo simulations based on the optimized insured strategy are deployed to price cyber premium loading for a general market consists of small companies, as well as for a particular company. Corresponding profit & loss distributions of carriers are computed to test the profitability of the pricing approach. In Chapter five, plans to hedge the insolvency risk of insurance institutions were employed. Finally, the findings and suggestions for future research are concluded in the last chapter.

Chapter 2

Background

2.1 Cyber Risk Insurance Market

In this section, the market situation of the cyber insurance industry is analyzed from the point of views of both insured companies and insurer companies. And the finding is that there exist sever risk exposure and adverse selection problems due to high price, limited coverage and un-preparation, and the key solution is to provide an acceptable product.

2.1.1 Insured: Management Operation Overview

a. Insufficient Knowledge
The world has underestimated the dangers of cyber attacks . The rank of cyber risk among top risks in the world was raised up from 15th in 2013 to 5th in 2015 [36]. Although the awareness of cyber risk is increasing rapidly, a significant percentage of organizations still of knowledge of cyber risks. In Europe, 79% of the companies have at best basic understanding; in other words, only 21% of organizations completely understand cyber threats [25]. In the US, to reduce the server cyber risks against organizations' underestimation, government introduced mandatory notification requirements, requirements that have now spread of over 90% of US states.

b. Insufficient Preparation
According to the Allianz Report [36], the top risk for which businesses are least prepared is cyber risk followed by supply chain disruption, natural catastrophes, political/social

upheaval and terrorism. In Europe, nearly 68% of organizations have not estimated the financial impacts of a cyber-attack; only 25% of organizations possess an incident response plan for real cyber events and 77% organizations do not assess suppliers or customers they trade with for cyber risk [25]. The top reason why companies are not prepared to combat cyber risk is underestimation (79%) [36].

c. Limited Coverage

Although the number of cyber risk insurance products increased rapidly after 2005, and the amount of new cyber risk insurance products provided in this decade is twice the number of Internet-related insurance products before 2005, the market coverage is still relatively small. Current available insurance policies are not sufficient to cover the financial and reputation losses due to cyber incidents. In a 2013 study of Europe, only 7% of the companies believed that the insurance available meets all of their needs [26]. Although 81% large organizations and 61% of small companies suffered from cyber crime in 2013, the market coverage was estimated to be between 6% and 10% [26], [41], [42]. In 2015, the percentage of organizations bought or were in the process of getting quotations for cyber insurance in Europe was 18% , which is almost double the number in 2013, but it is still small.

d. Increasing Demand for Insurance

As stated in the Betterley Report, nearly half of insurers reported premium growth of between 26% and 50%, and the annual gross written premium is as much as $2.75bn [3]. Cyber insurance was the only line with a consistent, substantial rate increase, averaging more than 15% in the US in 2015 [27]. This growth has found to be dampened by price competition as new insurers fight for market share. The cyber insurance worldwide market is now estimated to be worth around $2bn in premiums, with US businesses accounting for approximately 90% [26]. The cyber market is growing by double-digit figures year-on-year, and could reach $20bn or more in the next ten years," says Nigel Pearson, Global Head of Fidelity, AGCS [36].

2.1.2 Insurer: Product Overview

[3]**a. Non-standard Coverage**

The three main types of coverage are liability, remediation, and fines and penalties. Typically, liability coverage includes unauthorized accesses, privacy breaches (the theft, corruptions or deletion of electronic data from company computer systems), denial of service (the

[3] The results of section 2.2.2 are summarized from the Betterley Report 2015 [3]

denial of an authorized users access to a company computer system and the participation by the company's computer system in a denial of service directed against a third party's computer system), transmission of malicious code, personal injury and cyber extortions.

Remediation coverage consists of (1)computer legal costs (costs associated with any mandated forensic investigations to find the cause of a breach); (2) restoration service; (3)notification costs (voluntary and statutory notification); (4) privacy assistance expense (assisting any individual by providing credit/identity file monitoring services, call center fees) and (5) crisis management expenses (costs of protecting and re-establishing the companies reputation, consumer redress fund).

Fines and penalties refer to civil penalties (where insurable against by law) arising out of the violation of regulatory acts, the violation of privacy laws, as well as consumer-redress funds.

Payment Card Industry (PCI) coverage provided is divided into PCI fines and penalties and PCI assessments (fraud charges and card re-issuance costs). Almost all insurers (29 of the 31 companies) included in the Betterley Report provide PCI fines and penalties coverage, but half of them require endorsement for it. Most insurers cover fraud charges and card re-issuance costs, and half of them require endorsement. Coverage extensions are media liability and intellectual properties.

As for media liability, not only social media activities can be covered now, since all companies offer multimedia protection. For intellectual properties, (1) unauthorized use of advertising materials, slogans or title of others; (2) infringement of copyright, titles, slogans,trademarks, trade names, trade dresses, service marks or service names in covered materials; (3) plagiarism or unauthorized use of literary or artistic format characters or performance covered materials; (4) invasion or interference with an individual's right to publicity, and many other intellectual properties are protected.

b. Various Exclusions

None of the companies in the Betterley Report [3] includes offense involving patent infringement in the coverage. Almost 90% of the contracts exclude dishonest /fraudulent/ criminal/malicious acts, intentional acts, direct bodily injuries, direct property damages, infringement of patent/copyright trademarks, and contractual liability form coverages. Over half of the insurers exclude beaches of warranties/guarantees, theft of intellectual properties and hardware damages. A small number of insurers exclude failure to maintain security standards, transfer of funds to/from financial institutions, loss of use properties, personal injuries, advertising injuries, computer viruses, and wears and tears.

Regarding first-party coverage, data destruction, virus extraction, business interruption, denial of service, theft of data and extortion are widely covered; but theft of the economic value of intellectual properties, theft of money of security, theft of finished goods or work in processes or theft of computing resources are not included. Third-party coverage consists of privacy and network liability, regulatory liability, media liability, and technology errors and omissions. However, direct property damages and direct body injuries are not included. And less than half of the insurance institutions provide coverage for contingent properties and body injuries.

c. Lack of Mandatory Risk Management Requirement
Mandatory regulations and self-protect measures are similar to mandatory seat belts in car insurance, which could mitigate the vulnerability, but it is not widely included in cyber contracts. Nearly 90% of the carriers offer risk management services. Information portal and helpline service are widely offered, and more than 80% insurance companies help with pre-breach planning. However, only 55% of insurers offer active avoid strategies, only 20% of insurers require insureds to use remediation coverage service from designated service providers, and 16% insurers provide lists of service providers.

d. Lack of Re-insurers
Cyber risk products are facing the staggeringly fast increasing cyber incidents and costs. Moreover the accumulated risk will achieve more substantial likelihood in the future as more data storing in the cloud. This trend worry the re-insurers.

2.1.3 Key procedure: Design Suitable Product

We learned that the cyber crime industry is developing with high technology; cyber threat is operational, interdependent, and various for different regions, sectors, types of information and attacks. These characteristics make predicting related loss difficult. Thus, insurance companies restrict the capacity and coverage for cyber product and charge a high premium price. Adverse selection happens since only risky companies would transfer risk with a high price. Entities underestimate cyber threat are under massive exposure, after suffering enormous damage due to cyber crime, they gradually turn to cyber risk insurance carriers. The demand and supply of cyber insurance increase. According to the Betterley Report [3], although the number of insurance institutions providing cyber insurance is rising, the premium price is still increasing, which means the speed of increased demand is faster than that of increased supply. Cyber insurance is considered to be profitable in the following years. However, the high premium and limited coverage barricade many small and medium firms which are not able to afford expensive protection in risky system. These small and medium entities face growing vulnerabilities (due to the connection among industries). The exposed institutions will lessen the coverage power of insurance for the global cyber system. Providing more reasonable and acceptable contracts is a pressing task to encourage more organizations involved in the protected cyber system.

2.2 Cyber Management System

Similarly to managing other business risks, the approach to manage cyber risk could be clarified as first eliminate, then mitigate, absorb and at last transfer. Gordon et al. [16] proposed a four steps framework for managing cyber risk with insurance, including assessment of vulnerabilities, improvement of IT security, transfer with insurance and keep risk at an acceptable level. The authors also addressed the issues of pricing, adverse selection, and moral hazard. They suggested that to solve the adverse selection problem, insurance institutions could employ required information security audit before issuing a policy, as well as identify high-risk entities and differentiate the premium. They also stated that to reduce moral hazard, insurers should use deductibles and offer premium reductions for investment in self-defense. Research on cyber risk management could be summarized with the following framework (Figure 2.1).

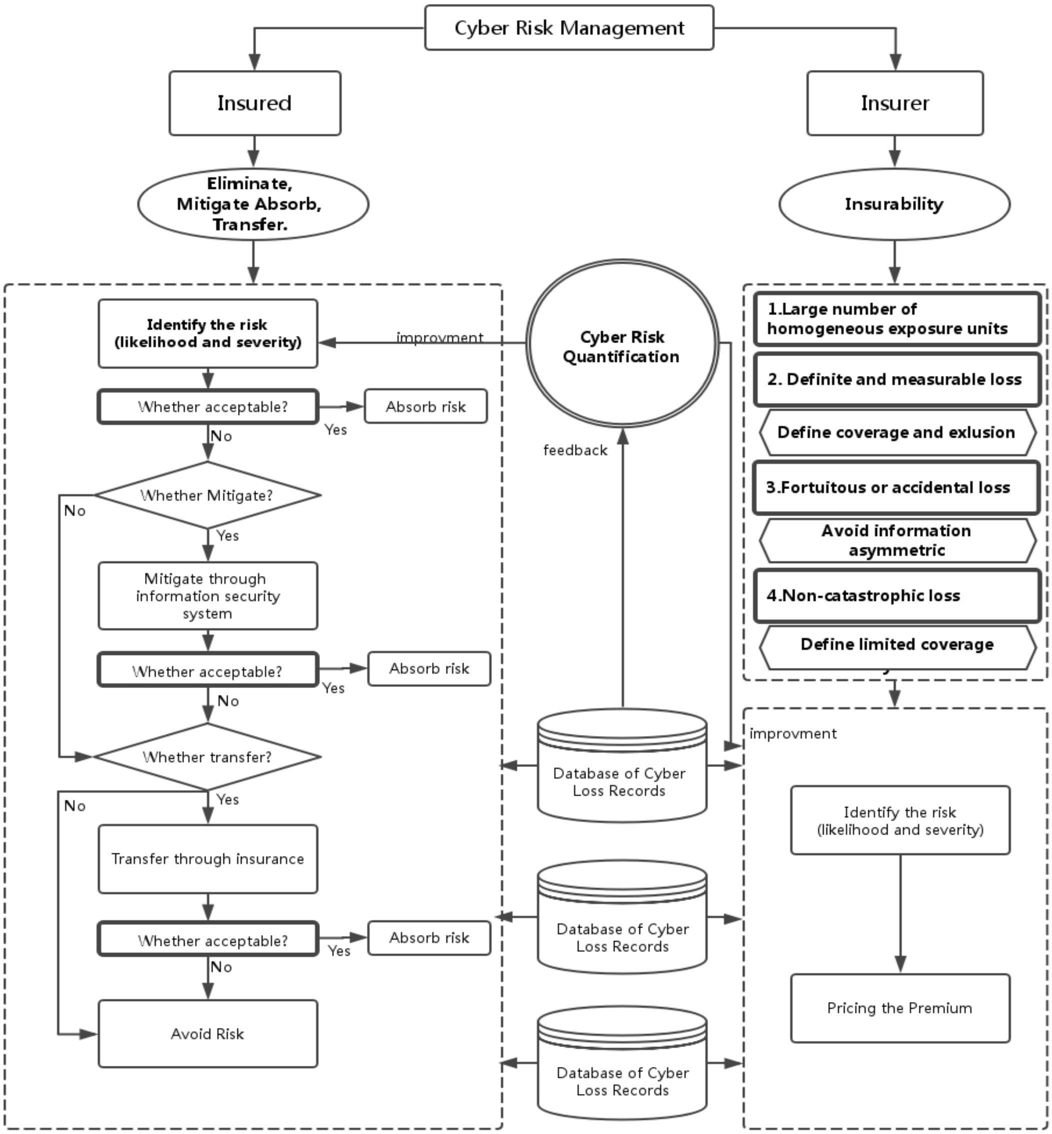

Cyber Risk Management
Insured
Insurer
Eliminate, Mitigate Absorb, Transfer.
Insurability
Identify the risk (likelihood and severity)
improvment
Cyber Risk Quantification
1.Large number of homogeneous exposure units
2. Definite and measurable loss
Define coverage and exlusion
3.Fortuitous or accidental loss
Avoid information asymmetric
4.Non-catastrophic loss
Define limited coverage
Whether acceptable?
Absorb risk
Yes
No
feedback
Whether Mitigate?
No
Yes
Mitigate through information security system
Whether acceptable?
Absorb risk
Yes
No
Whether transfer?
No
Yes
improvment
Database of Cyber Loss Records
Identify the risk (likelihood and severity)
Transfer through insurance
Database of Cyber Loss Records
Whether acceptable?
Absorb risk
Yes
No
Pricing the Premium
Avoid Risk
Database of Cyber Loss Records

Figure 2.1: Cyber Risk Management Framework

2.2.1 Insured: Framework of Management

Risk managers are looking for information security management strategies to minimize the investment in self-defense, premium for insurance, and the residual risk. Nie et al. [31] applied ruin theory on cyber risk modeling to determine optimal investment in information security, minimizing IT security costs. Security level of a system was assumed to be a quantifiable number. A surplus process was used to modify the security level considering current security level as the initial surplus and regarding security system investment as the premium income. The impact of a cyber incident was modeled as security loss and the arrival of cyber attacks was assumed following Poisson process. They provided that (1) high loss severity, low initial security level required greater investment to achieve the optimal cyber costs; (2) for high-frequency, low-severity attacks, information security investment could be reduced; (3) selection of time horizon is important when planning for cyber risk management.

Young, et al. [44] proposed a framework to quantify cyber risk, which established an optimization system including cyber risk, risk management investment and insurance discount for self-protection, minimizing the total costs. To be more specific, after identifying the threats, the first step is to estimate the likelihood of a cyber event and the potential lost based on the annual loss expectancy (ALE) metric introduced by the National Bureau of Standards. Insureds would decide whether the ALE need to be reduced. Then, the next step is to decide the amount of investment should be used in self-protection. Next, insureds would again decide whether to transfer the residual risk through cyber risk insurance and the final task is to estimate the discounted premium price for companies with self-protection. The advantages of this method are that it is an update-able approach which could dynamically include new loss data in the data pool and it is also consistent with game theory stimulating entities to adopt self-defense actions.

2.2.2 Insurer: Framework of Product Design

The profit of insurer comes from premiums exceed the claim over time and the amount of clients. Inaccurate determined premium, as well as inappropriate client behaviors will both account for the loss of insurers. Thus, establishing accurate quantified models for cyber risk and avoiding information asymmetry (adverse selection and moral hazard) are primary tasks for insurance institutions. Typically, carriers at first evaluate the insurability of a particular risk and decide whether they are willing to provide coverage for the risk fulfilling their profit goals. After that, insurance institutions would build models to identify the potential loss and design appropriate insurance contracts which provide coverage, and at the same time make profits.

The Berliner approach [2] provided an explanation for the situation that insurance coverage is not provided for every risk in the market, and established the existence of a no unambiguous insurability area with the a so-called gray zone that lies between the objective insurability and insurability area. This gray area includes risks that not all insurers wish to cover due to various risk aversions, but the risks are by all means covered by some. Biener and Eling [4] applied the Berliner approach analyzing the insurability of Micro insurance Market. Biener et al. [5] completed a similar analysis of insurability of cyber risk.

In their article [5], Biener, Eling, and Wirfs discussed the insurability of cyber risks applying the approach, distinguishing insurable and uninsurable risks, proposed by Berliner [2]. Biener et al. indicated that there are three main problems hinder the evolution of the cyber insurance market. First, the independent and predictable characteristics of losses are not confirmed. Second, information asymmetry is substantial in the market. Third, the limits of the coverage of cyber insurances vary. Provided there is room for improving the insurability of cyber policies, Bierner and colleagues concluded on a positive note. They claimed that the size of data related to losses caused by cyber incidents is increasing, which will reduce the problems associated with the randomness of loss occurrence in the future. They also suggested establishing minimum standards on cover limits to alleviate the different limits problems and researching methods to mitigate the prominent information asymmetry.

Apparently, cyber risk lies between the objective insurability and insurability area, which means not all insurance institutions are willing to cover it. However, cyber risk insurance has become an important part of information security management. Ishikawa, Sakurai [21] discussed the cost-effective of cyber insurance through Monte Carlo simulations under four scenarios and concluded that cyber risk insurance could reduce 65% of the costs of cyber incidents.

Actually, in practice, those insurance institutions providing relevant products assessed and qualified the risk with insurability employing empirical approaches. In their book, Kunreuther and Freeman [14] proposed two broad conditions for a risk to be insurable: (1) identifying the risks, (2) setting premiums for specific risks. Based on insurable risks,one should consider marketability as well as profitability. In other words, a risk is not insurable unless there is sufficient demand for the product at some price to cover the upfront costs of developing the product and the expenses associated with marketing policies. Kunreuther and Michel-Kerjan [24] used these insurable conditions in their analyzing of insurability of large-scale disasters. Karten [22] introduced his five criteria for insurability, which are fortuitousness, ambiguousness, estimability, independence, and size. Grzebiela [17] analyzed the insurability of electronic commerce risks based on the five criteria of Karten. Nowadays' measurement of insurability is consistent with Karten [22] and Kunreuther and Freeman [14]. According to [23] and [40], a few conditions considered being necessary for risks to be insurable are as follows: (1) There must be a sufficiently large number of homogeneous exposure units to make the losses reasonably predictable; (2) The loss produced by the risk must be definite and measurable; (3) The loss must be fortuitous or accidental; (4) The loss must not be catastrophic.

According to SINTEF [38], "A full 90% of all the data in the world has been generated over the last two years." The amounts and speed of information collection are far better than hundreds of years ago when the insurance industry first sprang up. Along with the increasing frequency and spectrum of cyber attacks, the database of cyber crimes is growing at an incredible rate, which will reduce the problems associated with randomness and prediction. Specific definitions are being developed for coverage and exclusion, information security auditions are required before issuing insurance contracts, discount are provided for active self-protection and limits have been set up as capacity of policies. Thus, cyber risks are increasingly identifiable and insurance for it is becoming price-able.

2.2.3 First Step in Insurance Designing: Identify Loss

According to Figure 2.1, quantify risk exposure is the first step in designing insurance contract. However, cyber risk is a relatively new emerging threat; interdependencies along with data paucity make predicting the loss and pricing insurance policies problematic. A risk factor view is hobbled by the difficulties of getting related loss data. And the copula method has become a generalized approach for loss and price modeling since it has the advantage of being a way of studying non-linear interdependencies.

Bohme and Kataria [6] demonstrate a twin-tier approach to capturing the relationships between the occurrences of losses. That is, the approach considers the correlation of cyber risk within a firm as the first tier, and regards the correlation across firms as the second tier. Specifically, this method includes building a supply-side model and a demand-side model and satisfying some market equilibrium conditions. First, to compute the supply-side model, the twin-tier approach uses a BB (Beta-Binomial) distribution involving internal correlation parameter r_I to represent the loss of a single firm; after that, several companies' loss marginal distributions are joined with the t-copula tool engaging global correlation parameter r_G. Second, a linear function of the number of computers affected is derived as the demand-side model. Finally, the equilibrium functions requiring the insurers' costs equal to the summation of the insurers' expected losses, all administrative expenses and capital required are solved. Through the procedure, the twin-tier model addresses a sound and extensible model of the cyber insurance market.

Mukhopadhyay et al. [28] elaborated a utility method model for cyber insurance claims with copulas based the Bayesian Belief Network (BBF) technique. In their model, MVN (multivariate normal) copula was used to capture the patterns of the joint distribution and the conditional distribution at the nodes of BBN. And the dollar loss at each node was supposed to be following the binomial distribution. They also proposed factors that should be considered when rating risk.

Hemantha Herath and Tejaswini Herath [18], [19], elaborated on an actuarial approach on a single firm level based on empirical loss distribution to price first-party cyber insurance. They applied Archimedean copulas–Clayton and Gumbel–on International Cyber Security Academy (ICSA) data of virus incidents and the number of infected computers. Copulas are used to model the joint loss distribution $\Pi = g(\pi, q)$ where π is the observed dollar losses from available data; q is the number of affected computers. The occurrence of the event is modeled by a binary variable ω; the arrival of intrusions per unit time is modeled by the Poisson distribution. The estimated copula-based loss distribution is used to perform Monte Carlo simulation, while the costs of cyber insurance is modeled by $C = \omega e^{-rT} P$, where P is the amount paid by insurance company. In the article, they discussed three different types of cyber insurance policy models: a policy with zero deductible, a policy with a deductible, a policy with co-insurance and a limit. They provided a reasonable premium table under three scenario; however it would have been better of they had perform empirical analysis with real loss data, and they could have included more variables than just the number of computers affected in the system.

Based on [18], [19], Xie [43] proposed their copula framework with bootstrapping approach to deal with the problem of data scarcity. They improved the estimation by introducing a copula-based residual bootstrapping procedure, showing that the bootstrapping sample is a better presentation of population than the original sample. Their implementations, on the same 15 data as [18] used, provided narrow bands for insurance prices under the three scenarios.

Mukhopadhyay et al. [28] established a Gaussian Copula-aided Bayesian Brief Network (CBBN) for Cyber vulnerability assessment (C-VA) and expected loss computation as well as a utility based preferred pricing model. However the model primarily considered the IT system, ignoring the characteristics of the insured, for example, the industry, the size, the number of customers and the type of information. Shah [37] priced and analyzed a Cyber Liability Insurance (CLI) contract using Gaussian and Gumble copulas and assessed contract-mitigation effectiveness. They confirmed that the efficiency of a CLI is related to the limit and the sub-limit. The authors also suggested that a cyber risk index would help in pricing and decreasing CLI contract premiums.

The most popular measurement tool used is ‘CyberTab worksheet’ by the economist intelligence Unit Ltd.. Insurance companies have also started to derive risk factors for cyber risk measurement, and with more companies taking part in cyber insurance market, sharing management information and loss records, more accurate measurement methods for cyber risk could soon be proposed.

As we can see from Figure 2.1, quantification is an intermediate link procedure getting feedback from and affecting both demand and supply parts of cyber insurance. The percentage of exposure asset that entities search for external coverage is consistent with the risk that insurance institutions need to run. This inspired us finding out a quantification method through the view of an insured. Deciding the transfered asset value through insureds’ optimized investment system and then pricing insurance products could better match the demand and supply of cyber risk products and speed up the procedure of covering the global cyber system.

Chapter 3

Optimized Insured Strategy

3.1 Quantification Method

One actuarial approach to quantifying risk is to use expected loss. Expected loss is the product of the probability of loss occurring and the value of the possible loss. In banking, the function of expected default loss is as follows:

$$Excepted\ Loss = EAD \times PD \times LGD, \tag{3.1}$$

where EAD is exposure at default, PD is the possibility of default and LGD represents loss given default. For cyber risk, we use a similar quantitative system.

$$Excepted\ Cyber\ Loss = EAA \times PA \times LGA, \tag{3.2}$$

where EAA is exposure at cyber accident, PA is the possibility of accident and LGA represents loss given accident. Inspired by Young et al. [44], we used the annualized loss expectancy (ALE) metric of the National Bureau of Standards [29], and the function describing the relationship between vulnerability and investment proposed by Gordon and Loeb [15] to build a quantitative function. According to the National Bureau of Standards, ALE is the product of Single Loss Expectancy (SLE) and Annualized Occurrence Rate (AOR).

$$ALE = SLE \times AOR, \tag{3.3}$$

where SLE is the product of Asset Value (AV) and Exposure Factor (EF).

$$SLE = AV \times EF, \tag{3.4}$$

For cyber risk, SLE is estimated as the product of exposure asset value (λ), the probability of a successful cyber attack (t) and vulnerability (ν,the ratio of exposed asset that will be lost in a successful attack)

$$SLE = \lambda \nu t \tag{3.5}$$

Gordon and Loeb [15] proposed several functions to simulate the changes of vulnerability when adding investment to a self-protection system. The model used in this research is as follows:

$$s(\nu, z) = \nu^{(az+1)} \qquad a > 0, \tag{3.6}$$

where s(ν; z) is the new vulnerability after investment z in the system. This function performs well since it satisfies the nature of information security systems.

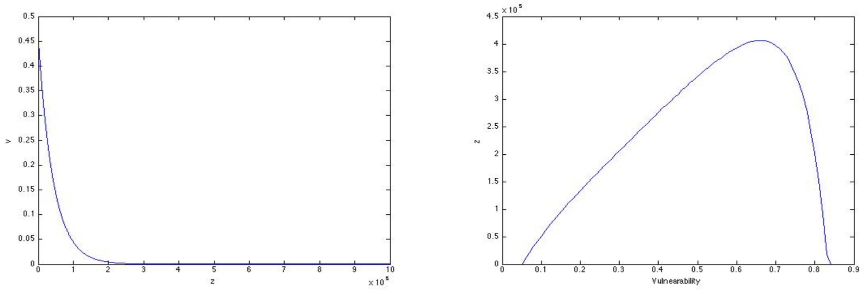


Figure 3.1: (1)Vulnerability versus investment(z) (2)Optimized z given vulnerability

- s(0; z) = 0: Given a system will not be successfully attacked, increased investment in information security will not change the likelihood of being attacked.
- s(v; 0) = ν: Given a specific system, if there is no investment, the vulnerability will not change.
- $\frac{\partial(s(z,\nu))}{\partial z} < 0$ and$\frac{\partial^2(s(z,\nu))}{\partial z^2} < 0$: For a specific system, the investment will increase the security level and reduce the vulnerability; however, the margin effectiveness is decreasing.

Figure 3.1 (1) shows that increasing investment in security-level enhancement will reduce the vulnerability to being attacked, The speed of reduction is at first fast and then becomes slow. For the optimized investment strategy of a company, as shown in Figure 3.1 (2), given its vulnerability, when ν is relatively small or large, the company's optimized investment is zero. The zero investment situation could be used to explain the adverse selection problem.

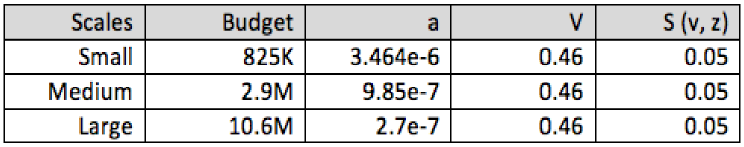
Based on the clarification above, we built a reasonable measurement of an entity's cyber risk.

$$ExceptedCyberLoss = EAA \times LGA \times PA = ALE = \lambda \times \nu \times (t \cdot AOR), \tag{3.7}$$

where ν refers to exposure during a cyber accident (EAA), (t$\cdot$ AOR) stands for the possibility of accident (PA), and s(ν; z) is loss given accident (LGA).

3.2 Optimized Strategies

According to Gordon and Loeb, 'a' is an important parameter for function s(ν; z), and 'a' could be explained as the weight term that represents the exposure level of Internet. Security operations with a high level of exposure will be less efficient than those with a low level of exposure. Thus, a high level of exposure corresponds to a small 'a'. Given that the information security budget for small, medium, and large companies are \$825K, \$2.90M and \$10.6M, respectively [44], all of them have an initial vulnerability of 0.46, and a final target vulnerability level of 0.05, we can estimate the value of 'a' for the three scales of companies. The estimated values of 'a's are used as parameters for the corresponding sizes of businesses in the following experiments.



Scales	Budget	a	V	S (v, z)
Small	825K	3.464e-6	0.46	0.05
Medium	2.9M	9.85e-7	0.46	0.05
Large	10.6M	2.7e-7	0.46	0.05

Table 3.1: 'a' values for three sizes of company

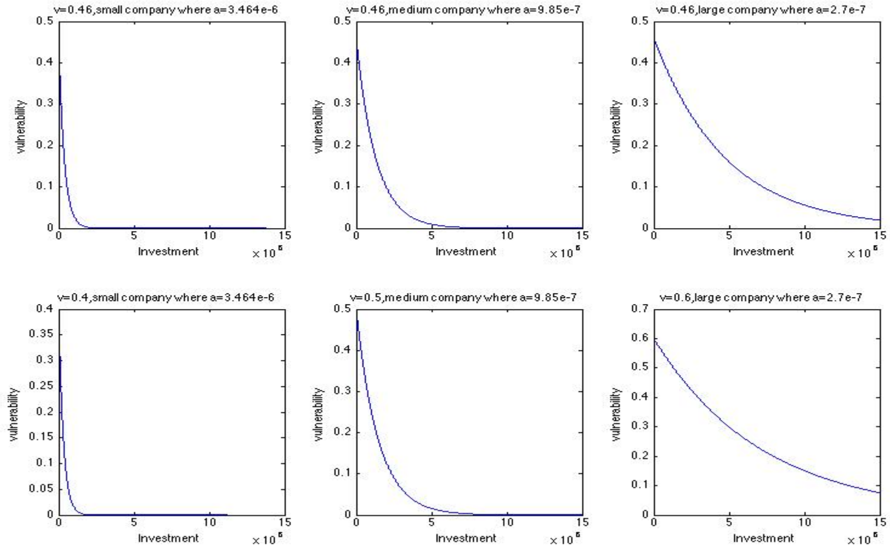
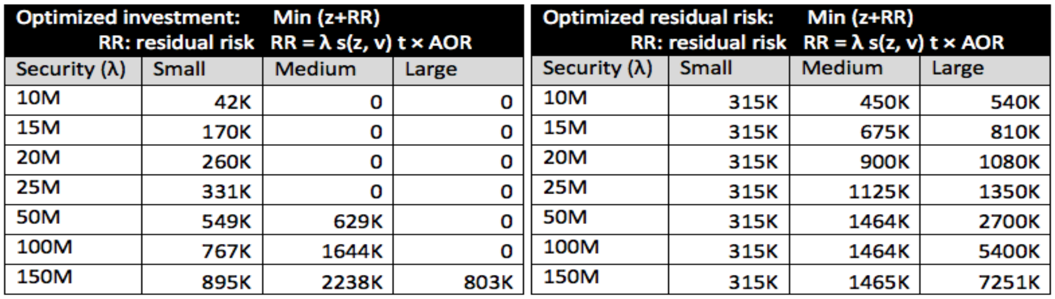


Figure 3.2: vulnerability decreased with z given initial ν and a

Figure 3.2 shows the changes of vulnerabilities when increasing investment for different 'a's and initial vulnerabilities (ν). It demonstrates that companies that face low levels of vulnerabilities (ν) are much more likely to take active measures to enhance self-defense levels, since the cost-effectiveness is larger. A low level of exposure (large value of 'a') performs more effectively.

3.2.1 Scenario 1

- Suppose a small company, a medium company and a large company are going to cover their cyber risk exposures, ranging from 10M to 150M, only with investment in information security enhancement.
- Suppose the vulnerabilities of the three companies are 0.4, 0.5, 0.6, respectively.
- Suppose RR represents residual risk, which is defined to be the ALE under new vulnerability after investment.
- Suppose AOR = 0.1 .
- The objective function is Min(z+RR).



Optimized investment: RR: residual risk		Min (z+RR) RR = λ s(z, v) t × AOR	
Security (λ)	Small	Medium	Large
10M	42K	0	0
15M	170K	0	0
20M	260K	0	0
25M	331K	0	0
50M	549K	629K	0
100M	767K	1644K	0
150M	895K	2238K	803K

Optimized residual risk: RR: residual risk		Min (z+RR) RR = λ s(z, v) t × AOR	
Security (λ)	Small	Medium	Large
10M	315K	450K	540K
15M	315K	675K	810K
20M	315K	900K	1080K
25M	315K	1125K	1350K
50M	315K	1464K	2700K
100M	315K	1464K	5400K
150M	315K	1465K	7251K

Table 3.2: vulnerability decreased with z given initial ν and a

Table 3.2 above shows the optimized investment (z) and residual risk (RR) of the three companies. The result is consistent with Figure 3.2 indicating that small companies that face low level of vulnerability are willing to invest to reduce the ratio of loss. To be more specific, only when the$\frac{\partial[s(\nu,z)\lambda\times AOR]}{\partial z} \leq -1$, is increase investment a wise choice. Notice that, only the small company exceed its budget of 825K. The Medium company will invest in security system when their risky asset is larger than 50M, and the large company will strengthen security levels on its own initiative when its risky asset is greater than 150M.

3.2.2 Scenario 2

• Suppose a small company, a medium company and a large company are going to cover cyber risk exposure, ranging form 10M to 150M, with investment in security enhancement as well as with insurance.
• Suppose the vulnerabilities of the three companies are 0.4,0.5,0.6, respectively.
• Suppose the insurance premium rate is $\theta = 0.08$, that is, the premium is $P = ALE \times (1+\theta)$.
• Suppose AOR = 0.1.
• Suppose companies cover all risk, that is RR = 0
• The objective function is Min(z+P) Figure 3.3 below shows that while investment in the security system is increased, the management expenses decrease at first then grow. The expense curves are consistent with the framework Nie.et al [31] proposed using surplus process to simulate information security systems.

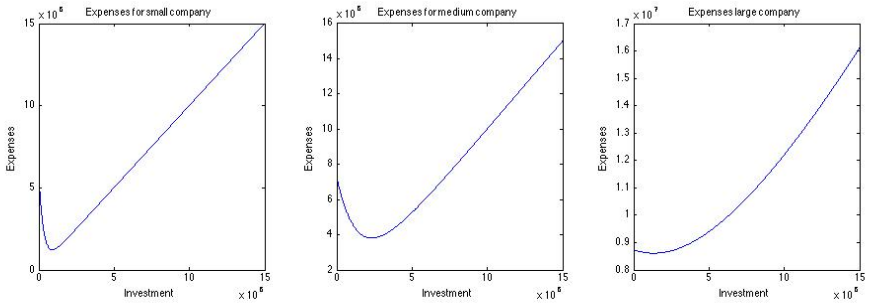
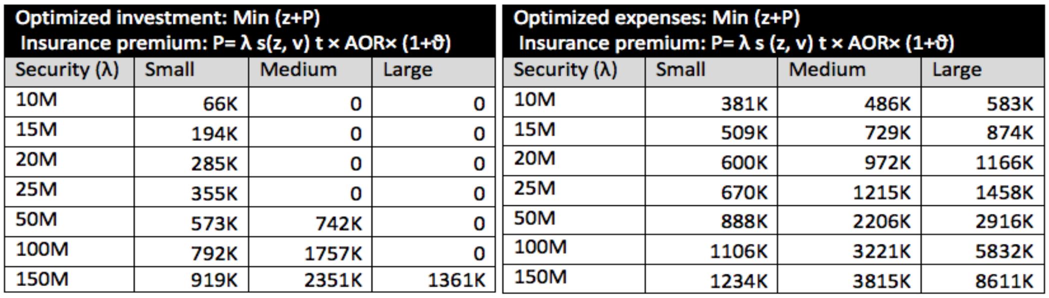


Figure 3.3: Cyber risk management expense curves for small, medium, large company



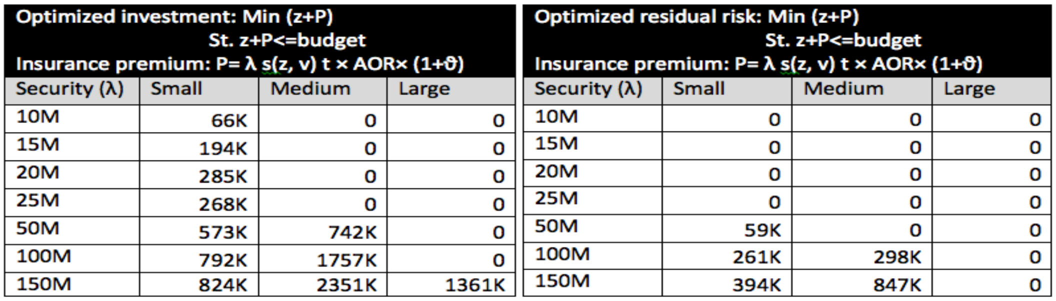
Optimized investment: Min (z+P) Insurance premium: P= λ s(z, v) t × AOR× (1+ϑ)			
Security (λ)	Small	Medium	Large
10M	66K	0	0
15M	194K	0	0
20M	285K	0	0
25M	355K	0	0
50M	573K	742K	0
100M	792K	1757K	0
150M	919K	2351K	1361K

Optimized expenses: Min (z+P) Insurance premium: P= λ s (z, v) t × AOR× (1+ϑ)			
Security (λ)	Small	Medium	Large
10M	381K	486K	583K
15M	509K	729K	874K
20M	600K	972K	1166K
25M	670K	1215K	1458K
50M	888K	2206K	2916K
100M	1106K	3221K	5832K
150M	1234K	3815K	8611K

Table 3.3: Optimized investment amount and expenses under scenario 2

Table 3.3 above describes the optimized investment and the minimized expenses derived by the optimization system. It suggests that companies will increase their investment to reduce more vulnerability before transferring risks, because they can reduce the costs of insurance premium and minimize the expenses for self-protection and risk transfer. Although companies pay premiums and thus spend more on risk management, the risk of experiencing a sudden huge loss result from a cyber attack is covered. In this situation, both the small company and the medium company will exceed their budgets.

- Suppose the expenses are restricted by the corresponding budgets.



Optimized investment: Min (z+P)
St. z+P<=budget
Insurance premium: P= λ s(z, v) t × AOR× (1+ϑ)

Security (λ)	Small	Medium	Large
10M	66K	0	0
15M	194K	0	0
20M	285K	0	0
25M	268K	0	0
50M	573K	742K	0
100M	792K	1757K	0
150M	824K	2351K	1361K

Optimized residual risk: Min (z+P)
St. z+P<=budget
Insurance premium: P= λ s(z, v) t × AOR× (1+ϑ)

Security (λ)	Small	Medium	Large
10M	0	0	0
15M	0	0	0
20M	0	0	0
25M	0	0	0
50M	59K	0	0
100M	261K	298K	0
150M	394K	847K	0

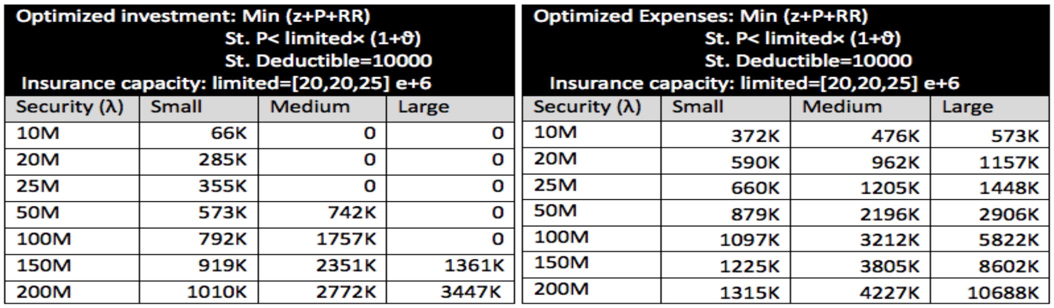
Table 3.4: Restricted optimized investment and residual risk under scenario 2

As we can see from table 3.4, under the restriction of budget, when the exposed asset value is greater than 50M, the small company will suffer from residual risk and so will the medium company when its exposed asset value is greater than 100M. However, most of the residual risks are reduced compared with not transferring risk. Although the coverage of cyber risk under optimized strategy is restricted by budget, insurance has great cost-effectiveness.

In tables above, the large company coverage all exposed asset and keep a balanced budget. But in practical, the range of cyber loss is huge, and typically, insurance companies set a capacity for the payments of claims. (According to [3], most of the insurance company have a capacity of $25M) And a more general situation includes deductibles. These make the optimization problem more complicated.

3.2.3 Scenario 3

- Suppose a small company, a medium company and a large company are going to cover their cyber risk exposure, ranging from 10M to 200M, with investment in security enhancement as well as with insurance.
- Suppose the vulnerabilities of the three companies are 0.4, 0.5, 0.6, respectively.
- Suppose the insurance premium rate is $\theta = 0.08$, that is, the premium is $P = ALE \times (1 + \theta)$.
- Suppose AOR = 0.1.
- Suppose companies cover as much risk as possible through enhancing the security-level and purchasing insurance.
- Suppose The insurers set capacity to be 20M for the small and the medium company, and 25M for the large company. And insurers charge 10,000 as deductible.
- The objective function is Min(z+P+RR).



Optimized investment: Min (z+P+RR)
St. P< limited× (1+ϑ)
St. Deductible=10000
Insurance capacity: limited=[20,20,25] e+6

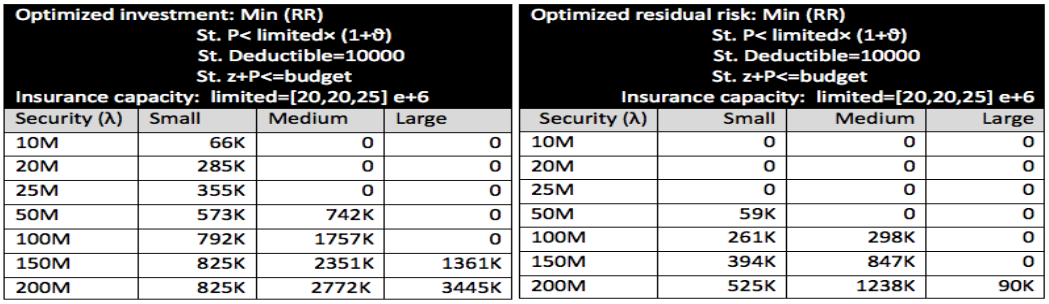
Security (λ)	Small	Medium	Large
10M	66K	0	0
20M	285K	0	0
25M	355K	0	0
50M	573K	742K	0
100M	792K	1757K	0
150M	919K	2351K	1361K
200M	1010K	2772K	3447K

Optimized Expenses: Min (z+P+RR)
St. P< limited× (1+ϑ)
St. Deductible=10000
Insurance capacity: limited=[20,20,25] e+6

Security (λ)	Small	Medium	Large
10M	372K	476K	573K
20M	590K	962K	1157K
25M	660K	1205K	1448K
50M	879K	2196K	2906K
100M	1097K	3212K	5822K
150M	1225K	3805K	8602K
200M	1315K	4227K	10688K

Table 3.5: Optimized investment amount and expenses under scenario 3

- Suppose expenses are restricted by budget: Min(RR).



Optimized investment: Min (RR)
St. P< limited× (1+ϑ)
St. Deductible=10000
St. z+P<=budget
Insurance capacity: limited=[20,20,25] e+6

Security (λ)	Small	Medium	Large
10M	66K	0	0
20M	285K	0	0
25M	355K	0	0
50M	573K	742K	0
100M	792K	1757K	0
150M	825K	2351K	1361K
200M	825K	2772K	3445K

Optimized residual risk: Min (RR)
St. P< limited× (1+ϑ)
St. Deductible=10000
St. z+P<=budget
Insurance capacity: limited=[20,20,25] e+6

Security (λ)	Small	Medium	Large
10M	0	0	0
20M	0	0	0
25M	0	0	0
50M	59K	0	0
100M	261K	298K	0
150M	394K	847K	0
200M	525K	1238K	90K

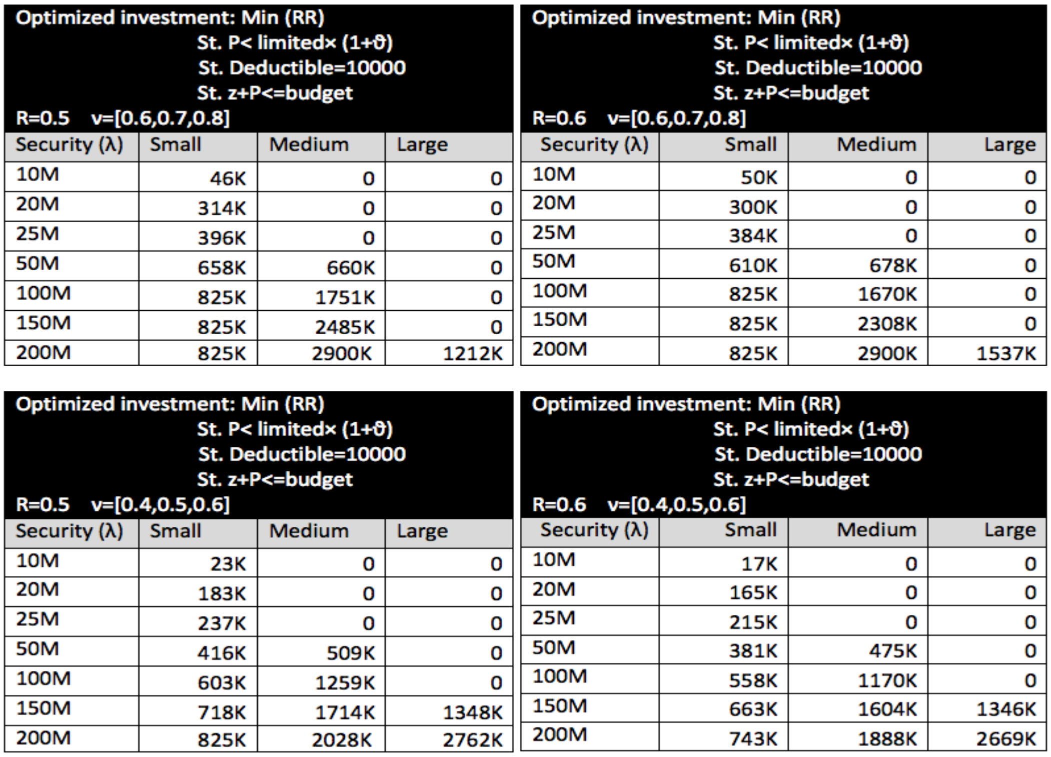
Table 3.6: Restricted optimized investment and residual risk under scenario 3

Table 3.6 suggests that under the restriction of budgets, the small company and the medium company will not change their investment strategy. The small company would like to invest as much as possible when risky asset is fairly large. However, for the large company, investment becomes less effective, and it will prefer transferring the risk with insurance. Moreover, the large company will not be able to cover all risks within its budget.

3.2.4 Scenario 4

It has been suggested that, insurance institutions should provide discount for companies perform better self-protection. In Young, et al. [44], they proposed a discount rate r to encourage companies reducing the probability of being attacked by building up the security system.

- Suppose a small company, a medium company and a large company are going to cover cyber risk exposure, ranging from 10M to 200M with investment in security enhancement, as well as with insurance.
- Suppose the vulnerabilities of the three companies are 0.4, 0.5, 0.6, respectively.
- Suppose the insurance premium rate is $\theta = 0.08$, that is, the premium is $P = ALE \times (1+\theta)$.
- Suppose companies cover as much risk as possible. That is: Min(RR)
- The insurers set capacity of 20M for the small and the medium company, and 25M for the large company. Insurance institutions charge $10,000 as deductible.
- Suppose the insurance companies provide discount for self-defense. The premium price with discount is $P = P_0 \times (1-\delta)$ and $\delta = r(1 - s(\nu; z))$.
- The objective function is Min(z+P+RR).
- The expenses are restricted by budgets.



Optimized investment: Min (RR)
St. P< limited× (1+ϑ)
St. Deductible=10000
St. z+P<=budget
R=0.5 v=[0.6,0.7,0.8]

Security (λ)	Small	Medium	Large
10M	46K	0	0
20M	314K	0	0
25M	396K	0	0
50M	658K	660K	0
100M	825K	1751K	0
150M	825K	2485K	0
200M	825K	2900K	1212K

Optimized investment: Min (RR)
St. P< limited× (1+ϑ)
St. Deductible=10000
St. z+P<=budget
R=0.6 v=[0.6,0.7,0.8]

Security (λ)	Small	Medium	Large
10M	50K	0	0
20M	300K	0	0
25M	384K	0	0
50M	610K	678K	0
100M	825K	1670K	0
150M	825K	2308K	0
200M	825K	2900K	1537K

Optimized investment: Min (RR)
St. P< limited× (1+ϑ)
St. Deductible=10000
St. z+P<=budget
R=0.5 v=[0.4,0.5,0.6]

Security (λ)	Small	Medium	Large
10M	23K	0	0
20M	183K	0	0
25M	237K	0	0
50M	416K	509K	0
100M	603K	1259K	0
150M	718K	1714K	1348K
200M	825K	2028K	2762K

Optimized investment: Min (RR)
St. P< limited× (1+ϑ)
St. Deductible=10000
St. z+P<=budget
R=0.6 v=[0.4,0.5,0.6]

Security (λ)	Small	Medium	Large
10M	17K	0	0
20M	165K	0	0
25M	215K	0	0
50M	381K	475K	0
100M	558K	1170K	0
150M	663K	1604K	1346K
200M	743K	1888K	2669K

Table 3.7: Optimized investment whenν=0.4,0.5,..0.8 ,R=0.5, 0.6

Tables above clarify that for companies with great vulnerability, increased discount r will encourage the managers to invest more in security level; however, for companies with small vulnerability level, increased discount rate r will result in a reduction in insurance premium as well as in investment for security system.

The reason is that high vulnerability and exposure contribute to high premium. The vulnerability would decrease a lot when investing more in information security system and thus lessened the insurance premium and $\Delta P > \Delta z$. For companies with low vulnerability, although increment in investment will reduce the premium,$\Delta P > \Delta z$, and if the decrease the fund for system self-defense, there is a chance that the expenses will still decrease given less system investment. Figure 3.7 shows the optimized investment given r ranging from 0.01 to 1.

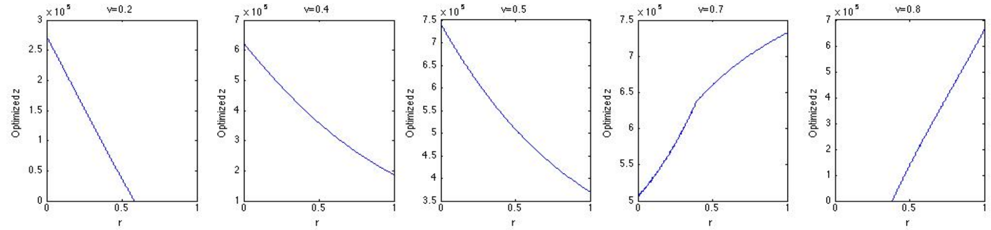
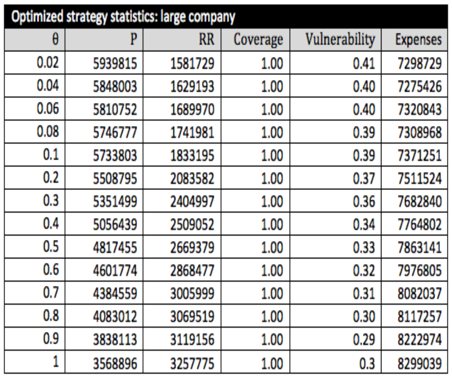


Figure 3.4: Optimized investment adjustment for different vulnerability levels

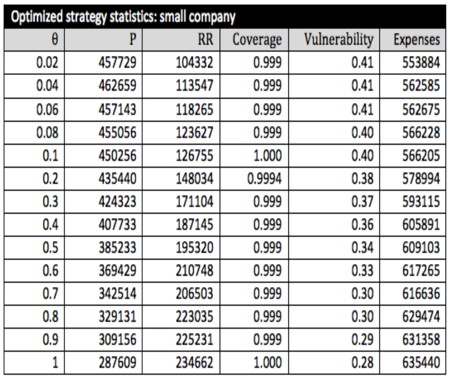
In that case, how to choose r becomes a taught problem, and another problem of r would be should we require $(1 + \theta)(1 - \delta) > 1$? That is, we should also consider whether r is acceptable for the insurers.

Another parameter that will effect insureds' investment strategy is the premium loading θ.



Optimized strategy statistics: large company

θ	P	RR	Coverage	Vulnerability	Expenses
0.02	5939815	1581729	1.00	0.41	7298729
0.04	5848003	1629193	1.00	0.40	7275426
0.06	5810752	1689970	1.00	0.40	7320843
0.08	5746777	1741981	1.00	0.39	7308968
0.1	5733803	1833195	1.00	0.39	7371251
0.2	5508795	2083582	1.00	0.37	7511524
0.3	5351499	2404997	1.00	0.36	7682840
0.4	5056439	2509052	1.00	0.34	7764802
0.5	4817455	2669379	1.00	0.33	7863141
0.6	4601774	2868477	1.00	0.32	7976805
0.7	4384559	3005999	1.00	0.31	8082037
0.8	4083012	3069519	1.00	0.30	8117257
0.9	3838113	3119156	1.00	0.29	8222974
1	3568896	3257775	1.00	0.3	8299039



Optimized strategy statistics: small company

θ	P	RR	Coverage	Vulnerability	Expenses
0.02	457729	104332	0.999	0.41	553884
0.04	462659	113547	0.999	0.41	562585
0.06	457143	118265	0.999	0.41	562675
0.08	455056	123627	0.999	0.40	566228
0.1	450256	126755	1.000	0.40	566205
0.2	435440	148034	0.9994	0.38	578994
0.3	424323	171104	0.999	0.37	593115
0.4	407733	187145	0.999	0.36	605891
0.5	385233	195320	0.999	0.34	609103
0.6	369429	210748	0.999	0.33	617265
0.7	342514	206503	0.999	0.30	616636
0.8	329131	223035	0.999	0.30	629474
0.9	309156	225231	0.999	0.29	631358
1	287609	234662	1.000	0.28	635440

Table 3.8: Optimized strategy for different premium loading for small and large companies

Table 3.8 above suggests that the premium rate parameter θ is related to the optimized vulnerability level. Given initial vulnerability (ν), increased premium loading parameter could encourage companies investing more in security enhancement. This section builds an optimization framework for insureds' management strategy. Since the choice of r is still unclear, the optimized model in scenario 3 is used in the following pricing process.

Chapter 4

Pricing Cyber Insurance with Monte Carlo Simulation

The investment fund z, and the residual risk RR can be derived based on the optimization system of scenario 3, when deductible, insurance capacity, premium rate (θ), risky asset value (λ), and initial vulnerability level (ν), and the insurance premium P are given.

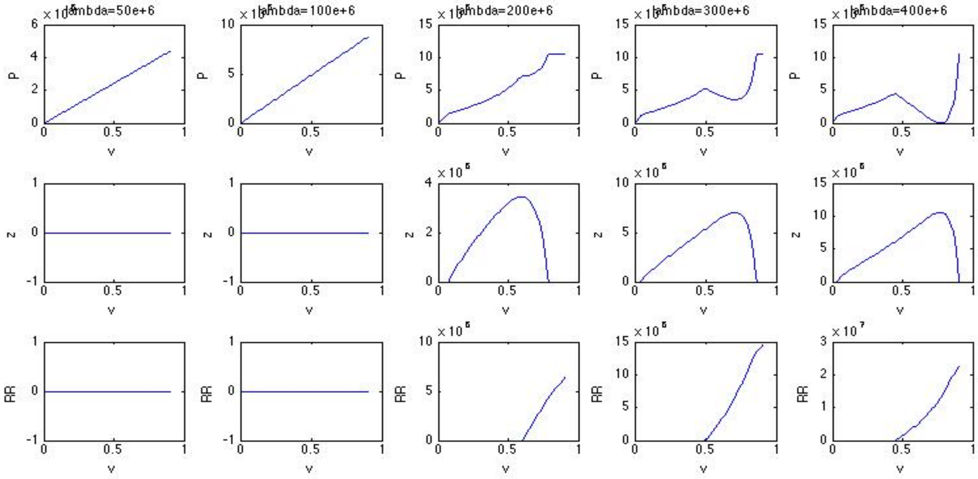


Figure 4.1: Optimized insurance premium, z and residual risk for a large company with risky assets ranging from 50M to 400M

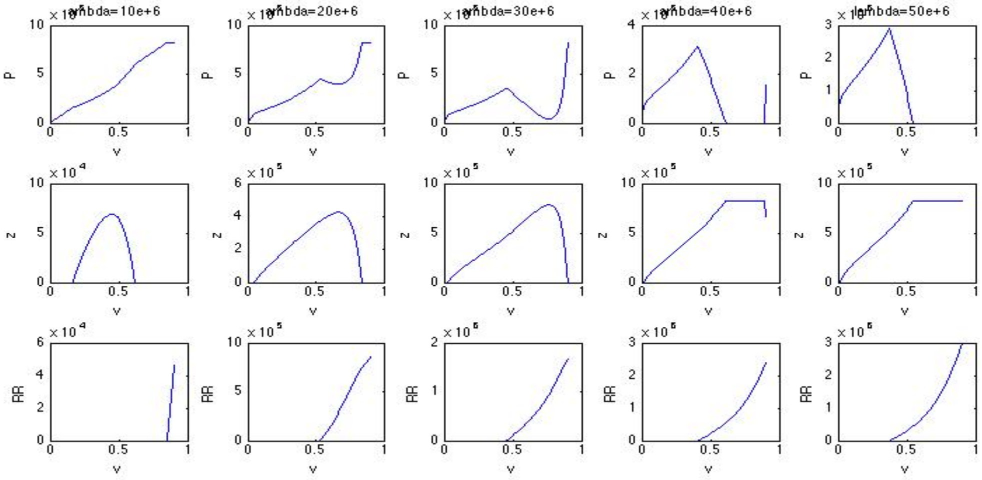


Figure 4.2: Optimized insurance premium, z and residual risk for a small company with risky assets ranging from 50M to 400M

Figure 4.1,4.2 suggest that the optimized strategy of large institutions has the same patterns as those of small companies. The following simulations will focus on a market consisting of small companies. Figure 4.2 indicates that for different amounts of risky assets (the exposed asset value in the graph is from 10M to 50M), insureds' optimized strategies (under budget restriction) change a lot. When vulnerability is less than 0.5, insureds prefer transferring risk through insurance products compared with when vulnerability is greater than 0.5. When vulnerability is extremely small or large, insureds would not invest in self-protection. For an exposed asset value larger than 20M, companies with vulnerability greater than 0.5 would not be able to cover all the risk under their average budget.

4.1 Monte Carlo Simulation for a Single Generalized Premium Rate

- Suppose 10000 small companies in the market have vulnerabilities following $U(0, 1)$.
- Suppose these 10000 companies follow their optimized investment strategies.
- Suppose cyber incidents' arrival following Poisson distribution with parameter E(Poisson)=0.1.
- Suppose the percentages of companies have risky asset value 10M, 20M, 50M are 90%, 8%, 2%,respectively.

- We ignore the interest rate during the time period T=1.
- Suppose that, to maintain a insurance institution, the insurer requires a profit rate of α after paying off the claims, where $\alpha = 0.05$.

The procedure of the simulation is as follows:

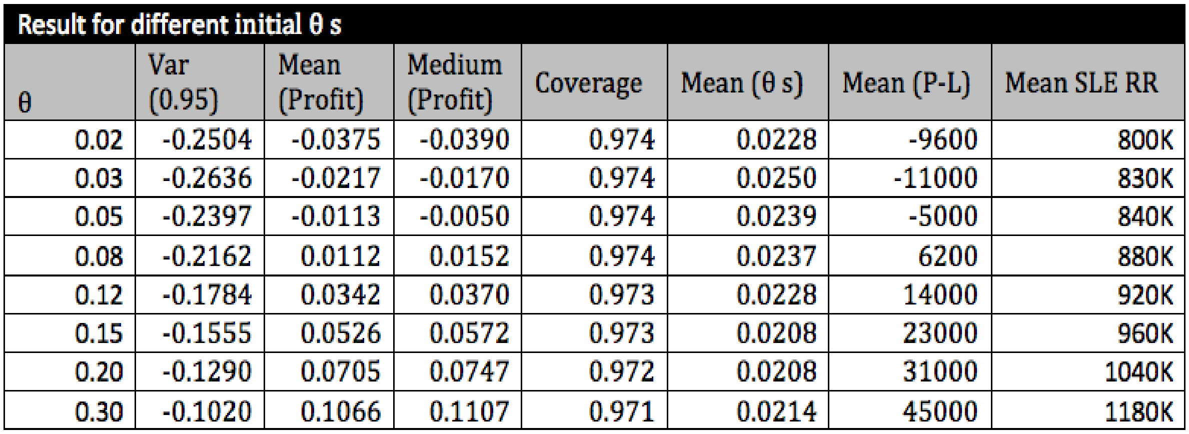
Step1: Generate m=10000 small companies with initial vulnerability $\nu \sim U(0, 1)$
Step2: For each company, generate its risky asset value: P(λ=10M)=0.9, P(λ=20M)=0.08, P(λ=50M)=0.02.
Step3: Given initial insurance premium rate, calculate the optimized strategy for each company, derive $ALE = \lambda ts(z; \nu) \times AOR$.
Step4: During time period T, generate cyber attacks from Poisson(0.1) distribution.
Step5: For each accident, generate Loss(L) from distribution N(λts(ν,z),σ^2)
Step6: At the end of T, calculate the total payments for all claims.
Step7: Calculate appropriate θ for this market.

$$P_i = ALE_i(1 + \theta) \quad fpri = 1, 2, ...10000 \tag{4.1}$$

$$\frac{(\sum P_i - \sum L - i)}{\sum P_i} = \alpha \tag{4.2}$$

$$\theta = \frac{\sum L_i}{(1 - \alpha)(\sum ALE_i)} - 1 \tag{4.3}$$

Step8: Repeat the above steps for n=1000 times and get $\theta_1, \theta_2, ...\theta_{1000}$ and take the average of all θs.
Step9: Compare the results with different initial θ_0s



Result for different initial θ s							
θ	Var (0.95)	Mean (Profit)	Medium (Profit)	Coverage	Mean (θ s)	Mean (P-L)	Mean SLE RR
0.02	-0.2504	-0.0375	-0.0390	0.974	0.0228	-9600	800K
0.03	-0.2636	-0.0217	-0.0170	0.974	0.0250	-11000	830K
0.05	-0.2397	-0.0113	-0.0050	0.974	0.0239	-5000	840K
0.08	-0.2162	0.0112	0.0152	0.974	0.0237	6200	880K
0.12	-0.1784	0.0342	0.0370	0.973	0.0228	14000	920K
0.15	-0.1555	0.0526	0.0572	0.973	0.0208	23000	960K
0.20	-0.1290	0.0705	0.0747	0.972	0.0208	31000	1040K
0.30	-0.1020	0.1066	0.1107	0.971	0.0214	45000	1180K

Figure 4.3: Simulation result with different θs

However, the histograms of profit & loss distribution with $\theta = 0.02$ and $\theta = 0.3$, show that the profits of the insurance company vary.

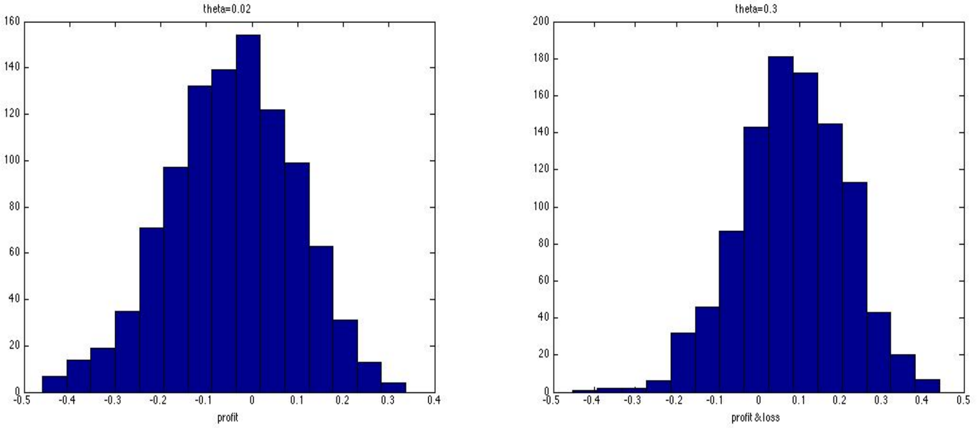
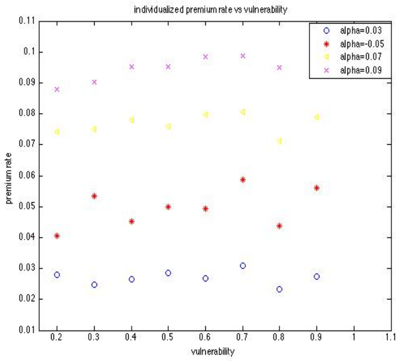


Figure 4.4: Profit distributions of the insurer when $\theta = 0.02$ and $\theta = 0.3$

4.2 Monte Carlo Simulation for Individualized Premium loading

For a given company, Monte Carlo simulation could also be used to decide the premium rate. The procedure is quiet similar to using Monte Carlo method pricing an option value of an underlying asset.

Step1: For a company, given its budget, exposed asset (λ), vulnerability (ν), initial premium rate θ_0, and other parameters for a policy(capacity, deductible), derive its optimized investment strategy.
Step2: Generate m=10000 possible accident arrival processes for the company during time period T, the accidents arrive following Poisson(0.1) process. time period T, the accidents arrive following Poisson(0.1) process.
Step3: For each accident, generate Loss(L) from the normal distribution N(λts(ν,z),σ^2)
Step4: At the end of T, calculate the amount of payments for all claims. (If the loss value is less than deductible, it would not be excluded from the claims, if the loss value is greater than the limited capacity, only limited amount will be paid).
Step5: Calculate appropriate θ for this particular company.
Step6: Repeat the above steps for n=1000 times and get $\theta_1, \theta_2..\theta_{1000}$.



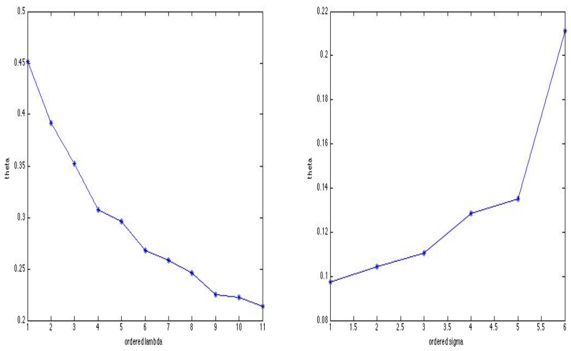


Figure 4.5: Premium loadings for a small company with ν=0.1,..0.9, α=0.03,... 0.09

Figure 4.6: Premium loadings for increased loss variance (σ) and increased risky asset(λ)

Figure 4.5 shows that, using Monte Carlo simulations to pricing cyber insurance according to individual's vulnerability level gives similar loading parameter for different νs.

In Figure 4.6, premium loading parameter increases when single loss expectancy is more fluctuated (larger variance for normal distribution). Increased exposed risky asset results in decreased premium rate, however higher premiums are charged for companies with large exposures.

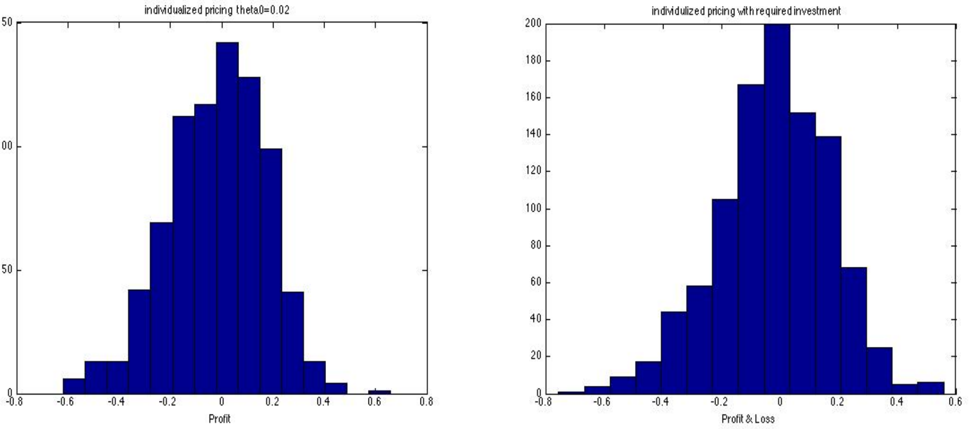


Figure 4.7: Profit & loss distribution of insurer under individualized pricing

An individualized pricing will centered the profit & loss distribution; however, the profit & loss distribution will have a long tail. Thus, individualized pricing largely increases the variance of the profit & loss distribution and contributes to higher risk.

Chapter 5

Reduce the Risk of Insolvency

According to Figure 4.2, companies with extremely large or small vulnerabilities and use insurance to transfer their risks would not be willing to investment in self-protection. And large vulnerabilities can cause large claims. If insurance institutions require those companies to invest, or in other words, if insurance institutions perform mandatory information security operations, the severity of losses and the risk of insolvency would be reduced. This is the same as the requirement of seat belt for car insurance. Monte Carlo simulations were used to compare different levels of vulnerabilities (0.1, 0.2, 0.3, 0.4,...0.9) with different amounts of required investment (1K, 2K, 3K, 4K, 5K).

- Suppose there are 10000 small companies in the market whose vulnerabilities are uniformly distributed in (0,1).
- Suppose these 10000 companies follow their optimized investment strategies.
- Suppose cyber incidents arrive following Poisson distribution with parameter 0.1, the probability of being successfully attacked is t= 0.9.
- Givenλ=10e+6, limit=20e+6, deductible=10000, premium rate θ=0.08.
- Calculate the profits under two scenarios with same initial vulnerabilities: (1) the insurance company has no requirement for investment (line 'o'); (2) the insurance company requires insureds to investment at least $z_0 \times \nu$ (line '*').

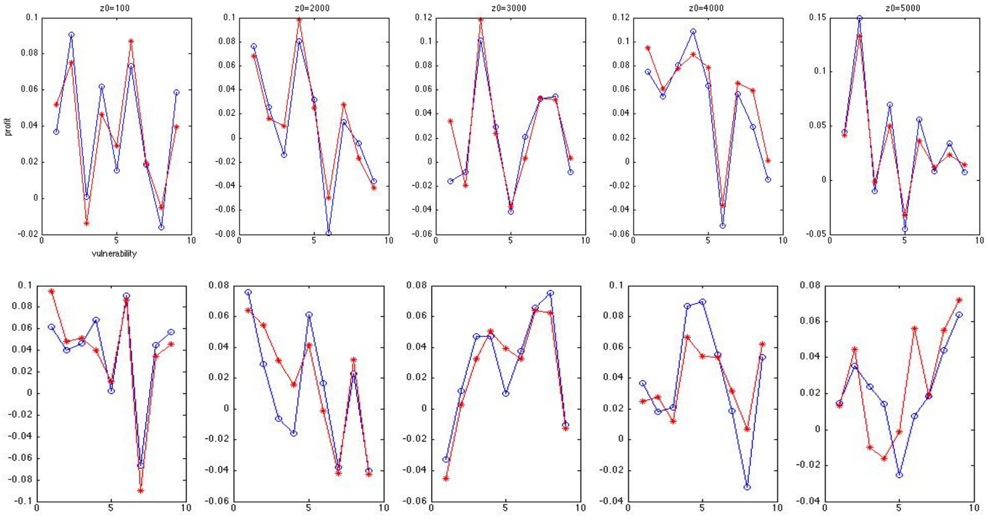


Figure 5.1: Two simulation results comparing policy has NO investment requirement ('o') and policy includes investment requirement('*')

Figure 5.1 shows how the profit & loss changes with z_0 ranging from 1000 to 5000 when vulnerability is greater than 0.1, 0.2, 0.3... 0.9. As we can see, comparing the profit lines, a 4000 or 5000 investment requirement for companies with vulnerabilities greater than 0.6, and a 1000 or 2000 investment requirement for companies with vulnerabilities less than 0.4 will increase the profit or reduce the loss.

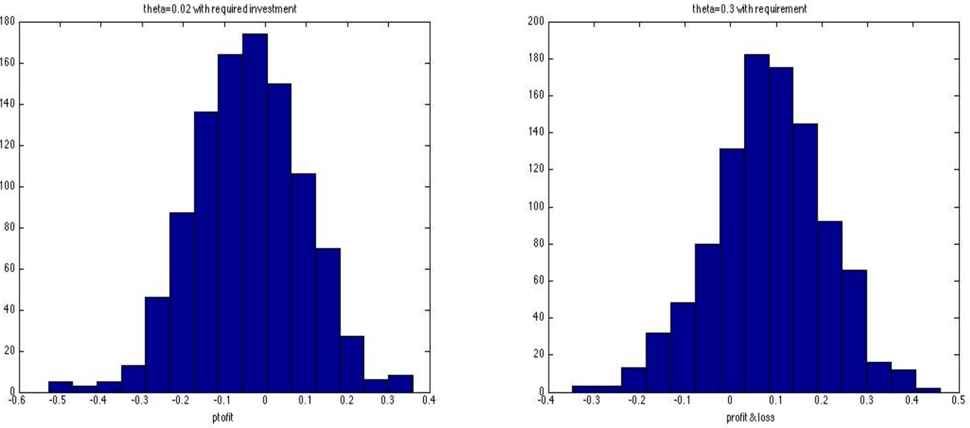


Figure 5.2: Profit distribution of insurers which required z_0 with θ=0.02 and $\theta = 0.3$

Compared Figure 5.2 with Figure 4.4, the probabilities of making large loss and large profit are both reduced, which proves that requiring self-protection operation or mandatory information security services could be used to moderate the variance of profit & loss distribution.

5.1 Long Term Contract with Adaptive Premium

For car insurance that provides a long-term contracts, an insured pays a premium every month. At the end of each year, there will be a decision of whether and how to adjust the premium rate. In that case, an insured who claims a lot will be considered to have higher vulnerability and will pay more for insurance products in the next term. At the same time, drivers who have a clean record of claims will get a discount on insurance. Cyber risk insurance could also be adjustable depending on historical claims, and in the long run, insurance companies will reduce the probability of making large profit or loss.

- Suppose there are 10000 small companies in the market whose vulnerabilities are uniformly distributed in (0,1). They will purchase a three-year insurance policy from the insurer.
- Suppose these 10000 companies follow their optimized investment strategies.
- At the end of each year, insured will adjust their investment and coverage from insurance based on their lessened vulnerabilities after the whole year's investment. However, companies who claimed during the year will add a penalty term to their lessened vulnerabilities, since a cyber crime will damage the information security system.
- Suppose cyber incidents arrive following Poisson distribution with parameter E(Poisson)= 0.1, for three years. The probability of being successfully attacked is t = 0.9.
- Given λ=10e+6, limit=20e+6, deductible=10000 Premium rate θ =0.02.

Step1: Generate m=10000 small companies with initial vulnerabilities $\nu \sim U(0,1)$.
Step2: For each company, generate its risky asset value: P(λ=10M)=0.9, P(λ=20M)=0.08, P(λ=50M)=0.02.
Step3: Given initial insurance premium rate, calculate the optimized strategy for each company, derive $ALE = \lambda ts(z;\nu) \times AOR$.
Step4: During time period T (T>1 for example T=3), generate cyber attacks from Poisson(0.1) distribution.
Step5: For each accident, generate SLE from distribution N(λts(ν,z),σ^2)
Step6: At the end of each year, calculate the total payments for all claims.
Step7: At the end of each year, update the vulnerability of each company based on its

investment (newν=s(ν,z)). For each company that has made claims in this year, add $0.5 \times (1 - new\nu)$ to its newν as a penalty term.
Step8: Calculate profit & loss for each year, as well as the average profit & loss for T.

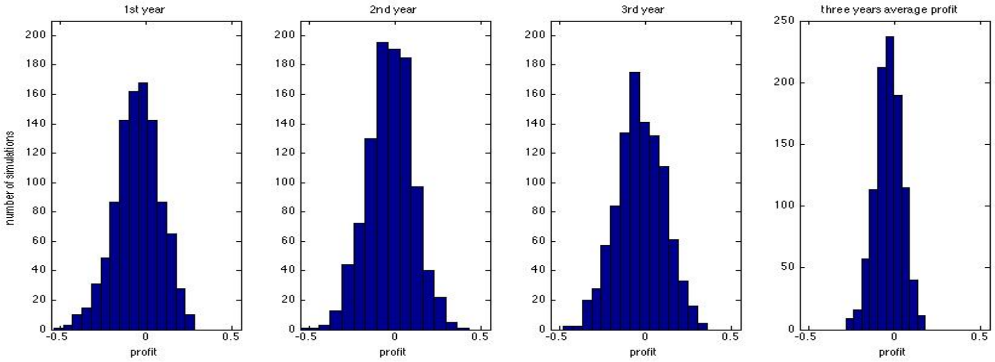


Figure 5.3: Histograms of profits for year 1,2,3 and the average profit for these years

Figure 5.3 shows the histograms of insurance company profits during the first, second, third years and the average profit of these three years. First, in the long run, the security level of insureds will be strengthen, and the optimized insurance coverage as well as the premium will be decreased. Second, companies that have been attacked would pay more premium in the next year/years. Finally the counteract effect of loss and gains among the years will reduce the risk for insurance institutions.

5.2 Other Approaches

A typical approach to keep the insurance industry financially viable is reinsurance. Reinsurance helps insurance companies remain solvent. Most cyber reinsurance is embedded in complementary treaties; for example, errors & omissions of directors & officers treaties on quota-share bases rather than under cyber standalone reinsurance treaties [35]. The issuance of insurance-linked securities (ILS) is also suggested to be a potential approach to providing reinsurance capacity. The uncertainty and the likelihood of a huge loss mean that cyber accidents are considered as potential catastrophic events. ILS has been issued in the form of 'catastrophe bonds', for example, extreme wind or longevity. Increase of the information sharing on cyber-risks and related data and the disclosure of cyber risks and events would help insurer and insureds better understand the risks, as well as get early warning of potential threats since cyber risks have the characteristic of highly interdependent. Standardizing of the security and resilience, regular audits of security investment, and testing of vulnerability also have been proposed as methodologies to reduce cyber threat as well as the chance of a suddenly catastrophic loss.

Chapter 6

Conclusion

Cyber risk is now considered to be one of the top ten global threats. Since all industries are becoming much more dependent on information technology, and companies are also becoming more closely related to supply chains and across counterparties, the world's exposure to cyber risk is driven to a high level. Insurance, as a typical tool for risk transfer, plays a significant role in cyber risk management. The destructive power of cyber attacks has been underestimated for decades, and risk managers have been gradually woken to the astonishing cyber crimes and frequent cyber accidents. There exists an imperative demand of cyber insurance products and reinsurance products. Although the number of institutions providing cyber risk insurance is rapidly increasing, it is inadequate for the risk management gap. Available products have varied limited coverages. Most cyber products focus on digital information breaches, Distributed Denial of Service attack (DDoS) or business interruptions, while property damage or bodily injury are hardly included. Few insurance institutions require mandatory self-defense operations. Information asymmetry hinders the development of cyber insurance. Quantifying cyber risk is essential for both insured and insurer, but is restricted by the scarcity of standard cyber loss data, the dependency of cyber events, the complicated relationship among cyber loss and sectors, information types, attack categories, organization scales and criminal motivations.

Considering the research on the optimized system of cyber risk management, variable was used to represent the vulnerability of a particular company and an 'expected default loss'-like function of 'expected cyber loss' was derived. An expected cyber loss equation was built to capture the relationship among a company's exposure level ('a'), exposure asset (λ), vulnerability (ν), the global system risk severity (the cyber attack frequency (AOR), and the rate of successful attack (t)). In this framework, companies with relatively low vulnerabilities and low exposure levels will benefit more through investment. And companies with high vulnerabilities will have relative small marginal gains for security level enhancement.

Simulations of the optimized management strategy show that cyber risk transfer has higher cost-effectiveness for companies exposed a lot to cyber threat than cyber risk mitigation through self-investment. Large corporations with small 'a' values suffering a high level of exposure would prefer insurance products. At the same time, under the budget restriction, insurance products can reduce more than half of the residual risk if they align with companies' information security systems. For small businesses with little exposure, increased investment in self-protection will dramatically diminish the corresponding cyber threats. However, restricted by insureds' budget and insurers' limited capacity, the insurance coverage is inadequate for large exposure. The relevant result is a considerable residual risk and a significant possibility of losing solvency. The discount parameter r is sensitive to an organization's vulnerability and the scale of its risky asset. However, premium loading parameter was shown to be related to an organization's optimized vulnerability and thus could be used to stimulate self-protection.

Based on insured optimized management strategy, Monte Carlo market simulations are used to decide the premium loading θ. An individualized pricing process gives that ν should be a variable that includes sufficiently varied information on companies; that is, given fixed variance of loss distribution and the amount of exposed risky asset, the premium loading parameter for companies' different vulnerabilities should be at the same level. A large variance of a loss distribution will promote the premium loading, and participations of large exposed companies could lessen the premium loading. Generalized pricing will contribute to a profit & loss distribution with a heavy tail, while individualized pricing will contribute to a profit & loss distribution with a long tail; in other words, there exists the probability of losing solvency. Insurance institutions should hedge against the risk of insolvency.

One way of controlling the variance of insurance companies' profit & loss is to require necessary investment amounts for information security systems. The current adverse selection has been confirmed. Large scales losses come from companies' high vulnerabilities. A mandatory investment requirement, for example, asking an amount of investment in self-defense equal to the product of a determined amount and vulnerability level, will smooth both the profit & loss and reduce the value at risk. Another way of mitigating loss is to provide long-term adaptive premium contracts, use companies' performances of self-enhancement and historical claim records to help maintain the dynamic equilibrium of premium and expected loss. A three-term yearly adjusted contract simulation shows excellent control of profit & loss. Other approaches, such as reinsurance, ILS should also be considered.

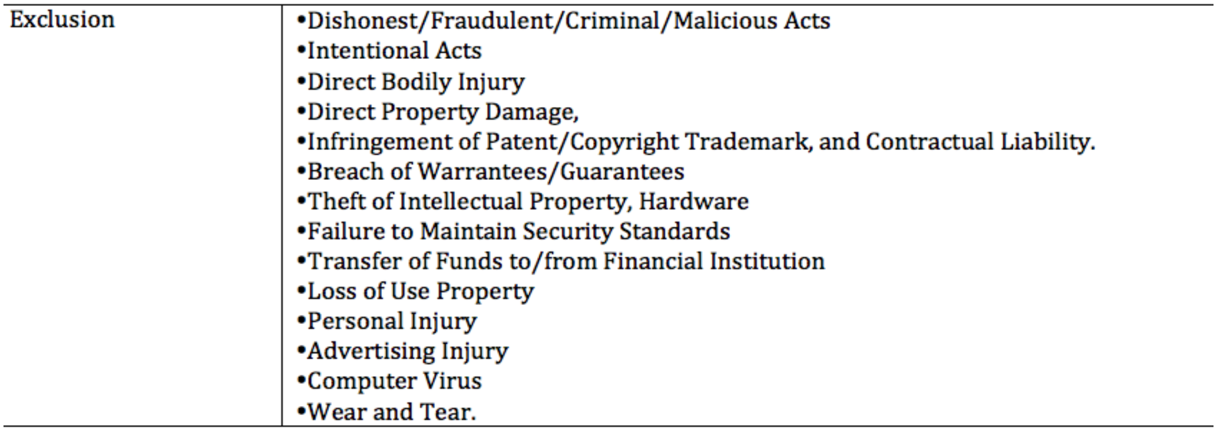
Nowadays cyber insurance products are considered to have high prices and limited coverage, and the reasons arise from both parties. Entities have underestimated the impact of cyber incidents, and they are not willing to contribute in the procedure of improving the safety level since there exists high interdependency of cyber risks among companies. The lack of participations in the cyber risk insurance market has aggravated the data paucity problem and hobbled the procedure of promoting a relatively accurate quantitative method for cyber risk. However, guidelines for cyber threat defense, cyber risk management, cyber insurance product design have been gradually introduced. Governments like the US and the UK have published laws and regulations to advance the process of cyber security maintenance. With the updated data pool of cyber event records, companies could share cyber risk management information and benefit from closer cooperation with each other; more-accurate risk factors could be included in the quantitative process; reputation and credit would be measured more suitably. Monte Carlo simulation pricing based on the insured optimized decision system introduced here with more accurate parameters can still be used. More-practical situations could be considered in the simulation. A future direction of related research could be the establishment of an empirical-data-based risk factor system, and more-specific estimation of the functions with ν and ‘a’.

APPENDICES

Appendix A

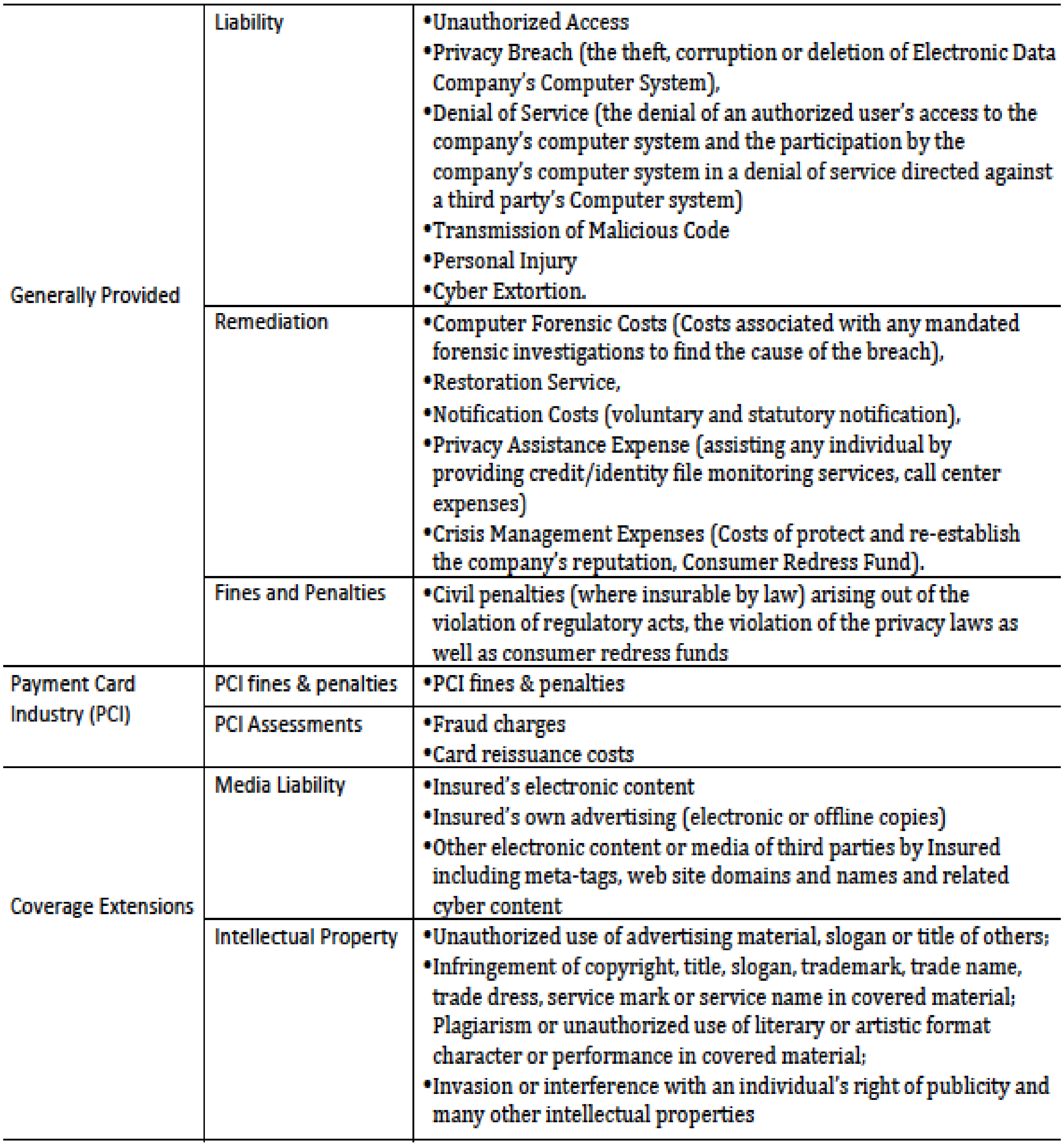
Related Concepts and Analysis

A.1 Tables of Coverages and Exclusions Included in Cyber Insurance



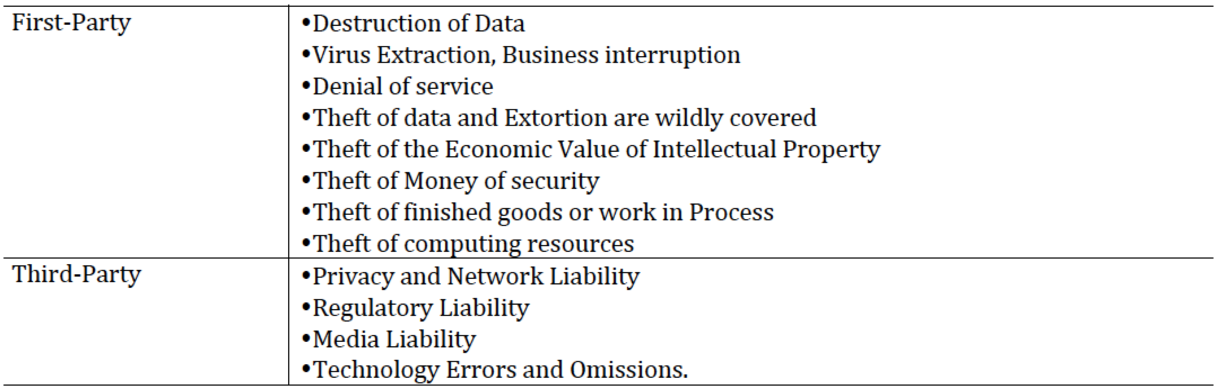
Exclusion	•Dishonest/Fraudulent/Criminal/Malicious Acts •Intentional Acts •Direct Bodily Injury •Direct Property Damage, •Infringement of Patent/Copyright Trademark, and Contractual Liability. •Breach of Warrantees/Guarantees •Theft of Intellectual Property, Hardware •Failure to Maintain Security Standards •Transfer of Funds to/from Financial Institution •Loss of Use Property •Personal Injury •Advertising Injury •Computer Virus •Wear and Tear.

Figure A.1: Exclusions in policy



Generally Provided	Liability	•Unauthorized Access •Privacy Breach (the theft, corruption or deletion of Electronic Data Company's Computer System), •Denial of Service (the denial of an authorized user's access to the company's computer system and the participation by the company's computer system in a denial of service directed against a third party's Computer system) •Transmission of Malicious Code •Personal Injury •Cyber Extortion.
	Remediation	•Computer Forensic Costs (Costs associated with any mandated forensic investigations to find the cause of the breach), •Restoration Service, •Notification Costs (voluntary and statutory notification), •Privacy Assistance Expense (assisting any individual by providing credit/identity file monitoring services, call center expenses) •Crisis Management Expenses (Costs of protect and re-establish the company's reputation, Consumer Redress Fund).
	Fines and Penalties	•Civil penalties (where insurable by law) arising out of the violation of regulatory acts, the violation of the privacy laws as well as consumer redress funds
Payment Card Industry (PCI)	PCI fines & penalties	•PCI fines & penalties
	PCI Assessments	•Fraud charges •Card reissuance costs
Coverage Extensions	Media Liability	•Insured's electronic content •Insured's own advertising (electronic or offline copies) •Other electronic content or media of third parties by Insured including meta-tags, web site domains and names and related cyber content
	Intellectual Property	•Unauthorized use of advertising material, slogan or title of others; •Infringement of copyright, title, slogan, trademark, trade name, trade dress, service mark or service name in covered material; Plagiarism or unauthorized use of literary or artistic format character or performance in covered material; •Invasion or interference with an individual's right of publicity and many other intellectual properties

Figure A.2: Coverage included in policy



First-Party	•Destruction of Data •Virus Extraction, Business interruption •Denial of service •Theft of data and Extortion are wildly covered •Theft of the Economic Value of Intellectual Property •Theft of Money of security •Theft of finished goods or work in Process •Theft of computing resources
Third-Party	•Privacy and Network Liability •Regulatory Liability •Media Liability •Technology Errors and Omissions.

Figure A.3: First-party and third party coverage in policy

A.2 Other Core Concepts of Cyber Insurance Product

Trigger: According to the report, the common triggers are failure to secure data, Loss caused by employee, acts by persons other than insureds and Loss resulting from theft or disappearance of private property.

Definition of Claims: 1. With respect to Privacy, network security and media: (a) Written demand against any Insured for monetary or non-monetary damages; (b) A civil proceeding against any Insured seeking monetary damages or non-monetary or injunctive relief, commenced by the service of a complaint or similar pleading; (c) An arbitration proceeding against any Insured seeking monetary damages or non-monetary or injunctive relief; (d) A regulatory proceeding. 2. With respect to data breach fund: a written report by the Insured to the Insurer of a failure by the insured or by an independent contractor for which the insured is legally responsible to properly handle, manage, store, destroy or otherwise control personal information; 3. With respect to network extortion: network extortion including, where applicable, any appeal therefrom.

Prohibited industry: Among 23 insurance entities that provide general product, more than 40% prohibit on-line gambling, payment processed and adult content industry. Associations faced large exposure as education institutions, social networking platform and information brokers as well as some professional companies such as lawyers, accountants and technology exclude by some insurers. Although most insurers provide product for financial institution, specific financial segment is excluded case by case, for example, debit card company.

A.3 Statistical Analysis of Data from Fusion Table

[5]

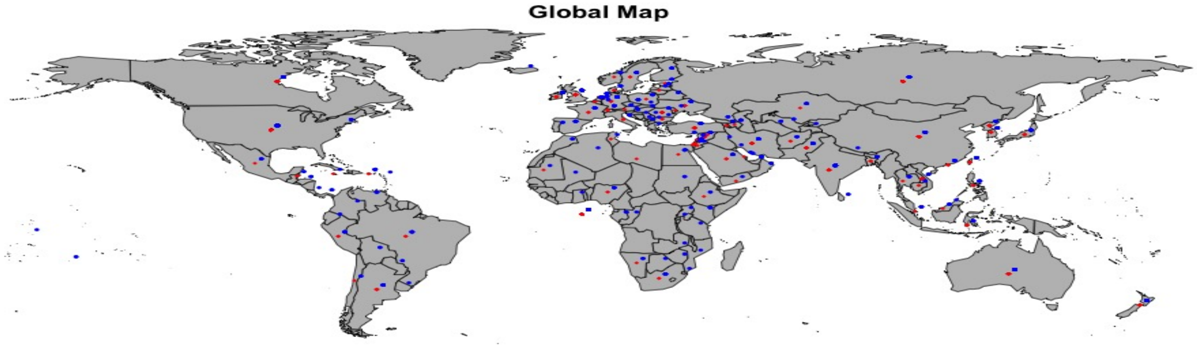


Figure A.4: Mapping of Cyber Incidents

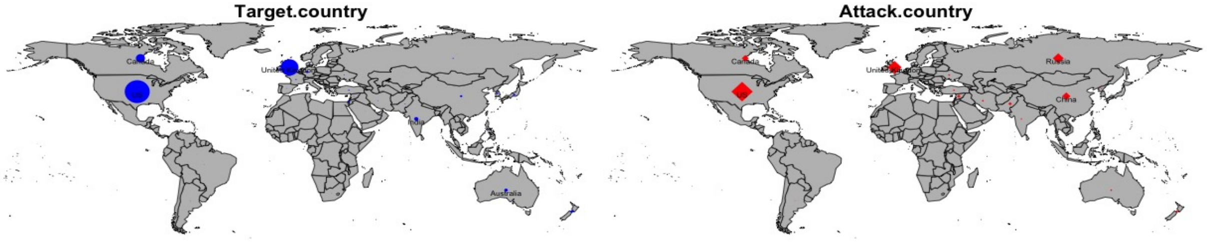
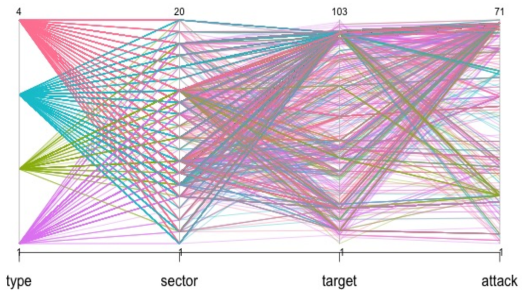


Figure A.5: Countries Attack and Countries Being Attacked

[5] This data is from Google fusion table, which is not a confirmed complete dataset, but could give us a general sense of global cyber incidents

The top five countries with most attackers are the USC, the UK, Russia, China and Canada. However 44.5% of the attack locations are unknown. The top five countries suffers a lot are the US,the UK, Canada, India and Australia. Only 2.3% of the target locations are unknown. This result confirms the hard-to-identify characteristic of cyber crime.



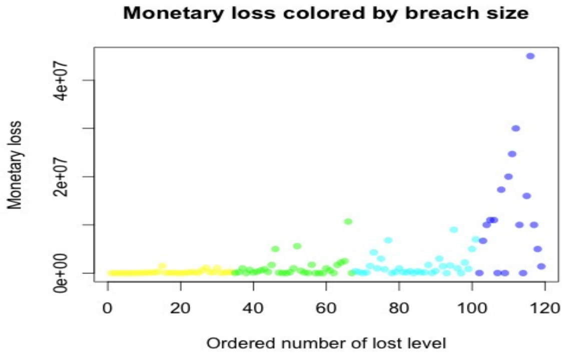


Figure A.6: Parallel Plot for Incidents

Figure A.7: Monetary Loss v.s. Scale of Breach

Figure A.6 shows that attacks could be within a country and between countries. The incidents generally randomly distributed and there exists large number of homogeneous exposure units. (The variable 'type' in the above graph represents the motive of cyber crime 1.Coercion 2. Espionage 3.Financial 4.Other). Figure A.7 shows that the average value of losses per record released vary in a large range.[30] A huge scale of breach not necessary contribute to a large loss.

Appendix B

Code for Simulation

B.1 Code for Individualized Pricing

```
function[profit,theta]=pricing(deductible,limited,theta0,
lambda0,sigma,a,budget,vulner,m,n,alpha)
 dtheta=1;
   while(dtheta>0.01)
      for k=1:n
          [zp,Pp,reR] = Optim(deductible,limited,theta0,lambda0,a,budget,vulner);
          if vulner<0.01;
             zp=0;
             Pp=0;
          end
          newv=vulner.^(a*zp+1);
          ALE=lambda0*newv*0.9*0.1;
          T=0;
          L=0;
          P=Pp;
          while(sum(T<1)>0)
             Tt=exprnd(1/0.1,m,1);
             T=T+Tt;
             Expo=normrnd(0,1,m,1);
             SLE=newv.*(sigma*Expo+lambda0);
             l=(rand(m,1)<0.9).*SLE.*(T<1);
```

```
            l=min(l-deductible,limited).*(T<1);
            l=max(l,0).*(T<1);
            L=L+l;
         end
         L(P==0)=0;
         net(k)=(P*m-sum(L));
         profit(k)=net(k)/sum(P*m);
         mtheta(k)=sum(L)/((ALE*m)*(1-alpha))-1;
     end
   %theta=quantile(mtheta,0.95)
    theta=mean(mtheta);
    dtheta=abs(theta-theta0);
    theta0=theta;
   end
end
```

B.2 Code for Three-year-term Profit and Loss

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
limited=20*1e+6;
theta0=0.02;
a=0.3464*1e-5;
budget=0.825*1e+6;
deductible=10000;
m=1000;
v=rand(m,1);
t=0.9;
ARO=0.1;
mu=10e+6;
sigma=(5e+10)^0.5;
%%%%%parameters for small company
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%given v,lambda
for j=1:1000
    v=rand(m,1);
    lambda=randsample([1,2,5],m,true,[0.9,0.08,0.02])*10e+6;
```

```
T=0;
L=0;
TM=[];
LM=[];
%z=4000*(v>0.6)+1000*(v<0.4);
while(sum(T<3)>0)
      Tt=exprnd(1/0.1,m,1);
      T=T+Tt;
      TM=[TM,T];
      Expo=normrnd(0,1,m,1);
      SLE=(sigma*Expo+lambda');
      l=(rand(m,1)<0.9).*SLE.*(T<3);
      l=min(l-deductible,limited).*(T<3);
      l=max(l,0).*(T<3);
      LM=[LM,l];
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%investment requirement
%z=4000*(v>0.6)+1000*(v<0.4);      %type1  reuquire investment
z=0*(v>0.6);                       %type3 no investment require
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
v1=v.^(a*z+1);
%%%%%
for i=1:m
    [zp,Pp,reR] = Optim(deductible,limited,theta0,lambda(i)
    ,a,budget-z(i),v1(i)); P1(i)=Pp;
end
L1=sum(LM.*(TM<=1),2).*newv1'       %year1 loss
L1=min(L1,limited);
%v2=newv1;                            %type1 no vulnerability punishment
v2=newv1+(1-newv1)*0.5.*(L1>0)' ;    %type2 vulnerability punishment
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%investment requirement
%z=4000*(v2>0.6)+1000*(v2<0.4); %type1 investment require
%z=4000*(L1>0); %type2 loss investment require
z=0*(L1>0); %type3 no investment reuiqre
v2=v2.^(a*z'+1) ; %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
for i=1:m
    [zp,Pp,reR] = Optim(deductible,limited,theta0,lambda(i),a,budget-z(i),v2(i));
```

```
        newv2(i)=v2(i).^(a*zp+1);
        P2(i)=Pp;
     end
     L2=sum(LM.*(TM<=2&TM>1),2).*newv2'; %year 2 loss
     L2=min(L2,limited);
     v3=newv2;                           %type1 no vulnerability punishment
     v3=newv2+(1-newv2)*0.5.*(L2>0)';    %type2 vulnerability punishment
     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%investment requirement
     %z=4000*(v3>0.6)+1000*(v3<0.4);     %type1 investment require
     %z=4000*(L2>0);                     %type2 loss investment require
      z=0*(L2>0);                        %type3 no investment reuiqre
     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
     v3=v3.^(a*z'+1) ;
     for i=1:m
        [zp,Pp,reR] = Optim(deductible,limited,theta0,lambda(i),a,budget-z(i),v3(i));
        newv3(i)=v3(i).^(a*zp+1);
        P3(i)=Pp;
     end
     L3=sum(LM.*(TM<=3&TM>2),2).*newv3';%year 3 loss
     L3=min(L3,limited);
     profit1(j)=(sum(P1)-sum(L1))/sum(P1);
     profit2(j)=(sum(P2)-sum(L2))/sum(P2);
     profit3(j)=(sum(P3)-sum(L3))/sum(P3);
     profit(j)=((sum(P1)-sum(L1))+(sum(P2)-sum(L2))+
     (sum(P3)-sum(L3)))/(sum(P1)+sum(P2)+sum(P3));
end
```

References

[1] Advisen. *Cyber Loss Count Data.* the U.S.: Advisen, 2016.

[2] B. Berliner. *Limits of insurability of risks.* Prentice Hall, 1982.

[3] Betterley. *Cyber Privacy Insurance Market Survey.* the U.S.: Betterley Risk Management Consultants, Inc, 2015.

[4] C. Biener and M. Eling. "Insurability in microinsurance markets: an analysis of problems and potential solutions". In *The Geneva Papers*, pages 196–234. Springer, 2016.

[5] C. Biener, M. Eling, and J.H. Wirfs. "Insurability of cyber risk: an empirical analysis". *The Geneva Papers on Risk and Insurance Issues and Practice*, 40(1):131–158, 2015.

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

[7] J.L. Cebula and L.R. Young. "A taxonomy of operational cyber security risks". Technical report, Carnegte-mellon UNIV Pittsburgh pa Software Engineering INST, 2010.

[8] DHL & Cisco. *Internet of Things in Logistics.* Germany: DHL Trend Research, Canada: Cisco Consulting Services, 2015.

[9] Marsh & McLennan Companies. *Cyber Risk Handbook 2015: Perspectives on Prevention, Preparation and Response.* the U.S. : Marsh & McLennan Companies, 2015.

[10] McAfee & CSIS. *Net losses: Estimating the Global Cost of Cyber Crime.* the U.S.: Center for Strategic and International Studies, 2014.

[11] S. Curtis. *British Companies Bombarded with Cyber Attacks.* Telegraph Science and Tech, 14, Apr, 2015.

[12] DBIR. *Verizons Data Breach Investigations Report.* the U.S.: DBIR, 9th edition.

[13] World Economic Forum. *The Global Risks Report 2016.* Geneva: World Economic Forum, 11th edition, 2016.

[14] P.K. Freeman and H.C. Kunreuther. *"Managing environmental risk through insurance"*, volume 9. Springer Science & Business Media, 1997.

[15] L.A. Gordon and M.P. Loeb. "The economics of information security investment". *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

[16] L.A. Gordon, M.P. Loeb, and T. Sohail. "A framework for using insurance for cyber-risk management". *Communications of the ACM*, 46(3):81–85, 2003.

[17] T. Grzebiela. "Insurability of electronic commerce risks". In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pages 9–pp. IEEE, 2002.

[18] H. Herath and T. Herath. "Copula-based actuarial model for pricing cyber-insurance policies". *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2(1):7–20, 2011.

[19] H.S.B. Herath and T.C. Herath. "Cyber-insurance: Copula pricing framework and implication for risk management". In *WEIS*, 2007.

[20] Ponemon Institution. *Cost of Cyber Crime :Global, 2015.* the U.S.: Ponemon Institution, 2015.

[21] T. Ishikawa and K. Sakurai. "A study of security management with cyber insurance". In *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication*, page 68. ACM, 2016.

[22] W.T. Karten. " How to expand the limits of insurability ". *Geneva Papers on Risk and Insurance. Issues and Practice*, pages 515–522, 1997.

[23] R.W. Klein. *"A Regulator's Introduction to the Insurance Industry".* NAIC, 1999.

[24] H.C. Kunreuther and E.O. Michel-Kerjan. "Climate change, insurability of large-scale disasters and the emerging liability challenge". Technical report, National Bureau of Economic Research, 2007.

[25] Marsh. *European 2013 Cyber Risk Survey Report.* the U.S.: Marsh, 2013.

[26] Marsh. *European 2015 Cyber Risk Survey Report.* the U.S.: Verzion, 2015.

[27] Marsh. *Marsh: Global Insurance Market Quarterly Briefing, 2015.* the U.S.: Marsh, 2015.

[28] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S.K. Sadhukhan. "Cyber-risk decision models: To insure it or not?". *Decision Support Systems*, 56:11–26, 2013.

[29] Guideline for Automatic Data Processing National Bureau of Standards. *Physical Security and Risk Management.* the U.S.:Federal Information Processing Standards Publication, 1974.

[30] NetDiligience. *Cyber Claim Study.* U.S.: NetDiligience, 2015.

[31] C. Nie, S. Wang, and S. Li. "Ruin theory application on cyber risk modeling. 2016.

[32] H. Ogut, S. Raghunathan, and N.M. Menon. "Information security risk management through self-protection and insurance". *The University of Texas at Dallas*, 2005.

[33] M. Pengelly. "Cyber is the biggest operational risk fear, say practitioners". Technical report, http://www.risk.net/operational-risk-and-regulation/news/2441963/cyber-is-biggest-operational-risk-fear-say-practitioners, January, 2016.

[34] PricewaterhouseCoopers. *The Global State of Information Security Survey.* the U.K.: PwC, 2015.

[35] PricewaterhouseCoopers. *Managing Cyber Risk in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015.* the U.K.: PwC, 2015.

[36] Allianz Global Corporate & Specialty SE. *Allianz Risk Barometer Top Business Risks.* Germany: Allianz SE and Allianz Global Corporate & Specialty SE, 2015.

[37] A. Shah. "Pricing and risk mitigation analysis of a cyber liability insurance–a case for cyber risk index". *Available at SSRN 2778606*, 2016.

[38] SINTEF. "Big data, for better or worse: 90% of world's data generated over last two years.". *ScienceDaily.*, www.sciencedaily.com/releases/2013/05/130522085217.html (accessed August 23, 2016).

[39] Allianz Global Corporate & Specialty. *A guide to Cyber risk*. Germany: AGCS, 2015.

[40] E.J. Vaughan and TM Vaughan. *Fundamentals of Risk and Insurance*. 11th edition, 2013.

[41] Taylor Wessing. *Cyber Risks : A Review of Cyber Liability Issues and Data Breach Response*. the U.K.: Taylor Wessing, 2015.

[42] Willis. *Willis Fortune 1000 Cyber Disclosure Report*. the U.K.: Willis, 2013.

[43] W. Xie. "Pricing cyber insurance: A copula approach with bootstrapping". 2016.

[44] D. Young, J. Lopez, M. Rice, B. Ramsey, and R. McTasney. "A framework for incorporating insurance in critical infrastructure cyber risk strategies". *International Journal of Critical Infrastructure Protection*, 2016.