March 2019

Managing Information Security Investments Under Uncertainty: Optimal Policies for Technology Investment and Information Sharing

Yueran Zhuo

MANAGING INFORMATION SECURITY INVESTMENTS UNDER UNCERTAINTY: OPTIMAL POLICIES FOR TECHNOLOGY INVESTMENT AND INFORMATION SHARING

A Dissertation Presented

by

YUERAN ZHUO

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

February 2019

Isenberg School of Management

MANAGING INFORMATION SECURITY INVESTMENTS UNDER UNCERTAINTY: OPTIMAL POLICIES FOR TECHNOLOGY INVESTMENT AND INFORMATION SHARING

A Dissertation Presented

by

YUERAN ZHUO

Approved as to style and content by:

Senay Solak, Chair

Hari J. Balasubramanian, Member

Traci J. Hess , Member

Mila G. Sherman, Member

George R. Milne, Ph.D. Program Director
Isenberg School of Management

To Seaghan.

ACKNOWLEDGMENTS

I would like to express my sincere thanks to my advisor Professor Senay Solak, for his continuous support, encouragement and constructive comments during my doctoral study. It was my great fortune to have him guide me through all the challenges throughout the years. With dedication and professionalism, he has also set me a role model toward working harder and becoming a better researcher.

I wish to present my thanks to my dissertation committee members, Professor Hari Balasubramanian, Professor Traci Hess, and Professor Mila Sherman. I am very grateful for their valuable insights and perspectives on my research. I would also like to thank all the faculty, stuff and friends in Isenberg School of Management as well as the Mechanical and Industrial Engineering department for their help and friendship.

In addition, I would like to pay my regards to Mr. Christopher Misra and his team for their practical insights, and to members of the Advanced Cyber Security Center for taking part in discussion regarding this research.

Finally, my deepest gratitude goes to my family – my parents Guifang, Shengguang, and my husband Tao – for their unconditional love and patience throughout my life. There is no way that I could have done this without them. My special thank goes to my son Seaghan for continuously reminding me what the true meaning of life is.

ABSTRACT

MANAGING INFORMATION SECURITY INVESTMENTS UNDER UNCERTAINTY: OPTIMAL POLICIES FOR TECHNOLOGY INVESTMENT AND INFORMATION SHARING

FEBRUARY 2019

YUERAN ZHUO

B.Sc., NANKAI UNIVERSITY

M.Eng., NANKAI UNIVERSITY

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Senay Solak

Information systems are an integral part of today's business environment. Businesses, government organizations, and the society rely on these systems for various transactions, most of which have huge financial implications. Hence, attacks that breach information systems result in interruption of operations, loss of data and customer confidence, constituting a significant threat to firms.

Such attacks have been increasing in frequency and sophistication over time, and defending the assets of a firm in response to these attacks has become a key operational issue. According to Ponemon (2016a), information security attacks cost a typical large firm $7.7 million per year on average, while Ponemon (2016b) reports that the average annual total cost of attacks on information systems has increased by 30% between year 2013 and 2016. In several cases, the cost of an information security attack can

reach very high levels, as evidenced through some recent major breaches released to the public, such as the Target breach in December 2013 with an estimated cost of $1 billion and the Home Depot breach in September 2014 with an estimated cost of $142 million (Vomhof, 2013). Based on an estimate by Lewis (2018), the global cost of crime that exploits information systems has exceeded half a trillion dollars per year.

The losses due to attacks on information systems can be mitigated through investments in information security technologies and services. Guttman and Roback (1995) and Hoo (2000) define information systems security as an integral element in the management of a firm, and highlight its importance as a key area for the successful operation of a business. Hence, most firms utilize separate information security budgets, dedicated for investment towards preserving the assets of the firm against attacks. While the type of business plays a role in determining the ratio of the information security budget with respect to a firm's overall information technology budget, it is well known that this ratio has been steadily increasing over the recent years, along with the actual dollar value allocated to information security (Peters, 2009, Richardson, 2010). Kessel and Allan (2013) note that 46% of the responding organizations in a survey reported increases in their information security budgets every year. Overall, the global information security investments are expected to increase from $73.6 billion in 2016 to $105.6 billion by 2021 with an estimated compound annual growth rate of more than 7% (Smith and Pike, 2017).

As information security budgets increase along with available investment options, firms are more concerned about the effectiveness of their investments in information systems security, and whether their investment portfolio is aimed towards maximizing returns (Richardson, 2010). This is a challenging process due to several factors, which involve the difficulty of measuring returns from information security investments, as well as that of defining the uncertainty around these returns. Moreover, the corresponding decision process is a dynamic one, where technological developments and

increasing sophistication in cyber attacks result in an ever-changing investment environment. Therefore, management of the investment problem in information system security using quantitative approaches has been seldom addressed in the literature and in industrial practice. To fill in this gap, in this thesis we study three practical problems related to information system security investment management.

In the *first problem*, we address two key decisions by a firm related to information security technology investments: (1) How much should the firm invest in information security technology? and (2) How should this investment be allocated over different categories of security technologies? As part of our findings, we derive a simple functional relationship between the potential total losses of a firm and the optimal amount that the firm should invest in information systems security. Related to this, we find that firms in finance, energy, and technology sectors should invest twice more in trying to detect information security breaches, than in trying to prevent them. In other industries, information security investments should be split evenly between preventive and detective measures. Moreover, the overall information security budgets for certain types of firms in the former set of industries should be on average 4% higher than other industries, even when the potential total losses under a security breach are the same.

In the *second problem*, we seek answers to three practical decision problems regarding information sharing in information system security: (1) What is the optimal level of information sharing for a firm as a function of the firm's technology investments? (2) What is the value of information sharing in information security? and (3) How do these findings vary over different operating environments? We build up a stochastic framework to capture the inter-relationship between information sharing and technology investments, where the two act as strategic counterparts of information system security. We find that, for firms with pre-fixed technology investment levels, the optimal information sharing level decreases as the marginal cost of infor-

mation sharing becomes higher, and there exists a threshold value such that firms are better off by not sharing information if the marginal cost of information sharing exceeds this threshold value. For the optimal information sharing level, we find that firms with larger security budgets should share 15% more information, when compared to optimal sharing levels of small to medium sized firms.

In the *third problem*, we study pricing strategies under asymmetric information sharing for information system security, where firms can either share information with other firms and obtain a monetary compensation for sharing more information or paying a price for sharing less or even no information. Specifically, we investigate two practical research questions: (1) What fair price should a firm pay participating information sharing in asymmetric sharing environment? (2) How would the price of information vary under different pricing strategies and other influencing factors? To this end, we develop analytical expressions of a firm's payoffs under an asymmetric information sharing environment. We also analyze the pricing of information as a function of a firm's technology investment level, its information sharing level, and the marginal cost of information sharing. Numerical analyses are conducted to identify the overall benefits to the information sharing firms due to the implementation of certain pricing strategies.

In conclusion, as one of the few studies on information system security investment problem, we derive managerial insights for both technology investment and information sharing decisions. The findings of this study is expected to improve the efficiency of information system security practice and help the firms better defend against attacks on their information systems.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

CHAPTER 1

INTRODUCTION

Information systems are an integral part of today's business environment. Businesses, government organizations, and the society rely on these systems for various transactions, most of which have huge financial implications. Hence, attacks that breach information systems result in interruption of operations, loss of data and customer confidence, constituting a significant threat to firms.[1].

Such attacks have been increasing in frequency and sophistication over time, and defending the assets of a firm in response to these attacks has become a key operational issue. According to Ponemon (2016a), information security attacks cost a typical large firm $7.7 million per year on average, while Ponemon (2016b) reports that the average annual total cost of attacks on information systems has increased by 30% between year 2013 and 2016. In several cases, the cost of an information security attack can reach very high levels, as evidenced through some recent major breaches released to the public, such as the Target breach in December 2013 with an estimated cost of $1 billion and the Home Depot breach in September 2014 with an estimated cost of $142 million (Vomhof, 2013). Based on an estimate by Lewis (2018), the global cost of crime that exploits information systems has exceeded half a trillion dollars per year.

The losses due to attacks on information systems can be mitigated through investments in information security technologies and services. Guttman and Roback

[1]While for conciseness purposes we refer to a 'firm' throughout the thesis, our discussions and analyses are applicable to any business, government organization or other institutional establishment that uses information systems.

(1995) and Hoo (2000) define information systems security as an integral element in the management of a firm, and highlight its importance as a key area for the successful operation of a business. Hence, most firms utilize separate information security budgets, dedicated for investment towards preserving the assets of the firm against attacks. While the type of business plays a role in determining the ratio of the information security budget with respect to a firm's overall information technology budget, it is well known that this ratio has been steadily increasing over the recent years, along with the actual dollar value allocated to information security (Peters, 2009, Richardson, 2010). Kessel and Allan (2013) note that 46% of the responding organizations in a survey reported increases in their information security budgets every year. Overall, the global information security investments are expected to increase from $73.6 billion in 2016 to $105.6 billion by 2021 with an estimated compound annual growth rate of more than 7% (Smith and Pike, 2017).

As information security budgets increase along with available investment options, firms are more concerned about the effectiveness of their investments in information systems security, and whether their investment portfolio is aimed towards maximizing returns (Richardson, 2010). This is a challenging process due to several factors, which involve the difficulty of measuring returns from information security investments, as well as that of defining the uncertainty around these returns. Moreover, the corresponding decision process is a dynamic one, where technological developments and increasing sophistication in cyber attacks result in an ever-changing investment environment. Therefore, management of the investment problem in information system security using quantitative approaches has been seldom addressed in the literature and in industrial practice.

To fill in this gap, in this thesis we study three practical problems related to information system security investment management. The first one is managing technology investment in information system security, and the second and third ones

extend the problem to include information sharing among the firms in these operations. In the remainder of this chapter we introduce the methodology adopted for the quantitative analysis, the background of these two classes of problems and how the research questions are defined upon them.

1.1 Stochastic Mathematical Programming

The information security environment has an ever-changing nature, which inevitably brings in uncertainty to the information security operations. While many methods can be applied to make decisions under uncertainty to solve theoretical and practical problems, in this thesis we choose to use stochastic mathematical programming to study the problem of information security investment management. In the following paragraphs, we introduce the stochastic mathematical programming method in a brief manner and provide some references.

Stochastic mathematical programming (SP) is a type of mathematical programming method. The first introduction of SP is by Dantzig (1955), where the author introduces a resource model that includes a random event as part of the optimization problem structure. In this model, the solution of the optimization problem is adapted to different outcomes of the random event, which presents a probabilistic nature of the problem. Since then, stochastic mathematical programming has become a widely applied method to solve many of the real-word optimization problems that involve uncertainty.

Stochastic mathematical programming - as a mathematical optimization modeling framework - consists of an objective function and a set of constraints. The constraints can be presented as either equalities or inequalities. Additionally, some parameters of the stochastic mathematical programming model are random variables. The probability distribution of these random variables are assumed to be known, which is the most important assumption of the stochastic mathematical programming method. In

solving the model, an optimal policy is identified that could maximize or minimize the expected value of the objective function over all possible realizations of the random parameters.

A very widely applied SP model is the two-stage SP model, where the decision process is made of two stages. In the first stage, a decision maker takes action without knowing any information about the realization of the random event. At the beginning of the second stage, after observing the realized values of the random parameters, the decision maker is assumed to take second stage follow-up actions in order to fine-tune the decision made earlier in the first stage.

The two-stage SP model can also be further generalized into a multi-stage SP model. Similar to the two-stage SP model, in a multi-stage SP model, there is an initial decision made at the beginning of the first stage. Afterwards, as more information is revealed about the random parameter in every stage, there is always a follow-up decision made at the beginning of the next stage based on newly observed information. In this thesis, we mainly focus on the two-stage SP model as its modeling framework fits the information security management structure.

The general formulation of a two-stage SP model is given as

$$\min_{x \in X} \{g(x) = f(x) + E_{\xi}[Q(x, \xi)]\} \tag{1.1}$$

where $Q(x, \xi)$ is the optimal value of the second-stage problem involving the random factor ξ such that

$$Q(x, \xi) \equiv \min_{y} \{q(\xi) | T(\xi)x + W(\xi)y = h(\xi)\}. \tag{1.2}$$

If the objective function and constraints are linear, then a deterministic equivalent of the above formulation can be written as:

$$\min_{x \in \mathbb{R}^n} \quad c^T x + E_\xi[\min_{y \in \mathbb{R}^m} q(\xi)^T y] \tag{1.3}$$

$$\text{subject to} \quad Ax = b \tag{1.4}$$

$$T(\xi)x + W(\xi)y = h(\xi) \tag{1.5}$$

$$x \geq 0, \quad y \geq 0 \tag{1.6}$$

Stochastic mathematical programming has been applied to many fields of study that involves decision making under uncertainty, and the literature contains a wide variety of references on the theoretical and practical issues of SP. We refer the readers to these studies for a more detailed discussion on SP, for example Wets (1983), Kall et al. (1994), Wallace and Ziemba (2005), Birge and Louveaux (2011), and Shapiro and Dentcheva (2014).

1.2 Technology Investment in Information System Security

There exist different ways that a firm can utilize its information security budget, such as developing its in-house information security systems, acquiring security measures from a vendor, or outsourcing the information security functions to a third party (Cezar et al., 2013). In practice, in-house security technology development tends to be very sophisticated and not amenable to most firms with few exceptions, while similarly the outsourcing strategy is not favored in many industries (Peters, 2009). Hence, in the first part of this thesis we focus on the most common utilization of an information security budget by firms: obtaining information security products through purchases from third-party providers. As part of this process, we mainly consider strategic product acquisitions, where the firm contracts with select vendors to acquire different categories of information security measures. This is a typical process for many firms, as it ensures standardization, utilizes of economies of scale, and provides streamlined support services.

As information security budgets increase along with available investment options, firms are more concerned about the effectiveness of their investments in information systems security, and whether their investment portfolio is aimed towards maximizing returns (Richardson, 2010). This is a challenging process due to several factors, which involve the difficulty of measuring returns from information security investments, as well as the difficulty of defining the uncertainty around these returns. Moreover, the corresponding decision process is a dynamic one, where technological developments and increasing sophistication in cyber attacks result in an ever-changing investment environment.

However, neither the existing industrial practice nor the academic literature has been able to produce definitive guidelines on such issues, due to two major challenges that are unique to information security investments. First, it is not known how to measure returns from investing in information systems security, and how to characterize the uncertainty around these returns. Second, the corresponding decision process involves a higher level of dynamics, where technological developments and increasing sophistication in threats to information systems result in an ever-changing investment environment. In this thesis, we first address these challenges, and then develop a framework to provide answers to two relevant operational questions by a firm: *how much should the firm invest in information systems security?*, and *how should this investment be allocated over different countermeasure categories?*

We address this dynamic decision problem in Chapter 3 by developing a high level framework aimed at providing guidance to firms when allocating their information security budgets into different types of investment options. The framework utilizes potential loss information specific to different industries, as well as general information on the characteristics of different types of attacks and information security investments. Analysis is then performed using this framework to suggest policies that would maximize expected returns from information security investments, where risk

aspects are also studied through a conditional value at risk approach. As part of our analyses, we also study different industries separately, and use data to derive generic policies that would maximize expected returns from information security investments.

1.3 Information Sharing in Information System Security

While firms strive to improve information system security by investing in different technologies, the increasing sophistication of information system attacks has also resulted in the need for joint information sharing endeavors among firms. A major difficulty for firms in defending against advanced information security attacks is the time gap between the attack and the corresponding response, which can be especially long when the firm has no previous knowledge of the kind of attack they are facing (Verizon, 2015). Information sharing, i.e. the practice of passing on experiences and knowledge of security information among firms, can be an effective approach for firms to alleviate the impact of this problem. Synthesizing the knowledge and experience of a larger community allows all parties to defend their assets more effectively against cyber attacks. It is evident through some past major breaches that such information sharing could have helped avoid major losses if it had been implemented successfully. Two such examples involve the Target data breach of December 2013 which cost the company direct losses of around $1 billion, and the Home Depot breach in September 2014, which resulted in losses of more than $140 million due to exposure of payment card data. It was later found that these two breaches were actually caused by the same malware attack, indicating the potential that the latter Home Depot breach could have been avoided if relevant information had been shared and proper protective actions had been taken accordingly.

In current practice, information sharing among firms for cybersecurity is mostly realized by forming alliances within a given industry. Some of these alliances are formed as Information Sharing and Analysis Centers (ISACs), which are specific to

each industry, such as the Financial Services-ISAC, Information Technology-ISAC, Healthcare and Public Health-ISAC and the Electric Sector-ISAC. Within each ISAC, member firms are encouraged to share information on any cyber attack, regardless of whether an attack was successful or not. The shared information usually includes methods/countermeasures a firm uses to defend against the attacks, vulnerabilities in these countermeasures, and methods that a firm applies to minimize the economic impact after a breach occurs (Gordon et al., 2003). All such information is collected and summarized by a centralized council within the ISAC and sent to the members in the form of alerts, guidance and recommendation reports. These reports would then help ISAC members provide better defense mechanisms against cyber threats, and reduce overall information security related costs.

Despite the benefits of information sharing in improving information system security, participation in ISACs and other similar alliances is still quite limited among firms. Some key reasons for this include: (1) the potential risk of losing competitive advantage due to the information shared with other firms; and (2) lack of economic incentive due to the difficulties in assessing the monetary value of information sharing, especially since the cost of sharing information in information system security practice is not negligible. These costs primarily include the fixed cost of joining information sharing alliances, personnel costs spent on security information gathering, and other relevant costs on information processing to ensure confidentiality in the information shared.

The first issue noted above is being addressed by standardizing information sharing procedures through legislative efforts, such as the U.S. Cybersecurity Information Sharing Acts of 2014 and 2015, which aim at creating a trustworthy environment for firms and other organizations participating in information sharing. The second issue, however, requires the development of procedures and measures in assessing the effectiveness of information sharing, especially when considered together with the

technology investment decisions on information system security. More specifically, since information sharing and technology investments are two major aspects of information system security practice, there exists an interplay between these two types of investments. Naturally, information sharing would boost the effectiveness of security countermeasures. However, as both information sharing and security countermeasures are costly to the firms, there must be a balance as to how much information to share and how much to invest in technology so that the overall expenditure is minimized. To this end, in this study we seek to answer the following research questions: *What is the optimal level of information sharing for a firm as a function of the firm's technology investments? What is the value of information sharing in information security? How do these findings vary over different operating environments?* We address these questions in Chapter 4.

1.4 Asymmetric Information Sharing in Information System Security

When two or more firms are in an information sharing alliance, the amount of information that the firms provide might vary due to multiple factors, such as size, technology investment capacity, and the information security environment for the firm. As a result, in many cases even the well-intended firms are unable to share the same level of information as they receive from other firms. In some other cases, a firm might be inhibited from sharing information due to regulations on privacy protection, but such a firm might still be in need of shared information to support information security operations. We refer to such a situation as asymmetric information sharing. This asymmetry in information sharing levels might reduce the impact of any incentives for sharing information, and can lead to reduced levels of information sharing. Given this setting, information sharing alliances are confronted with the challenges

of maintaining a fair information sharing environment, which would ensure similar or proportional returns for firms in the alliance.

A possible solution to the problem, as discussed by Hendriks (2006), is to impose charges on the shared information and treat it as a commodity. In this way, firms can acquire knowledge of attacks and other practical security knowledge from other firms at a fair price. The firms that share information would then receive compensation for the shared information, which might serve as a motivation for the continuation of participation in information sharing.

In the current practice, firms are typically charged a membership fee by Information Sharing and Analysis Centers for participating in information sharing activities. Although the membership fees for ISACs are calculated based on the sizes of the firms, the application of a membership fee does not totally address the problems that may arise due to asymmetric information sharing. First, although the firms are distinguished by their sizes, the level of membership fee being charged does not reflect the level of information provided or received by individual firms. Second, while the collected membership fees help maintain the operation of the ISAC, it does not provide monetary compensation to firms that share more information, therefore does not create a big incentive for continuous information sharing. Lastly, the membership fees for ISACs do not consider the willingness to pay attitudes of firms that may prefer not to share as much information, but to purchase such information from other firms.

In this study we aim to address these issues by seeking answers to the following research questions: *What fair price should a firm pay participating information sharing in asymmetric sharing environment?* and, *How would the price of information vary under different pricing strategies and other influencing factors?* To this end, in Chapter 5 we develop analytical expressions of a firm's payoffs under an asymmetric information sharing environment. We also analyze the pricing of information as a function of a firm's technology investment level, its information sharing level,

and the marginal cost of information sharing. Numerical analyses will be conducted to identify the pricing of information in an information sharing firms with multiple firms, as well as the overall benefits to the information sharing community due to the implementation of certain pricing strategies.

CHAPTER 2

LITERATURE REVIEW

In this chapter we introduce the related research literature on information security investment problems, which are categorized as two main aspects of information system security management problem we include in this thesis, namely the information security technology investment and security information sharing.

2.1 Related Research on Information Security Technology Investment

Current literature on managing investments for information systems security can be categorized into three classes: empirical studies, economic approaches, and portfolio approaches. *Empirical studies* on information security investments are usually based on extensive surveys or field studies of businesses. Some examples include industry technical reports such as Baker (2009), Richardson (2010), Ponemon (2011), and Verizon (2014b), where each report contains important statistics about the latest information security practices, and concludes with brief managerial suggestions for businesses according to those findings.

The other academic empirical studies tend to focus on particular perspectives. Kwon and Johnson (2011) analyze the influence of regulatory factors on information security investment decisions in the healthcare sector, while Baldwin et al. (2013) evaluate the impacts of some widely adopted economic methods on information security policy. Similarly, Rowe and Gallaher (2006) study information security investment strategies in the private sector based on a series of field studies. The literature of

empirical studies typically involves descriptive methods, and serve to provide information that can be used to assess the value of information assets and effectiveness of countermeasures. Specifically, we refer to several of these studies to characterize the information assets, attacks and countermeasure categories in our model in order to better reflect the information security practice in reality and obtain general data-based managerial insights that can be recommended to different types of firms.

The *economic approaches* have been naturally applied to the information security investment problem due to its financial nature. The literatures on this topic usually adopts classical cost-benefit metrics such as net present value (NPV), return on investment (ROI) and internal rate of return (IRR), which are selectively adopted by firms as decision aids for information security investment planning in practice (Gordon and Loeb, 2005). Gordon and Loeb (2002) first proposes a general ROI information investment model based on simple assumptions and concluded that information security investments of a firm should not exceed 37% of the total information security related potential losses. This result has been further discussed and compared by several studies under different restrictive conditions, such as Hausken (2006), Willemson (2006), Bojanc and Jerman-Blažič (2008), Huang et al. (2008). Some other studies use game-theoretical approaches to maximize the information security payoffs by analyzing the intentions and interactions between the firm and potential hackers (Cavusoglu et al., 2004, 2008, Gao et al., 2013, 2015).

However, these economic studies tend to leave out some of the key characteristics of information security investments, such as budget limitations and specific attributes of different types of countermeasures. Besides, the economic models usually assumes the countermeasures to be acting independently, hence cannot capture the possible joint effects of combining countermeasures with different specifics. In terms of modeling of the information security attacks, many of the game-theoretical approaches focus on customized malicious attacks, but ignores a vast majority of other breaches that

are triggered by non-malicious, non-targeting attacks. In our analysis, we utilize an ROI structure similar to the study of Gordon and Loeb (2002) when defining the general problem framework, but use a portfolio approach to achieve a more detailed and realistic investment setting involving budget constraints, different specifications of investment options, synergy effects of countermeasure combinations and a complete spectrum of attacks under an uncertain information security environment.

With much more complex and comprehensive problem set-ups, the literature using *portfolio approaches* to model information security investments have been rare. Studies using this approach typically model the information security investments as allocating funds into several investment options with different investment levels. Hoo (2000) first describes a framework consisting of multiple 'safeguards' impacting 'bad events'. The study uses an influence diagram and analyzes several alternative investment policies under budget limitations. A similar study is Rees et al. (2011), where the authors develop a decision tool to capture investment-return trade-offs and search for a near-optimal countermeasure portfolio using a genetic algorithm. Sawik (2013) builds a mixed integer model to study the selection of information security countermeasures with pre-fixed investment levels over a set of predefined risk cases. Another distinctive work is Garvey and Patel (2014), where the authors propose a series of frameworks to evaluate an information security system's performance and its economic benefits via analytical hierarchy process. A set of information security options is then selected according to these measures through a portfolio-based approach.

While these studies all aim to provide optimal investment strategies to information security practitioners, they usually build the models without considering specific features of the investment options, i.e., countermeasures. For studies using optimization methods, the synergistic effects of multiple countermeasure combinations have been seldom addressed in these models. Furthermore, it is difficult to incorporate uncertainties in these models to present the evolving nature of information security

attacks as it would expand the complexity of the models. Our work adds to the existing studies by considering a holistic mapping over different categories of information assets, attacks, and countermeasures, while also capturing the uncertainty and risk in the changing information security environment. Unlike any of the existing studies, we aim to provide firm-specific recommendations for information security investments that can be directly applied to their operational decision making settings. A summary of the main contributions of this chapter is illustrated in Table 2.1, where we list different studies in the literature and specify the properties addressed in each study.

2.2 Related Research on Information Sharing in Information System Security

The information sharing problem is first discussed in the economics literature. Clarke (1983) and Gal-Or (1985) study information sharing behaviors by oligopoly firms and derive similar conclusions that the mutual sharing of information does not happen spontaneously among firms despite the maximization of joint welfare. However, some studies focus on certain natural incentives for sharing information, and show that sharing information would be easily implementable under certain conditions. For example, Li (1985) finds that if all the firms have access to equally accurate information, then a firm would be willing to share some firm-specific information. Also, Shapiro (1986) suggests that the sharing of cost information can be made possible by firms joining an association with an information-sharing agreement. These studies from the economics literature, although not directly related to information security, provide important insights that can be applied to information sharing in cybersecurity, and we use these insights to help develop the modeling framework in this chapter.

As part of the of operations research literature, the topic of information sharing is widely studied within supply chain management. Initially motivated by the bullwhip

Table 2.1: Summary of existing literature on information security investment and contributions of this study

	Use economic models to measure investment returns	Consider both malicious and non-malicious attacks	Differentiate the specifics of countermeasures	Include uncertainty in the model	Use optimization	Provide decision-making tool for direct use by the firms	Use data obtained from real information security practice	Application of results and analyses to different industries
Baker (2009)		✓	✓				✓	
Richardson (2010)		✓	✓				✓	
Ponemon (2011)		✓	✓				✓	✓
Verizon (2014b)		✓	✓				✓	✓
Kwon and Johnson (2011)	✓	✓	✓			✓	✓	
Rowe and Gallaher (2006)	✓				✓	✓	✓	
Gordon and Loeb (2005)	✓	✓		✓	✓	✓		
Gordon and Loeb (2002)	✓	✓		✓	✓	✓		
Willemson (2006)	✓			✓		✓		
Hausken (2006)	✓			✓		✓		
Bojanc and Jerman-Blažič (2008)	✓			✓		✓		
Huang et al. (2008)	✓			✓		✓		
Cavusoglu et al. (2004)	✓	✓		✓				
Cavusoglu et al. (2008)	✓		✓	✓				
Gao et al. (2013)	✓			✓		✓		
Gao et al. (2015)	✓			✓		✓		
Hoo (2000)	✓	✓	✓	✓		✓		
Rees et al. (2011)	✓	✓	✓	✓	✓	✓		
Sawik (2013)	✓	✓	✓	✓	✓	✓		
Garvey and Patel (2014)	✓	✓	✓	✓		✓		
This study	✓	✓	✓	✓	✓	✓	✓	✓

effect in supply chains, Lee et al. (1997) propose the sharing of information between supply chain partners in order to improve efficiency and reduce costs. Assuming a coordinated structure across the supply chain, the value of information sharing within the supply chain is investigated by some follow-on studies such as Gavirneni et al. (1999), Lee et al. (2000), and Yu et al. (2001). Considering the competitive environment among the supply chain members, some studies further explore the incentives for information sharing. It is generally recognized that firms tend not to share information voluntarily, but rather seek for cooperation or trade for shared information from other firms (Chen, 2003, Li, 2002, Shang et al., 2015). The findings on the supply chain information sharing problem also shed light on the problem of security information sharing. In this study, we focus on the motivation, value and incentives of information sharing in the context of information security, while also noting that there exist clear differences between these two types of information sharing.

Information sharing in information security has been rarely discussed in detail in the literature. The study by Gordon and Loeb (2002) is among the earliest studies about information sharing in cybersecurity. The paper compares the sharing of information for information security purposes and for general commercial purposes, and points out the necessity of a central coordinator in the practice of security information sharing. While it is unanimously agreed in the literature that a central coordinator is needed for cybersecurity information sharing among the firms, Hausken (2007) and Gao et al. (2014) discuss the role of the central coordinator further by considering a situation where the central coordinator has control over information security investments and information sharing at the same time. They conclude that higher levels of intervention by the central coordinator does not always lead to better joint welfare. Therefore, in our study, we design the role of the central coordinator to be flexible with moderate level of power such that it intervenes only for information sharing purposes. Gordon et al. (2003) study the impact of information sharing on

information security investments using a game-theoretic model, and determine the conditions under which information sharing promotes or hinders information security investments. The authors in that study assume that there is a relationship between information sharing level and the effectiveness of information security investments. This key assumption lays the foundation for the modeling of information security investment and information sharing, and is adopted in several other studies including this study. Inspired by the rising trend of promoting information security information sharing, Gal-Or and Ghose (2005) and Gao and Zhong (2016) conduct studies on the incentives for sharing security information in a competitive environment. Using similar game-theoretical approaches, these papers analyze the information sharing and investment behaviors of a specific industry, namely the information technology industry, where product demand and revenue are directly affected by information security performance. Conclusions are drawn about the benefits of security information sharing to the firms, and it is noted that joint value is maximized with the firms sharing information in a coordinated manner. These findings, although valuable from public policy perspective, have their applications limited to the information technology industry. In our work, we develop a generic model that can be used by a wide spectrum of industries whose core business does not necessarily relate to the marketing of information technology products.

2.3 Related Research on Asymmetric Information Sharing and Information Pricing

While the topic of asymmetric information sharing in information system security has been rarely discussed in the literature, several studies involving applications in other fields exist. Sharpe (1990) studies the impact of asymmetric information in the bank loaning practice, where the banks are more willing to lend to return customers than new customers, as they have less information about the latter. The study

concludes that the inefficiency caused by information asymmetry can be eliminated by signing special contracts with all customers that contain protection terms against future problems. Brunnermeier (2001) does a thorough review on research articles regarding asset pricing under asymmetric information for assets such as real estate or stocks, and emphasize the information aspects of asset price dynamics. The author describes several models including market microstructure models, dynamic models, and herding models, and demonstrate how asymmetric information affects asset prices as well as how to find optimal trading strategies. Different from the above literature, the asymmetric information in our study is not used for generating extra revenue for the firm, but to help reduce overall information security costs. In our work we also treat the asymmetric information itself as a commodity, and the pricing strategy is applied to this special commodity while considering the asymmetry aspects in information .

The pricing of information has also been discussed in the economic literature under a buyer-seller context. Varian (1996) studies the selling of information containing products such as electronic journals. The author concludes that a firm can generate additional revenue by providing different information contents at different prices. While the concept of variation in information containing products is somewhat similar to the variation in information sharing levels in information system security, the information that is being priced by Varian (1996) is not assumed to create any measurable revenue for the buyer as in this study. Arora and Fosfuri (2005), on the other hand, study the pricing of information where the information would help the buyer make better investment decisions. A simple optimal pricing strategy is found as the charging of a fixed price to buyers with high expected returns while for buyers with low expected returns the price is defined as a portion of their future revenue. Unlike these studies, the participants in our context do not have fixed roles as buyers or sellers, but can switch their roles by changing their information sharing level. Therefore,

the optimal pricing strategy in our study is expected to be affected by many factors in addition to the return on investment levels.

CHAPTER 3

OPTIMAL POLICIES FOR TECHNOLOGY INVESTMENT IN INFORMATION SYSTEM SECURITY

In this chapter, we address two key decisions by a firm related to information security technology investments: *how much should the firm invest in information security technology?*, and *how should this investment be allocated over different categories of security technologies?* To this end, we derive a simple functional relationship between the potential total losses of a firm and the optimal amount that the firm should invest in information systems security. We further model the technology investments in information system security using a two-stage stochastic programming model, and conduct policy analysis using real data.

The remainder of this chapter is organized as the follows: In Section 3.1 we introduce a general framework for technology investments in information system security practice, and in Section 3.2, we present a stochastic programming model for the problem. Detailed policy analyses using real data are presented in Section 3.3. Finally, in Section 3.4 we summarize our results and present the conclusions.

3.1 General Framework for Investing in Information Systems Security

Effective protection of the confidentiality, integrity and availability of a firm's information systems, which is the main objective of information systems security, requires systematic investment and resource allocation decisions by the firm. In this

section, we present a generic framework defining such information security investment decisions, and how an optimization model can be built upon them.

3.1.1 Components of the Framework

We start the construction of our framework by identifying the key components that define the investment environment for information systems security. These include information assets that a firm holds, attacks that target these assets, and countermeasures that a firm can deploy to protect its assets against such attacks. We utilize a higher level categorization structure in defining the different components in our framework in order to allow for identification of general insights applicable to a broad range of situations. Otherwise, a lower level abstraction of the inputs would imply more of a custom and specific analysis for the organization studied, rather than generic findings for different industries.

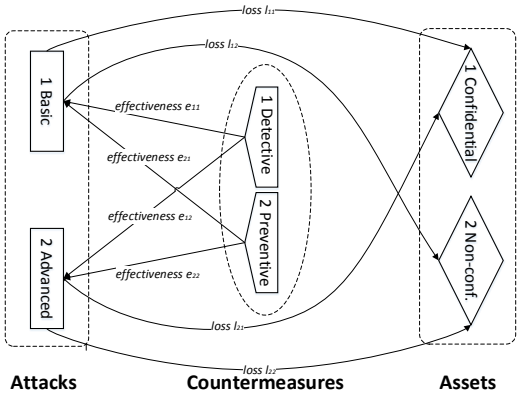
Assets. A firm's assets in our context refer to the collection of systems and information the firm possesses as part of business operations, with three defining characteristics for each asset: confidentiality, integrity, availability. Noting the distinction of confidentiality among the three aspects, Herson et al. (2003) suggest that a firm's information assets can be grouped broadly as being either confidential or non-confidential. Confidential assets correspond to data containing information that should not be disclosed to any third parties. This can include customer personal data, intellectual property, and other restricted files. On the other hand, non-confidential assets refer to any other assets that have monetary value and relate to information system availability and integrity, such as functional hardware. We adopt this categorization as part of our policy analyses in Section 3.3.

Attacks. Attacks correspond to all types of threats to a firm's information systems. A commonly adopted classification of attacks on information systems is a three-shell structure proposed by Richardson (2010), with the inner shell representing basic

attacks, the middle shell representing malware attacks and outer shell representing more sophisticated or advanced attacks. Basic attacks are typically simple and opportunistic attacks that are pervasively spread to the public to exploit vulnerabilities in information systems. Malware attacks, on the other hand, are an extended version of the basic attacks, which have some level of customization based on the industry targeted. Advanced attacks are usually the most sophisticated attacks and are generally customized for an individual organization. Richardson (2010) notes that most malware attacks would also fall into the category of advanced attacks, because malware attacks are likely to be customized as well, making the boundary between the two kinds of attacks somewhat vague. Hence, in our analysis we include malware attacks as part of the advanced attacks, and use two main categorizations for attacks on information systems, namely the basic and advanced attacks.

Countermeasures. Information security countermeasures are the set of measures protecting a firms information assets against attacks. They include both security technologies and 'soft' security measures such as establishing policies and training employees. Based on the protection mechanism used, Stoneburner et al. (2002) classify the types of countermeasures into two major categories: preventive and detective countermeasures. Preventive countermeasures include methods such as biometrics, encryption, and access control lists, and are aimed at preparing the firm against attacks before any breach can take place. On the other hand, detective countermeasures are aimed at identifying and removing an attack during or after the occurrence of a breach. Such measures include tools such as anti-virus software, content monitoring tools, and intrusion detection systems. Note that the soft measures mentioned above can be classified into either countermeasure category, depending on the nature of the measure. In this study, we enumerate some most common countermeasures based on findings from the literature and data obtained from our collaborating organizations.

Figure 3.1: Cross-relationships between the information assets of a firm, attacks targeting these assets, and countermeasures that can be deployed against the attacks.

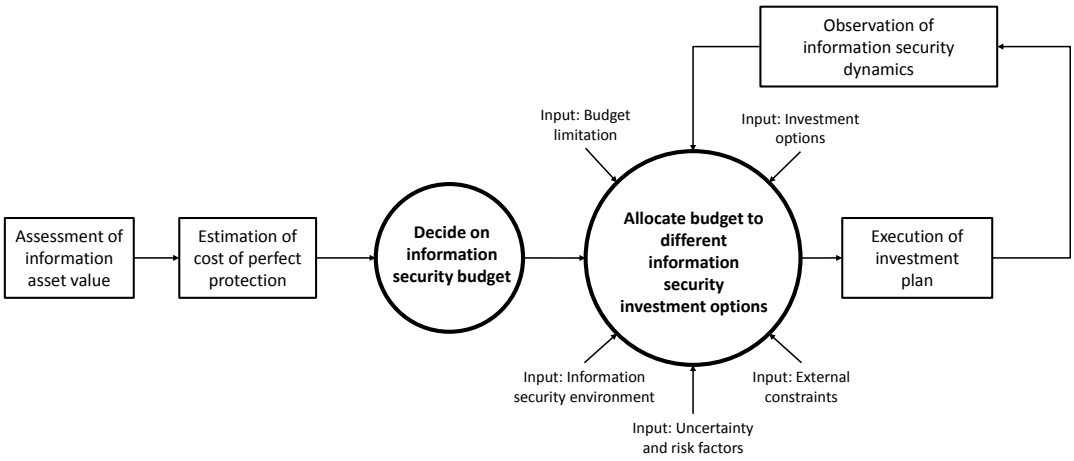


A list of these countermeasures and their classifications into the two categories are provided in Table 3.1 as part of the discussion in Section 3.3.1.

The three major components of information systems security is connected by multidimensional cross-relationships as illustrated in Figure 3.1. As shown, the two major categories of assets can be targeted by both basic and advanced attacks, while both preventive and detective countermeasures can be deployed against the two categories of attacks. Hence, a firm's information security investment strategy, i.e. how much to invest in each type of countermeasure, should depend on the distribution of the potential *losses* over the basic and advanced attacks, denoted by l_{as} where a and s respectively refer to the attack and asset type, as well as the *effectiveness* of each type of countermeasure on these attack categories, denoted by e_{oa} with o and a representing the countermeasure and attack type.

Clearly, the distributions of attack types and information assets would vary for different types of firms. We specifically consider ten representative industries covering a quite wide spectrum of organizations prone to attacks on their information systems, namely *finance, retail, hospitality, healthcare, transportation, manufacturing, professional services, public sector, information technology and energy industries*. These ten

Figure 3.2: Representation of the dynamic decision process for information security investments of a firm.



major industries are identified and described by a series of reports published by Verizon Communications (Verizon, 2012, 2014a). Under our general modeling framework and methodology, the conclusions and insights obtained by studying these ten industries can shed light on a great variety of firms based on the information environment and protection objectives they operate under.

3.1.2 The Investment Decision Process

Investment in information systems security is an iterative multi-step procedure involving the three components introduced above. In Figure 3.2 we provide a visual representation of the typical steps involved in this dynamic process, which we further describe below.

The process starts with the firm assessing the value of its assets, which corresponds to the maximum possible loss that the firm can incur due to a breach of its information systems. The next step is the estimation of the expected costs for perfect protection (ECOPP). This step involves an assessment of the costs of providing the highest level of protection for the firm's information systems without considering any

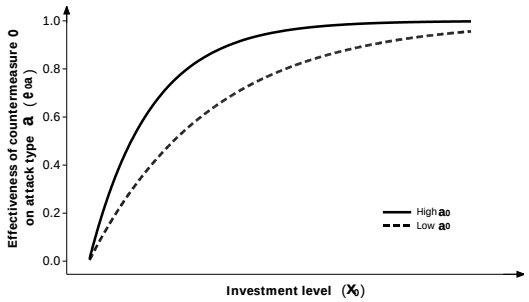
budget limitations. These two measures serve as inputs in addressing the first key operational decision presented in the third step: *how much should the firm invest in information systems security?*. Knowing this optimal investment level, the firm considers all relevant factors, and decides on the allocation of the budget over the set of countermeasures identified for potential investment. This step provides answers to the second key operational question: *how should the information security budget be allocated over different countermeasure categories?*. After the identification and implementation of an investment portfolio, the firm continuously observes the cybersecurity dynamics and learns about the effectiveness of the implemented countermeasures. The investment portfolio is then updated as necessary at specific intervals. Our analysis in this study captures these dynamics by modeling learning effects and portfolio adjustment options under a stochastic optimization framework, and aims to provide insights for the two key operational decisions highlighted above.

3.2 Stochastic Modeling of Information Security Investments

We assume that a firm maintains a set $\mathcal{S} = \{s_1, s_2\}$ of information assets, where s_1 corresponds to confidential assets, while s_2 refers to non-confidential assets as described in Section 3.1.1. The assets of the firm are subject to a set $\mathcal{A} = \{a_1, a_2\}$ of attacks with a_1 and a_2 referring to basic and advanced attacks, respectively. The expected loss l_{as} due to an attack $a \in \mathcal{A}$ on asset $s \in \mathcal{S}$ represents the value to be protected and is typically expressed in dollars. This value can be estimated by considering all possible expenditures that would result due to the consequences caused by an attack. Such expenses might consist of staff time, additional labor, compensation and other services provided to customers, as well as any reduction in the market share of the firm due to reputation related impacts.

In response to the potential attacks on its information systems, the firm deploys a set $\mathcal{O} = \{o_1, o_2\}$ of countermeasures, consisting of detective and preventive security

Figure 3.3: Illustration of the change in the effectiveness e_{oa} of a countermeasure category as a function of investment x_o in that category, and the impact of α_o.



measures denoted respectively as o_1 and o_2. Each countermeasure type $o \in \mathcal{O}$ has an estimated level of effectiveness $e_{oa}(x_o)$ on attack type $a \in \mathcal{A}$, which is a function of the amount x_o invested in countermeasure type o. The effectiveness function $e_{oa}(x_o)$ is defined separately for each attack and countermeasure pair, and refers to the percent reduction of losses on any information asset due to attack type a achieved by utilizing countermeasure type o. For example, $e_{o_1a_1}(x_{o_1}) = 0.8$ would imply that an 80% reduction in potential losses can be achieved against basic attacks by investing x_{o_1} dollars in detective countermeasures. It is worthwhile noting that the countermeasures are designed towards protection against different types of attacks, as opposed to being designed for specific information assets. Hence, the effectiveness of a countermeasure is defined separately for each type of attack, and is independent of the asset type the countermeasure might be protecting.

3.2.1 Functional Representation of Countermeasure Effectiveness and Information Asset Loss

An important issue relates to the definition of the effectiveness function $e_{oa}(x_o)$ for each information security countermeasure and attack type. First, we note that while a theoretical upper bound for $e_{oa}(x_o)$ would be 1, such an effectiveness level is practically not achievable. Hence, we let $\beta_{oa} < 1$ denote the maximum attainable

effectiveness by countermeasure type $o \in \mathcal{O}$ against attack type $a \in \mathcal{A}$. Given this, the effectiveness function $e_{oa}(x_o)$ must satisfy the following conditions, as also noted by Gordon and Loeb (2002): $e_{oa}(0) = 0$; $e_{oa}(x_o) \to \beta_{oa}$ as $x_o \to \infty$; $\frac{\partial e_{oa}(x_o)}{\partial x_o} > 0$; and $\frac{\partial^2 e_{oa}(x_o)}{\partial x_o^2} < 0$ for all $o \in \mathcal{O}$ and $a \in \mathcal{A}$. These properties imply that the function $e_{oa}(x_o)$ has to be concave and monotonically increasing on $x_o \in [0, \infty)$, while asymptotically achieving the highest effectiveness level β_{oa}. Based on these conclusions, we define the following function to model the effectiveness rate of a countermeasure category against a given type of attack on information systems:

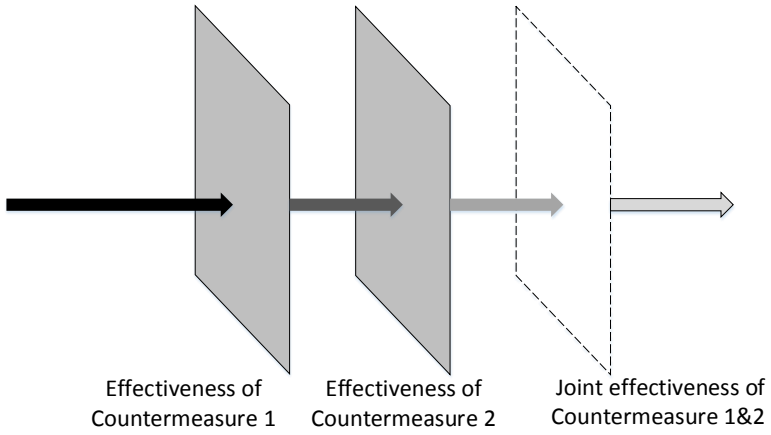
$$e_{oa}(x_o) = \beta_{oa} - e^{-(\alpha_o x_o - \ln \beta_{oa})} = \beta_{oa} - \beta_{oa} e^{-\alpha_o x_o} \qquad \forall o \in \mathcal{O}, a \in \mathcal{A} \tag{3.1}$$

where α_o is the marginal rate that the effectiveness curve reaches the maximum level β_{oa} as a function of the investment x_o. In other words, for the same maximum achievable effectiveness level β_{oa}, high values of α_o would imply that the higher effectiveness levels can be achieved through less investment than a case with lower α_o values. This is demonstrated visually through an example in Figure 3.3.

While the effectiveness function for a countermeasure category o on attack type a corresponds to a relative measure defining the percent decrease in potential losses due to the utilization of such countermeasures, the return from an investment in a countermeasure needs to be defined in absolute terms in dollars. Given the expected maximum possible loss l_{as} due to attack type a on information asset s, we define the realized losses after countermeasure implementation as $f_a l_{as}(1 - e_{oa}(x_o))$, where f_a represents the frequency of attack type a based on the estimated number of such attacks during the planning period. The loss reduction here is a result of reduced number of successful attacks, and this leads to a multiplicative form for the total overall losses, expressed as $\sum_s \sum_a f_a l_{as}(\prod_o (1 - e_{oa}(x_o)))$. We can visualize this structure by conceiving the information security countermeasures as layers of fences, through which the attack infiltrates but gets weakened in terms of expected impact layer after

layer. Assuming that the countermeasures will be functioning separately, the attack confronted by the next layer is always what is left after the screening by the previous layer. Thus, the contribution of the next layer to the overall effectiveness can be defined through multiplication of its effectiveness by what is left. We provide a visual illustration of this representation in Figure 3.4.

Figure 3.4: Layer based structural illustration of the effectiveness provided by multiple types of countermeasures



Building upon this protection process, we further consider joint effectiveness of information security countermeasures as a separate layer in the system, as joint effectiveness of two countermeasures against an attack is not necessarily the product of their individual effectiveness rates. One can view the joint effectiveness of two countermeasures as a virtual layer added to the individual countermeasure effectiveness layers. To capture this structure, we define the interdependency coefficient $\rho_{oo'}$ for two countermeasure categories $o, o' \in \mathcal{O}$, and use it to represent the loss under joint effectiveness between the two countermeasures as $f_a l_{as} \sqrt{1 - e_{oo'a}(x_o, x_{o'})}$, where $e_{oo'a}(x_o, x_{o'}) \in [0, 1]$ and is defined as:

$$e_{oo'a}(x_o, x_{o'}) = \rho_{oo'} e_{oa}(x_o) + \rho_{oo'} e_{o'a}(x_{o'}) - \rho^2_{oo'} e_{oa}(x_o) e_{o'a}(x_{o'}) \qquad \forall_{o,o' \in \mathcal{O}, a \in \mathcal{A}} \quad (3.2)$$

We note through Lemma 3.1 and Proposition 3.1 below that this representation is generic, and can be used to represent any type of joint effectiveness relationship between two countermeasure types.

Lemma 3.1 *Given investment levels x_o and $x_{o'}$ on two information security countermeasures o and o', the joint effectiveness function* (3.2) *is nondecreasing in $\rho_{oo'}$, $e_{oa}(x_o)$ and $e_{o'a}(x_{o'})$ for all $\rho_{oo'} \in [0, \min\{\frac{1}{\beta_{oa}}, \frac{1}{\beta_{o'a}}\}]$.*

Proof All proofs are included in Appendix A. □

Proposition 3.1 *Given a pair of information security countermeasures with individual effectiveness functions $e_{oa}(x_o)$ and $e_{o'a}(x_{o'})$, there always exists $\rho_{oo'} \in [0, \min\{\frac{1}{\beta_{oa}}, \frac{1}{\beta_{o'a}}\}]$ such that the joint effectiveness function $e_{oo'a}(x_o, x_{o'})$ can be defined for all values of x_o and $x_{o'}$.*

In practice, the parameter $\rho_{oo'}$ can be estimated based on expert opinions, usually developed through observations of historical performances of the countermeasures. When two countermeasure types o and o' have no correlation, $\rho_{oo'}$ is assumed to be 0. In the case where there exist joint effects, $\rho_{oo'}$ takes a positive value. Note that the relationship between any two countermeasures is assumed to be either neutral or synergistic, i.e. one never impeding another. Thus, $\rho_{oo'}$ takes a value in the interval $[0, \min\{\frac{1}{\beta_{oa}}, \frac{1}{\beta_{o'a}}\}]$. In our analyses in Section 3.3, we utilize a specific value estimated for $\rho_{oo'}$ based on available data, but also consider sensitivity analysis around this value to develop additional insights.

The structure above also allows the joint effectiveness function to be expressed through a nice implicit multiplicative form as follows:

$$1 - e_{oo'a}(x_o, x_{o'}) = (1 - \rho_{oo'} e_{oa}(x_o))(1 - \rho_{oo'} e_{o'a}(x_{o'})) \qquad \forall_{o,o' \in \mathcal{O}, a \in \mathcal{A}} \tag{3.3}$$

which in turn enables a compact expression of the overall loss function for the information assets of the firm. Note that defining $\rho_{oo} = 1$, the term $\sqrt{1 - e_{oo'a}(x_o, x_{o'})}$

reduces to $1 - e_{oa}(x_o)$ when $o = o'$. Hence, in order to express the total losses after information security investments by taking into account the joint effectiveness functions, we modify the total loss expression $\sum_s \sum_a f_a l_{as}(\prod_o (1 - e_{oa}(x_o)))$ as:

$$L(\mathbf{x}) = \sum_{s \in \mathcal{S}} \sum_{a \in \mathcal{A}} f_a l_{as} \left(\prod_{o,o' \in \mathcal{O}} \sqrt{1 - e_{oo'a}(x_o, x_{o'})} \right) \tag{3.4}$$

where $\mathbf{x}$ represents the vector defining the investments in different countermeasure categories.

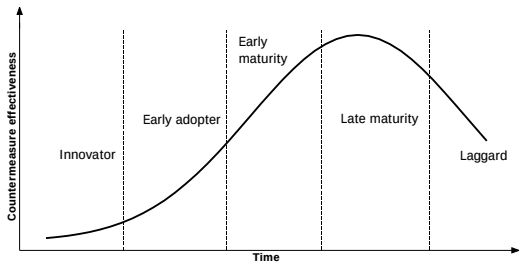
3.2.2 Modeling the Dynamics of Information Security Countermeasure Effectiveness

Information systems have an ever-changing nature, inevitably bringing in uncertainty to the process of investing in information security. The most significant uncertainty involves the effectiveness of countermeasures both due to the dynamic nature of attacks and also due to the probabilistic evolution of success in defending a firm's information assets against these attacks.

Given that attack patterns might evolve over time, we introduce a time dimension into the attack frequency as $f_a(t)$ which allows for non-homogeneity in attack frequencies over time. In response, countermeasures are also designed to be updated frequently in order to adapt to the evolution of the attacks, resulting in a life cycle based variation in a countermeasure's maximum attainable effectiveness β_{oa} over time. Hence, we also update the definition of this parameter so that it might vary as a function of time t, specifically as $\beta_{oa}(t)$. However, the exact nature of this countermeasure effectiveness life cycle curve is not known to a firm, which can only be estimated probabilistically for use as part of the information security investment planning process, as we later describe in Section 3.2.3.

The widely applied notion of product life cycle curve is first introduced by Rogers (2010) to describe the diffusion of product innovation, where a life cycle curve is par-

Figure 3.5: Five phases of the information security product life cycle curve defined similarly to Rogers (2010).

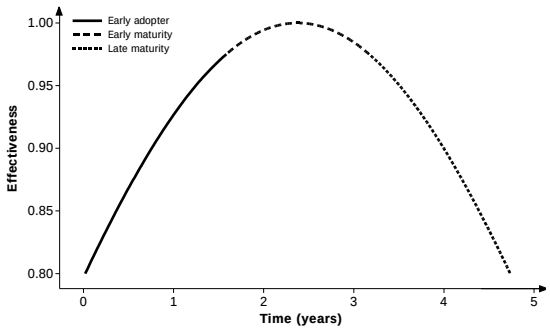


titioned into five phases as shown in Figure 3.5. Technologies for information systems security also have effectiveness levels that vary depending on where the product is in its life cycle. Noting that security products are mostly well tested after development and become obsolete relatively fast after the late maturity phase, we follow Lipner (2004) and consider a three phase life cycle for the effectiveness of information security countermeasures. These phases correspond to early adopters, early maturity, and late maturity phases as illustrated in Figure 3.6a. In the early adopter phase, the countermeasure is first introduced to the market, while at the early maturity phase the product gets gradually accepted and improved through market experience. Lastly, at the late maturity phase, the countermeasure is challenged and eventually replaced by competing products, resulting in its obsolescence.

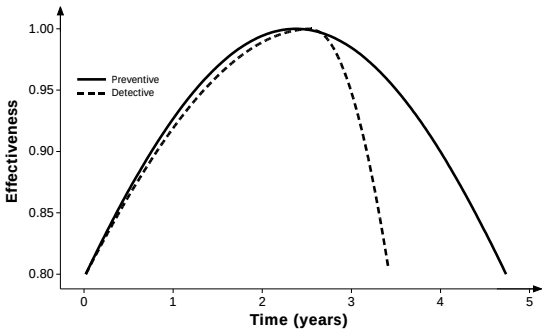
The specific shape of the effectiveness life cycle curve is different for preventive and detective technologies. Oberheide et al. (2008) suggest that detective countermeasures tend to have a sharp drop in their effectiveness towards the end of the product's life cycle. This is because such products are dependent on continuous updates by vendors, e.g. anti-virus and anti-spyware applications relying on signature information about the latest virus database, so that the infiltrated attacks can be detected in a timely manner. Thus, the effectiveness of these countermeasures drop at a higher rate once such updates stop. Preventive countermeasures, on the other hand, are more robust

Figure 3.6: Life cycle curves for information security products based on effectiveness against attacks.

(a) Three stages of a countermeasure life-cycle curve.



(b) Effectiveness life-cycle curves for the two major categories of information security countermeasures.



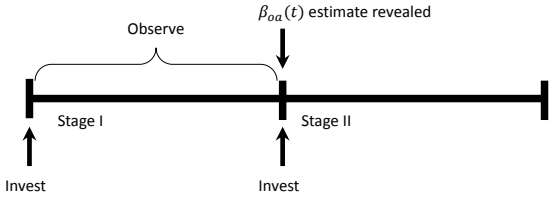
in the late maturity phase as their effectiveness relies primarily on the product design itself, as opposed to being dependent on continuous updates, such as in the cases of encryption algorithms and access control techniques. A firm typically contracts with the same information security countermeasure provider for a general category of products due to cost and standardization purposes. Therefore, it is expected that a specific category of countermeasures provided by a supplier would follow a specific life cycle curve. Considering these characteristics, as well as product life cycle information available at McAfee (2013) and Symantec (2014), it is possible to plot general representative maximum effectiveness life cycle curves for preventive and detective countermeasures separately. These curves depicting $\beta_{oa}(t)$ for the two cases are shown in Figure 3.6b. We provide more details on these effectiveness curves in Section 3.3.1.

3.2.3 Modeling the Uncertainty in Information Security Countermeasure Effectiveness

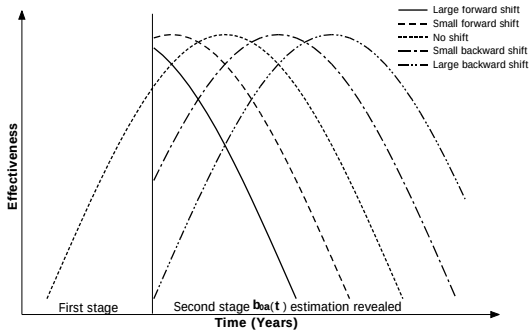
While the maximum attainable effectiveness of a countermeasure will generally follow a life cycle curve, exact information on the shape of this curve or where a

Figure 3.7: Uncertainty and learning in information security investments.

(a) The two-stage decision process representing the uncertainty and learning in information security investments.



(b) Demonstration of different realizations of $\beta_{oa}(t)$ in the second period, after initial investment and learning in the first period.



specific product is placed on that curve at the time of acquisition and implementation is not known due to the uncertainties associated with technological performance. As a product is put to use and its performance over time is observed, the firm will gain knowledge about this information, specifically as to where the product might be on its life cycle curve. This new information can be used to readjust budget allocations over different countermeasure types. Hence, when selecting countermeasures for investment, the firm needs to account for such uncertainty and the corresponding learning process that will take place.

The above effects can be captured through a two-stage process, where the firm makes an initial investment over a set of countermeasure categories, and then can readjust these investments based on endogenous information about the performance of the measures invested in. This process is depicted in Figure 3.7a, where an estimate for the parameter $\beta_{oa}(t)$ for each countermeasure category o and attack type a is assumed to be revealed in the second stage for future periods, and the revised decisions are based on these revelations. We further describe this process through the case shown in Figure 3.7b. As depicted in the figure, the decision maker assumes that the countermeasure effectiveness curve follows the segments of an 'expected' effectiveness

function in the first stage. The five possible realizations at the second stage can be either a large forward shift, a small forward shift, a no shift case, a small backward shift, or a large backward shift. The backward and forward shifts correspond to life cycle curves that respectively indicate less and more maturity at the start of the implementations, implying that the firm's initial assumptions on the structure of the life cycle curve were not accurate.

In this two-stage stochastic setup, each combination of life cycle curve realizations for the countermeasure-attack pairs correspond to a scenario, as two countermeasure types are not necessarily equally sensitive to different attacks. In other words, the effectiveness curves and their realizations are considered not for each countermeasure, but for each countermeasure-attack pair separately.

3.2.4 Two-stage Stochastic Programming Model with Endogenous Uncertainty

The decision framework described above can be modeled through a stochastic programming approach involving endogenous uncertainty, where the latter is due to the dependence between the investment decisions made and the realization of learning effects on the performance of different information security countermeasures. We assume that a certain level of investment is necessary for information gathering on the performance of the acquired countermeasures.

First, in order to describe the dynamics involving changes of the parameters $\beta_{oa}(t)$ over time, we discretize the planning horizon and represent such dynamics by using discrete time intervals. We let $t = 1, 2, \ldots, T$ refer to each of these intervals, and append the definition of the maximum effectiveness level and the attack frequency through the addition of a time subscript as β_{oat} and f_{at}, respectively. Based on a typical budget planning process that takes place every year with an initial assessment of the investments at the end of the first quarter, it can be assumed that the second

stage decisions would take place after this initial assessment. For a generalized formulation, we assume that the second stage decisions occur at the end of time period T', which implies that periods $1, 2, \ldots, T'$ correspond to first stage periods, while the second stage periods are $T'+1, T'+2, \ldots, T$. We refer to the set of time periods in each stage as $\mathcal{T}^1$ and $\mathcal{T}^2$, respectively.

It was described in Section 3.2.3 that the uncertainty structure in the model involves a set of scenarios, each of which corresponds to a possible combination of life cycle curve realizations β_{oat} for $t \in \mathcal{T}^2$ for different countermeasure-attack category pairs. We denote a given scenario by $\omega \in \Omega$, where Ω is the set of all scenarios, and append the notation for the uncertain parameter β_{oat} with a scenario index to read as $\beta_{oat\omega}$. Similarly, all second stage variables in the problem need to be defined through a scenario index, as they correspond to decisions that will be implemented after the realization of the scenario outcome. These decision variables are further described later in this section.

As noted above, our framework aims to capture the learning effects on the effectiveness of the countermeasures that are implemented after the initial investment period, which are dependent on the amount of investment made into a countermeasure category. In other words, enough sampling needs to occur to reach a conclusion as to where a certain category of countermeasures is on the corresponding life cycle, and this can only be achieved by making sufficient investment in that category. We refer to this sufficient level of investment for a countermeasure category o as θ_o. If the initial investment in a countermeasure category is less than the threshold θ_o, then no information will be gained and the later period investments will be made based on the life cycle structure initially assumed, although in reality the effectiveness of the countermeasure category may be different than these assumed levels. Given that the realization of new information is dependent on the investment decisions made, this implies a setting with endogenous uncertainty (Solak et al., 2010). To model

this structure in our formulation, we define the binary variable σ_o for each $o \in \mathcal{O}$, where it takes on a value of 1 if $x_o^1 \geq \theta_o$, and 0 otherwise, where x_o^1 corresponds to the initial period investment in countermeasure category o. Note that we define the investment decisions separately for the first and second stages as x_o^1 and $x_o^{2\omega}$ respectively, where the latter variable is defined for each scenario as these decisions are made after scenario realizations.

Moreover, the process of investing in information systems security takes place under certain constraints. A key limitation deals with the budget constraint such that the total investment over the planning period can not be larger than a total available budget B. Moreover, the actual investment plan can always be influenced by external factors, such as minimum protection requirements imposed by laws or regulations. To that end, we define the parameters $\underline{x}_o$ and $\underline{e}_{oa}$ to represent lower bounds on the investments and effectiveness rates for each countermeasure $o \in \mathcal{O}$ against attack $a \in \mathcal{A}$.

Given these definitions, a stochastic programming formulation for the information security investment problem can be expressed as follows, where x_o^1 is also defined over all scenarios as $x_o^{1\omega}$ for a more compact representation of the formulation. Each $x_o^{1\omega}$ is then set equal to each other through nonanticipativity constraints used in stochastic programming. We also define the set $\mathcal{K} = \{1, 2\}$ to contain the stage indices in the following formulation:

$$\min_{\mathbf{x},\mathbf{e},\mathbf{b}\in R^{+},\sigma\in\{0,1\}} \sum_{\omega\in\Omega} p^{\omega}\left[\sum_{k\in\mathcal{K}}\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}}\sum_{t\in\mathcal{T}} f_{at} l_{ast}\left(\prod_{o,o'\in\mathcal{O}}\sqrt{1-e^{k\omega}_{oo'at}(x^{k\omega}_{o},x^{k\omega}_{o'})}\right)+\sum_{k\in\mathcal{K}}\sum_{o\in\mathcal{O}} x^{k\omega}_{o}\right] \tag{3.5}$$

$$\text{s.t.} \quad e^{k\omega}_{oo'at}(x^{k\omega}_{o},x^{k\omega}_{o'}) = \rho_{oo'}e^{k\omega}_{oat}(x^{k\omega}_{o})+\rho_{oo'}e^{k\omega}_{o'at}(x^{k\omega}_{o'})-\rho^{2}_{oo'}e^{k\omega}_{oat}(x^{k\omega}_{o})e^{k\omega}_{o'at}(x^{k\omega}_{o'}) \quad \forall o,o'\in\mathcal{O},a\in\mathcal{A},t\in\mathcal{T},k\in\mathcal{K},\omega\in\Omega \tag{3.6}$$

$$e^{1\omega}_{oat}(x^{1\omega}_{o}) = \beta_{oat}-\beta_{oat}e^{-\alpha^{1}_{o}x^{1\omega}_{o}} \quad \forall o\in\mathcal{O},a\in\mathcal{A},t\in\mathcal{T}^{1},\omega\in\Omega \tag{3.7}$$

$$e^{\omega}_{oat}(x^{2\omega}_{o}) = b^{\omega}_{oat}-b^{\omega}_{oat}e^{-\alpha^{2}_{o}x^{2\omega}_{o}} \quad \forall o\in\mathcal{O},a\in\mathcal{A},t\in\mathcal{T}^{2},\omega\in\Omega \tag{3.8}$$

$$b^{\omega}_{oat} = \beta_{oat}(1-\sigma_{o})+\beta_{oat\omega}\sigma_{o} \quad \forall o\in\mathcal{O},a\in\mathcal{A},t\in\mathcal{T}^{2},\omega\in\Omega \tag{3.9}$$

$$e^{k\omega}_{oat}(x^{k\omega}_{o}) \geqslant \underline{e}^{k}_{oa} \quad ; \quad x^{k\omega}_{o} \geqslant \underline{x}^{k}_{o} \quad \forall o\in\mathcal{O},a\in\mathcal{A},t\in\mathcal{T},k\in\mathcal{K},\omega\in\Omega \tag{3.10}$$

$$x^{1\omega}_{o} \leq \theta_{o}+\mathbf{M}\sigma_{o} \quad ; \quad x^{1\omega}_{o} \geq \theta_{o}+\mathbf{M}(\sigma_{o}-1) \quad \forall o\in\mathcal{O},\omega\in\Omega \tag{3.11}$$

$$\sum_{k\in\mathcal{K}}\sum_{o\in\mathcal{O}} x^{k\omega}_{o} \leq B \quad \forall\omega\in\Omega \tag{3.12}$$

$$x^{1\omega}_{o} = x^{1\omega'}_{o} \quad \forall\omega,\omega'\in\Omega,o\in\mathcal{O} \tag{3.13}$$

In this model, the objective function (3.5) involves the minimization of the sum of the investment costs and expected losses of the firm over the planning horizon. This represents the expected total expenditure or total cost under information security investment. The risk attitude of the decision maker is assumed to be risk neutral in this representation, whereas we describe the inclusion of risk in the framework in Section 3.2.6. Constraints (3.6) through (3.8) define the effectiveness of countermeasures in both joint and individual forms. Note that the maximum achievable effectiveness level β_{oat} in (3.8) is replaced by its second stage counterpart b^{ω}_{oat}, which is a variable defined by equation (3.9). This relationship stipulates b^{ω}_{oat} to be realized as the scenario-dependent value $\beta_{oat\omega}$ only if $\sigma_{o} = 1$, i.e. if investment in a countermeasure category is greater than the corresponding threshold. Otherwise, no information is revealed so that β_{oat} will still be used in the second stage. Constraints (3.10) reflect the minimum protection requirements imposed by external factors in terms of countermeasure effectiveness and investment levels in both the first and sec-

ond stages. Constraints (3.11), where $\mathbf{M}$ denotes a tight bound as in typical big-M formulations, define the binary variable σ_o. Constraints (3.12) state the investment budget limitation over the entire planning horizon, while constraints (3.13) are the nonanticipativity constraints that ensure that first stage decisions are the same for all scenarios.

In the form presented above, our model is a mixed integer nonlinear program with a non-convex feasible set and objective function, as can be inferred from the presence of square root functions and products of variables. However, we derive a tractable convex reformulation of the problem as described in the next subsection.

3.2.5 Linearization of the Nonlinear Stochastic Programming Formulation

In the above formulation, objective function (3.5) and the constraints (3.6)-(3.8) involve nonlinearities, which we linearize through a set of systematic procedures. We first express the objective function (3.5) through an equivalent representation as follows:

$$\min_{\mathbf{x},\mathbf{e},\mathbf{b}\in R^{+},\sigma\in\{0,1\}} \sum_{\omega\in\Omega} p^{\omega} \left[\sum_{k\in\mathcal{K}} \sum_{s\in\mathcal{S}} \sum_{a\in\mathcal{A}} \sum_{t\in\mathcal{T}} f_{at} l_{ast} e^{\frac{1}{2}\sum_{o,o'\in\mathcal{O}} \ln\left(1-e^{k\omega}_{oo'at}(x^{k\omega}_{o},x^{k\omega}_{o'})\right)} + \sum_{k\in\mathcal{K}} \sum_{o\in\mathcal{O}} x^{k\omega}_{o} \right] \tag{3.14}$$

which follows from

$$\prod_{o,o'\in\mathcal{O}} \sqrt{1-e^{k\omega}_{oo'at}(x^{k\omega}_{o},x^{k\omega}_{o'})} = e^{\ln\prod_{o,o'\in\mathcal{O}}\sqrt{1-e^{k\omega}_{oo'at}(x^{k\omega}_{o},x^{k\omega}_{o'})}} = e^{\frac{1}{2}\sum_{o,o'\in\mathcal{O}}\ln\left(1-e^{k\omega}_{oo'at}(x^{k\omega}_{o},x^{k\omega}_{o'})\right)}$$

Given the relationship defined by (3.3), we can replace the term $\ln\left(1-e^{k\omega}_{oo'at}(x^{k\omega}_{o},x^{k\omega}_{o'})\right)$ with a variable $E^{k\omega}_{oo'at}(x^{k\omega}_{o},x^{k\omega}_{o'})$, and replace constraint (3.6) with the following constraint:

$$E^{k\omega}_{oo'at}(x^{k\omega}_o, x^{k\omega}_{o'}) = I^{k\omega}_{oo'at}(x^{k\omega}_o) + I^{k\omega}_{o'oat}(x^{k\omega}_{o'}) \qquad \forall o,o' \in \mathcal{O}, a \in \mathcal{A}, t \in \mathcal{T}, k \in \mathcal{K}, \omega \in \Omega \tag{3.15}$$

where the new variables $I^{k\omega}_{oo'at}(x^{k\omega}_o)$ are defined such that $I^{k\omega}_{oo'at}(x^{k\omega}_o) = \ln(1-\rho_{oo'}e^{k\omega}_{oat}(x^{k\omega}_o))$. We note through the following proposition that $I^{k\omega}_{oo'at}$ is convex in the investment variable $x^{k\omega}_o$, and thus it is possible to utilize a piecewise approximation for $I^{k\omega}_{oo'at}(x^{k\omega}_o)$ through a set of linear constraints:

Proposition 3.2 *The function* $I^{k\omega}_{oo'at}(x^{k\omega}_o) = \ln(1 - \rho_{oo'}e^{k\omega}_{oat}(x^{k\omega}_o))$ *is convex in* $x^{k\omega}_o$.

Based on this result, and the fact that the optimization problem has a minimization objective, $I^{k\omega}_{oo'at}(x^{k\omega}_o)$ can be approximated in a piecewise linear fashion by a series of M constraints. Specifically for $k = 1$, we have:

$$I^{1\omega}_{oo'at,m}(x^{1\omega}_o) \geq u^{1\omega}_{oo'at,m}x^{1\omega}_o + v^{1\omega}_{oo'at,m} \qquad \forall o,o' \in \mathcal{O}, a \in \mathcal{A}, t \in \mathcal{T}^1, \omega \in \Omega, m = 1,\ldots,M \tag{3.16}$$

where the parameters $u^{k\omega}_{oo'at,m}$ and $v^{k\omega}_{oo'at,m}$ respectively represent the slopes and intercepts for the piecewise linear constraints. Note that this piecewise representation of $I^{k\omega}_{oo'at}(x^{k\omega}_o)$ implies the removal of constraints (3.7)-(3.9) from the formulation. However, a challenge is brought by constraints (3.8) and (3.9), as b^{ω}_{oat} is dependent on the binary variable σ_o. Therefore, the piecewise approximation of constraint (3.8) needs to be achieved by the design of two sets of switching constraints using σ_o itself for $k = 2$:

$$I^{2\omega}_{oo'at,m}(x^{2\omega}_o) \geq u^{2\omega}_{oo'at,m}x^{2\omega}_o + v^{2\omega}_{oo'at,m} - \mathbf{M}\sigma_o \quad \forall o,o' \in \mathcal{O}, a \in \mathcal{A}, t \in \mathcal{T}^2, \omega \in \Omega, m = 1,\ldots,M \tag{3.17}$$

$$I^{2\omega}_{oo'at,m}(x^{2\omega}_o) \geq u^{2\omega}_{oo'at,m}x^{2\omega}_o + v^{2\omega}_{oo'at,m} - \mathbf{M}(1 - \sigma_o) \quad \forall o,o' \in \mathcal{O}, a \in \mathcal{A}, t \in \mathcal{T}^2, \omega \in \Omega, m = 1,\ldots,M \tag{3.18}$$

As a final step, we transform the remaining nonlinear term of $e^{\frac{1}{2}\sum_{o,o'\in\mathcal{O}} E^{k\omega}_{oo'at}(x^{k\omega}_o, x^{k\omega}_{o'})}$ in the objective function through another piecewise linear approximation. To this end, we set $D^{k\omega}_{at} = \frac{1}{2}\sum_{o,o'\in\mathcal{O}} E^{k\omega}_{oo'at}(x^{k\omega}_o, x^{k\omega}_{o'})$, which implies the adding of the following constraints to the formulation:

$$D^{k\omega}_{at} = \frac{1}{2}\sum_{o,o'\in\mathcal{O}} E^{k\omega}_{oo'at}(x^{k\omega}_o, x^{k\omega}_{o'}) \qquad \forall a\in\mathcal{A}, t\in\mathcal{T}, k\in\mathcal{K}, \omega\in\Omega \tag{3.19}$$

$$Y^{k\omega}_{at} \geq h^{k\omega}_{at,m} D^{k\omega}_{at} + g^{k\omega}_{at,m} \qquad \forall a\in\mathcal{A}, t\in\mathcal{T}, k\in\mathcal{K}, \omega\in\Omega, m=1,\ldots,M \tag{3.20}$$

where $Y^{k\omega}_{at}(x^{k\omega}_o)$ approximates the term $e^{\frac{1}{2}\sum_{o,o'\in\mathcal{O}} E^{k\omega}_{oo'at}(x^{k\omega}_o, x^{k\omega}_{o'})}$.

Overall, the linearized formulation for the information security investment optimization problem can be expressed as:

$$\min_{\mathbf{x},\mathbf{E},\mathbf{I},\mathbf{D},\mathbf{Y}\in R^+,\sigma\in\{0,1\}} \sum_{\omega\in\Omega} p^\omega \left[\sum_{k\in\mathcal{K}}\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}}\sum_{t\in\mathcal{T}} f_{at} l_{ast} Y^{k\omega}_{at} + \sum_{k\in\mathcal{K}}\sum_{o\in\mathcal{O}} x^{k\omega}_o\right] \tag{3.21}$$

$$\text{s.t.} \quad (3.10)-(3.13), (3.15)-(3.20)$$

3.2.6 Inclusion of Risk in the Decision Framework

Risk, defined by the variation of returns over different realizations of uncertainty, is indispensable in any type of investment problem, supplementary to the expected return values. While investments in information systems security do not generate additional direct revenue to the firm as in a standard investment problem, risk concerns are very important for such investments due to the possibility of huge losses for a firm. We capture the risk attitude of a decision maker in our framework through minimization of the conditional value at risk (CVaR) measure, which represents the expected loss that will be incurred if the realized losses lie in the top $1-\xi$ percentile of the total loss distribution. Rockafellar and Uryasev (2000) discuss the minimization of conditional value at risk in portfolio optimization and describe a formulation structure, which has also been adopted in some other studies (e.g. Noyan (2012)).

Extending this methodology, we express a linearized formulation for the information security investment optimization problem with conditional value at risk as follows:

$$\min_{\mathbf{v},\eta,\mathbf{x},\mathbf{E},\mathbf{I},\mathbf{D},\mathbf{Y}\in R^{+},\sigma\in\{0,1\}} \quad (1+\lambda)\left[\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}}\sum_{t\in\mathcal{T}^1} f_{at}l_{ast}Y_{at}^{1}+\sum_{o\in\mathcal{O}}x_o^1\right] + \sum_{\omega\in\Omega}p^{\omega}\left[\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}}\sum_{t\in\mathcal{T}^2} f_{at}l_{ast}^{\omega}Y_{at}^{2\omega}+\sum_{o\in\mathcal{O}}x_o^{2\omega}\right] + \lambda(\eta+\frac{1}{1-\xi}\sum_{\omega\in\Omega}p^{\omega}v^{\omega}) \tag{3.22}$$

$$\text{s.t.} \quad v^{\omega}\geq\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}}\sum_{t\in\mathcal{T}^2} f_{at}l_{ast}^{\omega}Y_{at}^{2\omega}+\sum_{o\in\mathcal{O}}x_o^{2\omega}-\eta \qquad \forall\omega\in\Omega \tag{3.23}$$

$$(3.10)-(3.13),(3.15)-(3.20)$$

The optimization model under risk minimizes a weighted sum of the expected total costs and conditional value at risk under the uncertainty of countermeasure effectiveness. In the formulation above, λ denotes the weight parameter, while η is the variable defining the threshold to be used for calculation of the conditional value at risk. In other words, η corresponds to the $\xi-$quantile of the distribution of costs. The scenario-specific variable v^{ω} in constraint (3.23) defines the difference between realized total losses for the firm and the threshold loss level η when the former exceeds the latter. Hence, higher v^{ω} values imply the occurrence of higher losses, which a firm - based on risk attitude - may prefer to avoid in the expense of increased expected losses. To this end, weight parameter λ in the objective function (3.22) is a risk attitude indicator for the firm. A larger λ value implies a more risk-averse attitude, while a smaller λ would imply a more risk seeking approach. As part of our policy analyses, we consider different risk attitudes and discuss how optimal investment insights vary under such cases.

3.3 Policy Analysis based on Practical Data

In this section we implement our information security investment models according to generic data obtained from partner organizations. Additional information gathered from the literature is also used to identify general policy results for potential adoption by firms in different industries.

3.3.1 Description of Data

We perform an online survey to information security practitioners in member firms of the Advanced Cyber Security Center of the New England area in the United States. The survey is aimed towards identifying key input parameters of our information security investment model, including maximum attainable effectiveness levels of the security controls, attack frequencies, potential total loss of breaches and expected cost of perfect protection on the assets.

The survey contains 19 questions which clearly articulate the purpose of the survey. To ensure the respondents provide truthful feedback without concerning leakage of private information, the survey is send out completely anonymously. Response are collected from 8 information security management/executive practitioners and 6 information security technician/engineers. 3.1.

The types of assets, attacks, and countermeasures under each category were listed as shown in Table 3.1. A complete presentation of the input structure used in the analyses is shown in Table 4.1, with a brief description of the sources from which the data is derived. No specific bounds representing the effect of regulations were used in the implementations, as currently there are no such enforced general requirements on firms.

The interdependency of specific countermeasure options can be evaluated based on expert opinions and experience in practice, by comparing performances of protection under controlled conditions. In our model, since the countermeasures are presented

Table 3.1: Typical categorization of attacks, assets and countermeasures for information security investments

Attacks	Countermeasures
Basic attacks:	*Detective countermeasures:*
Keyloggers and spyware	Anti-virus software
Backdoor or command control	Anti-spyware software
Unauthorized access via weak access control lists	Content monitoring
Unauthorized access via stolen credentials	Forensic tools
Physical theft of assets	Intrusion detection system software
Brutal force attack	Log management software
Advanced attacks:	
Abuse of system access/privileges	*Preventive countermeasures:*
Violation of acceptable use and other policies	Biometrics
Phishing	Data loss prevention
Packet sniffer	Encryption
Pretexting	Firewall
Assets	Intrusion prevention system
Non-confidential assets:	Public key infrastructure
Point of sale server	Server-based access control list
Network devices	Static account logins/passwords
Database server	Specialized wireless security
End-user system	Smart cards and other one-time tokens
Mobile devices	Virtualization-specific tools
Confidential assets:	Vulnerability/patch management
Customer personal information	Virtual private network
Payment card information	Staff training programs
Off-line data	

Table 3.2: Description of data used to represent parameters of the decision framework

Notation	Value Used	Description	Data Source
$\max_t\{\beta_{11}\}$	0.5091[a]	Maximum effectiveness of detective countermeasures on basic attacks	Survey data
$\max_t\{\beta_{12}\}$	0.5788	Maximum effectiveness of detective countermeasures on advanced attacks	Survey data
$\max_t\{\beta_{21}\}$	0.7646	Maximum effectiveness of preventive countermeasures on basic attacks	Survey data
$\max_t\{\beta_{22}\}$	0.5277	Maximum effectiveness of preventive countermeasures on advanced attacks	Survey data
$l_{11} + l_{12}$[b]	\$205	Expected loss in both asset categories caused by a basic attack	Ponemon (2016b)
$l_{21} + l_{22}$	\$236	Expected loss in both asset categories caused by an advanced attack	Ponemon (2016b)
α_1	2.0098×10^{-10}	Cost effectiveness parameter for achieving maximum protection for preventive countermeasures	Survey data
α_2	3.1230×10^{-10}	Cost effectiveness parameter for achieving maximum protection for detective countermeasures	Survey data
θ_1	$5.526 \times 10^{-2} PTL$[c]	Investment threshold for observing life cycle curve trend for preventive countermeasures	Survey data
θ_2	$6.404 \times 10^{-2} PTL$	Investment threshold for observing life cycle curve trend for detective countermeasures	Survey data

[a] β_{oa} values vary over time, and only the mean value is shown in the table.

[b] $l_{11} + l_{12}$ and $l_{21} + l_{22}$ add up to a constant respectively, but the ratio f_{1t}/f_{2t} varies across different industries. For the ten major industries such ratios are presented in Table 3.6.

[c] All monetary values are defined as a multiple of potential total loss, which is denoted by PTL in this table.

Table 3.3: Stochastic scenarios of life-cycle and effectiveness realizations.

Scenario Name	High effectiveness and long life-cycle for both controls.
HL	High effectiveness and long life-cycle for both controls.
LL	Low effectiveness and long life-cycle for both controls.
HS	High effectiveness and short life-cycle for both controls.
LS	Low effectiveness and short life-cycle for both controls.
MM	Medium effectiveness and medium life-cycle for both controls.

in an aggregated fashion, it is required that the interdependency also be assessed at the category level. To that end, we note that there exist some countermeasures of the preventive category having a related counterpart in the detective category, and vice versa. These countermeasures, such as firewall and anti-virus software or intrusion prevention systems and intrusion detection systems, are aimed at providing similar protections by complementing each other through adaptation of different strategies. Therefore, the interdependency of countermeasures on the category-level can be measured by the portion of adoption of types of countermeasures with the above features. Our survey of the partner organization suggests a portion of total protection is credited to synergy effects of such countermeasures, which corresponds to a value of $\rho_{12} = \rho_{21} = 0.32$. We specifically consider this value in our analyses in the following sections, but also perform sensitivity analysis around this interdependence measure by considering the impact of different values of ρ_{12}.

In addition, the countermeasure effectiveness life cycle curves are created as described in Section 3.2.2 based on the illustration in Figure 3.6b. The span of the life cycle curves are estimated according to product release dates and end-of-service dates derived from the technical support information of different countermeasure types (McAfee, 2013, Symantec, 2014). While the stochastic scenarios consider two aspects of effectiveness and life-cycle length (indicating maturity level), for computational tractability, we propose the following five scenarios described in Table 3.3.

In the above description, high effectiveness is defined as one standard deviation above the mean, low effectiveness is one standard deviation below the mean, and

Table 3.4: Probability distributions of security controls' effectiveness.

Type of β	Mean	Standard deviation
β_{11}: Detective control to advanced attack	0.579	0.252
β_{12}: Detective control to basic attack	0.509	0.309
β_{21}: Preventive control to advanced attack	0.527	0.223
β_{22}: Preventive control to basic attack	0.765	0.194

Table 3.5: Probability distribution of five scenarios in maturity and effectiveness of security controls after the initial investment period.

Scenario	HL	LL	HS	LS	MM
Probability	0.0531	0.2407	0.0531	0.2407	0.4124

medium effectiveness being around the mean. The categories of life-cycle length are defined following similar manner, with long life-cycle being one standard deviation above the mean, short life-cycle being one standard deviation below the mean, and medium effectiveness being around the mean. The effectiveness of two countermeasures are assumed to be following normal distributions which fit into the survey sample, with the parameters provided in the following Table 3.4:

The probability of each of the five scenarios can then be calculated as joint probability of the effectiveness and life-cycle realizations defined accordingly. These probability values are displayed in Table 3.5 after normalization.

Table 3.6: Frequency of basic attacks over all attacks based on Verizon (2016).

Industry category	Industry name	$\frac{f_{2t}}{f_{1t}+f_{2t}}$
Category I	Hospitality	0.9751
	Retail	0.7843
Category II	Entertainment	0.7500
	Manufacturing	0.7178
	Healthcare	0.6850
	Education	0.6683
	Information technology	0.6176
	Public sector	0.5909
Category III	Professional service	0.5446
	Financial service	0.4559
	Average value across industries	0.6478

In Table 3.6 we list the ratio of advanced attacks over all attacks targeting information systems for the different industries considered. For analysis purposes, the industries are grouped into three major categories according to the similarity of the corresponding advanced attack ratios. For each industry category, one frequency ratio value is adopted to represent all the industries in that category. We utilize this setup, and obtain several practical insights for firms in each category as described in the following subsections.

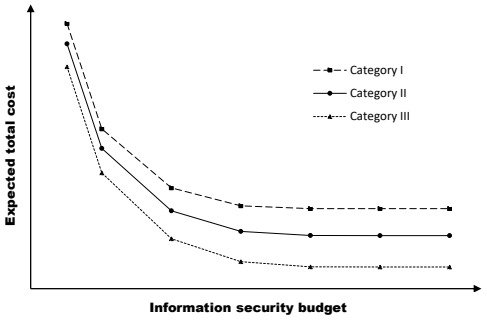
3.3.2 Analysis I: Optimal Investment in Information Systems Security

Determining the total information security budget is an important decision, as defined through our first key operational question of how much the firm should invest in information security. As has been emphasized by Hoo (2000), Gordon and Loeb (2002) and Huang et al. (2008), the total required investment needs to be sufficiently discussed and demonstrated before being put into the information security endeavor. The results in this section are aimed at helping information security practitioners justify their budget requirements as well as enhancing the efficiency of budget utilization for information systems security. We specifically seek answers to the following questions: Given the type of attacks that a firm faces, as well as the potential losses due to these attacks, *what should be the optimal level of information security investment by the firm?* Furthermore, does this investment level change based on the risk attitude of the firm?

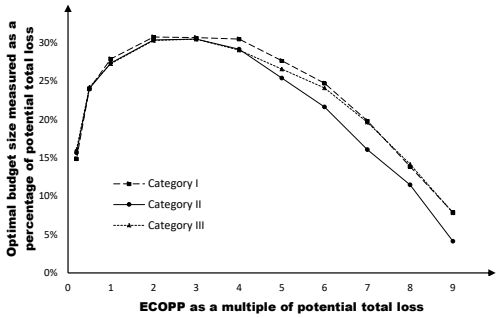
Clearly, the answers to these questions are expected to vary based on the asset and attack mix in the information security environment that a firm operates under. These conditions differ according to the industry and the size of the firm. However, we first show that the mix of assets does not play a role in the optimal level of investment in information security, and that only the total value of the assets is important. This is described through Proposition 3.3 as follows:

Figure 3.8: Budget size for information security investments

(a) Change in expected costs as a function of information security budget for different industry categories.



(b) Optimal budget size as a function of the estimated cost of perfect protection.



Proposition 3.3 *Optimal level of investment in information systems security is independent of the mix of information assets that the firm holds.*

Based on this result, we investigate how the optimal investment level would vary as a function of the total value of assets for different types of firms. In our analysis, the optimal investment level is represented as a percentage of the total value of the information assets that the firm holds. In Figure 3.8a we use a generic representation under a risk neutral assumption and demonstrate our findings for the major industries we consider in this study. The horizontal axis in the plot is investment in information systems security, and the vertical axis shows the value of expected total costs after investments. Given that the specific optimal investment levels are dependent on the value of the information assets of the firm, in the figure we only display the relative trend of the relationship with actual absolute values omitted. This provides an illustration of the general pattern observed for the relationship between information security investment and total costs, which holds for all asset configurations. In the figure, each industry category is represented by a separate curve, where there always exists a leveling point when increasing the investment will no longer yield a decrease in expected total costs. In other words, any investment beyond that

level is not cost-effective. We refer to the budget size at this leveling point as the *optimal level of investment in information systems security.* According to the figure, the leveling points for Category I, II, and III industries appear at almost the same position, indicating a universal optimal budget level for all industries with different advanced/basic attack ratios. The expected total cost, on the other hand, presents an increasing trend as the percentages of advanced attack get higher, which is due to the higher expected loss value of an advanced attack. *Hence, while firms in different industries generally has the same optimal budget level on investments, firms in Hospitality and Retail are expected to cost more on information system security than firms from other industries.*

As we noted above, Figure 3.8a is a generic representation, as the specific dollar value for the optimal investment level is a function of asset values and countermeasure costs. To that end, we express the optimal investment level for a given firm as a function of the estimated cost of perfect asset protection for that firm, which was discussed as part of the decision process depicted in Figure 3.2. The term 'perfect protection' in this context implies that a very high percentage of the maximum possible total loss is avoided. In our analyses, such percentage value is taken to be 99.9% and is controlled by adjusting the parameter α_o, which is the indicator of the cost effectiveness in achieving the maximum effectiveness level β_o for countermeasure o. In Figure 3.8b we present curves showing the optimal level of investment in information systems security as a function of ECOPP for different industry categories. This figure serves as a reference for firms in determining their optimal information security investment levels, where they would first define their ECOPP in terms of a multiple of potential total losses that they can incur, and then find out where they lie in the curve shown for the corresponding industry category. While ECOPP values are likely to vary for each firm, as they depend on the size and value of a firm's information

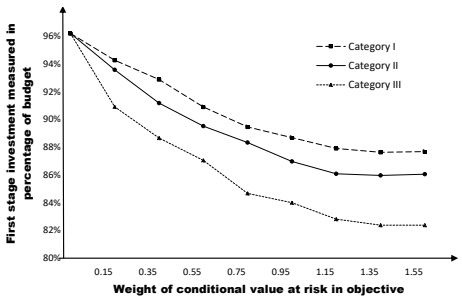
assets, a relative ordering of industry categories can be made in terms of how costly perfect protection would be at a general level.

According to Ponemon (2016a), the finance, energy and healthcare sectors suffer the highest costs due to attacks on information systems while several other industries like education, hospitality and entertainment sectors incur relatively lower costs. If the purchase price of countermeasures is assumed to be the same for users from all industries, the firms in finance and healthcare fields, where potential total losses are higher, are likely to lie to the left of the horizontal axis in Figure 3.8b, where perfect protection costs are measured as a percentage of the potential total loss. The opposite is likely to hold for most firms in the hospitality and healthcare industries, where potential total losses are relatively lower and thus ECOPP is higher when defined as a multiple of potential total loss.

As shown in Figure 3.8b, the optimal investment level is not a monotone function of ECOPP. It first increases, and then drops down after reaching a maximum. Hence, a general observation is that *if ECOPP is less than twice the potential total losses, the higher the ECOPP for a firm, the higher the optimal investment in information security.* Also indicated in the plot, industries from Category I and II have slightly higher optimal investment levels as the ECOPP becomes greater than three times of potential total loss. Based on these observations, the *overall information security budgets for firms in Categories I and II should be on average 4% higher than the other industries.* In addition to identifying the current position on the corresponding curve in Figure 3.8b and determining the optimal investment levels, a firm can also closely follow the dynamics due to internal and external factors, and update their optimal budget size as ECOPP varies due to such dynamics while planning over a long run.

We further note that the characterizations of optimal investment levels above is consistent with the conclusion of Gordon and Loeb (2002) that a firm should never invest more than 37% of the potential total loss on information security. Given our

Figure 3.9: Initial period investment in information security as a function of the risk measure for different industry categories.



consideration of the several other attributes in the investment process, our analysis provides more specific guidelines and tighter upper bounds under similar settings to those considered by Gordon and Loeb (2002). We give a proof of this below as part of Proposition 3.4, based on a deterministic case similar to that of Gordon and Loeb (2002).

Proposition 3.4 *If information security countermeasures and attacks are aggregated into a single category under a deterministic setting, then the optimal investment in information systems security by a firm should not exceed* $\frac{\beta}{e}$ *of the potential total losses that the firm can incur.*

We also consider the impact of risk attitude on the optimal information security investment level by studying the pattern illustrated in Figure 3.8a under different weights of the CVaR component in the objective function of the optimization model. Based on the results of this analysis, it is observed that the overall optimal total investment levels do not vary under different emphasis levels on risk, and we conclude that *the optimal size of the information security budget is insensitive to risk under the presented framework, and that only optimal budget allocations vary with risk.*

Related to this, we note that the initial period investments do vary under different risk parameter settings. Given its dependence on the operational environment

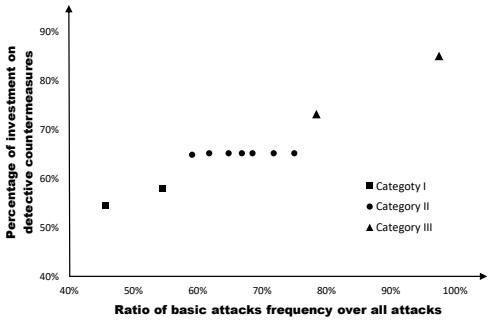
for a firm, we display our findings separately for each industry category in Figure 3.9. As shown in the figure, while holding all other conditions equal, the initial period investments decrease as the risk weight parameter increases. This indicates that when risk is highly emphasized, it is better to reduce the initial period investment thus leave more leeway for the second stage where information on the effectiveness of countermeasures becomes available. In other words, *firms should utilize a gradually increasing rate of usage for the information security budget within a given planning period. The higher the emphasis on risk reduction, the higher this rate of increase should be.* It is also noticed that the rate of decrease in the initial investment levels as a function of emphasis on risk reduction is faster for the Category III industries in comparison to the other two categories. This suggests that firms in these industries, such as public sectors, financial service and professional service should be even more conservative in the first learning stage, leaving more budget flexibility for the potential variation in the second stage. This might be due to the fact that the security controls are generally less effective on advanced attacks, making it especially difficult to withstand risk in these situations. In other words, the value of second stage investment is higher in cases where a firm faces a higher rate of advanced attacks. These observations also lead to the conclusion that *the higher the emphasis on risk reduction, the higher the value of information on information security countermeasure effectiveness for a firm.* Hence, information sharing between different organizations would result in information security risk reduction for all parties involved.

3.3.3 Analysis II: Optimal Allocation of the Information Security Budget over Countermeasure Categories

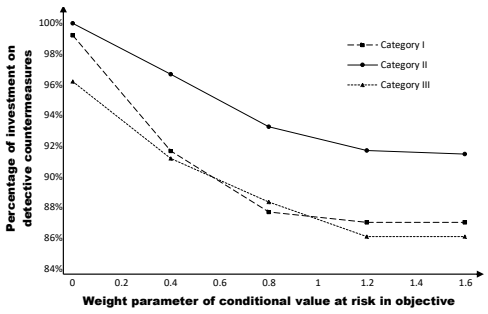
In this section we investigate optimal budget allocation policies for information security investments in different industries, which are distinguished based on the type of information environment that they operate in. Given these different environments,

Figure 3.10: Budget allocation over information security countermeasure categories for different industries.

(a) Percentage of investment on detective countermeasures.



(b) Budget allocation under different risk weights.



the general question that we try to answer in this section is: *what should be the optimal allocation of budget over detective and preventive countermeasures for different industries?* Furthermore, how does this vary according to the risk attitude of a firm?

We show in Figure 3.10a the optimal allocation structure identified for different industries identified by the ratio of basic attacks among all attacks they encounter. The vertical axis shows the percentage of investment on detective countermeasures in the initial investment period, and the horizontal axis corresponds to different industry categories aligned in the order of the ratio of basic attacks over advanced attacks faced. The reason for the consideration of the initial period investment here is that the decision maker can always resolve the model based on a rolling horizon, and apply the results from the first stage decisions. It can be observed that when all other conditions are as described for the two kinds of countermeasures, the correlation between the operational environment and the investment structure is obvious: when basic attacks are more prevalent, the firm should invest more on detective countermeasures. For industries where advanced attacks dominate basic attacks, the firm should allocate more resources on preventive countermeasures. Based on this finding and considering industry characteristics, we can specifically state that *Category II firms, including*

Entertainment, Manufacturing, Healthcare, Education and Information technology in industries, should invest about twice more in detective technologies than preventive ones, corresponding to an approximate split of 65% versus 35%. Meanwhile, for Category I and Category III firms the percentage of investment on detective measures is approximately the same as the rate of basic attacks among all the attacks.

Related to this analysis, we also study how a firm's risk attitude changes the optimal allocation of the information security budget over the preventive and detective countermeasures. In Figure 3.10b we show the budget allocation over the two countermeasures as a function of the weight of the conditional value at risk component in the objective function. The results imply that the ratio of investments on the two types of countermeasures shows some declining trend for all the three categories. However, such trend is not so significant at very high levels of risk emphasis. Hence, it can be concluded based on the results that the budget split between two countermeasures is not so sensitive towards the risk attitude of the firm.

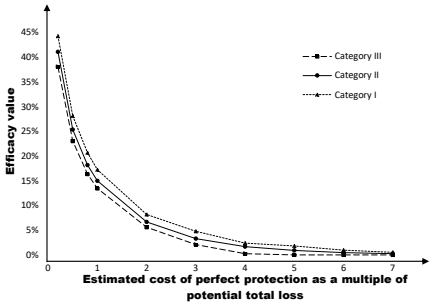
3.3.4 Analysis III: Efficiency of Optimal Policies for Investing in Information Security

We have noted above that the potential total loss is a key determinant for the optimal information security budget of a firm. A relevant question involves how much of such potential loss can be avoided under the optimal policy. More specifically, *what is the difference between expected costs under optimization and potential total loss?* We answer this question by studying the ratio of saved-cost with respect to potential total loss. This ratio is referred to as efficiency value of optimal policies, as higher values of this ratio would imply relatively more 'bang for the buck' to be achieved through an optimal investment policy.

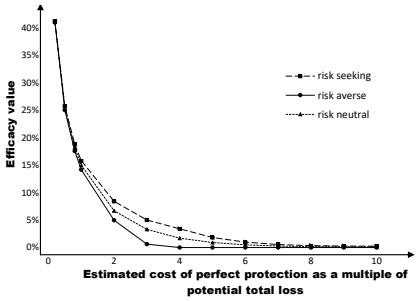
In Figure 3.11a we display the ratio of saved-cost, which is the difference between potential total loss and expected loss under optimal policy, with respect to optimal

Figure 3.11: Efficiency value of optimal policies for information security investments as a function of ECOPP.

(a) Efficiency value of optimal policies for different industry categories under a risk neutral setting.



(b) Efficiency value of optimal policies for Category II industries under different risk attitudes.



costs. The efficiency value measures are displayed as a function of ECOPP for different industry categories under a risk neutral setting, where the ECOPP values are defined as multiples of potential total loss. As shown in the figure, ratio of ECOPP and optimal cost does not follow a linear trend, and rather appears to decrease in a convex manner. For some general insights, we note that when ECOPP approaches zero, the saved-cost is almost the same as potential total loss, while when ECOPP is seven times the potential total losses the saved-cost drops to zero. This implies that optimal policies provide more efficiency especially when ECOPP is small with respect to potential total losses. In addition, we observe that the efficiency values of optimal policies presents a slightly decreasing order for Category III, Category II and Category I industries, respectively.

ECOPP in most cases is relatively small for large firms in comparison to potential total losses, as for these firms the losses caused by attacks on their information systems are likely to be very large. A recent example is the Target breach which resulted in costs of more than $1 billion for the company (Vomhof, 2013). On the other hand, a smaller firm is likely to have lower potential total loss values resulting in high ECOPP values in terms of potential total loss. Hence, large-sized firms are likely to lie on the

left side of Figure 3.11a, while smaller firms would be more on the right side. Thus, it can be concluded that the *optimal policies are relatively of more value for larger firms than smaller firms.* However, for small-sized firms, if the potential losses decrease or ECOPP increases due to complexity and frequency of attacks, the increase in the efficiency value of optimal policies will be almost exponential.

As a second analysis on this issue, we also consider how risk attitude impacts the efficiency value of optimal policies in information security investments by a firm. In Figure 3.11b we take Category II industries as an example and display the same information shown in Figure 3.11a under risk averse and risk seeking objectives. While the shape of the curve appears to be relatively independent of risk attitude of the firm, we do observe that as the firm's risk attitude is shifting towards being more risk seeking, the value of optimal policies becomes even higher.

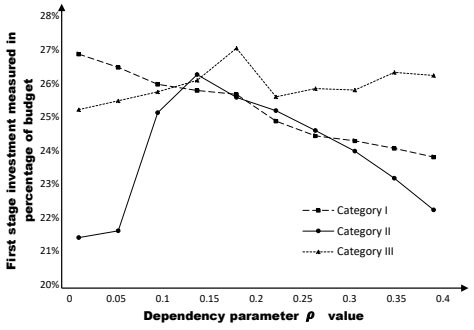
3.3.5 Analysis IV: Sensitivity Around the Interdependence Measure and Attack Frequency

Sensitivity Around the Interdependence Measure. In this section we study the impact of the dependency parameter between the two categories of countermeasures in our framework. The standard ρ_{12} value in our numerical implementations is taken as 0.45 based on estimates obtained through survey results. In the following analysis we vary this value from 0 to 0.45, and observe the changes in the initial period investment levels provided by the corresponding optimal solutions. The goal of this analysis, which is performed for different industry categories in order to obtain industry-specific features, is to assess the impact of $\rho_{oo'}$ on the optimal investment policy.

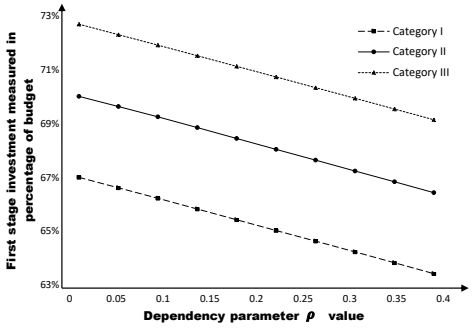
As shown in Figure 3.12a, the initial period total investment levels vary as a function of the ρ value differently for each industry category. For industries in Category III, the curve follows a slight increasing trend as the dependency parameter increases

Figure 3.12: Analysis with varying dependency parameter ρ.

(a) Initial period investments under different values of dependency parameter ρ.



(b) Expected total costs under different values of dependency parameter ρ.

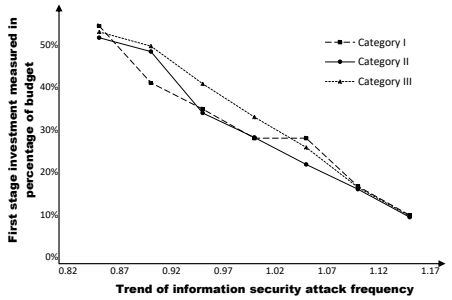


from zero to the estimated value of 0.45. As for the other industries, however, this behavior is reversed. While this is the case, we also note that the differences in the investment levels are not very large. The gap between the highest and lowest investment levels in Figure 3.12a is less than 6% of the budget. We also consider the total costs under different dependency measure values, and find that the total costs under each case vary less than 1%, which is indicated through Figure 3.12b. In the figure, as expected, the total costs monotonically drop with an increasing ρ_{12} value. Hence, it can be concluded that consideration of dependency between different categories of countermeasures has a visible, but somewhat small effect in an investment optimization framework. This also implies that our results should hold even if our estimation of the dependency measure is not perfectly accurate, as the conclusions do not appear to be sensitive to small deviations in the value of the dependency measure used in the analysis.

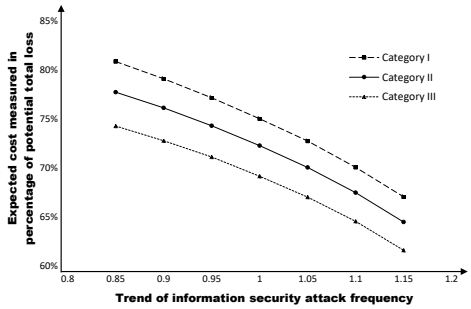
Sensitivity Around the Attack Frequency. In the previous analyses it has been assumed that the frequency of attacks on information systems per time unit is a fixed value over the entire planning horizon. In this section we further consider the cases of varying attack frequencies over time and observe the impact on initial

Figure 3.13: Analysis with different attack frequency trends on information systems.

(a) Initial period investments under different attack frequency trends.



(b) Expected total costs under different attack frequency trends.



period investment levels. Specifically, we examine the first stage investments where the annual increasing rate of attacks ranges from -15% to 15%. The comparative analysis was performed by assuming that the total number of attacks remain the same in each case, but the realizations of attacks are such that they either decrease or increase in a linear fashion over a given budget period.

The dilemma that a decision maker may have under changing attack frequencies is how much to invest in the early stages. Under the increasing trend of attack frequencies, the intuition suggests that investing more in the early stage is also likely to provide coverage for more intense attacks in the future. While under the decreasing trend of attack frequencies, investing more in the initial periods might seem somewhat counter effective as early stage installations of some countermeasures may not be as valuable in the later stage when the attack frequency drops.

However, the analysis shows quite opposite strategies to the intuitions above. In Figure 3.13a we show that as the frequency trend is shifting from increasing to decreasing, the investment levels in the initial periods become higher for all industries. The seemingly counter-intuitive results are actually related to the stochastic structure in the problem framework. Under the increasing trend of attack frequency, the uncertainty in potential loss is also larger in the later stages. Thus, investing less in

the initial periods leaves more leeway for the second stage to cope with higher loss realizations. As for the decreasing attack frequency trend, investing more in the initial periods means more resources can be utilized when the attacks are more intense and the assets are at higher risk. Although some of the countermeasures invested in the initial periods may have less value when attacks fade out, it is more essential to have the initial periods covered well with the current setting. In addition, we also observe in Figure 3.13b that the expected total costs under the three different attack frequency trends display an increasing pattern as attack frequencies decrease, though the rate of increase in Category II and III industries are subtle. This structure is likely due to the value of learning, such that the decreasing attack rates would imply less potential value due to learning effects in later stages of the budget period. Hence, proper allocation of early and later stage information security investments is especially of value in increasing attack rate scenarios, where better balancing the tradeoffs between learning through early investments and more effectiveness through later stage investments produces more returns.

3.4 Conclusions

The severity of attacks targeting business information systems and the challenges in dealing with them are a major concern not only in the U.S., but also all over the globe. As a result, how much to invest on information systems security and how to allocate available resources over different countermeasure categories are critical issues that need to be addressed by information security practitioners. One of the greatest challenges in optimizing information security investments is defining a reasonable and generally applicable metric to measure the cost effectiveness of information security protection. Moreover, the inherent dynamic and stochastic nature of information security environment contributes to the complexity of managing such investments. In this study, we address these challenges and develop a comprehensive framework that

involves the major components in information security investment management. A stochastic optimization model is then built upon this framework that adopts high-level categorizations and captures a generic view of the decision making process with learning effects.

Despite the fact that available data on information security investments is scarce and usually not as irreproachable as desired, in this study we extract and utilize the best data available in the literature, as well as data that we obtained from our industry collaborators. Particularly, we take into consideration of the differences in operational environments of various industries when conducting our analyses. Risk attitude is also explicitly included in the form of sensitivity analysis around a risk measure as part of our efforts to derive broad references for managers. In that regard, we first identify an optimal investment level that is most effective in achieving a desired protection level for a firm. Next, we study the allocation of investments over information security countermeasures, where the results suggest that for industries such as finance and energy it is better to rely more heavily on detective countermeasures. For other industries, a more even allocation of budget over preventive and detective countermeasures is recommended. Furthermore, our analysis shows that smaller firms will benefit more from optimizing information security investments, which also holds true for firms facing very high costs for covering all their assets against attacks on their information systems. We also show that our modeling of interdependency between countermeasures is quite robust and that the findings would not be significantly impacted in case of estimation errors in the values of interdependency measures used. Finally, we also conclude that firms should be more conservative in investments while the attack frequency is increasing, as opposed to committing to large information security investments early in the budgeting period.

Beyond our analyses and findings, which are based on current available data and high-level aggregation of the information security components, we note that our work

provides a general framework that can be extended as more precise information becomes available, such as more detailed effectiveness information on individual countermeasures, potential loss information on certain assets due to specific attacks, and operational environment/asset configuration of other industries. Customized application of the framework to individual firms using specific firm data is also possible.

CHAPTER 4

OPTIMAL POLICIES FOR INFORMATION SHARING IN INFORMATION SYSTEM SECURITY

In this chapter we discuss the sharing of information in information system security practice. As introduced earlier in Section 1.3, this study is aimed at providing answers to the following practical research questions: *What is the optimal level of information sharing for a firm as a function of the firm's technology investments? What is the value of information sharing in information security? How do these findings vary over different operating environments?*. To this end, we re-model the information system security problem by integrating information sharing with technology investment, and conduct analytical and numerical studies for policy analysis.

The remainder of this chapter is organized as follows: In Section 4.1 we introduce the general structure of the information sharing problem under the context of information system security. In Section 4.3, we present a stochastic programming model for information system security investment management with information sharing. Detailed policy analysis using analytical and numerical approaches are presented in Sections 4.2 and 4.4. Finally, in Section 4.5 we summarize our results and present the conclusions.

4.1 A Framework for Information Sharing in Information System Security

Information sharing within the context of information system security has seldom been modeled through an optimization based approach. This is mainly due to the

challenges involving (i) the quantification of information sharing levels; (ii) the characterization of the regulatory drive for sharing information; (iii) the modeling of the cost and return structures; and (iv) the modeling of the role of technology investments in this context. In this section, we introduce the framework for information sharing by explaining how these key aspects of the modeling characteristics are captured in our model.

4.1.1 Quantification of Information Sharing Level

There is a variety of information that can be shared by firms to exchange knowledge on information security practice (Gordon et al., 2003, Gal-Or and Ghose, 2005, Weiss, 2015). In general, the information being shared includes: (1) breach information on cyber-attacks, and whether these attacks are successful or not, (2) vulnerabilities in information security countermeasures, (3) methods used to defend against cyber-attacks to protect a company's assets, and (4) methods to minimize the economic impact of a security breach once it has been detected. As all these types of information are gathered in different formats and transferred via different channels, it is difficult to quantify the amount of information being shared in absolute terms. In order to resolve this issue, several studies in the literature have adopted a quantification method for information sharing by scaling the sharing level to a fractional value between 0 and 1.

From a practical perspective, we assume that information security experts of a firm would standardize all the information that is being collected by their firm, and a decision will be made to decide what portion of such information that is going to be shared with other firms. Moreover, as various types of information can serve distinct purposes with different levels of importance, this assumption also implies that different kinds of information can be assigned different weights according to their relative significance. In the remainder of this study, we assume the collection

and weighing of information is already done by the firm, and information sharing level is denoted by $i \in [0, 1]$, where $i = 0$ means the firm does not participate in any information sharing, and $i = 1$ means the firm is willing to share complete information with other firms.

4.1.2 Information Sharing under a Centralized Coordinator

Despite the potential benefits of information sharing in the cybersecurity practice, spontaneous and voluntary sharing of information does not typically happen among firms. As analyzed in the game-theoretical studies of Gordon et al. (2003), Gal-Or and Ghose (2005), and Hausken (2007), when the firms act independently, the situation eventually leads to a Bertrand-Nash equilibrium where no information is shared among the firms. There are also several realistic concerns of the firms that prevent their participation in information sharing, such as protecting the privacy of the business, losing competitiveness in the industry, and the potential for being taken advantage of by free-riders. However, studies point out that when a centralized coordinator exists and manages the information sharing of the firms, both the social welfare and firms' returns are likely to be maximized. To this end, we assume in this study that the firms are managed under the control of a central coordinator.

In practice, information sharing alliances act as a central coordinator, where their roles include gathering of information on vulnerability and threats, providing two-way information sharing among firms, managing rapid response communications between firms in the event of an attack, and conducting education and training programs. In addition, the responsibilities of the central coordinator also includes monitoring and balancing the information sharing levels of each firm to ensure fairness. In other words, each firm participating in an ISAC is required to share information no less than a common minimum level, which can be decided based on negotiation and mutual agreement.

Building upon the discussion above, we propose a structural setup for security information sharing that is aimed to reflect the practical environment in the current practice. In this setup, a firm that joins a member-based information sharing alliance agrees on a desired information sharing level i^* with other member firms. The firm then gives out the corresponding portion of collected information to the central coordinator, and then obtains the same level of shared information i^* collected and synthesized from other firms. This setup ensures that the firm would always receive the same level of shared information as its own information sharing level.

4.1.3 Modeling the Cost of Information Sharing

Another challenge in modeling information sharing in cybersecurity is the definition and calculation of related costs. While many industries have well-developed metrics for technology investment costs and returns, such metrics do not exist for information sharing. As a result, it is difficult for information system security practitioners to come up with a monetary value for specific information sharing levels, which further impedes the firms' participation in information sharing activities. To overcome this challenge, in this study we describe a cost modeling process that we use in developing a cost function as part of our framework.

As mentioned in the legislative documents and literature (Gordon et al., 2003, Gal-Or and Ghose, 2005, Weiss, 2015), the cost of security information sharing has two main aspects. The first aspect deals with the routine costs of data collection and administrative interactions with the information sharing alliance. The second aspect is related to the risk of information leakage to hackers, which may increase the likelihood of customized cyber attacks towards the firm. We refer to these two types of costs as direct and indirect costs of information sharing, respectively. In addition, many firms are also concerned that sharing security related information may weaken their competitiveness in business. However, we note that the sharing of information is

conducted anonymously under the management of a centralized coordinator, ensuring a layer of protection on any confidential information. Such protection mechanism is also required by the Cybersecurity Information Sharing Act, which serves as a legislative support for the firms. Overall, the concern for losing competitiveness may hinder a firm's incentives for sharing information, but it typically does not constitute a practical problem when a centralized coordinator is involved.

Concepts related to the direct cost of information sharing has been discussed in several studies, specifically as it applies to business information disclosure (Edmans et al., 2013, Elliott, 1994). It is explicitly stated in these studies that the cost of sharing information is positively correlated with the level of information being disclosed. For the cost of information sharing in information system security, empirical studies have suggested a linear cost function with a fixed rate per unit of shared information (Berg et al., 2013). It can also be interpreted intuitively that the total workload of information sharing is proportional to the quantity of information being shared, resulting in a linear relationship between the direct costs and the information sharing level. To this end, we define $\kappa_d i$ as the total direct cost of sharing information at a level i, where κ_d is the unit cost. The parameter κ_d can be assessed by considering the required workload for information collection and the hourly rates of personnel involved.

The indirect costs of information sharing, on the other hand, need to be assessed based on expert opinions. These costs can be measured by the expected value of losses due to an advanced attack resulting from any potentially leaked information. While the cost of a customized attack due to information leakage can be estimated as a fixed value based on the content of the shared information, the likelihood of information leakage is positively related to the level of information shared. Specifically, by assuming that each unit of shared information has the same chance of exposure to potential attackers, it can be concluded that the likelihood of information leakage

is a linear function of the information sharing level, which in turn implies a similar relationship between the total indirect costs and the level of information shared. Therefore, we denote the indirect costs of information sharing as $\kappa_{_l} i$, where $\kappa_{_l}$ is the unit indirect cost, which also equals to the expected losses due to information leakage under complete information sharing, i.e. when $i = 1$.

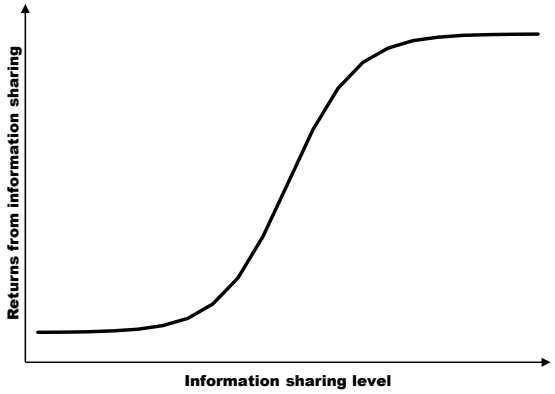
Eventually, the overall cost of information sharing at level i is the summation of direct costs $\kappa_{_d} i$ and indirect costs $\kappa_{_l} i$. Since both cost components are linear functions of information sharing level i, in the remainder of the discussion we no longer distinguish between direct costs and indirect costs, but use a general cost parameter $\kappa = \kappa_{_d} + \kappa_{_l}$ to build our modeling framework.

4.1.4 Modeling Returns from Information Sharing

While it is typically accepted that information system security can be improved at lower cost levels by sharing information (Weiss, 2015), the returns from information sharing are still unclear to most practitioners, as a quantitative measure is not clearly applicable. As part of addressing this issue, we consider approaches discussed in the literature and some actual observations from the information sharing practice, and propose a metric to model returns from information sharing.

Previous studies on information sharing in information system security consider information sharing as a direct addition to a firm's investment on information security technologies. A simplistic method of modeling information sharing is to add a certain level of "virtual investment" on top of the actual technology investment level. While several studies on information sharing in information system security have adopted this modeling structure (Gordon et al., 2003, Gal-Or and Ghose, 2005, Hausken, 2006, 2007), this simple linear relationship does not fully capture the two key effects between a virtual investment level and the information sharing level, namely the learning and saturation effects, which are based on observations from the practice of

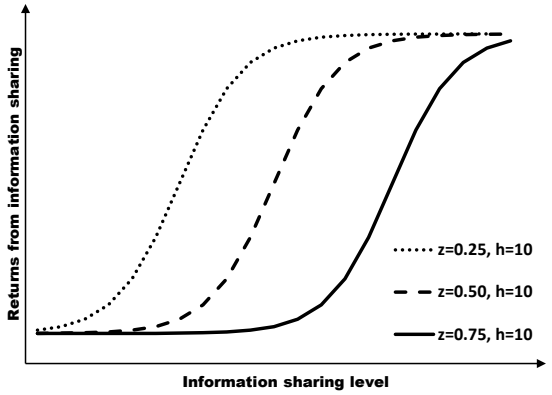
Figure 4.1: Learning and saturation effects in information sharing



information sharing in information system security. The learning effect corresponds to the phenomenon that the firm does not benefit as much when information sharing level is very low, but gains increase when the firms increase their mutual information sharing level to a certain extent. The saturation effect, on the other hand, refers to the fact that when information sharing level reaches to a certain value, there exist diminishing marginal returns. A graphical illustration of these learning and saturation effects is shown in Figure 4.1.

To model the learning and saturation effects in information sharing, we introduce a return function $\phi(i)$ to define the returns from sharing information at level i. $\phi(i)$ corresponds to the percent additive effect on a firm's technology investments due to sharing of information, and is defined to have the following properties: (1) $\frac{\partial\phi(i)}{\partial i} \geq 0$ for $i \in [0,1]$, (2) $0 \leq \phi(i) \leq 1$, and (3) there exists a value $i_z \in [0,1]$ such that $\frac{\partial^2\phi(i)}{\partial i^2} \geq 0$ for $0 \leq i \leq i_z$ and $\frac{\partial^2\phi(i)}{\partial i^2} \leq 0$ for $i_z \leq i \leq 1$. Property (1) defines $\phi(i)$ as a non-decreasing function, while property (2) depicts the range of the function. Property (3) implies the learning effects by defining $\phi(i)$ as a convex increasing function until some level i_z, and then as a concave increasing function for $i > i_z$.

Figure 4.2: Examples of $\phi(i)$ for different parameter z values



Given these definitions, we adopt the logistic function representation for $\phi(i)$, such that $\phi(i) = \frac{1}{1+e^{-h(i-z)}}$. In this representation, parameter h controls the steepness of the curve, and can be set to a value such that $\phi(0)$ is close enough to 0 and $\phi(1)$ is close enough to 1. Parameter z is referred to as the sigmoid midpoint, and is an indicator of the relative lengths of the learning and saturation periods on the curve. More specifically, a smaller z value would indicate fast learning and slow saturation, while large z values would imply the opposite. A few examples of $\phi(i)$ for different parameter z values are shown in Figure 4.2.

As suggested by Gordon et al. (2003), the returns from information sharing for a firm are proportional to the technology investment levels of the other firms in an information sharing alliance. To model this effect, a scaling factor $\gamma \in [0, 1]$ is introduced to represent the aggregate investment level by the other firms, where the lower bound 0 implies no technology investments by other firms, and the upper bound 1 corresponds to the case of other firms investing at least as much as the decision-making firm. In our study, we adopt this scaling factor to describe the "virtual investment" through information sharing. If x is the original technology investment level and $\phi(i)$ is the percent additive effect on technology investments for sharing

information at level i, then this implies an additional "virtual investment" of $x\gamma\phi(i)$ by the firm. However, this virtual investment is reduced if the aggregated effect of technology investments by other firms is less than that of the decision-making firm. The factor γ defines this discount, and thus total virtual investment effect is expressed as $x\gamma\phi(i)$.

4.1.5 Modeling the Relationship between Technology Investments and Information Sharing

Information sharing and technology investment have been considered as strategic counterparts of information system security (Gal-Or and Ghose, 2005), as these two major components intervene with each other in practice: the sharing of information among firms has a positive impact on the technology investments, and technology investments funds the eventual sources of the shared information. In order to capture a holistic picture of the information system security practice, it is important that a modeling framework includes both aspects of information sharing and technology investment. We achieve this by integrating the information sharing component into the technology investment model introduced in Chapter 3.

As introduced in Section 4.1.4, information sharing would generate an additive "virtual investment" effect of on the actual technology investment on information system security. Due to this effect, the original technology investment representation in the problem formulation of (3.5)-(3.13) in Chapter 3 needs to be adjusted accordingly. To this end, we define a new decision variable ϵ to represent the cumulative investment effects, i.e. the actual investment plus the "virtual" investment effect generated by information sharing. Based on previous discussions, we have for a given countermeasure $o \in \mathcal{O}$ that $\epsilon_o = x_o + \frac{x_o\gamma_o}{1+e^{-h(i-z)}}$. Since the technology investment level is differentiated between countermeasure categories, we note that the information sharing efficacy factor γ is defined separately for each countermeasure.

The effectiveness of technology countermeasures is one of the most important terms within the framework of the technology investment problem as described in Chapter 3. As a function of the technology investment level x, this term is subject to reformulation with the adjusted technology investment level ϵ. By replacing variable x with ϵ, the effectiveness of countermeasure protection under the information sharing context is expressed as $e(\epsilon) = \beta - \beta e^{-\alpha^{\epsilon}}$. The joint effectiveness of two countermeasure categories can then be rewritten as

$$e_{oo'}(\epsilon_o, \epsilon_{o'}) = \rho_{oo'} e_o(\epsilon_o) + \rho_{oo'} e_{o'}(\epsilon_{o'}) - \rho^2_{oo'} e_o(\epsilon_o) e_{o'}(\epsilon_{o'}),$$

with parameter $\rho_{oo'}$ being the interdependency coefficient for two countermeasure categories as introduced in Section 3.2.1.

In addition, the endogenous uncertainty set-up is also dependent upon the adjusted technology investment level. In Section 3.2.4, it is defined that if original technology investment for a certain countermeasure category falls below a threshold θ, then the exact position of the life-cycle curve will not be realized in the second phase of planning. However, with the contribution of information sharing, such threshold is reached easier due to the additive virtual investments, reflecting the fact that the firm learns about the countermeasure maturity though shared knowledge and experience by other firms. The revised formulation of the corresponding constraints is given as the following, with $\mathbf{M}$ being an arbitrarily large number and σ_o being a binary variable indicating whether the adjusted investment level exceeds or does not exceed the threshold:

$$\epsilon_o \leq \theta_o + \mathbf{M}\sigma_o \quad ; \quad \epsilon_o \geq \theta_o + \mathbf{M}(\sigma_o - 1).$$

4.1.6 Modeling the Total Cost of Information System Security Investments under Information Sharing

As discussed in Section 3.2.1, the total cost of information system security investments consists of two parts: the loss due to attacks and investment expenditures. The inclusion of information sharing into the problem framework would affect both parts of the overall cost function. Without information sharing, the actual loss due to attacks is defined as the potential total loss discounted by the overall countermeasure effectiveness. Namely, we have this cost term as $\sum_{t\in\mathcal{T}}\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}} f_{at}l_{as}\prod_{o,o'\in\mathcal{O}}\sqrt{1-e_{oo'a}(x_o,x_{o'})}$, where term $\sum_{t\in\mathcal{T}}\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}} f_{at}l_{as}$ represents the summation of potential total losses over all assets $s\in\mathcal{S}$ caused by all types of attacks $a\in\mathcal{A}$, over the planning period $t\in\mathcal{T}$. The overall countermeasure effectiveness is expressed as the product of the joint terms, namely as $\prod_{o,o'\in\mathcal{O}}\sqrt{1-e_{oo'a}(x_o,x_{o'})}$.

Based on the reformulation of joint effectiveness, the formulation of actual loss would utilize the adjusted investment levels ϵ_o as opposed to the original technology investment levels x_o, such that it becomes $\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}} f_{at}l_{as}\prod_{o,o'\in\mathcal{O}}\sqrt{1-e_{oo'a}(\epsilon_o,\epsilon_{o'})}$. With the inclusion of information sharing, $e_{oo'a}(\epsilon_o,\epsilon_{o'})$ implies a stronger countermeasure effectiveness, hence further reducing the actual losses in comparison with the original model without information sharing. On the other hand, the investment expenditure must also include the cost of information sharing κi, indicating an increase in the overall cost of information system security. The complete formulation for the total cost of information system security investments under information sharing can then be expressed as:

$$\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}} f_{at}l_{as}\left(\prod_{o,o'\in\mathcal{O}}\sqrt{1-e_{oo'a}(\epsilon_o,\epsilon_{o'})}\right)+\sum_{o\in\mathcal{O}}x_o+\kappa i \tag{4.1}$$

4.2 Optimal Information Sharing under Fixed Technology Investment

Before we develop a comprehensive numerical optimization model, in this section we perform some structural analyses for security information sharing. For tractability of our analysis in this section, we apply some reasonable simplifications to the original modeling framework. The modifications assume a deterministic situation where a firm wants to participate in information sharing with its technology investment level being fixed beforehand, and where countermeasure categories are aggregated into a single category.

In information system security practice, it is not unusual that information sharing is planned and administered after technology investment is made. In many cases, the management of a firm might consider information sharing as a secondary priority, and can make the decision on how much information to share separately from the technology investment decisions. Therefore, the findings in this section can provide insightful guidance to practitioners who may decide on information sharing after already having decided on technology investments.

As noted above, we consider a model where technology investment level x is fixed and information sharing level i is treated as the sole decision variable. Under this setting, the objective function is expressed as follows:

$$\min_{i\in[0,1];x\in[0,B]} \sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}} f_{at}l_{as} - \sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}(\beta - \beta e^{-\alpha(x+\frac{\gamma x}{1+e^{-h(i-z)}})}) + x + \kappa i \quad (4.2)$$

We start by a convexity analysis of the cost function (4.2) through the following:

Lemma 4.1 *The cost function* (4.2) *is convex in* i *for* $i \in [0, z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}]$ *and concave in* i *for* $i \in [z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}, 1]$.

Proof Proof. All proofs are included in Appendix B. □

This result allows us to determine the following conclusion on as to when it is beneficial for a firm to share information with other firms. An intuitive thought is that firms can avoid sharing information if the marginal cost of sharing information is very high. To this end, we have the following result:

Theorem 4.1 *Let i^* be the solution to the first order condition of function* (4.2)*. If* $i^* \geq z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}$*, then for a fixed technology investment level* x*, there exists a threshold* $\bar{\kappa} = \frac{\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{atlas}\beta e^{-\alpha x}\left(1-e^{-\alpha(x+\frac{\gamma x}{1+e^{-h(i^*-z)}})}\right)}{i^*}$*, such that if* $\kappa \geq \bar{\kappa}$*, the firm is better off by not sharing any information at all.*

Theorem 4.1 specifies that sometimes the firm is better off by not participating in information sharing if their information system security situation meets certain conditions. Due to the complexity of cost function (4.2), the closed form solution for this marginal cost threshold $\bar{\kappa}$ cannot be derived analytically, but has to be obtained numerically according to the parameter setup for the cost function. However, we are able to derive an upper bound for $\bar{\kappa}$ which can be applied as a quick screening condition. This upper bound is given through Corollary 4.1 as follows:

Corollary 4.1 *If marginal information sharing cost* κ *is such that* $\kappa \geq \frac{\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}} f_{atlas}\alpha\gamma x h\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)e^{-\alpha\left(x+\frac{\gamma x}{1+\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}}\right)}}{\left(1+\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)^2}$*, then the firm should not share any information.*

As introduced in Section 4.1.3, information sharing costs include both direct operational costs and indirect costs due to potential information leakage. We note that while the direct cost of routine information sharing activities tend to be manageable, the indirect costs of potential information leakage could be quite high for a firm, resulting in the marginal cost κ of information sharing exceeding the allowable threshold

$\bar{\kappa}$. Given that situation, a firm should either decrease the expected cost of information leakage by reinforcing its privacy protection methods or by not participating in information sharing to avoid any potential losses.

As the last set of analysis in this section, we study how optimal information sharing level reacts to changes in the marginal cost of information sharing. The finding is given through the following proposition:

Proposition 4.1 *For $\kappa < \bar{\kappa}$, the optimal information sharing level i^* decreases as marginal information sharing cost κ increases.*

This result in Proposition 4.1 implies that the firms are encouraged to share more information if the marginal cost of information sharing is lower, given that such marginal cost is already below the limiting threshold $\bar{\kappa}$. While confirming the intuition of many practitioners about information sharing, it can be interpreted that when information sharing becomes expensive, the returns that a firm would receive from sharing a high level of information cannot offset the extra costs. This finding would serve as a motivation for firms to collaborate and reinforce better protection mechanisms on information, so that the marginal cost of information sharing can stay within a reasonable range.

While analytical results in this section provide some high-level managerial insights for information security practice, we note that there exist more complex situations in information system security, specifically when the technology investment level and information sharing level are both treated as decision variables. In those situations, the simplifications made in the analytical analyses in this section will no longer apply. Therefore, we introduce a stochastic optimization model and conduct numerical analyses accordingly. The results from analytical and numerical analyses together are aimed to provide a comprehensive view as how to manage integrated information sharing with technology investment in information security.

4.3 Two-stage Stochastic Model of Information System Security Investment under Information Sharing

In this section, we formally present the stochastic model formulation for information system security investments under information sharing. The two-stage stochastic modeling structure is adopted from the general modeling framework in Chapter 3, by including the new information sharing related constraints discussed in this chapter. The complete formulation of the two-stage stochastic model of information system security investment with information sharing is given as follows:

$$\text{Minimize} \quad \sum_{\omega\in\Omega} p^{\omega}\left[\sum_{k\in\mathcal{K}}\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}}\sum_{t\in\mathcal{T}} f_{at} l_{ast}\left(\prod_{o,o'\in\mathcal{O}}\sqrt{1-e^{k\omega}_{oo'at}(\epsilon^{k\omega}_{o},\epsilon^{k\omega}_{o'})}\right)\right.$$
$$\left.+\sum_{k\in\mathcal{K}}\sum_{o\in\mathcal{O}} x^{k\omega}_{o}+\sum_{k\in\mathcal{K}}\kappa i^{k\omega}\right] \tag{4.3}$$

$$\text{Subject to} \quad \epsilon^{k\omega}_{o}=x^{k\omega}_{o}\left(1+\frac{\gamma}{1+e^{-h(i^{k\omega}-z)}}\right) \qquad \forall k\in\mathcal{K},o\in\mathcal{O},\omega\in\Omega \tag{4.4}$$

$$e^{k\omega}_{oo'at}(\epsilon^{k\omega}_{o},\epsilon^{k\omega}_{o'})=\rho_{oo'}e^{k\omega}_{oat}(\epsilon^{k\omega}_{o})+\rho_{oo'}e^{k\omega}_{o'at}(\epsilon^{k\omega}_{o'})-\rho^{2}_{oo'}e^{k\omega}_{oat}(\epsilon^{k\omega}_{o})e^{k\omega}_{o'at}(\epsilon^{k\omega}_{o'})$$
$$\forall o,o'\in\mathcal{O},a\in\mathcal{A},t\in\mathcal{T},k\in\mathcal{K},\omega\in\Omega \tag{4.5}$$

$$e^{1\omega}_{oat}(\epsilon^{1\omega}_{o})=\beta_{oat}-\beta_{oat}e^{-\alpha^{1}_{o}\epsilon^{1\omega}_{o}} \qquad \forall o\in\mathcal{O},a\in\mathcal{A},t\in\mathcal{T}^{1},\omega\in\Omega \tag{4.6}$$

$$e^{2\omega}_{oat}(\epsilon^{2\omega}_{o})=b^{\omega}_{oat}-b^{\omega}_{oat}e^{-\alpha^{2}_{o}\epsilon^{2\omega}_{o}} \qquad \forall o\in\mathcal{O},a\in\mathcal{A},t\in\mathcal{T}^{2},\omega\in\Omega \tag{4.7}$$

$$\epsilon^{1\omega}_{o}\le\theta_{o}+\mathbf{M}\sigma_{o} \quad , \quad \epsilon^{1\omega}_{o}\ge\theta_{o}+\mathbf{M}(\sigma_{o}-1) \qquad \forall o\in\mathcal{O},\omega\in\Omega \tag{4.8}$$

$$\sum_{k\in\mathcal{K}}\sum_{o\in\mathcal{O}} x^{k\omega}_{o}+\sum_{k\in\mathcal{K}}\kappa\left(i^{k\omega}\right)\le B \qquad \forall\omega\in\Omega \tag{4.9}$$

$$i^{1\omega}=i^{1\omega'} \qquad \forall\omega,\omega'\in\Omega,o\in\mathcal{O} \tag{4.10}$$

$$0\le i^{k\omega}\le 1 \qquad \forall k\in\mathcal{K},\omega\in\Omega \tag{4.11}$$

$$(3.9), \quad (3.13),$$

The objective of the proposed two-stage stochastic model above is to minimize the expected overall cost of information system security, which includes the expected losses due to attacks, as well as expenditure on technology investment and information

sharing. The loss term $\sum_{k\in\mathcal{K}}\sum_{s\in\mathcal{S}}\sum_{a\in\mathcal{A}}\sum_{t\in\mathcal{T}} f_{at}l_{ast}\left(\prod_{o,o'\in\mathcal{O}}\sqrt{1-e^{k\omega}_{oo'at}(\epsilon^{k\omega}_{o},\epsilon^{k\omega}_{o'})}\right)$ is based on the discussion in Section 4.1.6, with the summation of losses over the decision stages $k \in \mathcal{K}$ and time periods $t \in \mathcal{T}$. The expenditure terms of technology and information sharing investment are also calculated over the decision stages by summing them over decision stages $k \in \mathcal{K}$. The notation p^{ω} indicates the probability of scenario $\omega \in \Omega$, where the definition of the scenarios is based on the life-cycle status of the countermeasures in the second stage. In the two-stage stochastic setting, the second stage total cost is dependent on the scenario realization, and hence the objective is defined as an expectation over the scenario probabilities..

As introduced in Section 4.1.5, constraint (4.4) defines the "virtual investment" generated by information sharing for each technology countermeasure $o \in \mathcal{O}$. Constraint (4.5) is the joint effectiveness of countermeasures with adjusted technology investment levels, which is defined over all possible countermeasure pairs $o, o' \in \mathcal{O}$. Note that the joint effectiveness of countermeasures is expressed as a function of individual countermeasure effectiveness, which is given by constraints (4.6) - (4.7). Variable b^{ω}_{oat} in constraint (4.7) has the same meaning as introduced in Chapter 3, which is the realized value of maximum attainable effectiveness of countermeasure $o \in \mathcal{O}$ against attack $a \in \mathcal{A}$ at each time period in the second stage. Constraint (4.8) defines the threshold θ_o in technology investment level of the countermeasure. Constraint (4.9) is the budget constraint, which limits the total expenditure of technology investment and information sharing within budget B for every scenario $\omega \in \Omega$. Constraint (4.10) is the non-anticipativity constraints for the two-stage stochastic model. Similar to the definition of constraint (3.13), which is introduced in Chapter 3, constraint (4.10) fixes the information sharing level to be the same value in every scenario in the first stage, and allows the optimal information sharing level to vary in the second stage as technology investment levels change according to different life-cycle development realizations.

4.3.1 Solution Methodology

The information system security investment model under information sharing as introduced above is a non-convex nonlinear optimization problem as the cost function contains complex products of multiple decision variables with some non-linear constraints. In this section, we improve the computational tractability by reformulating the model through a series of steps that involve piecewise linearization including bilinear terms.

First, we note that the non-linear terms in (4.3), (4.5), (4.6), and (4.7) can be approximated using piece-wise linearization similar to the discussion by Section 3.2.5. To start, we define new variables $E^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'})$ and $I^{k\omega}_{oo'at}(\epsilon^{k\omega}_o)$ such that $E^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'}) = \ln\left(1 - e^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'})\right)$ and $I^{k\omega}_{oo'at}(\epsilon^{k\omega}_o) = \ln(1 - \rho_{oo'} e^{k\omega}_{oat}(\epsilon^{k\omega}_o))$. Constraint (4.5) can then be expressed in a simple linear form as:

$$E^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'}) = I^{k\omega}_{oo'at}(\epsilon^{k\omega}_o) + I^{k\omega}_{o'oat}(\epsilon^{k\omega}_{o'}) \qquad \forall o,o' \in \mathcal{O}, a \in \mathcal{A}, t \in \mathcal{T}, k \in \mathcal{K}, \omega \in \Omega \tag{4.12}$$

The new variable $I^{k\omega}_{oo'at}(\epsilon^{k\omega}_o)$ can be approximated in a piecewise linear fashion by a series of M constraints. Specifically, constraint (4.6) can be viewed as a special case of $I^{k\omega}_{oo'at}(\epsilon^{k\omega}_o)$ where $k = 1$ as:

$$I^{1\omega}_{oo'at,m}(\epsilon^{1\omega}_o) \geq u^{1\omega}_{oo'at,m}\epsilon^{1\omega}_o + v^{1\omega}_{oo'at,m} \qquad \forall o,o' \in \mathcal{O}, a \in \mathcal{A}, t \in \mathcal{T}^1, \omega \in \Omega, m = 1,\ldots,M \tag{4.13}$$

Following the same approach, constraint (4.7) can be replaced by the design of two sets of switching constraints using the binary variable σ_o and piecewise approximation of $I^{k\omega}_{oo'at}(\epsilon^{k\omega}_o)$ for $k = 2$:

$$I^{2\omega}_{oo'at,m}(\epsilon^{2\omega}_o) \geq u^{2\omega}_{oo'at,m}\epsilon^{2\omega}_o + v^{2\omega}_{oo'at,m} - \mathbf{M}\sigma_o \qquad \forall o,o' \in \mathcal{O}, a \in \mathcal{A}, t \in \mathcal{T}^2, \omega \in \Omega, m = 1,\ldots,M \tag{4.14}$$

$$I^{2\omega}_{oo'at,m}(\epsilon^{2\omega}_o) \geq u^{2\omega}_{oo'at,m}\epsilon^{2\omega}_o + v^{2\omega}_{oo'at,m} - \mathbf{M}(1 - \sigma_o) \qquad \forall o,o' \in \mathcal{O}, a \in \mathcal{A}, t \in \mathcal{T}^2, \omega \in \Omega, m = 1,\ldots,M \tag{4.15}$$

The product term in the objective function is reformulated using $E^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'})$ as:

$$\prod_{o,o' \in \mathcal{O}} \sqrt{1 - e^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'})} = e^{\ln \prod_{o,o' \in \mathcal{O}} \sqrt{1-e^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'})}}$$
$$= e^{\frac{1}{2} \sum_{o,o' \in \mathcal{O}} \ln\left(1-e^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'})\right)} = e^{\frac{1}{2} \sum_{o,o' \in \mathcal{O}} E^{k\omega}_{oo'at}(x^{k\omega}_o, x^{k\omega}_{o'})} \tag{4.16}$$

with the term $e^{\frac{1}{2} \sum_{o,o' \in \mathcal{O}} E^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, x^{k\omega}_{o'})}$ approximated by a set of linear constraints as follows:

$$Y^{k\omega}_{at} \geq h^{k\omega}_{at,m} \sum_{o,o' \in \mathcal{O}} E^{k\omega}_{oo'at}(\epsilon^{k\omega}_o, \epsilon^{k\omega}_{o'}) + g^{k\omega}_{at,m} \quad \forall a \in \mathcal{A}, t \in \mathcal{T}, k \in \mathcal{K}, \omega \in \Omega, m = 1, \ldots, M \tag{4.17}$$

As the next step, we transform the non-linear term in constraint (4.4) as product of $x^{k\omega}_o$ and $1 + \frac{1}{1+e^{-h(i^{k\omega}-z)}}$ to a bilinear term $X^{k\omega}_o P^{k\omega}$, with new variables $X^{k\omega}_o = x^{k\omega}_o$ and $P^{k\omega}$ defined as $P^{k\omega} = 1 + \frac{1}{1+e^{-h(i^{k\omega}-z)}}$. The following set of constraints is then added to the model to approximate $P^{k\omega} = 1 + \frac{1}{1+e^{-h(i^{k\omega}-z)}}$ as linear terms:

$$P^{k\omega}_l = \tau^{k\omega}_l i^{k\omega} + \upsilon^{k\omega}_l \qquad \forall k \in \mathcal{K}, o \in \mathcal{O}, \omega \in \Omega, l = 1, \ldots, L \tag{4.18}$$

For the linear approximation of the bilinear term $X^{k\omega}_o P^{k\omega}$, we utilize a two dimensional grid where the axes correspond to the values of $X^{k\omega}_o$ and $P^{k\omega}$. Let the upper and lower bounds of $X^{k\omega}_o$ and $P^{k\omega}$ be $\overline{X^{k\omega}_o}$, $\underline{X^{k\omega}_o}$, $\overline{P^{k\omega}}$, and $\underline{P^{k\omega}}$, respectively. We discretize $X^{k\omega}_o$ and $P^{k\omega}$ into S and T intervals respectively to form the grid. Furthermore, we introduce auxiliary variables $\pi^{k\omega}_{o,m,n}, m = 1, \ldots, S, n = 1, \ldots, T$ and two specially ordered set of type 2 (SOS2) variables $\mu^{k\omega}_{o,m}$ and $\nu^{k\omega}_{o,n}$. Letting the variable $XP^{k\omega}_o$ correspond to an approximation of the value of $x^{k\omega}_o P^{k\omega}$, we can approximate the bilinear term $X^{k\omega}_o P^{k\omega}$ through the following set of constraints:

$$\sum_{m,n} \pi_{o,m,n}^{k\omega} = 1 \qquad \forall k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.19}$$

$$P^{k\omega} = \sum_{m,n} (\underline{P^{k\omega}} + \left(\overline{P^{k\omega}} - \underline{P^{k\omega}}\right) \frac{m-1}{S}) \pi_{o,m,n}^{k\omega} \qquad \forall k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.20}$$

$$X_o^{k\omega} = \sum_{m,n} (\underline{X_o^{k\omega}} + \left(\overline{X_o^{k\omega}} - \underline{X_o^{k\omega}}\right) \frac{n-1}{T}) \pi_{o,m,n}^{k\omega} \qquad \forall k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.21}$$

$$XP_o^{k\omega} = \sum_{m,n} (\underline{P^{k\omega}} + \left(\overline{P^{k\omega}} - \underline{P^{k\omega}}\right) \frac{m-1}{S}) (\underline{X_o^{k\omega}} + \left(\overline{X_o^{k\omega}} - \underline{X_o^{k\omega}}\right) \frac{n-1}{T}) \pi_{o,m,n}^{k\omega} \qquad \forall k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.22}$$

$$\mu_{o,m}^{k\omega} = \sum_{n} \pi_{o,m,n}^{k\omega} \qquad \forall m,k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.23}$$

$$\nu_{o,n}^{k\omega} = \sum_{m} \pi_{o,m,n}^{k\omega} \qquad \forall n,k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.24}$$

$$\mu_{o,m}^{k\omega}, \nu_{o,n}^{k\omega} \in SOS2 \qquad \forall m,n,k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.25}$$

$$\pi_{o,m,n}^{k\omega} \geq 0 \qquad \forall m,n,k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.26}$$

We refer to the set of constraints (4.19) - (4.26) as $\mathcal{XP}_o^{k\omega}$. After transforming the objective function (4.3), constraints (4.4), (4.5), (4.6), and (4.7) as described above, we can express the overall convex reformulation of the information system security investment under information sharing model as follows:

$$\min_{\mathbf{x},\mathbf{i},\mathbf{E},\mathbf{I},\mathbf{Y}\in R^+,\sigma\in\{0,1\}} \sum_{\omega\in\Omega} p^{\omega} \left[\sum_{k\in\mathcal{K}} \sum_{s\in\mathcal{S}} \sum_{a\in\mathcal{A}} \sum_{t\in\mathcal{T}} f_{at} l_{ast} Y_{at}^{k\omega} + \sum_{k\in\mathcal{K}} \sum_{o\in\mathcal{O}} x_o^{k\omega} + + \sum_{k\in\mathcal{K}} \kappa_i i^{k\omega} \right] \tag{4.27}$$

$$\text{s.t.} \quad (3.9)-(3.13), (4.9)-(4.11), (4.12)-(4.18)$$

$$P^{k\omega}, X_o^{k\omega}, XP_o^{k\omega}, \mu_{o,m}^{k\omega}, \nu_{o,n}^{k\omega}, \pi_{o,m,n}^{k\omega} \in \mathcal{XP}_o^{k\omega} \qquad \forall m,n,k\in\mathcal{K}, o\in\mathcal{O}, \omega\in\Omega \tag{4.28}$$

The above formulation is a linear stochastic integer programming model, and can be solved directly to obtain the optimal information sharing and technology investment levels for both stages, where the first stage solutions are of interest to a decision maker.

4.4 Numerical Analysis and Policy Results

In this section, we perform numerical analyses to identify some policy results for information sharing in information security. More specifically, we numerically study the two-stage stochastic model described in Section 4.3, where the technology investment levels x_o and information sharing level i are simultaneously considered as decision variables. Managerial insights are provided by analyzing the problem with real data. In the remainder of this section, we first introduce the data that we utilize for our findings, and then present a set of policy analyses. We specifically focus on optimal information sharing levels and value of information sharing under different operating environments.

4.4.1 Description of Data

As part of the data gathering process, surveys were performed at a partner organization, where the proposed framework was observed from a practical perspective. These surveys included questions aimed at identifying the distinct categorizations of information system assets, attacks, and countermeasures. In addition to the survey data, we also utilized data obtained from the literature for our analyses. The parameter values obtained through these means are listed in Table 4.1.

Other parameters related to information sharing are the marginal cost of information sharing, κ_d, indirect unit cost κ_l, parameters h and z in return function $\phi(i)$, and γ, the aggregate investment level on information system security by other firms. The direct cost information obtained through our surveys include billable work hours of associated personnel, cost of holding business meetings with partner firm representatives and the membership fees of joining information sharing associations. For the indirect costs due to information leakage, we adopt the published data by Ponemon (2016b) and estimate the expected cost of an advanced cyber attack due to information leakage. A summary of these parameter values is listed in Table 4.2. For

Table 4.1: Description of data used to represent parameters of the decision framework

Notation	Value Used	Description	Data Source
$\max_t\{\beta_{11}\}$	0.5091[a]	Maximum effectiveness of detective countermeasures on basic attacks	Survey data
$\max_t\{\beta_{12}\}$	0.5788	Maximum effectiveness of detective countermeasures on advanced attacks	Survey data
$\max_t\{\beta_{21}\}$	0.7646	Maximum effectiveness of preventive countermeasures on basic attacks	Survey data
$\max_t\{\beta_{22}\}$	0.5277	Maximum effectiveness of preventive countermeasures on advanced attacks	Survey data
$l_{11} + l_{12}$	\$205	Expected loss in both asset categories caused by a basic attack	Ponemon (2016b)
$l_{21} + l_{22}$	\$236	Expected loss in both asset categories caused by an advanced attack	Ponemon (2016b)
α_1	2.0098×10^{-10}	Cost effectiveness parameter for achieving maximum protection for preventive countermeasures	Survey data
α_2	3.1230×10^{-10}	Cost effectiveness parameter for achieving maximum protection for detective countermeasures	Survey data
θ_1	$5.526 \times 10^{-2} PTL$[b]	Investment threshold for observing life cycle curve trend for preventive countermeasures	Survey data
θ_2	$6.404 \times 10^{-2} PTL$	Investment threshold for observing life cycle curve trend for detective countermeasures	Survey data

[a] β_{oa} values vary over time, and only the maximum value is shown in the table.

[b] All monetary values are defined as a multiple of potential total loss, which is denoted by PTL in this table.

Table 4.2: Summary of the parameter values related to information sharing costs, where each value implies a multiple of potential total loss

Notation	Value	Description and details	Data source
κ_d	0.095	Direct marginal cost of information sharing	Survey data
	0.053	Expenses on billable work hours of related personnel	
	0.015	Expenses on holding business meetings	
	0.027	Membership fees of information sharing organization	
κ_l	0.175	Indirect marginal cost of information sharing	Ponemon (2016b)
	0.75	Estimated cost of cyber attack due to information leakage	
	0.24	Probability of cyber attack due to information leakage	

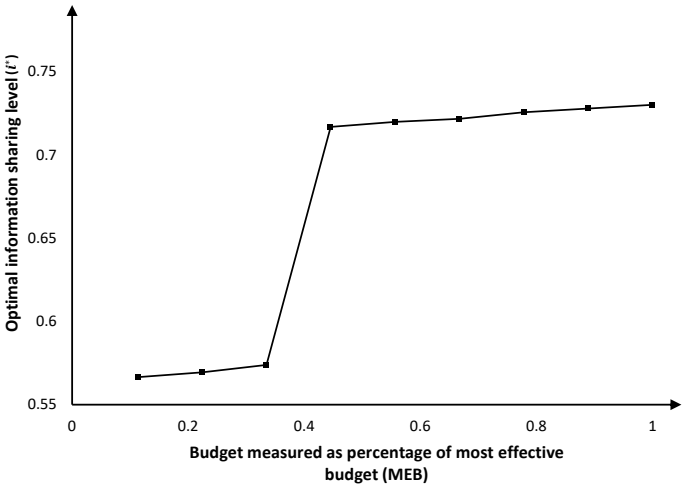
parameters of return function $\phi(i)$, we take the sigmoid mid-point value z to be 0.5 by assuming the learning effects and saturation effects in information sharing as being equally strong. The steepness parameter h is set to be $h = 13.81$, such that the point of inflection $z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}$ is always between 0 and 1 under different technology investment levels within the budget. As the aggregated investment level of other firms varies according to different information security technology investment environment levels, we set the initial value of γ to be 1, and then conduct a sensitivity analysis around this value to study its impact on information sharing levels.

The first problem we study through numerical analysis is the optimal information sharing level in information system security. While in Section 4.2 we describe some structural properties about optimal information sharing level from a static sense, in this section we are able to obtain the optimal information sharing level numerically based on the stochastic model, and observe how it varies as other parameters in information system security changes.

4.4.2 Optimal Level of Information Sharing under Different Budget Sizes

We first study how the budget level affects information sharing in information system security. To further discuss the findings, here we introduce the concept of *most effective budget (MEB)* under the information sharing context. As one of the results in Section 3.3.2, the overall expected total costs decrease in a convex manner as investment level increases, but converges to an asymptotical level after budget reaches MEB. Such a leveling point also exists when information sharing is considered, where this leveling point in expected total costs corresponds to a budget that covers both technology investment and information sharing costs. This MEB value typically depends on the potential total losses without protection, marginal ratio α_o of investment effectiveness of technology countermeasures, and information sharing cost

Figure 4.3: Optimal information sharing level under different budget sizes



κ. Ideally, a firm would set the budget size equivalent to MEB so that the maximum extend of protection is achieved without potential waste of funds.

However, MEB may not always be achievable in practice, especially by small to medium sized firms which may have limited information system security budgets. In that case, technology investment and information sharing would compete for the available budget, and how much information to share becomes a key strategic problem. We perform numerical analyses over the budget size from 0 to the level of MEB to observe how the optimal information sharing level varies according to different budget sizes. The results are shown in Figure 4.3.

As can be observed in Figure 4.3, the optimal information sharing level i^* increases with the budget size in a non-linear manner. When the budget size is less than one third of MEB, the optimal information sharing level i^* stays below 0.6, and increases rapidly as the budget grows from 30% to 40% of MEB. When the budget size is higher than one half of MEB, the information sharing level remains at a relatively high level. *This indicates that firms with budgets above half of MEB should share about 15% more information.*

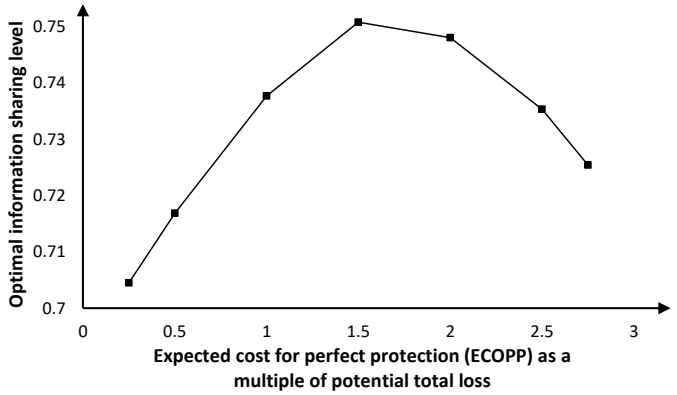
The fact that optimal information sharing level i^* is never zero indicates that under the given assumptions the firms would always benefit from information sharing when the marginal cost of information sharing κ is below the threshold $\bar{\kappa}$, even at lower budget levels. Generally, firms with larger security budgets, which typically corresponds to larger companies, should share more information to take advantage of the virtual investment effect. For smaller to medium size companies, for which the optimal information sharing level is lower, increasing the information system security budget to levels near MEB would benefit the firm both in terms of technology returns and also due to larger levels of information sharing to be performed. On the other hand, if a firm cannot afford to increase its budget over one half of MEB, then they may consider not participating in information sharing due to affordability issues.

4.4.3 Optimal Level of Information Sharing under Different Expected Cost of Perfect Protection

In this section, we study the relationship between the optimal information sharing level i^* and overall ECOPP values, as introduced in Section 3.3.2, by running sensitivity analysis over a set of different ECOPP_o values and solving for optimal information sharing levels i^*. As part of this analysis, the budget size for information system security is assumed to be equal to MEB in order to eliminate the influence of the budget constraint. The results are illustrated in Figure 4.4, where the overall ECOPP values are measured as a multiple of the potential total losses of a firm.

As can be observed in Figure 4.4, the information sharing level first increases as ECOPP increases, but slightly decreases from a maximum point when ECOPP is measured as 1.5 times of potential total losses. Since ECOPP is a measure reflecting the affordability of technology countermeasures for a firm, the drop in information sharing level can potentially be explained by the ineffectiveness of general information security investments due to higher costs. However, for firms that have a limited

Figure 4.4: Optimal information sharing level under different ECOPP values

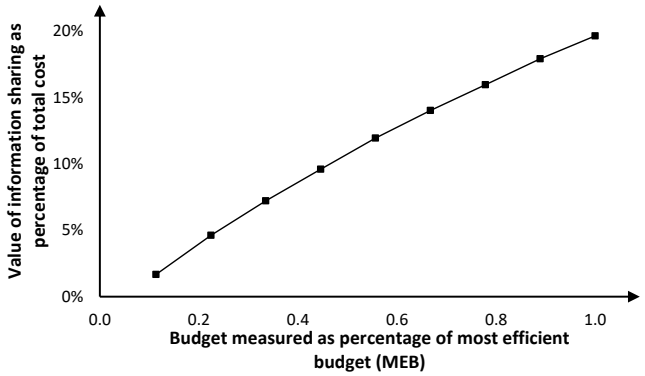


budget but are more prone to information system security attacks, the ECOPP value is likely to fall into the range between 1-1.5 times of potential total losses. *Such businesses should place more emphasis in information sharing, with potential optimal information sharing levels being about 5% higher than those firms with ECOPP values less than their potential total losses.*

4.4.4 Value of Information Sharing

To further study the economic incentives of information sharing in information system security investments, in this section we present two sets of analysis on the value of information sharing. The value of information sharing is calculated as the percentage difference between the expected total cost of information security investments with information sharing and the costs without information sharing. We first show the value of information sharing under different budget sizes measured as multiples of MEB, and then compare the value of information sharing for firms with different ECOPP values. It is also worthwhile noting that the information sharing alliances often consist of companies with different technology investment levels, resulting a variety of information sharing environments for different firms. To address this operational factor, in the latter part of the analysis we compare the value of information sharing for firms under different information sharing environments, which

Figure 4.5: Value of information sharing under different budget sizes



is defined by the aggregated technology investment level of the firms that mutually share information.

4.4.4.1 Value of Information Sharing under Different Budget Sizes

The change in the value of information sharing as a function of budget size is shown in Figure 4.5. As shown in the figure, the value of information sharing is always increasing as the budget size gets closer to MEB. Similar to the findings discussed for the optimal information sharing level, the best value for information sharing is attained at higher levels of information security investments. *Therefore, firms of large sizes or with relatively higher security budgets should be more motivated in participating in information sharing.*

In addition, the value of information sharing concavely increases as a function of budget size, which is different from the S-shaped curve observed for the optimal information sharing level in Figure 4.3. This result serves as another motivation for firms to further push for higher levels of information security budgets, as return rates increase as a function of the budget size. This is in contrast with the case in Figure 4.3, where there is not a significant need to increase the information sharing level as long as the budget size is smaller than MEB.

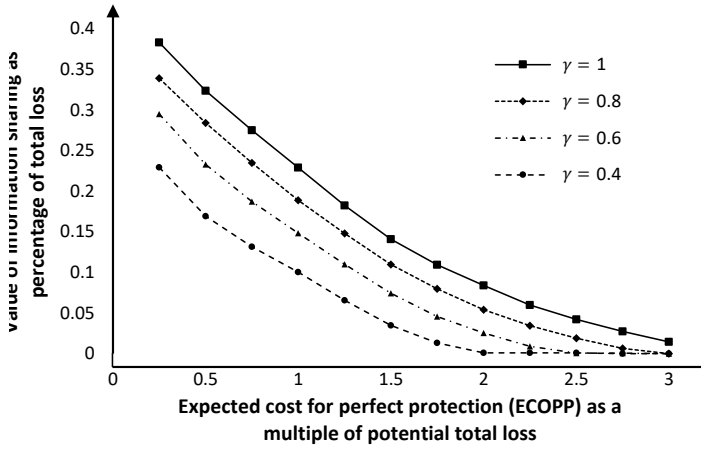
4.4.4.2 Value of Information Sharing under Different ECOPP and Investment Environments

As a final analysis, we study the impact of ECOPP on the value of information sharing for different firms. Since ECOPP reflects the affordability of information security technology, an increase in ECOPP would indicate a more challenging information security environment. Figure 4.6 shows the value of information sharing under different ECOPP values. Comparing with the increasing information sharing level i^* as a function of ECOPP in Section 4.4.3, Figure 4.6 shows that the value of information sharing decreases as the information security technology becomes more expensive, which can be seen as a reflection of the declining cost-effectiveness of overall information system security investments in tougher investment environments.

Moreover, as discussed earlier in Section 4.1.4, technology investments by other firms in an information sharing alliance can play an important role on the value of information sharing, as represented through the value of the parameter γ. To further study this impact, we compare the value of information sharing as a function of ECOPP for different levels of aggregated technology investment factor γ. This comparison is presented in Figure 4.6 by showing the trend in value of information sharing as a function of ECOPP for different settings of γ values.

As shown in Figure 4.6, while the value of information sharing as a function of ECOPP follows a decreasing trend, it is obvious that aggregated technology investment factor γ of the other firms is positively correlated with the value of information sharing, under same ECOPP levels. This result is in line with the intuition that when the partner firms allocate more resources to information security technology investments, the experience and knowledge they gather would be more informative. Consequently, information shared by such firms is of more value to the other firms who learn through their shared information. On the other hand, if all the other

Figure 4.6: Value of information sharing under different ECOPP and investment environments



partner firms have lower information security technology investments, the value of information sharing for the decision-making firm will be negatively impacted.

As a managerial insight for forming alliances for information sharing, the findings of this analysis suggest that *firms would benefit from building alliances with other firms that have similar information security technology investment levels.* In this way, all the firms would achieve a relatively high value out of information sharing in a fair manner without any concerns for free-riding effects. Meanwhile, small to medium size firms might be motivated to cooperate with larger-sized firms to take advantage of their information security technology investments scales.

4.5 Conclusion

With the need for joint efforts on information system security by all types of firms under an increasingly challenging cyber environment, information sharing has been encouraged by both the U.S. legislation and business practice. Therefore, how much information to share and the value of information sharing have become key practical questions for information security practitioners. To answer these questions,

in this study, we design a framework which includes technology investments and information sharing as two intertwining components of information system security. The framework also includes quantification metrics to measure information sharing levels and corresponding returns. The dynamics of information system security investments are captured through a two-stage stochastic programming structure. We take into consideration different operational situations and perform policy analyses involving structural and numerical results. More specifically, we first study a simplified analytical model where technology investment level is fixed in advance of the firm participating in information sharing. We find that there exists a threshold in marginal cost of information sharing such that a firm is better off by not sharing any information if the marginal cost exceeds this threshold.

Next, we study the optimization problem of minimizing total information security costs where information sharing and technology investment decisions are made simultaneously. For the optimal level of information sharing, we show that the optimal information sharing level increases slowly with the budget size for firms with very low or very high budgets, but at a faster rate for budget sizes around one half of the most effective budget. As a result, large firms with sufficient information security budgets should typically share 15% more information when compared with small to medium sized firms with budgets less than half of MEB. We also find that the optimal information sharing level is concavely increasing with the expected cost of perfect protection of a firm, indicating that firms prone to cyber attacks are encouraged to participate more in information sharing. Furthermore, we examine the value of information sharing under different operational conditions including budget sizes, expected costs of perfect protection, and aggregate levels of technology investments by other firms. The results show that the value of information sharing is increasing with the budget size, and decreasing with expected cost of perfect protection. Moreover, the value of

information sharing is highest when all firms in an information alliance have similar levels of technology investment.

As one of the few studies on information sharing of information system security, our work adds to the literature by providing a framework of information system security investment problems that captures both aspects of technology investment and information sharing. While in this study we assume a fair information sharing environment under the management of a centralized coordinator, the framework can also be extended to accommodate more complex situations where asymmetric information sharing is unavoidable, which we do in Chapter 5.

CHAPTER 5

ASYMMETRIC INFORMATION SHARING IN INFORMATION SYSTEM SECURITY

In this chapter we address the problems proposed by the end of Chapter 4 by seeking answers to the following research questions: (1) What fair price should a firm pay participating information sharing in asymmetric sharing environment? (2) How would the price of information vary under different pricing strategies and other influencing factors? To this end, we develop analytical expressions of a firm's payoffs under an asymmetric information sharing environment and analyze the pricing of information under two distinct pricing strategies through analytical and numerical analysis.

The remainder of this chapter is organized as follows: in Section 5.1 we introduce two pricing strategies of asymmetric information sharing and discuss them under three distinct settings. Policy insights based on practical data is presented in 5.1.4 through an numerical example. Finally, in Section 4.5 we summarize our results and present the conclusions.

5.1 Pricing Strategies for Asymmetric Information Sharing under Deterministic Setting

Our analysis of asymmetric information sharing in the information security context considers three distinct settings. In the first case, we assume a two-firm alliance, where only one of the firm provides security information. In the second case, both firms share information in different levels. Finally, in the third case, we consider the

sharing of information among multiple firms. For each of these cases, we study the functional relationship between the level of information shared by each firm at any price that the firm needs to pay for being part of the information sharing alliance.

5.1.1 Case I: One-way Information Sharing Between Two Firms

Consider a setup with two firms involved in an information sharing alliance. We assume without loss of generality that Firm A provides information to Firm B , while Firm B does not provide any information but is willing to pay a price p for the information it receives from Firm A.

For notational simplicity, we use the generic functions (5.1)-(5.2) to represent the information security related losses of a Firm A and Firm B under technology investment level $x_{_A}$ and $x_{_B}$ without information sharing;

$$g(x_{_A}, 0) = \sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} (1 - \beta_{_A} + \beta_{_A} e^{-\alpha_{_A} x_{_A}}) \tag{5.1}$$

$$g(x_{_B}, 0) = \sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} (1 - \beta_{_B} + \beta_{_B} e^{-\alpha_{_B} x_{_B}}) \tag{5.2}$$

For the paying Firm B , we use function (5.3) to represent its information security related losses under technology investment level $x_{_B}$ when receiving shared information at level $i_{_A}$ from sharing Firm A.

$$g(x_{_B}, i_{_A}) = \sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} (1 - \beta_{_B} + \beta_{_B} e^{-\alpha_{_B}(x_{_B} + \gamma_{_A}\phi_{_A}(i_{_A}) x_{_B})}) \tag{5.3}$$

5.1.1.1 Pricing with Fixed Technology Investment Level

An important issue regarding the payoffs for the information acquiring firm is how technology investment is handled in accordance with the acquired information. In practice, when information sharing is new to the firm and technology investment level is not easily adjusted, Firm B would maintain the same technology level $x_{_B}$ with

or without acquiring shared information from Firm A. In this subsection, we discuss the pricing strategy under this situation with fixed technology investment levels.

Following the modeling structure introduced in Chapters 3 and 4, the overall information security cost of Firm A before and after sharing information can be expressed as the following:

$$Before: \quad g(x_{_A}, 0) + x_{_A} \tag{5.4}$$

$$After: \quad g(x_{_A}, 0) + x_{_A} + \kappa_{_A} i_{_A} - p \tag{5.5}$$

$$Difference: \quad -\kappa_{_A} i_{_A} + p \tag{5.6}$$

The overall information security cost of Firm B before and after sharing information can be expressed as:

$$Before: \quad g(x_{_B}, 0) + x_{_B} \tag{5.7}$$

$$After: \quad g(x_{_B}, i_{_A}) + x_{_B} + p \tag{5.8}$$

$$Difference: \quad g(x_{_B}, 0) - g(x_{_B}, i_{_A}) - p \tag{5.9}$$

The benefit of information sharing is entirely reflected from the reduced information security related costs in Firm B , which follows:

$$g(x_{_B}, 0) - g(x_{_B}, i_{_A}) = \sum_{a \in \mathcal{A}} \sum_{s \in \mathcal{S}} \sum_{t \in \mathcal{T}} f_{at} l_{as} \left(\beta_{_B} e^{-\alpha_{_B} x_{_B}} - \beta_{_B} e^{-\alpha_{_B} \left(x_{_B} + \gamma_{_A} \phi(i_{_A}) x_{_B} \right)} \right) \tag{5.10}$$

Give this, we propose a simple asymmetric information pricing strategy for this case, which equally splits the benefits of information sharing between the two firms. We refer to this pricing strategy as *equal benefits strategy*. Based on this assumption,

the fair price p^{eb} such that the overall cost differences for Firm A (equation 5.6) and Firm B (equation 5.9) equal to each other:

$$\begin{aligned}\kappa_{A} i_{A} + p^{eb} =& g(x_{B}, 0) - g(x_{B}, i_{A}) - p^{eb} \\ p^{eb} =& \frac{1}{2}(g(x_{B}, 0) - g(x_{B}, i_{A}) - \kappa_{A} i_{A})\end{aligned} \tag{5.11}$$

The fair price under the equal benefits pricing strategy would make sure that both the information sharing firm and the information acquiring firm benefit from the practice of information sharing, which serves as a motivation for the collaboration between the two parties. On the other hand, certain conditions have to be met before the two firms participate in one-way information sharing relationship, which is illustrated through the following Theorem:

Theorem 5.1 *The two firms will not benefit from information sharing practice if the marginal cost of information sharing for Firm A exceeds the following threshold* $\bar{\kappa_{A}}$*:*

$$\bar{\kappa_{A}} \equiv \frac{\sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_{B} e^{-\alpha_{B} x_{B}} \left(1 - e^{-\alpha_{B}(x_{B} + \frac{\gamma_{A} x_{B}}{1+e^{-h(i_{A}^{*} - z)}})}\right)}{i_{A}^{*}} \tag{5.12}$$

where i_{A}^{*} *is the solution to the first order condition of function* (5.11) *such that*

$$i_{A}^{*} \geq z - \frac{\ln\left(\sqrt{\frac{\alpha_{B}^{2}\gamma_{B}^{2}x_{B}^{2}}{4} + 1} + \frac{\alpha_{B}\gamma_{A}x_{B}}{2}\right)}{h}$$

Theorem 5.1 implies that Firm A's marginal cost of information sharing should match Firm B's ability to generate benefits through technology investment. Specifically, if Firm A has a high risk of information leaking or complex information sharing protocols, it might not be cost-effective for Firm B to collaborate with Firm A in information sharing.

When the marginal information sharing cost κ_A is lower than the above threshold $\bar{\kappa_A}$, the sharing Firm A can potentially increase its information sharing level in return for higher prices paid by Firm B . Firm B can also change its technology investment level to generate more benefits using the acquired information. Details on these relationships are given by the following proposition 5.1:

Proposition 5.1 *When the marginal cost of information sharing for Firm A is lower than the threshold given by* (5.12)*, the fair price for one-way information sharing with equal benefit strategy is:*

(1) increasing with Firm B's technology investment level x_B *on* $[0, x_B^*)$ *and then decreasing on* $[x_B^*, +\infty)$*, where* $x_B^* = \frac{\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_B \alpha_B \left(1+\gamma_A \phi_A(i_A)\right)\right)}{\alpha_B\left(1+\gamma_A\phi_A(i_A)\right)}$*;*

(2) highest regarding to i_A *when* i_A *equals to* $i^*_{A_{(0)}}$*, where* $i^*_{A_{(0)}}$ *is the solution to the first order condition of function* (5.11) *such that* $i^*_{A_{(0)}} \geq z - \frac{\ln\left(\sqrt{\frac{\alpha_B^2\gamma_B^2 x_B^2}{4}+1}+\frac{\alpha_B\gamma_A x_B}{2}\right)}{h}$.

5.1.1.2 Pricing under Re-optimized Technology Investments

As discussed in Section 4.4.2, information acquiring firms are better off by investing according to the MEB on security technologies, which usually means different investment levels before and after acquiring shared information. While some firms new to the information sharing practice may not have such flexibility, most firms can achieve this by developing advanced investment mechanisms to incorporate shared information. In such cases, the re-optimized technology investment level will affect the fair price value with the equal benefit strategy.

Consider a similar setup as in Section 5.1.1 but with Firm B investing x_B^* before acquiring Firm A's information and x_B^{**} afterwards. The overall information security cost of Firm B before and after sharing information can be expressed as:

$$Before: \quad g(x^*_{_B}, 0) + x^*_{_B} \tag{5.13}$$

$$After: \quad g(x^{**}_{_B}, i_{_A}) + x^{**}_{_B} + p \tag{5.14}$$

$$Difference: \quad g(x^*_{_B}, 0) - g(x^{**}_{_B}, i_{_A}) + x^*_{_B} - x^{**}_{_B} - p \tag{5.15}$$

The overall cost of Firm A before and after sharing information remains the same as in (5.4)-(5.6) The fair price under equal benefit strategy that sets the pay-off for Firm A and Firm B as the same can then be expressed as:

$$p^{eb^*} = \frac{1}{2}\left(g(x^*_{_B}, 0) - g(x^{**}_{_B}, i_{_A}) + x^*_{_B} - x^{**}_{_B} + \kappa_{_A} i_{_A}\right) \tag{5.16}$$

By solving for the $x_{_B}$ values that minimizes Firm B's overall cost, we can obtain the fair price under equal benefit strategy when Firm B invest at the level of MEB and re-optimizes its technology investment level after obtaining shared information. The following theorem gives the closed-form expression for pricing strategies under this case:

Theorem 5.2 *When the paying Firm B invest according to MEB and re-optimizes its technology investments after acquiring information, the fair price* p^{eb^*} *for the information shared by Firm A is:*

$$\begin{aligned} p^{eb^*} =& \frac{1 + \ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_{_B} \alpha_{_B}\right)}{2\alpha_{_B}} \\ & - \frac{1 + \ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_{_B} \alpha_{_B}\left(1 + \gamma_{_A}\phi(i_{_A})\right)\right)}{2\alpha_{_B}\left(1 + \gamma_{_A}\phi(i_{_A})\right)} + \frac{1}{2\kappa_{_A} i_{_A}} \end{aligned} \tag{5.17}$$

Comparing the pricing structure with and without re-optimization of technology investments, we can draw conclusions similar to those in Section 4.4.2. Under asymmetric information sharing, firms can get higher overall payoffs by always investing according to MEB. This finding is summarized by the following corollary:

Corollary 5.1 *For a two firm information sharing alliance with one-way information sharing, the pay-offs for both firms would increase if the buying Firm B re-optimizes its technology investment level. The increase in the pay-off for each Firm amounts to:*

$$\left(\frac{1}{2}\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B}\big(1+\gamma_{_A}\phi(i_{_A})\big)\right)^{-\frac{(1+\gamma_{_A}\phi(i_{_A}))\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B})}{\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B}\left(1+\gamma_{_A}\phi(i_{_A})\right))}}$$
$$-\frac{1}{2\alpha_{_B}\big(1+\gamma_{_A}\phi(i_{_A})\big)}+\frac{\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B}\right)}{2\alpha_{_B}}$$
$$-\frac{\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B}\big(1+\gamma_{_A}\phi(i_{_A})\big)\right)}{2\alpha_{_B}\big(1+\gamma_{_A}\phi(i_{_A})\big)} \tag{5.18}$$

5.1.2 Case II: Mutual Information Sharing between Two Firms

As a second case, we consider two firms that both share information but not necessarily at the same sharing level. Without loss of generality, we assume Firm B pays a positive price $p_{_B}$ to Firm A. Firm B is referred to as "paying firm" and Firm A is referred to as "non-paying firm". The price paid by Firm A is therefore a negative value $p_{_A}=-p_{_B}$. Similar to Section 5.1.1.1, we first assume that the firms would not re-optimize their technology investment levels. The overall information security costs of Firm A before and after sharing information can be expressed as:

$$Before: \quad g(x_{_A},0)+x_{_A} \tag{5.19}$$
$$After: \quad g(x_{_A},i_{_B})+x_{_A}+\kappa_{_A}i_{_A}-p, \tag{5.20}$$
$$Difference: \quad g(x_{_A},0)-g(x_{_A},i_{_B})-\kappa_A i_{_A}+p \tag{5.21}$$

Similarly, the overall information security costs of Firm B before and after sharing information can be expressed as:

$$Before: \quad g(x_{_B},0)+x_{_B} \tag{5.22}$$
$$After: \quad g(x_{_B},i_{_A})+x_{_B}+\kappa_{_B}i_{_B}+p, \tag{5.23}$$
$$Difference: \quad g(x_{_B},0)-g(x_{_B},i_{_A})-\kappa_B i_{_B}-p \tag{5.24}$$

5.1.2.1 Pricing with Fixed Technology Investment Level

Under the equal benefit pricing strategy, the fair price that Firm B should pay to Firm A can be calculated by setting the overall payoff of information sharing as the same for the two firms:

$$g(x_{_A}, 0) - g(x_{_A}, i_{_B}) - \kappa_A i^A + p^{eb} = g(x_{_B}, 0) - g(x_{_B}, i_{_A}) - \kappa_B i_{_B} - p^{eb} \tag{5.25}$$

The fair prices $p^{eb} = p_{_B} = -p_{_A}$ can be calculated as:

$$p^{eb} = \frac{1}{2}\Big(\big(g(x_{_B}, 0) - g(x_{_B}, i_{_A}) - \kappa_{_B} i_{_B}\big) - \big(g(x_{_A}, 0) - g(x_{_A}, i_{_B}) - \kappa_{_A} i_{_A}\big) \Big) \tag{5.26}$$

While both firms are sharing information with each other and splitting their benefits in an even manner according to the equal benefit strategy, the payoffs for a firm might be very different from the financial contribution credited to its shared information. Such differences in payoffs and contributions can impact the firms' motivation for sharing information. To this end, we propose a second pricing strategy for asymmetric information sharing.

The second pricing strategy addresses the contribution of each firm through their information sharing activity. We refer to this method as *exchange return pricing strategy*. Under this strategy, a decision making firm's overall payoff is equal to the reduced costs by the other firm subtracted by the decision making firm's information sharing costs. The two firm's overall payoffs are no longer equal to each other:

$$\text{Firm } A\text{'s payoff} = g(x_{_B}, 0) - g(x_{_B}, i_{_A}) - \kappa_{_A} i_{_A} \tag{5.27}$$

$$\text{Firm } B\text{'s payoff} = g(x_{_A}, 0) - g(x_{_A}, i_{_B}) - \kappa_{_B} i_{_B} \tag{5.28}$$

Based on this, the fair price under exchanged return strategy for the previously described two firms A and B can be given as:

$$p_{_B} = p^{er} = g(x_{_B}, 0) - g(x_{_B}, i_{_A}) - g(x_{_A}, 0) + g(x_{_A}, i_{_B}) \tag{5.29}$$

Through the payoff functions (5.27)-(5.28), it is made clear that the return generated by the firms should cover each other's sharing costs, or it would lead to the firm's payoff being negative. Moreover, two firms are simultaneously motivated to share according to the best information sharing levels, leading to the maximum net return of the information sharing alliance. The strategy would also encourage transparency between the two firms regarding communication on sharing costs, technology efficacy, and potential total costs, which are the essential contents of shared information as discussed in Chapter 4.

While the fair price payoffs for the two firms are substantially different with equal benefit and the exchange return polices, it is possible that the two firms eventually reach a final price that lies in between p^{eb} and p^{er} through negotiation, which can address fairness and contribution in a balanced way.

5.1.2.2 Pricing under Re-optimized Technology Investment Levels

In this subsection, we consider the situation where both firms invest in security technologies according to MEB with re-optimization after mutual sharing information. Similar to Section 5.1.1.2, the optimal technology investment levels are denoted as x^* before information sharing and x^{**} after information sharing. The overall costs of the two firms before and after information sharing are expressed as follows:
Firm A :

$$Before: \quad g(x_{_A}^*, 0) + x_{_A}^* \tag{5.30}$$

$$After: \quad g(x_{_A}^{**}, i_{_B}) + x_{_A}^{**} + \kappa_{_A} i_{_A} - p, \tag{5.31}$$

$$Difference: \quad g(x_{_A}^*, 0) - g(x_{_A}^{**}, i_{_B}) + x_{_A}^* - x_{_A}^{**} - \kappa_{_A} i_{_A} + p \tag{5.32}$$

Firm B :

$$Before: \quad g(x_B^*, 0) + x_B^* \tag{5.33}$$

$$After: \quad g(x_B^{**}, i_A) + x_B^{**} + \kappa_B i_B + p, \tag{5.34}$$

$$Difference: \quad g(x_B^*, 0) - g(x_B^{**}, i_A) + x_B^* - x_B^{**} - \kappa_B i_B - p \tag{5.35}$$

Based on these, the fair price with the equal benefit strategy is given as:

$$\begin{aligned} p_B = p^{eb^*} = \frac{1}{2}\Big(& \big(g(x_B^*, 0) - g(x_B^{**}, i_A) + x_B^* - x_B^{**} - \kappa_B i_B\big) \\ & - \big(g(x_A^*, 0) - g(x_A^{**}, i_B) + x_A^* - x_A^{**} - \kappa_A i_A\big)\Big) \end{aligned} \tag{5.36}$$

On the other hand, the fair price under exchange return strategy is given as:

$$p_B = p^{eb^*} = \Big(\big(g(x_A^*, 0) - g(x_A^{**}, i_B) + x_A^* - x_A^{**}\big) - \big(g(x_B^*, 0) - g(x_B^{**}, i_A) + x_B^* - x_B^{**}\big)\Big) \tag{5.37}$$

In the following theorem, we give the closed-form fair prices for firms making technology investments according to MEB with re-optimization after information sharing under both pricing strategies:

Theorem 5.3 *When both firms invest according to their MEBs and re-optimize the technology investment levels after acquiring information, the fair prices p^{eb^*} and p^{er^*} are given as follows.*

$$\begin{aligned} p^{eb^*} = & \frac{1 + \ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_B \alpha_B\right)}{2\alpha_B} \\ & - \frac{1 + \ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_B \alpha_B \big(1 + \gamma_A \phi(i_A)\big)\right)}{2\alpha_B \big(1 + \gamma_A \phi(i_A)\big)} + \frac{1}{2\kappa_A i_A} \\ & - \frac{1 + \ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_A \alpha_A\right)}{2\alpha_A} \\ & + \frac{1 + \ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_A \alpha_A \big(1 + \gamma_B \phi(i_B)\big)\right)}{2\alpha_A \big(1 + \gamma_B \phi(i_B)\big)} - \frac{1}{2\kappa_B i_B} \end{aligned} \tag{5.38}$$

$$
\begin{aligned}
p^{er^*} =& \frac{1+\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B}\right)}{\alpha_{_B}} \\
&- \frac{1+\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B}\left(1+\gamma_{_A}\phi(i_{_A})\right)\right)}{\alpha_{_B}\left(1+\gamma_{_A}\phi(i_{_A})\right)} \\
&- \frac{1+\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_A}\alpha_{_A}\right)}{\alpha_{_A}} \\
&+ \frac{1+\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_A}\alpha_{_A}\left(1+\gamma_{_B}\phi(i_{_B})\right)\right)}{\alpha_{_A}\left(1+\gamma_{_B}\phi(i_{_B})\right)}
\end{aligned} \tag{5.39}
$$

5.1.3 Case III: Information Sharing Among Multiple Firms

In the third case, we discuss the pricing strategies of information sharing in a multiple-firm alliance. As introduced in Chapter 4, a centralized coordinator is assumed to be responsible for collecting and distributing the shared information, and in this case, re-distributing payments among the firms. To start, we give a simpler example with three firms – Firm A , Firm B and Firm C . The prices paid by the three firms are denoted as $p_{_A}$, $p_{_B}$ and $p_{_C}$. A positive value would imply the firm pays an amount to the coordinator and a negative values means the firm receives money from the central coordinator. Considering that the firms use same technology investment levels throughout the information sharing processes, the cost difference before and after information sharing for the three firms can be expressed as follows:

$$\text{Firm } A: \quad g(x_{_A},0) - g(x_{_A},i_{_B},i_{_C}) - \kappa_{_A} i_{_A} + p_A \tag{5.40}$$

$$\text{Firm } B: \quad g(x_{_B},0) - g(x_{_B},i_{_A},i_{_C}) - \kappa_{_B} i_{_B} + p_B \tag{5.41}$$

$$\text{Firm } C: \quad g(x_{_C},0) - g(x_{_C},i_{_A},i_{_B}) - \kappa_{_C} i_{_C} + p_C \tag{5.42}$$

Function $g(x_{_A},i_{_B},i_C)$ represents the information security related losses for Firm A with technology investment level $x_{_A}$, acquired shared information level $i_{_B}$ from Firm B and $i_{_C}$ from Firm C . Similar notation is applied for Firm B and Firm C . After acquiring shared information from Firm B and Firm C , Firm A's losses due to information attacks are reduced to:

$$g(x_{_A}, i_{_B}, i_{_C}) = \sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\left(1 - \beta_{_A} + \beta_{_A} e^{-\alpha_{_A}\left(1+\gamma_{_B}\phi(i_{_B})+\gamma_{_C}\phi(i_{_C})\right)x_{_A}}\right) \quad (5.43)$$

Where Firm B and Firm C's information sharing effects are both included as "virtual investments" in the exponent $e^{-\alpha_{_A}\left(1+\gamma_{_B}\phi(i_{_B})+\gamma_{_C}\phi(i_{_C})\right)}$. We can calculate the fair prices based on this return structure under the equal benefit strategy and the exchange return strategy as follows.

5.1.3.1 Pricing with Fixed Technology Investment Level

In this three-firm information sharing alliance, the equal benefit strategy based fair prices $p_{_A}^{eb}$, $p_{_B}^{eb}$ and $p_{_C}^{eb}$ will ensure the overall payoffs for the three firms are all equal to each other:

$$\begin{aligned}
&g(x_{_A}, 0) - g(x_{_A}, i_{_B}, i_C) - \kappa_{_A} i_{_A} + p_A \\
&= g(x_{_B}, 0) - g(x_{_B}, i_{_A}, i_{_C}) - \kappa_{_B} i_{_B} + p_B \\
&= g(x_{_C}, 0) - g(x_{_C}, i_{_A}, i_{_B}) - \kappa_{_C} i_{_C} + p_C \\
&= \frac{1}{3}\big(g(x_{_A}, 0) + g(x_{_B}, 0) + g(x_{_C}, 0) - g(x_{_A}, i_{_B}, i_C) - g(x_{_B}, i_{_A}, i_{_C}) - g(x_{_C}, i_{_A}, i_{_B}) \\
&- \kappa_{_A} i_{_A} - \kappa_{_B} i_{_B} - \kappa_{_C} i_{_C}\big) \qquad (5.44)
\end{aligned}$$

Based on this, the fair prices $p_{_A}^{eb}$, $p_{_B}^{eb}$ and $p_{_C}^{eb}$ can be calculated as the following expressions:

$$p_A^{eb} = \frac{2}{3}\big(g(x_A,0) - g(x_A,i_B,i_C) - \kappa_A i_A\big)$$
$$- \frac{1}{3}\big(g(x_B,0) - g(x_B,i_A,i_C) - \kappa_B i_B + g(x_C,0) - g(x_C,i_A,i_B) - \kappa_C i_C\big) \quad (5.45)$$
$$p_B^{eb} = \frac{2}{3}\big(g(x_B,0) - g(x_B,i_A,i_C) - \kappa_B i_B\big)$$
$$- \frac{1}{3}\big(g(x_A,0) - g(x_A,i_B,i_C) - \kappa_A i_A + g(x_C,0) - g(x_C,i_A,i_B) - \kappa_C i_C\big) \quad (5.46)$$
$$p_C^{eb} = \frac{2}{3}\big(g(x_C,0) - g(x_C,i_A,i_B) - \kappa_C i_C\big)$$
$$- \frac{1}{3}\big(g(x_A,0) - g(x_A,i_B,i_C) - \kappa_A i_A + g(x_B,0) - g(x_B,i_A,i_C) - \kappa_B i_B\big) \quad (5.47)$$

The return of information sharing contributed by a firm can be seen as the total cost savings of all the other firms due to the decision making firm's shared information. Taking Firm A as an example and holding everything else unchanged, the overall payoffs for Firm B and Firm C are added up as $g(x_B,i_C)+g(x_C,i_B)$. After accounting for Firm A's shared information, the summation of the payoffs for Firm B and Firm C becomes $g(x_B,i_A,i_C)+g(x_C,i_A,i_B)$, and the returns due to information shared by Firm A are the difference of the above two terms:

$$g(x_B,i_C) + g(x_C,i_B) - g(x_B,i_A,i_C) - g(x_C,i_A,i_B)$$

Hence, the exchange return based fair price for Firm A is given as the following:

$$p_A^{er} = g(x_B,i_C) + g(x_C,i_B) - g(x_B,i_A,i_C) - g(x_C,i_A,i_B)$$
$$- g(x_A,0) + g(x_A,i_B,i_C) + \kappa_A i_A \quad (5.48)$$

Similarly, the exchange return based fair price for Firm B and Firm C can be expressed as:

$$p_B^{er} = g(x_A, i_C) + g(x_C, i_A) - g(x_A, i_B, i_C) - g(x_C, i_A, i_B)$$
$$- g(x_B, 0) + g(x_B, i_A, i_C) + \kappa_B i_B \tag{5.49}$$
$$p_C^{er} = g(x_A, i_B) + g(x_B, i_A) - g(x_A, i_B, i_C) - g(x_B, i_A, i_C)$$
$$- g(x_C, 0) + g(x_C, i_A, i_B) + \kappa_C i_C \tag{5.50}$$

Based on the structures from (5.45)-(5.47) and (5.48)-(5.50), we can summarize the fair price under equal benefit strategy and exchange return strategy in a generalized multiple firms setting. For an information sharing alliance Γ with $|\Gamma|$ as the number of firms, the fair prices for any firm $R \in \Gamma$ are as follows:

$$p_R^{eb} = \frac{|\Gamma| - 1}{|\Gamma|}\Bigg(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\big(\beta_R e^{-\alpha_R x_R} - \beta_R e^{-\alpha_R\left(x_R + \sum_{I\in\Gamma, I\neq R}\gamma_I \phi(i_I) x_R\right)}\big)\Bigg)$$
$$- \frac{1}{|\Gamma|}\sum_{K\in\Gamma, K\neq R}\Bigg(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\big(\beta_K e^{-\alpha_K x_K} - \beta_K e^{-\alpha_K\left(x_K + \sum_{I\in\Gamma, I\neq K}\gamma_I \phi(i_I) x_K\right)}\big)\Bigg) \tag{5.51}$$

$$p_R^{er} = \sum_{K\in\Gamma, K\neq R}\Bigg(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\big(\beta_K e^{-\alpha_K\left(x_K + \sum_{I\in\Gamma, I\neq K, R}\gamma_I \phi(i_I) x_K\right)}$$
$$- \beta_K e^{-\alpha_K\left(x_K + \sum_{I\in\Gamma, I\neq K}\gamma_I \phi(i_I) x_K\right)}\big)\Bigg)$$
$$- \Bigg(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\big(\beta_R e^{-\alpha_R x_R} - \beta_R e^{-\alpha_R\left(x_R + \sum_{I\in\Gamma, I\neq R}\gamma_I \phi(i_I) x_R\right)}\big)\Bigg) \tag{5.52}$$

5.1.3.2 Pricing under Re-optimized Technology Investment Levels

Following the Section 5.1.1.2 and 5.1.2.2, in this subsection we study the fair prices when firms invest according to MEB and re-optimize technology investments in the multi-firm information sharing alliance.

We use x_R^* and x_R^{**} to denote the technology investment level according to MEB before and after information sharing by Firm $R \in \Gamma$. The fair prices can then be adapted from (5.56) as:

$$p_{R}^{eb^*} = \frac{|\Gamma|-1}{|\Gamma|}\Bigg(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\big(\beta_{R}e^{-\alpha_{R}x_{R}^{*}} - \beta_{R}e^{-\alpha_{R}\left(x_{R}^{**}+\sum_{I\in\Gamma,I\neq R}\gamma_{I}\phi(i_{I})x_{R}^{**}\right)}\big) + x_{R}^{*} - x_{R}^{**}\Bigg)$$
$$- \frac{1}{|\Gamma|}\sum_{K\in\Gamma,K\neq R}\Bigg(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\big(\beta_{K}e^{-\alpha_{K}x_{K}^{*}} - \beta_{K}e^{-\alpha_{K}\left(x_{K}^{**}+\sum_{I\in\Gamma,I\neq K}\gamma_{I}\phi(i_{I})x_{K}^{**}\right)}\big) + x_{K}^{*} - x_{K}^{**}\Bigg) \tag{5.53}$$

$$p_{R}^{er^*} = \Bigg(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\big(\beta_{R}e^{-\alpha_{R}x_{R}} - \beta_{R}e^{-\alpha_{R}\left(x_{R}+\sum_{I\in\Gamma,I\neq R}\gamma_{I}\phi(i_{I})x_{R}\right)}\big) + x_{R}^{*} - x_{R}^{**}\Bigg)$$
$$- \sum_{K\in\Gamma,K\neq R}\Bigg(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\big(\beta_{K}e^{-\alpha_{K}\left(x_{K}+\sum_{I\in\Gamma,I\neq K,R}\gamma_{I}\phi(i_{I})x_{K}\right)}$$
$$- \beta_{K}e^{-\alpha_{K}\left(x_{K}+\sum_{I\in\Gamma,I\neq K}\gamma_{I}\phi(i_{I})x_{K}\right)}\big) + x_{K}^{*} - x_{K}^{**}\Bigg) \tag{5.54}$$

By solving for the optimal technology investment levels x_{R}^{*} and x_{R}^{**}, we can further derive the closed-form fair price for a Firm R in a set of information sharing alliance Γ by the following theorem:

Theorem 5.4 *In an information sharing alliance composed of a set Γ of firms, firm R's prices to pay under equal benefit and exchange return strategies are as follows:*

$$p_{R}^{eb^*} = \frac{|\Gamma|-1}{|\Gamma|}\Bigg(\frac{1+\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{R}\alpha_{R})}{\alpha_{R}}$$
$$- \frac{1+\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{R}\alpha_{R}(1+\sum_{I\in\Gamma,I\neq R}\gamma_{I}\phi(i_{I}))\right)}{\alpha_{R}(1+\sum_{I\in\Gamma,I\neq R}\gamma_{I}\phi(i_{I}))}\Bigg)$$
$$- \frac{1}{|\Gamma|}\sum_{K\in\Gamma,K\neq R}\Bigg(\frac{1+\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{K}\alpha_{K})}{\alpha_{K}}$$
$$- \frac{1+\ln\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{K}\alpha_{K}(1+\sum_{I\in\Gamma,I\neq K}\gamma_{I}\phi(i_{I}))\right)}{\alpha_{K}(1+\sum_{I\in\Gamma,I\neq K}\gamma_{I}\phi(i_{I}))}\Bigg) \tag{5.55}$$

$$
\begin{aligned}
p_R^{er^*} = & \Bigg(\frac{1 + \ln(\sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_{R} \alpha_{R})}{\alpha_{R}} \\
& - \frac{1 + \ln\left(\sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_{R} \alpha_{R} (1 + \sum_{I\in\Gamma, I\neq R} \gamma_{I} \phi(i_{I})) \right)}{\alpha_{R}(1 + \sum_{I\in\Gamma, I\neq R} \gamma_{I} \phi(i_{I}))} \Bigg) \\
& - \sum_{K\in\Gamma, K\neq R} \Bigg(\frac{1 + \ln(\sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_{K} \alpha_{K} (1 + \sum_{I\in\Gamma, I\neq K, I\neq R} \gamma_{I} \phi(i_{I})))}{\alpha_{K}(1 + \sum_{I\in\Gamma, I\neq K, R} \gamma_{I} \phi(i_{I}))} \\
& - \frac{1 + \ln(\sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_{K} \alpha_{K} (1 + \sum_{I\in\Gamma, I\neq K} \gamma_{I} \phi(i_{I})))}{\alpha_{K}(1 + \sum_{I\in\Gamma, I\neq K} \gamma_{I} \phi(i_{I}))} \Bigg)
\end{aligned} \tag{5.56}
$$

The two fair prices under the equal benefit strategy and the exchange return strategy with the firms re-optimizing technology investment levels after information sharing is compared through an numerical example in the next subsection.

5.1.4 Numerical Analysis

As introduced earlier in Section 5.1.1 and Section 5.1.2, the equal benefit strategy and exchange return strategy each feature a different way to address "fairness" of pricing in information sharing. The equal benefit strategy addresses fairness in terms of the absolute value in payoffs, while the exchange return strategy re-allocates the payoffs according to the share of "contribution" made by a firm. In this section, we study the implications of these two pricing strategies through a practical data-based numerical example. As part of the analysis, we compare the fair prices and overall payoffs under the two strategies in a multiple firm information sharing setting. Policy insights are drawn from the analysis, which provides guidelines for firms intending to practice information sharing through a similar multi-firm setting.

In this numerical example, we consider an information sharing alliance consisting of 10 firms. To model the real information sharing alliance in an industry environment, we utilize the data obtained from the surveys we described in Chapter 3 when creating the firms' profiles. For analysis purposes, we assume that the 10 firms all have similar abilities to pay for information security technologies as indicated by the parameter α, and that the technologies all have similar efficacy as indicated by pa-

Table 5.1: Parameter set ups for the firm profiles

PTL		β_R	α_R	γ_R	κ_R
Uniform(20,872,808,	54,669,745)	0.59505	1.29E-06	0.053	0.27PTL

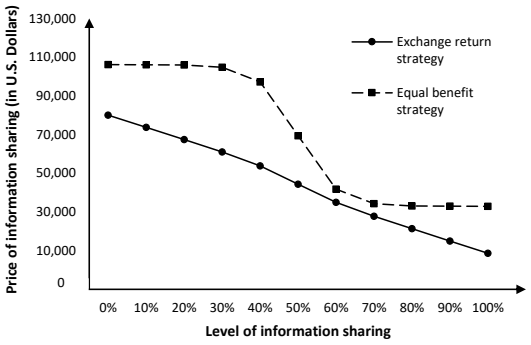
rameter β. The scaling factor γ is considered as being proportional to the optimal technology investment levels without information sharing. All these above parameters are standardized as being equal to the mean values obtained from the survey results. Moreover, to examine the differences in behaviors between larger sized firms and smaller sized firms, we allow the potential total losses to vary uniformly within 40% of the mean average PTL value from the survey results. The marginal cost of information sharing is set to be 0.27% of PTL as discussed earlier in Chapter 4. A full list of the 10 firm profiles are listed in Table 5.1.

We first compare the fair prices with the equal benefits strategy and the exchange return strategy in a decision making firm with varying information sharing levels. Specifically, we observe such trends in a typical smaller firm S (with PTL greater than 20% of all firms) and in a typical larger firm L (with PTL greater than 80% of all firms). As shown in Figure 5.1a, firm S would always pay higher prices under the exchange return strategy than the equal benefit strategy, with the prices getting closest to each other at 70% information sharing level. For the larger firm L, as shown in Figure 5.1b,the price based on the exchange return strategy is higher than the equal benefit-based price when the firm's information sharing level is below 65% or above 95%, and lower the than equal benefit-based price when the firm's sharing level is between the two threshold values. It is implied that *smaller firms or firms with lower information sharing levels tend to pay less under the equal benefit strategy than the exchange return strategy. Larger firms with near-optimal information sharing levels can potentially pay less under the exchange return strategy.*

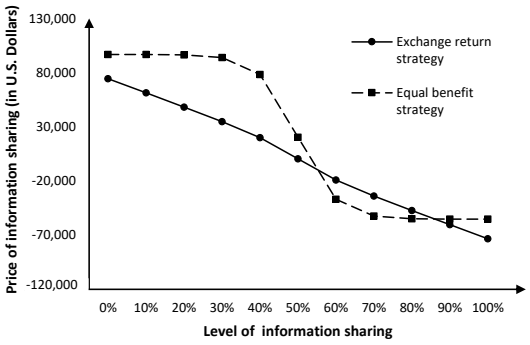
The payoffs for a smaller firm S and larger firm L are shown in Figure 5.2, under the equal benefit and the exchange return strategies. For the smaller firm S, as

Figure 5.1: Fair price under equal benefit and exchange return strategies.

(a) Fair price for a typical small firm S.



(b) Fair price for a typical large firm L.



shown in Figure 5.2a, the payoffs under the exchange strategy is always exceeded by the payoff under the equal benefit strategy. For the larger firm L, exchange return strategy can yield higher payoff when its information sharing level lies between the 65% – 95% range. From an overall payoff perspective, *smaller firms or firms with lower information sharing levels are favored under the equal benefit strategy, while larger firms investing near optimal information sharing levels are better off under the exchange return strategy.*

It is worth noting that, as illustrated in Figure 5.2a and Figure 5.2b, the equal benefit strategy would allow firms receive positive payoffs even when they do not share any information. While such phenomenon will not occur under a two-firm mutual information sharing setting, it shows that *free-riding is possible under equal benefit strategy in multiple firm information sharing settings.* To this end, it is recommended that *the exchange return strategy is applied for multiple firm information sharing alliances to ensure fairness.*

Finally, we consider an overview of the price differences and payoff differences under the two pricing strategies for all the firms in the alliance. Figure 5.3 shows the differences in prices and payoffs under the equal benefit and exchange return strategies for all 10 firms in the information sharing alliance. According to Figure 5.3, some firms

Figure 5.2: Overall payoffs under equal benefit and exchange return strategies.

(a) Overall payoffs for a typical small firm S. (b) Overall payoffs for a typical large firm L.

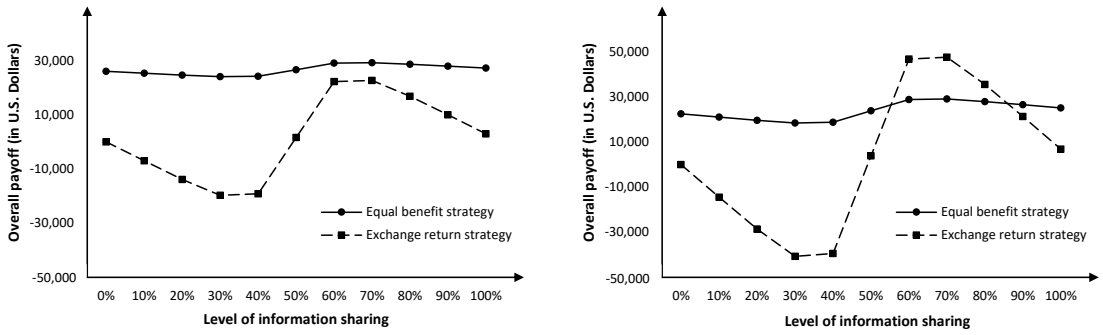
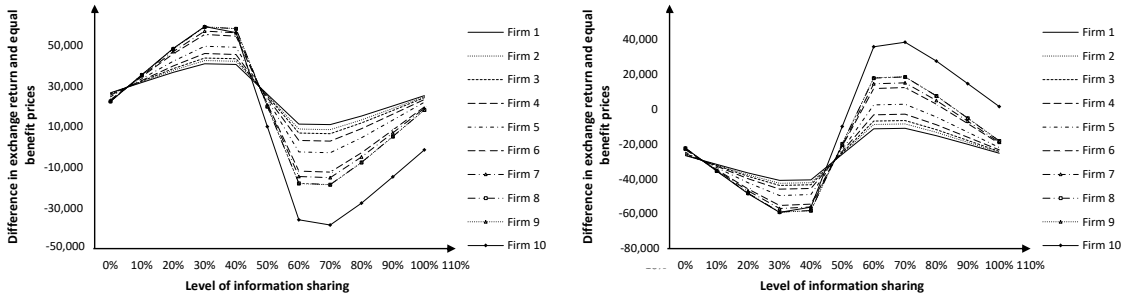


Figure 5.3: Differences in prices and overall payoffs under two pricing strategies for all 10 firms.

(a) Differences in price for all 10 firms under two pricing strategies.

(b) Differences in overall payoffs for all 10 firms under two pricing strategies.



would resemble firm S, who constantly favor the equal benefit strategy, as the price is always lower than that under the exchange return strategy. The other firms resemble firm L, who would favor the exchange return strategy by sharing according to the optimal levels. It is also observed that the differences in prices and payoffs under the two strategies are reduced to minimum when firms mutually agree to share around their own optimal information sharing levels. Therefore, *if equal benefit strategy is to be selected due to small firms' advocacy, pushing firms to share according to optimal information sharing levels would preserve fairness to the maximum extent.*

5.2 Conclusion

While information sharing can potentially help firms strengthen their information security defense, the asymmetry in information sharing often makes it difficult for the firms to collaborate. In this chapter, we study the pricing strategies of asymmetric information sharing, which addresses the benefit allocation among the participating firms and provides incentives for sharing information. We discuss the asymmetric information sharing in three distinct settings that covers most asymmetric information sharing scenarios in reality: two firms one-way information sharing, two firms mutual information sharing and multiple firms mutual information sharing. Through the two firm one-way information sharing case, we give the condition that makes asymmetric information sharing cost-effective for the firms. Next, while discussing the two firm mutual information sharing case, we proposed two different pricing strategies: the equal benefit strategy and the exchange return strategy. Under each strategy, we give the fair price of information sharing for the applied cases. We also solved the close-form expression of fair prices for firms that adjust technology investment MEB levels according to the sharing of information.

We demonstrate the differences in equal benefits strategy and exchange return strategy through an numerical example based on real-world data for policy insights. We find that free-riding can possibly happen in a multiple firm information sharing alliance under the equal benefit strategy, with smaller sizes or with low information sharing levels most likely to exploit this strategy. Hence, we recommend that the exchange return strategy to be applied in such setting to ensure fairness. In case that equal benefit strategy to be applied due to other reasons, we demonstrate that fairness is best preserved if all members of the alliance share according to optimal information sharing level that maximizes the return on information sharing.

As one of the few studies on asymmetric information sharing using operations management approach, the findings of this chapter can provide policy insights for

the firms that are intended to participate in information sharing. For those existing industry-based information sharing alliances, the analytical models from this chapter can assist the centralized coordinators to come up with their specialized pricing strategy. As future work, this problem could also be combined with a game-theoretical model by considering firm's intension, motivation and potential competition with each other. The performance of these pricing strategies under dynamic environments is also an interesting topic for future studies.

CHAPTER 6

CONCLUSIONS AND FUTURE RESEARCH

In this dissertation, we study the management of information system security investment using operations management approaches. Three relevant problems are studied throughout the thesis. In the first study, we address the key decisions involved in information security technology investments. In the second study, we discuss information sharing in information system security. In the third study, we investigate in the pricing strategies under asymmetric information sharing for information system security.

In Chapter 1 and Chapter 2, we provide general introduction and literature review regarding the background for the problems studied in this thesis. In Chapter 3, we study the first problem of information system security technology investment problem. To this end, we derive a simple functional relationship between the potential total losses of a firm and the optimal amount that the firm should invest in information systems security. Related to this, we find that firms in finance, energy, and technology sectors should invest twice more in trying to detect information security breaches, than in trying to prevent them. In other industries, information security investments should be split evenly between preventive and detective measures. Moreover, the overall information security budgets for certain types of firms in the former set of industries should be on average 4% higher than other industries, even when the potential total losses under a security breach are the same. As some additional conclusions, we find that the value of these optimal policies is higher for small to

medium sized firms, while a gradual investment strategy over a budget period is better than early utilization of the budget at the beginning of this period.

In Chapter 4, we study the second problem of information sharing in information system security. We build up a stochastic framework to capture the inter-relationship between information sharing and technology investments, where the two act as strategic counterparts of information system security. We find that, for firms with pre-fixed technology investment levels, the optimal information sharing level decreases as the marginal cost of information sharing becomes higher, and there exists a threshold value such that firms are better off by not sharing information if the marginal cost of information sharing exceeds this threshold value. For the optimal information sharing level, we find that firms with larger security budgets should share 15% more information, when compared to optimal sharing levels of small to medium sized firms.

In Chapter 5, we discuss the third problem of asymmetric information sharing in information system security. We evaluate two pricing strategies for asymmetrical information sharing under three distinct settings. We give analytical expressions of the fair price values under the different pricing strategies and come up with policy insights through both analytical and numerical analysis. For two firm information sharing setting, we find that firms could benefit from information sharing only when marginal information sharing cost is below certain threshold. For multiple firms information sharing setting, we recommend that the exchange return strategy to be applied to ensure fairness, whereas the equal benefit strategy can be potentially exploited by small size and low-level information sharing firms.

We believe that firms can benefit from our work either through direct implementation for specific guidance, or through indirect use of several policy results obtained. An important characteristic of our studies is that we build our models by using real-world data through survey to information system security practitioners. As one of the few studies on information system security investment management through opera-

tions management approaches, our work also set the first step for futures studies on related topics that can be explored by researchers in the field of management science.

As potential future research for the information system security technology investment, we note that parameter calibration and model validation is critical for any future implementation of the presented framework. Therefore, future work may involve assessment of accuracy of quantification of relevant measures as well as expert opinions used in the model. The observed performance of information system security through applying managerial insights on technology investment would also constitute an important extension to our study in terms of its practical significance.

For future research regarding information sharing in information system security, it is of value to analyze firm's behavior and motivations by considering competition and strategic decisions. Current modeling framework in this thesis considers the firms are all willing to cooperate and exactly follows the strategies proposed by the decision makers. Hence, if such assumptions were to be relaxed and firms are allowed to act according to their own interest, their individual decisions are likely to vary from what are found in this work.

Lastly, for the problem of asymmetric information sharing in information system security, potential extension of this work can focus on the uncertainty within the decision-making process. Specifically, in addition to the uncertainty in maximum effectiveness of technology countermeasures, we can future extend the stochastic setting to cover the dynamics in information sharing efficacy. It would also be interesting to analyze the pricing strategies of asymmetric information sharing behave under different risk measures.

APPENDIX

PROOFS OF ANALYTICAL RESULTS

Proof of Lemma 3.1

The proof is by showing that the partial derivatives of $e_{oo'a}(x_o, x_{o'})$ with regard to $\rho_{oo'}$, $e_{oa}(x_o)$ and $e_{o'a}(x_{o'})$ are nonnegative in the range $\rho_{oo'} \in [0, \min\{\frac{1}{\beta_{oa}}, \frac{1}{\beta_{o'a}}\}]$. To this end, we calculate the partial derivatives as follows:

$$\begin{aligned}\frac{\partial e_{oo'a}(x_o, x_{o'})}{\partial \rho_{oo'}} &= e_{oa}(x_o) + e_{o'a}(x_{o'}) - 2\rho_{oo'} e_{oa}(x_o) e_{o'a}(x_{o'}) \\ &= e_{oa}(x_o)(1 - \rho_{oo'} e_{o'a}(x_{o'})) + e_{o'a}(x_{o'})(1 - \rho_{oo'} e_{oa}(x_o))\end{aligned}$$

Without loss of generality we assume that $\beta_{oa} \geq \beta_{o'a}$. Hence, per the lemma statement, we have that $\rho_{oo'} \leq \min\{\frac{1}{\beta_{oa}}, \frac{1}{\beta_{o'a}}\} = \frac{1}{\beta_{oa}}$. It follows that:

$$\begin{aligned}\frac{\partial e_{oo'a}(x_o, x_{o'})}{\partial \rho_{oo'}} &\geqslant e_{oa}(x_o)(1 - \frac{e_{o'a}(x_{o'})}{\beta_{oa}}) + e_{o'a}(x_{o'})(1 - \frac{e_{oa}(x_o)}{\beta_{oa}}) \\ &\geqslant e_{oa}(x_o)(1 - \frac{\beta_{o'a}}{\beta_{oa}}) \geqslant 0\end{aligned}$$

where by definition $e_{o'a}(x_{o'}) \leq \beta_{o'a}$.

The second and third cases can be shown using a similar setup. We show the derivation for the case of $e_{oa}(x_{o'})$ below:

$$\begin{aligned}\frac{\partial e_{oo'a}(x_o, x_{o'})}{\partial e_{oa}(x_{o'})} &= \rho_{oo'} - \rho_{oo'}^2 e_{o'a}(x_{o'}) = \rho_{oo'}(1 - \rho_{oo'} e_{o'a}(x_{o'})) \\ &\geqslant \rho_{oo'}(1 - \frac{e_{o'a}(x_{o'})}{\beta_{oa}}) = \rho_{oo'}(1 - \frac{\beta_{o'a}}{\beta_{oa}}) \geqslant 0\end{aligned}$$

Similarly, we can easily show that $\frac{\partial e_{oo'a}(x_o,x_{o'})}{\partial e_{oa}(x_o)} \geq 0$. Hence, given the nonnegativity of the partial derivatives in the calculations above, the lemma holds. $\square$

Proof of Proposition 3.1

First, we show that a real-valued $\rho_{oo'}$ always exists for any $e_{oa}(x_o)$, $e_{o'a}(x_{o'})$, $e_{oo'a}(x_o, x_{o'}) \in [0,1]$. To this end, we express equation $e_{oo'a}(x_o, x_{o'}) = \rho_{oo'}e_{oa}(x_o) + \rho_{oo'}e_{o'a}(x_{o'}) - \rho^2_{oo'}e_{oa}(x_o)e_{o'a}(x_{o'})$ as a quadratic equation of $\rho_{oo'}$ as follows:

$$-e_{oa}(x_o)e_{o'a}(x_{o'})\rho^2_{oo'} + [e_{oa}(x_o) + e_{o'a}(x_{o'})]\rho_{oo'} - e_{oo'a}(x_o, x_{o'}) = 0 \tag{A.1}$$

Considering the roots of this equation, we get:

$$\rho^+_{oo'} = \frac{[e_{oa}(x_o) + e_{o'a}(x_{o'})] + \sqrt{\Delta}}{2e_{oa}(x_o)e_{o'a}(x_{o'})} \qquad \rho^-_{oo'} = \frac{[e_{oa}(x_o) + e_{o'a}(x_{o'})] - \sqrt{\Delta}}{2e_{oa}(x_o)e_{o'a}(x_{o'})} \tag{A.2}$$

where the discriminant Δ is defined as:

$$\begin{aligned}
\Delta &= [e_{oa}(x_o) + e_{o'a}(x_{o'})]^2 - 4e_{oa}(x_o)e_{o'a}(x_{o'})e_{oo'a}(x_o, x_{o'}) \\
&= [e_{oa}(x_o)]^2 + [e_{o'a}(x'_o)]^2 + 2e_{oa}(x_o)e_{o'a}(x_{o'}) - 4e_{oa}(x_o)e_{o'a}(x_{o'})e_{oo'a}(x_o, x_{o'}) \\
&\geqslant e^2_{oa} + e^2_{o'a} + 2e_{oa}(x_o)e_{o'a}(x_{o'}) - 4e_{oa}(x_o)e_{o'a}(x_{o'}) \\
&= [e_{oa}(x_o) - e_{o'a}(x_{o'})]^2 \geqslant 0
\end{aligned} \tag{A.3}$$

which follows from the fact that $e_{oo'a}(x_o, x_{o'}) \in [0,1]$. Hence, the roots $\rho^+_{oo'}$ and $\rho^-_{oo'}$ exist. Moreover, because $e_{oo'a}(x_o, x_{o'}) \in [0,1]$, it is obvious that both $\rho^+_{oo'}$ and $\rho^-_{oo'}$ are positive since $e_{oa}(x_o) + e_{o'a}(x_{o'}) = \sqrt{[e_{oa}(x_o) + e_{o'a}(x_{o'})]^2} \geqslant \sqrt{\Delta}$ always holds.

We now show that $\rho_{oo'} \in [0, \min\{\frac{1}{\beta_{oa}}, \frac{1}{\beta_{o'a}}\}]$, when the effectiveness measures are in the range $[0,1]$. This mainly follows from Lemma 1. Given that the joint effectiveness is increasing in the individual effectiveness functions $e_{oa}(x_o)$ and $e_{o'a}(x'_o)$, the lowest

and highest values for $e_{oo'a}(x_o, x_{o'})$, which are respectively 0 and 1, would be realized when the individual effectiveness functions are at their lowest and highest levels. Hence, for $e_{oa}(x_o) = e_{o'a}(x'_o) = e_{oo'a}(x_o, x_{o'}) = 0$, we note that $\rho_{oo'} = 0$ satisfies relationship

$$e_{oo'a}(x_o, x_{o'}) = \rho_{oo'} e_{oa}(x_o) + \rho_{oo'} e_{o'a}(x_{o'}) - \rho^2_{oo'} e_{oa}(x_o) e_{o'a}(x_{o'})$$

For the highest values of $e_{oa}(x_o) = \beta_{oa}$, $e_{o'a}(x'_o) = \beta_{o'a}$, and $e_{oo'a}(x_o, x_{o'}) = 1$, without loss of generality we can consider $\rho^-_{oo'}$ only. For the given values, we have $\rho^-_{oo'} = \frac{\beta_{oa}+\beta_{o'a}-\sqrt{\Delta}}{2\beta_{oa}\beta_{o'a}}$, where $\Delta = (\beta_{oa} + \beta_{o'a})^2 - 4\beta_{oa}\beta_{o'a} = (\beta_{oa} - \beta_{o'a})^2$. It follows that:

$$\begin{aligned}\rho^-_{oo'} &= \frac{\beta_{oa} + \beta_{o'a} - \sqrt{(\beta_{oa} - \beta_{o'a})^2}}{2\beta_{oa}\beta_{o'a}} = \frac{\beta_{oa} + \beta_{o'a} - |\beta_{oa} - \beta_{o'a}|}{2\beta_{oa}\beta_{o'a}} = \frac{2\min\{\beta_{oa}, \beta_{o'a}\}}{2\beta_{oa}\beta_{o'a}} \\ &= \frac{1}{\max\{\beta_{oa}, \beta_{o'a}\}} = \min\{\frac{1}{\beta_{oa}}, \frac{1}{\beta_{o'a}}\} \end{aligned} \tag{A.4}$$

Given that the joint effectiveness function $e_{oo'a}(x_o, x_{o'})$ is increasing in $\rho_{oo'}$ as shown in Lemma 1, there always exists $\rho_{oo'} \in [0, \min\{\frac{1}{\beta_{oa}}, \frac{1}{\beta_{o'a}}\}]$ such that $e_{oo'a}(x_o, x_{o'})$ can be defined for all values of x_o and $x_{o'}$. □

Proof of Proposition 3.2

The proof is by showing that the second derivative of function $I^{k\omega}_{oo'at}(x^{k\omega}_o)$ is non-negative. Given the definition of $e^{k\omega}_{oat}(x^{k\omega}_o)$ in relationship

$$e_{oa}(x_o) = \beta_{oa} - e^{-(\alpha_o x_o - \ln \beta_{oa})} = \beta_{oa} - \beta_{oa} e^{-\alpha_o x_o}$$

we have that:

$$I^{k\omega}_{oo'at}(x^{k\omega}_o) = \ln(1 - \rho_{oo'}\beta^{k\omega}_{oat} + \rho_{oo'}\beta^{k\omega}_{oat} e^{-\alpha_o x^{k\omega}_o})$$

It follows that:

$$\frac{\partial^2 I^{k\omega}_{oo'at}}{\partial {x^{k\omega}_o}^2} = \frac{\rho_{oo'}\beta^{k\omega}_{oat}\alpha^2_o e^{-\alpha_o x^{k\omega}_o}(1 - \rho_{oo'}\beta^{k\omega}_{oat})}{(1 - \rho_{oo'}(\beta^{k\omega}_{oat} - \beta^{k\omega}_{oat} e^{-\alpha_o x^{k\omega}_o}))^2}$$

By Proposition 1, we have $\rho_{oo'} \in [0, \min\{\frac{1}{\beta^{k\omega}_{oat}}, \frac{1}{\beta^{k\omega}_{o'at}}\}]$. Hence, $1 - \rho_{oo'}\beta^{k\omega}_{oat} \geqslant 0$. Moreover, all other components in the numerator are nonnegative by definition. Given that the denominator consists of a squared term, it is also nonnegative, implying that $\frac{\partial^2 I^{k\omega}_{oo'at}}{\partial {x^{k\omega}_o}^2} \geqslant 0$, and that the function $I^{k\omega}_{oo'at}(x^{k\omega}_o)$ is convex in $x^{k\omega}_o$. □

Proof of Proposition 3.3

The proof follows from the definition of the objective function

$$\sum_{\omega\in\Omega} p^{\omega} \left[\sum_{k\in\mathcal{K}} \sum_{s\in\mathcal{S}} \sum_{a\in\mathcal{A}} \sum_{t\in\mathcal{T}} f_{at} l_{ast} Y^{k\omega}_{at} + \sum_{k\in\mathcal{K}} \sum_{o\in\mathcal{O}} x^{k\omega}_o \right]$$

which we can rewrite as:

$$\sum_{\omega\in\Omega} p^{\omega} \left[\sum_{k\in\mathcal{K}} \sum_{a\in\mathcal{A}} \sum_{t\in\mathcal{T}} f_{at} \left(\sum_{s\in\mathcal{S}} l_{ast} \right) Y^{k\omega}_{at} + \sum_{k\in\mathcal{K}} \sum_{o\in\mathcal{O}} x^{k\omega}_o \right]$$

Based on this representation, coefficients in the objective function depend only on the sum of the losses in the set of assets, as opposed to individual asset losses. Given that the parameters l_{ast} are not part of the constraint structure, the optimal resource allocation, and hence the optimal level of cybersecurity budget is independent of the mix of assets that the firm holds. □

Proof of Proposition 3.4

Let $Z(x)$ denote the objective function representing the total costs, while an aggregated notation without any subscripts is used to denote the other parameters and variables in the model. Based on this, the objective can be expressed as:

$$Z(x) = fl(1 - \beta + \beta e^{-\alpha x}) + x$$

Taking the first order derivative of $Z(x)$ with respect to x:

$$\frac{\partial Z(x)}{\partial x} = fl\beta e^{-\alpha x}(-\alpha) + 1$$

The second order derivative of the above function shows convexity as:

$$\frac{\partial^2 Z(x)}{\partial x^2} = f^2 l^2 \beta^2 \alpha^2 e^{-\alpha x} + 1 > 0$$

By setting the first order derivative equal to 0, the optimal investment level can be identified as $x^* = \frac{1}{\alpha} \ln(\alpha\beta fl)$. The ratio of the optimal investment level x^* to the potential total loss fl is then given as $\frac{\ln(\alpha\beta fl)}{\alpha fl}$. Denoting $\alpha\beta fl$ by z, the above ratio can be rewritten as $\beta f(z)$ where $f(z) = \frac{\ln z}{z}$. The function $f(z)$ has a single maximum at $f'(z) = 0$, when $z = e$. Therefore, we have that

$$\frac{x^*}{fl} = \frac{\beta \ln(\alpha\beta fl)}{\alpha fl} \leqslant \frac{\beta}{e}$$

□

Proof of Lemma 4.1

To begin, the second order derivative of objective (4.2) as a function of i can be written as:

$$\sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} \alpha\beta\gamma h^2 x e^{-h(i-z)} e^{-\alpha(x + \frac{\gamma x}{1+e^{-h(i-z)}})} \left(-e^{-2h(i-z)} + \alpha\gamma x e^{-h(i-z)} + 1\right)$$

after collecting the common term. Because the parameters $f_{as}, l_{as}, \alpha, \beta, \gamma, h, x$ are all positive, the term $\sum_{a\in\mathcal{A}} \sum_{s\in\mathcal{S}} \sum_{t\in\mathcal{T}} f_{at} l_{as} \alpha\beta\gamma h^2 x e^{-h(i-z)} e^{-\alpha(x + \frac{\gamma x}{1+e^{-h(i-z)}})}$ is positive as well.

Denoting $y = e^{-h(i-z)}$, the second term $-e^{-2h(i-z)} + \alpha\gamma x e^{-h(i-z)} + 1$ from the second order derivative above can be treated as a quadratic function of $e^{-h(i-z)}$ as $G(y) = -y^2 + \alpha\gamma x y + 1$. Note that $y = e^{-h(i-z)}$ is a monotonically decreasing function when $i \in [0, 1]$, with lower bound $y|_{i=1} = e^{-h(1-z)}$ being a value that is very close to 0, and upper bound $y|_{i=0} = e^{hz}$ is an arbitrarily large value according to the value setting of parameter h and z.

By setting the quadratic function equal to zero and solve for the positive root of $G(y) = -y^2 + \alpha\gamma xy + 1 = 0$, it can be shown easily that function $G(y) \geq 0$ when $y \in [e^{-h(1-z)}, \sqrt{\frac{\alpha^2\gamma^2x^2}{4} + 1} + \frac{\alpha\gamma x}{2}]$ and $G(y) < 0$ when $y \in (\sqrt{\frac{\alpha^2\gamma^2x^2}{4} + 1} + \frac{\alpha\gamma x}{2}, e^{hz}]$. Equivalently, the above condition can be written regarding variable i as

$$\begin{aligned} -e^{-2h(i-z)} + \alpha\gamma x e^{-h(i-z)} + 1 &< 0, \qquad i \in [0, z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4} + 1} + \frac{\alpha\gamma x}{2}\right)}{h}] \\ -e^{-2h(i-z)} + \alpha\gamma x e^{-h(i-z)} + 1 &\geq 0, \qquad i \in [z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4} + 1} + \frac{\alpha\gamma x}{2}\right)}{h}, 1] \end{aligned}$$

Therefore, second order derivative of the objective function (4.2) is positive on $[z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}, 1]$ and negative on $[0, z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}]$. Therefore, the conclusion of Lemma 4.1 follows. □

Proof of Theorem 4.1

We start the proof of Theorem 4.1 by showing monotonicity of the objective (4.2) as a function of i. The first order derivative of objective (4.2) as a function of i is denoted as

$$F'(i) = -\frac{\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \alpha\beta\gamma h x e^{-h(i-z)} e^{-\alpha(x + \frac{\gamma x}{1+e^{-h(i-z)}})}}{\left(1 + e^{-h(i-z)}\right)^2} + \kappa$$

Following the conclusion of Lemma 4.1, the first order derivative of objective $F'(i)$ as is decreasing on $i \in [0, z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}]$, and increasing on $i \in [z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}, 1]$, with a minimum value reached at $i_0 = z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}$.

Next, we note that h is chosen to be a large enough number such that when $i = 0$, $e^{hz} \approx 0$, and when $i = 1$, $\frac{1}{1+e^{-h(1-z)}} \approx 0$. It can be shown by applying L'Hospital's rule that $F'(0) \approx \kappa > 0$ as well as $F'(1) \approx \kappa > 0$. Hence, the first order condition

$F'(i) = 0$ has two roots $i^*_{(1)}$ and $i^*_{(2)}$ if and only if the minimum value $F'(i_0) < 0$, and their values satisfies the inequality $i^*_{(1)} < i_0 < i^*_{(2)}$. The signs of $F'(i)$ can be further determined as: $F'(i) \geq 0, i \in [0, i^*_{(1)}] \cup [i^*_{(2)}, 1]$ and $F'(i) < 0, i \in [i^*_{(1)}, i^*_{(2)}]$

Based on the monotonicity of the first order derivative $F'(i)$, and the conclusion in Lemma 4.1 , the objective function (4.2) then has two local maxima at $i = i^*_{(1)}$ and $i = 1$, and two local minima at $i = i^*_{(2)}$ and $i = 0$. Therefore, the minimum occurs at $i = 0$ if the objective function $F(i)$ has $F(0) > F(i^*_{(2)})$. Hence the conclusion of Theorem 1 follows. □

Proof of Corollary 4.1

From the proof of Theorem 4.1, the minimum value of the first order derivative is $F'(i_0)$ where $i_0 = z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}$. Hence, the first order derivative as a function of i is positive on $i \in [0, 1]$ if $F'(i_0) > 0$, and the objective function would be increasing on $i \in [0, 1]$. The condition of $F'(i_0) > 0$ can be written in explicit form as

$$-\frac{\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\alpha\beta\gamma hx e^{-h(z-\frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}-z)} e^{-\alpha(x+\frac{\gamma x}{1+e^{-h(z-\frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}-z)}})}}{\left(1+e^{-h(z-\frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}-z)}\right)^2} + \kappa > 0$$

and simplified to

$$\kappa \geq \frac{\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}} f_{at}l_{as}\alpha\gamma xh\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)e^{-\alpha\left(x+\frac{\gamma x}{1+\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}}\right)}}{\left(1+\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)^2}$$

as in Corollary 4.1. □

Proof of Proposition 4.1

From the proof of Theorem 4.1, the first order derivative of objective function $F'(i) = -\frac{\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\alpha\beta\gamma hxe^{-h(i-z)}e^{-\alpha(x+\frac{\gamma x}{1+e^{-h(i-z)}})}}{\left(1+e^{-h(i-z)}\right)^2} + \kappa$ is increasing on $i \in [z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}, 1]$. Denote function $T(i) = F'(i) - \kappa$, then function $T(i)$ is also increasing on $i \in [z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}, 1]$.

Next, conditioned on $\kappa \leq \frac{\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}} f_{at}l_{as}\alpha\gamma xh\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)e^{-\alpha\left(x+\frac{\gamma x}{1+\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}}\right)}}{\left(1+\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)^2}$, there exist $i^* > z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}$ such that $F'(i^*) = 0$ and $T(i^*) = -\kappa$. When κ increase to a greater value κ_l but still satisfies the condition above, there also exist a value of $i_l^* > z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}$ such that $T(i_l^*) = -\kappa_l$. As function $T(i)$ is increasing on $i \in [z - \frac{\ln\left(\sqrt{\frac{\alpha^2\gamma^2x^2}{4}+1}+\frac{\alpha\gamma x}{2}\right)}{h}, 1]$, it can be concluded by the property of inverse function that $i_l^* < i^*$ since $T(i_l^*) < T(i^*)$. Therefore, the conclusion of Proposition 4.1 holds. □

Proof of Theorem 5.1

The proof of Theorem 5.1 can be seen as a variation of the proof of Theorem 4.1. Specifically, by replacing notation β, x, and α with $\beta_{_B}$, $x_{_B}$, and α_B; replacing γ, i, and κ with $\gamma_{_A}$, $i_{_A}$, and $\kappa_{_A}$, the result of Theorem 5.1 follows. □

Proof of Proposition 5.1

To proof the item (1) in Proposition 5.1, we first show the convexity of the fair price under equal benefit strategy as a function of technology investment level $x_{_B}$. In expanded form, the fair price as a function of $x_{_B}$ can be written as:

$$p^{eb}(x_{_B}) = g(x_{_B},0) - g(x_{_B},i_{_A}) = \frac{1}{2}\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\Bigg(\beta_{_B}e^{-\alpha_{_B}x_{_B}} - \beta_{_B}e^{-\alpha_{_B}\left(x_{_B}+\gamma_{_A}\phi(i_{_A})x_{_B}\right)}\Bigg) - \frac{1}{2}\kappa_{_A}i_{_A} \quad \text{(A.5)}$$

The first order derivative of $x_{_B}$ is given as:

$$\frac{\partial p^{eb}(x_{_B})}{\partial x_{_B}} = \frac{1}{2}\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B}\Bigg(\left(1+\gamma_{_A}\phi(i_{_A})x_{_B}\right)e^{-\alpha_{_B}\left(1+\gamma_{_A}\phi(i_{_A})x_{_B}\right)x_{_B}} - e^{-\alpha_{_B}x_{_B}}\Bigg) \quad \text{(A.6)}$$

The second order derivative of $x_{_B}$ is given as:

$$\frac{\partial^2 p^{eb}(x_{_B})}{\partial x_{_B}^2} = \frac{1}{4}\left(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_{_B}\alpha_{_B}\right)^2 e^{-\alpha_{_B}x_{_B}}\left(1-\left(1+\gamma_{_A}\phi(i_{_A})x_{_B}\right)e^{-\alpha_{_B}x_{_B}}\right) \quad \text{(A.7)}$$

It can be shown by testing the first order derivative and second order derivative as in (A.6) and (A.7) that $p^{eb}(x_{_B})$ is monotonically increasing on $\left[0, \frac{\ln(1+\gamma_{_A}\phi(i_{_A}))}{\alpha_{_B}\gamma_{_A}\phi(i_{_A})}\right)$ concavely, and monotonically decreasing on $\left(\frac{\ln(1+\gamma_{_A}\phi(i_{_A}))}{\alpha_{_B}\gamma_{_A}\phi(i_{_A})}, \infty\right)$ convexly. Therefore, item (1) of Proposition 5.1 follows.

The proof of item (2) in Proposition 5.1 follows the same approach as in the proof of 4.1. To proof item (2) in Proposition 5.1, we first consider the fair price as a function of $i_{_A}$:

$$p^{eb}(i_{_A}) = g(x_{_B},0) - g(x_{_B},i_{_A}) = \frac{1}{2}\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\Bigg(\beta_{_B}e^{-\alpha_{_B}x_{_B}} - \beta_{_B}e^{-\alpha_{_B}\left(x_{_B}+\gamma_{_A}\phi(i_{_A})x_{_B}\right)}\Bigg) - \frac{1}{2}\kappa_{_A}i_{_A} \quad \text{(A.8)}$$

Following the proof of Theorem 4.1, it can be shown that function (A.8) has two local minima at $i_{_A} = i^*_{_{A_{(0)}}}$ and $i_{_A} = 0$ and two local maxima at $i_{_A} = i^*_{_{A_{(1)}}}$ and $i_{_A} = 1$, where $i_{_A} = i^*_{_{A_{(0)}}}$ and $i_{_A} = i^*_{_{A_{(1)}}}$ are the two solutions of $\frac{\partial p^{eb}(i_{_A})}{\partial i_{_A}} = 0$. Moreover, the condition

$i^*_{A_{(0)}} \geq z - \frac{\ln\left(\sqrt{\frac{\alpha_B^2\gamma_B^2 x_B^2}{4}+1}+\frac{\alpha_B\gamma_A x_B}{2}\right)}{h}$ has ensured that $p^{eb}(i_A) \geq p^{eb}(0)$. Therefore, the conclusion of item (2) in Proposition 5.1 follows. □

Proof of Theorem 5.2

The close-form expression of the MEB for Firm B before and after information sharing can be solved following similar manner as discussed in the proof of Proposition 3.4. By solving for the first order condition of Firm B's total cost before and after information sharing:

$$Before: \quad \frac{\partial g(x_B, 0)}{\partial x_B} + 1 = -\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_B \alpha_B e^{-\alpha_B x_B} + 1 = 0$$

$$After: \quad \frac{\partial g(x_B, i_A)}{\partial x_B} + 1$$

$$= -\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as} \beta_B \big(1+\gamma_A\phi(i_A)\big)\alpha_B e^{-\alpha_B\left(1+\gamma_A\phi(i_A)\right)x_B} + 1 = 0$$

We can then obtain the close-form expression of x_B^* and x_B^{**} as:

$$x_B^* = \frac{\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\beta_B\alpha_B)}{\alpha_B} \tag{A.9}$$

$$x_B^{**} = \frac{\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\beta_B\big(1+\gamma_A\phi(i_A)\big)\alpha_B)}{\big(1+\gamma_A\phi(i_A)\big)\alpha_B} \tag{A.10}$$

Plugging in (A.9) and (A.10) into the fair price under equal benefit strategy as given by (5.16), the results of Theorem 5.2 follows. □

Proof of Corollary 5.1

We first note in this proof that, under equal benefit strategy, the payoff for Firm A and Firm B are equal. When Firm B always invest according to the pre-information sharing MEB, the payoffs for each firm is:

$$g(x_B^*, 0) - g(x_B^*, i_A) - p$$

Whereas when Firm B adjust its technology investment according to new MEB after information sharing, the payoffs for each firm is:

$$g(x_{_B}^*, 0) - g(x_{_B}^{**}, i_{_A}) + x_{_B}^* - x_{_B}^{**} - p$$

The increase in overall payoffs by re-optimization can be expressed as:

$$g(x_{_B}^*, i_{_A}) - g(x_{_B}^{**}, i_{_A}) + x_{_B}^* - x_{_B}^{**} \tag{A.11}$$

Plugging in the $x_{_B}^*$ and $x_{_B}^{**}$ values as given in (A.9) and (A.10), we have:

$$g(x_{_B}^*, i_{_A}) = \sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}(1-\beta_{_B}) + \left(\frac{1}{\alpha_{_B}}\right)^{1+\gamma_{_A}\phi_{_A}(i_{_A})} \tag{A.12}$$

$$g(x_{_B}^{**}, i_{_A}) = \sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}(1-\beta_{_B}) + \frac{1}{\alpha_{_B}(1+\gamma_{_A}\phi_{_A}(i_{_A}))} \tag{A.13}$$

Combining (A.9)-(A.10), (A.12)-(A.12) with (A.11), the conclusion of Corollary 5.1 follows. □

Proof of Theorem 5.3

The proof of Theorem 5.3 is similar to that of Theorem 5.2. By setting the first order derivative of Firm A's total costs before and after sharing information as functions of $x_{_A}$, respectively, we have:

$$Before: \quad \frac{\partial g(x_{_A}, 0)}{\partial x_{_A}} + 1 = -\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\beta_{_A}\alpha_{_A} e^{-\alpha_{_A} x_{_A}} + 1 = 0$$

$$After: \quad \frac{\partial g(x_{_A}, i_{_B})}{\partial x_{_A}} + 1$$

$$= -\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at} l_{as}\beta_{_A}\big(1+\gamma_{_B}\phi(i_{_B})\big)\alpha_{_A} e^{-\alpha_{_A}\left(1+\gamma_{_B}\phi(i_{_B})\right)x_{_A}} + 1 = 0$$

We can then obtain the close-form expression of x_A^* and x_A^{**} as:

$$x_A^* = \frac{\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_A\alpha_A)}{\alpha_A} \tag{A.14}$$

$$x_A^{**} = \frac{\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_A\big(1+\gamma_B\phi(i_B)\big)\alpha_A)}{\big(1+\gamma_B\phi(i_B)\big)\alpha_A} \tag{A.15}$$

Plugging in (A.9)-(A.10), (A.16)-(A.17) into the fair price under equal benefit strategy and exchange return strategies as given by (5.36)-(5.37), the results of Theorem 5.3 follows. □

Proof of Theorem 5.4

The proof of Theorem 5.4 follows the same approaches as in the proofs of Theorem 5.2 and 5.3. We first show the MEBs of technology investment for Firm R before and after information sharing by solving the first order conditions:

$$Before: -\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_R\alpha_R e^{-\alpha_R x_R} + 1 = 0$$

$$After: -\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_R\big(1+\sum_{I\in\Gamma,I\neq R}\gamma_I\phi(i_I)\big)\alpha_R e^{-\alpha_A\left(1+\sum_{I\in\Gamma,I\neq R}\gamma_I\phi(i_I)\right)x_R} + 1 = 0$$

Where the close-form expression of x_R^* and x_R^{**} can be given as:

$$x_R^* = \frac{\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_R\alpha_R)}{\alpha_R} \tag{A.16}$$

$$x_R^{**} = \frac{\ln\big(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_R\big(1+\sum_{I\in\Gamma,I\neq R}\gamma_I\phi(i_I)\big)\alpha_R\big)}{\big(1+\sum_{I\in\Gamma,I\neq R}\gamma_I\phi(i_I)\big)\alpha_R} \tag{A.17}$$

The MEBs for other firm Ks can be obtained in a similar fashion as:

$$x_K^* = \frac{\ln(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_K\alpha_K)}{\alpha_K} \tag{A.18}$$

$$x_K^{**} = \frac{\ln\big(\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{T}} f_{at}l_{as}\beta_K\big(1+\sum_{I\in\Gamma,I\neq K}\gamma_I\phi(i_I)\big)\alpha_K\big)}{\big(1+\sum_{I\in\Gamma,I\neq K}\gamma_I\phi(i_I)\big)\alpha_K} \tag{A.19}$$

Plugging in (A.16)-(A.19) into the fair prices under equal benefit and exchange return strategies as given by (5.55) and (5.56), the results of Theorem 5.4 follows. □

BIBLIOGRAPHY

Arora, A., A. Fosfuri. 2005. Pricing diagnostic information. *Management Science* **51**(7) 1092–1100.

Baker, W. 2009. Data breach investigations supplemental report. Tech. rep., Verizon Inc., New York City, NY.

Baldwin, A., Y. Beres, G. Duggan, M. Mont, H. Johnson, C. Middup, S. Shiu. 2013. Economic methods and decision making by security professionals. *Economics of Information Security and Privacy III*. Springer, 213–238.

Berg, N., C. Chen, M. Kantarcioglu. 2013. Experiments in information sharing. arXiv preprint: 1305.5176.

Birge, J., F. Louveaux. 2011. *Introduction to stochastic programming*. Springer Science & Business Media, New York City, NY.

Bojanc, R., B. Jerman-Blažič. 2008. Towards a standard approach for quantifying an ict security investment. *Computer Standards & Interfaces* **30**(4) 216–222.

Brunnermeier, M. 2001. *Asset pricing under asymmetric information: Bubbles, crashes, technical analysis, and herding*. Oxford University Press on Demand.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2004. A model for evaluating IT security investments. *Communications of the ACM* **47**(7) 87–92.

Cavusoglu, H., S. Raghunathan, W. Yue. 2008. Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems* **25**(2) 281–304.

Cezar, A., H. Cavusoglu, S. Raghunathan. 2013. Outsourcing information security: contracting issues and security implications. *Management Science* **60**(3) 638–657.

Chen, F. 2003. Information sharing and supply chain coordination. *Handbooks in Operations Research and Management Science* **11**(2) 341–421.

Clarke, R. 1983. Collusion and the incentives for information sharing. *The Bell Journal of Economics* **14**(2) 383–394.

Dantzig, G. 1955. Linear programming under uncertainty. *Management Science* **1**(3-4) 197–206.

Edmans, A., M. Heinle, C. Huang. 2013. The real costs of disclosure. Tech. rep., National Bureau of Economic Research, Cambridge, MA.

Elliott, R. 1994. Costs and benefits of business information disclosure. *Accounting Horizons* **8**(4) 80.

Gal-Or, E. 1985. Information sharing in oligopoly. *Econometrica: Journal of the Econometric Society* **53**(2) 329–343.

Gal-Or, E., A. Ghose. 2005. The economic incentives for sharing security information. *Information Systems Research* **16**(2) 186–208.

Gao, X., W. Zhong. 2016. A differential game approach to security investment and information sharing in a competitive environment. *IIE Transactions* **48**(6) 511–526.

Gao, X., W. Zhong, S. Mei. 2013. Information security investment when hackers disseminate knowledge. *Decision Analysis* **10**(4) 352–368.

Gao, X., W. Zhong, S. Mei. 2014. A game-theoretic analysis of information sharing and security investment for complementary firms. *Journal of the Operational Research Society* **65**(11) 1682–1691.

Gao, X., W. Zhong, S. Mei. 2015. Security investment and information sharing under an alternative security breach probability function. *Information Systems Frontiers* **17**(2) 423–438.

Garvey, P, S. Patel. 2014. Cybersecurity economics: measuring economic-benefit returns on cybersecurity investments - a family of analytical frameworks. *Proceedings of the IEEE Military Communications Conference*. Baltimore, MD.

Gavirneni, S., R. Kapuscinski, S. Tayur. 1999. Value of information in capacitated supply chains. *Management Science* **45**(1) 16–24.

Gordon, L., M. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* **5**(4) 438–457.

Gordon, L., M. Loeb. 2005. *Managing cybersecurity resources: a cost-benefit analysis*. McGraw-Hill, New York City, NY.

Gordon, L., M. Loeb, W. Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* **22**(6) 461–485.

Guttman, B., E. Roback. 1995. *An introduction to computer security: the NIST handbook*. DIANE Publishing, Darby, PA.

Hausken, K. 2006. Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers* **8**(5) 338–349.

Hausken, K. 2007. Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy* **26**(6) 639–688.

Hendriks, C. 2006. When the forum meets interest politics: strategic uses of public deliberation. *Politics & Society* **34**(4) 571–602.

Herson, D., P. Davis, Y. Klein, U. Essen, H. Tabuchi. 2003. Generally accepted information security principles. Tech. rep., National Institute of Standards and Technology, Reston, VA.

Hoo, K. 2000. How much is enough? A risk management approach to computer security. Ph.D. thesis, Stanford University.

Huang, C., Q. Hu, R. Behara. 2008. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics* **114**(2) 793–804.

Kall, P., S. Wallace, P. Kall. 1994. *Stochastic programming*. Springer.

Kessel, P., K. Allan. 2013. Under cyber attack: E&Y's global information security survey 2013. Tech. rep., Ernst & Young, Hartford, CT.

Kwon, J., M. Johnson. 2011. An organizational learning perspective on proactive vs. reactive investment in information security. *Proceedings of the Workshop on the Economics of Information Security*. Fairfax, VA.

Lee, H., V. Padmanabhan, S. Whang. 1997. Information distortion in a supply chain: the bullwhip effect. *Management Science* **43**(4) 546–558.

Lee, H., K. So, C. Tang. 2000. The value of information sharing in a two-level supply chain. *Management Science* **46**(5) 626–643.

Lewis, J. 2018. Economic impact of cybercrime – no slowing down. Tech. rep., McAfee, Inc., Santa Clara, CA.

Li, L. 1985. Cournot oligopoly with information sharing. *The RAND Journal of Economics* **16**(4) 521–536.

Li, L. 2002. Information sharing in a supply chain with horizontal competition. *Management Science* **48**(9) 1196–1212.

Lipner, S. 2004. The trustworthy computing security development lifecycle. *Proceedings of the Computer Security Applications Conference*. Tucson, AZ.

McAfee. 2013. McAfee product&technology support lifecycle. URL `https://www.mcafee.com/enterprise/en-us/support/product-eol.html`. Retrieved January 6, 2013.

Noyan, N. 2012. Two-stage stochastic programming involving CVaR with an application to disaster management. *Computers and Operations Research* **39**(3) 541–559.

Oberheide, J., E. Cooke, F. Jahanian. 2008. CloudAV: N-Version antivirus in the network cloud. *Proceedings of the USENIX Security Symposium*. San Jose, CA.

Peters, S. 2009. CSI computer crime and security survey. Tech. rep., Computer Security Institute, New York City, NY.

Ponemon, L. 2011. Cost of data breach study: United States. Tech. rep., Ponemon Institute, Traverse City, MI.

Ponemon, L. 2016a. 2016 cost of cyber crime study & the risk of business innovation. Tech. rep., Ponemon Institute, Traverse City, MI.

Ponemon, L. 2016b. 2016 ponemon cost of data breach study. Tech. rep., Ponemon Institute, Traverse City, MI.

Rees, L.P., J.K. Deane, T.R. Rakes, W.H. Baker. 2011. Decision support for cybersecurity risk planning. *Decision Support Systems* **51**(3) 493–505.

Richardson, R. 2010. CSI computer crime and security survey. Tech. rep., Computer Security Institute, New York City, NY.

Rockafellar, R., S. Uryasev. 2000. Optimization of conditional value-at-risk. *Journal of Risk* **2** 21–42.

Rogers, E. 2010. *Diffusion of innovations*. Simon and Schuster, New York City, NY.

Rowe, B., M. Gallaher. 2006. Private sector cyber security investment strategies: an empirical analysis. *Proceedings of the Workshop on the Economics of Information Security*. Cambridge, UK.

Sawik, T. 2013. Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems* **55**(1) 156–164.

Shang, W., A. Ha, S. Tong. 2015. Information sharing in a supply chain with a common retailer. *Management Science* **62**(1) 245–263.

Shapiro, A., D. Dentcheva. 2014. *Lectures on stochastic programming: modeling and theory*. SIAM, Philadelphia, PA.

Shapiro, C. 1986. Exchange of cost information in oligopoly. *The Review of Economic Studies* **53**(3) 433–446.

Sharpe, S. 1990. Asymmetric information, bank lending, and implicit contracts: a stylized model of customer relationships. *The Journal of Finance* **45**(4) 1069–1087.

Smith, E., S Pike. 2017. Worldwide semiannual security spending guide 2017. URL `https://www.idc.com/getdoc.jsp?containerId=IDC_P33461`. Retrieved May 10, 2017.

Solak, S., J-P. Clarke, E. Johnson, E. Barnes. 2010. Optimization of R&D project portfolios under endogenous uncertainty. *European Journal of Operational Research* **207**(1) 420–433.

Stoneburner, G., A. Goguen, A. Feringa. 2002. Risk management guide for information technology systems. Tech. rep., National Institute of Standards and Technology, Reston, VA.

Symantec. 2014. Symantec corporation enterprise support. URL `https://support.symantec.com/en_US.html`. Retrieved December 18, 2012.

Varian, Hal R. 1996. Pricing electronic journals. *D-Lib Magazine* **2**(6) 1–7.

Verizon. 2012. Data breach investigation industry snapshots. Tech. rep., Verizon, Inc., New York City, NY.

Verizon. 2014a. Data breach investigation industry snapshots. Tech. rep., Verizon, Inc., New York City, NY.

Verizon. 2014b. Data breach investigation report. Tech. rep., Verizon, Inc., New York City, NY.

Verizon. 2015. 2015 data breach investigations report. Tech. rep., Verizon RISK Lab, New York, NY.

Vomhof, J. 2013. Target's data breach fraud cost could top $1 billion, analyst says. *Charlotte Business Journal*, 3 February 2014.

Wallace, S., W. Ziemba. 2005. *Applications of stochastic programming*. SIAM, Philadelphia, PA.

Weiss, N Eric. 2015. *Legislation to facilitate cybersecurity information sharing: Economic analysis*. Congressional Research Service.

Wets, R. 1983. Stochastic programming: Solution techniques and approximation schemes. *Mathematical Programming: the State of the Art*. Springer, 566–603.

Willemson, J. 2006. On the Gordon & Loeb model for information security investment. *Proceedings of the Workshop on the Economics of Information Security*. Philadelphia, PA.

Yu, Z., H. Yan, T. Edwin. 2001. Benefits of information sharing with supply chain partnerships. *Industrial Management & Data Systems* **101**(3) 114–121.