CERIAS Tech Report 2010-36
Entitled Essays on Information Risk Management in Electronic Markets
by Juhee Kwon
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Juhee Kwon

Entitled Essays on Information Risk Management in Electronic Markets

For the degree of DOCTOR OF PHILOSOPHY

Is approved by the final examining committee:

Jacquelyn R. Rees Ulmer
Chair

Kemal Altinkemer

Manohar U. Kalwani

Tawei (David) Wang

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Jacquelyn R. Rees Ulmer

Approved by: Mark E. Bagnoli 06/23/2010
Head of the Graduate Program Date

Graduate School Form 20
(Revised 1/10)

PURDUE UNIVERSITY
GRADUATE SCHOOL

Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:
Essays on Information Risk Management in Electronic Markets

For the degree of DOCTOR OF PHILOSOPHY

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Teaching, Research, and Outreach Policy on Research Misconduct (VIII.3.1)*, October 1, 2008.*

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

Juhee Kwon
Printed Name and Signature of Candidate

06/23/2010
Date (month/day/year)

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/viii_3_1.html

ESSAYS ON INFORMATION RISK MANAGEMENT IN ELECTRONIC MARKETS

A Dissertation !

Submitted to the Faculty !

of

Purdue University

by

Juhee Kwon

In Partial Fulfillment of the !

Requirements for the Degree !

of

Doctor of Philosophy

August 2010 !

Purdue University

West Lafayette, Indiana

UMI Number: 3444806

All rights reserved !

INFORMATION TO ALL USERS !
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion. !

UMI 3444806
Copyright 2011 by ProQuest LLC. !
All rights reserved. This edition of the work is protected against
unauthorized copying under Title 17, United States Code.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

ACKNOWLEDGEMENTS

I wish first to thank my advisor, Dr. Jacquelyn R. Rees Ulmer. She has provided all the guidance and assistance during my doctoral studies. I really appreciate the weekly meetings held for my research and she was there whenever I needed advice and support. I also would like to express the deepest appreciation to my committee members, Dr. Kemal Altinkemer, Dr. Manohar U. Kalwani, and Dr. Tawei (David) Wang for serving on my thesis committee and for their very valuable comments, encouragements, and time.

Finally, I would like to thank all my family members and friends for believing in me and for their encouragement. No matter what I want to do, they always support my decision and motivate me to achieve more.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Kwon, Juhee. Ph.D., Purdue University, August 2010. Essays on Information Risk Management in Electronic Markets. Major Professor: Jacquelyn R. Rees Ulmer.

Within the modern, hyper-connected business landscape with the pervasive and extensive usage of IT, effective and efficient information risk management is imperative for firms to support inside IT governance as well as the outside communities or markets that they service. Therefore, this dissertation empirically studies a firm's internal and external strategies for ensuring information risk management in two essays.

First, information risk management is about not just technology, but also is about all business processes involving policies and practices for ensuring confidentiality, integrity and availability of information assets. Then, successful information risk management can be achieved only if top level executives give it their complete support and commitment across all required functions of a firm. Therefore, the first essay conducts a comprehensive analysis to investigate the effects of IT executive status in a Top Management Team (TMT) on information risk management.

Second, firms have collected information about customers through websites to utilize high-quality marketing techniques such as personalized services or offerings with consequences that are potentially both beneficial and harmful to customers. The second essay aims to find out the impacts of different privacy-related aspects such as policies and

practices on consumer willingness to provide personal information over the Internet, particularly in regards to website types and the types of requested information.

The results of the dissertation can give firms insights into how to internally set IT executives' compensation strategies as well as to delegate authority and responsibility for ensuring confidentiality, integrity, and availability of information assets. Also, they shed light on how to externally set up their privacy practices for customer willingness to invest in a long-term business relationship.

CHAPTER 1. INTRODUCTION

As *e*-Commerce has emerged as an innovative model of doing business, organizations have successfully leveraged information technology in their business strategies, products, and services over the Internet (Kalikiri K., 2009). As the Internet has become the primary interface through which their employees, business partners as well as customers interact, a large portion of corporate and consumer data have traveled across the Internet and information has, rapidly become the key business differentiator. Hence, the information needs to be accurate and up-to-date to enable an enterprise to make good business decisions and it needs to be available when the business requires access to it. Failure of information risk management to meet various transaction needs in an organized and secure environment could create losses of both reputation and sales. For example, a recent survey showed that an enterprise's information breaches significantly resulted in damage to reputation and brand by 85% of respondents (Ernst & Young, 2008). Therefore, information risk management has been of critical concern to companies as well as a source of competitive advantage. It needs to become a real enterprise-wide strategic issue, taking it out of the IT domain and aligning it with a corporate governance approach. However, information risks are easily overlooked by those who focus only on the IT side of the equation, failing to see that human resources and policies are the most likely cause of any risk in information systems (Dameri, 2008; N. Y. Kim, Robles, Cho, Lee, & Kim, 2008).

Information risk management has recently become a thriving and fast-moving research area. Researchers and practitioners have strived to understand and assess how an organization should go about implementing the components of information risk management, which combines technical, procedural, and people-orientated components for the purpose of minimizing risks posed to information assets as well as enhancing an organization's capability to manage risks. A large body of research argues that information risk management requires a more holistic point-of-view rather than a simple, one-dimensional position, the outputs of which lack applicability in the field of information risk management (Armstrong & Sambamurthy, 1996; Dhillon & Backhouse, 2001; Ransbotham & Mitra, 2009; Sambamurthy & Zmud, 1999). Most of all, the integration of technical and human aspects of information security can provide a better understanding of the different facets of information risks for managers and therefore may be better able to make informed choices (Kokolakis & Kiountouzis, 2000).

This dissertation approaches the issues in information risk management from two different perspectives in order to provide insights into (1) how an enterprise can set IT executives compensation strategies as well as delegate authority and responsibility to ensure its information risk management as internally part of corporate governance, (2) how the effect of customers' privacy concerns could be affected by a firm's privacy protection and expected benefits, and how types of requested information and website types moderate the effects of privacy concerns, awareness of privacy protection and expected benefits on consumer willingness to provide personal information as externally part of consumer relationship management on electronic channels.

The first essay provides a comprehensive analysis to investigate the effects of IT executive status in a Top Management Team (TMT) on information risk management. The study employs logistic regression to examine 1,462 firms from 2003 to 2008 with publicly announced information breaches, IT internal control weaknesses as identified by external auditors, and executive compensation data. The results demonstrate that IT executive involvement in a TMT and fair compensation levels across and within firms are associated with a decrease in IT internal controls weaknesses and information breaches, while IT executive turnover is associated with their increases. The paper also investigates how contract types moderate the effect of IT executive compensation under task uncertainty of information risk management. The effect of compensation among IT executives across firms is stronger with a behavior-based contract on successful information risk management, rather than with an outcome-based contract. On the other hand, if there is a pay difference between IT and non-IT executives within a firm, the effect is better with an outcome-based contract rather than with a behavior-based contract. As a comprehensive analysis across organizational strategy, accounting, and information systems, this study gives firms new insights into how to set compensation strategies as well as delegate authority and responsibility for ensuring information risk management.

The second essay empirically develops and examines an extended model for consumer willingness for information disclosure, in which privacy concerns and benefits are competing and where the effects of awareness of privacy protection may influence each other. In particular, the paper hypothesizes a set of the interaction effects of various

environmental factors (i.e., types of requested information and website types) on the relationships between privacy-related factors and consumer willingness to provide personal information. The Internet survey was conducted from March 2009 to May 2009 and had 685 respondents, of which 615 were valid. A Structural Equation Model (SEM) approach using Partial Least Squares (PLS) by incorporating latent multiplicative variables was employed to test the hypotheses of this study. The completely standardized path coefficients of the structural model provide evidence for the hypothesized interaction effects by examining the role of website types on the strength of the relationships among privacy concerns, awareness, expected benefits and willingness to provide financial/overall personal information. These results suggest researchers and practitioners should not assume that personal information disclosure reflects simply a lack of privacy concerns, but recognize consumer willingness to disclose personal information could be increased by making consumers more aware of the firm's privacy protection and benefits based on its service types and types of requested information. Then, website providers need to be vigilant in seeking ways to promote benefits exchanged with personal information and their privacy protection practices.

This dissertation provides two different perspectives of studying information risk management. The first essay emphasizes how enterprises should set up internal strategies such as compensation strategies and authority delegation for ensuring information risk management across a firm. Since information risks are not just about technology but also about business process with entire organizational involvement, it is

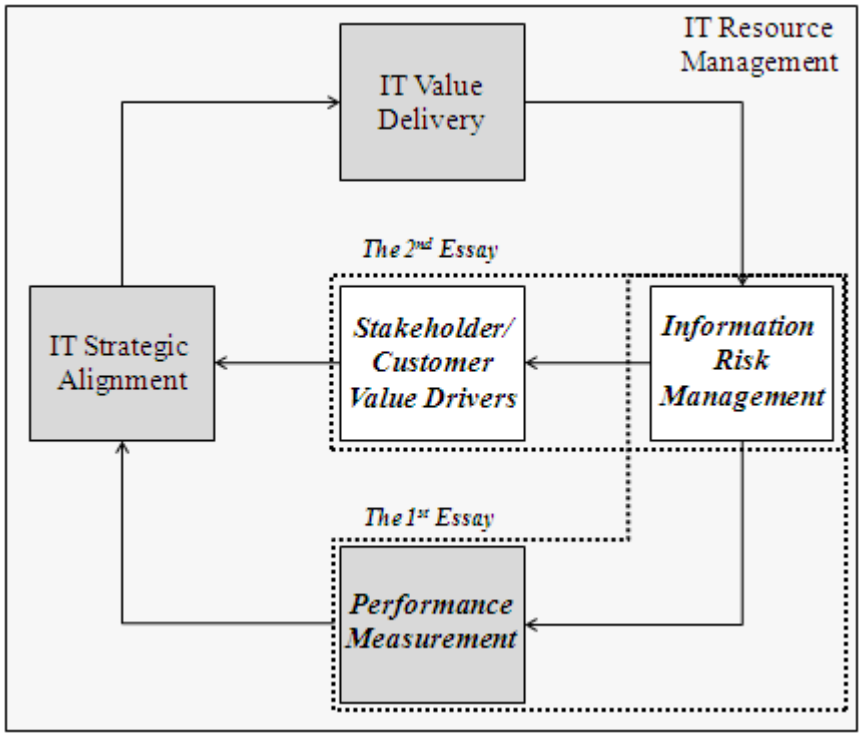
important for enterprises to appropriately align finance and human resources with their security policy and practices for information assets. The second essay formally investigates how information privacy concerns influence the extent of consumer willingness to provide several types of personal information (e.g., contact, demographic, browsing habit, and finance information) with website types and how expected benefits influence the extent of consumer willingness to provide such information. More importantly, this study can give firms insights into how a firm can provide privacy protection, benefits, and specific information practices to motivate consumers to disclose each type of personal information based on its website type.

The remainder of the dissertation is organized as follows. Chapter 2 contains general literature review for this dissertation. Chapter 3 includes the first essay which examines the relationship between information risk management and IT Executives' Status in a Top Management Team. The theoretical framework and the results are discussed in the subsections, and Chapter 4 presents the second essay where we discuss the effects of privacy concerns, awareness of privacy protection, and expected benefits on customer willingness with types of personal information and website types. Lastly, Chapter 5 concludes the dissertation.

CHAPTER 2. LITERATURE REVIEW

2.1 Overview

The universal need to demonstrate good IT governance to shareholders and customers is the driver for risk management and control over IT in organizations based on a clear risk management policy and comprehensive control framework (ITGI, 2005; Li, Lim, & Wang, 2007; Raghupathi, 2007).



Source: Board Briefing on IT Governance (ITGI, 2005)

Figure 2.1 Focus Areas of IT Governance

Figure 2.1 depicted how the main focus areas for IT governance are related. This dissertation focuses on information risk management, addressing the safeguarding of IT

assets, controls and continuity of operations with two different perspectives: from an internal perspective, performance measurement related to information breaches and IT internal control weaknesses, and from an external perspective, consumer value drivers to provide high-quality products or services.

Practitioners and regulators have been concerned about operational and systemic risk, within which technology risk and information assurance issues are prominent (ITGI, 2006; Li, et al., 2007). Previous literature has emphasized that risk management initiatives point to the utter dependence of all enterprises on IT infrastructures and risk awareness of senior corporate executives, since all information risk management effort in an IT context, impacts future investments in technology, the extent to which IT assets are protected and the level of assurance required (Armstrong & Sambamurthy, 1996; Enns, Huff, & Higgins, 2003; McFadzean, Ezingeard, & Birchall, 2007; Preston, Chen, & Leidner, 2008; Smaltz, Sambamurthy, & Agarwal, 2004).

As IT becomes more critical for enterprise survival in addition to enabling growth, information risk management requires planned and purposeful management processes, which include sustaining awareness of the strategic role of IT at top management level, creating IT guiding principles, monitoring the business impact of the IT, and evaluating benefits delivered by IT projects (Dhar & Sundararajan, 2007; Posthumus & von Solms, 2005; Raghupathi, 2007). Then, successful information risk management surely drives competitive strategies, increases overall revenue generation, improves customer satisfaction and/or assures customer retention.

Thus, this dissertation approaches information risk management with two different perspectives: an internal strategy perspective in embedding accountability into the enterprise and a customer perspective in providing high-quality services such as personalization by consumer self-disclosure. The goal of this literature review is to develop a better understanding of the two perspectives of information risk management. In order to do this, we must first understand how IT executive status in TMT affects a firm's performance on information risk management. We therefore begin our review by articulating why is important that a set of responsibilities and practices exercised by executive management with the goal of providing strategic direction and ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. We then review individuals' behavioral intentions (or willingness) and actions with privacy-related factors and how individuals' willingness to provide personal information comprises their privacy concerns in the e-Commerce context.

2.2 Information Risk Management for Performance Measurement

Information risk management encompasses technology, business processes, and people. Many organizations have considered information as an important asset and therefore information risk management has become the common denominator in all areas of risk addressed by corporate governance standards including strategic, financial, technical, operational, and regulatory risk (Johnston & Hale, 2009). Information risk management should be recognized as a fundamental governance process rather than simply a technology management issue. This is critical in meeting overall governance objectives and fully realizing the benefits of effective information risk management to

the entire enterprise (McFadzean, et al., 2007). Assuring security, privacy, reliability of information been then emphasized again and again as a main IT practice across all functional departments. Since many organizations have considered information as an important asset, information risk management has become the common denominator in all areas of risk addressed by corporate governance standards including strategic, financial, technical, operational, and regulatory risk.

Most of all, information risk management should be managed as an enterprise issue, horizontally, vertically, and cross-functionally throughout the organization. To do so, executive leaders understand their accountability and responsibility with respect to information risk management for the organization, for their stakeholders and customers in the markets they serve (Cai, Keasey, & Short, 2006; Posthumus & von Solms, 2005; von Solms, 2005). Executive leaders visibly engaged in the management and oversight of the enterprise risk management activities and support this work with adequate financial resources, effective management, risk based policies, and annual reviews and audit (Straub & Welke, 1998; J. Wang, Chaudhury, & Rao, 2008).

Researchers and practitioners have argued that successful information risk management can be achieved only through effective board oversight, in which board of directors has to control risk using a comprehensive perspective across an entire organization (K. Campbell, Gordon, Loeb, & Zhou, 2003; Gordon & Loeb, 2002; Staw, 1980). Thus, information risk management is considered an integral part of normal strategic, capital, and operational cycles and has achievable, measurable objectives that are integrated into strategic and operation plans, and implemented with effective

controls and metrics across an organization (Johnston & Hale, 2009; Sale, 2006). The performance of these tasks could be measured against performance parameters in information security and IT controls. Given the cross-functional role of IT executives across an entire organization, we argue that it is imperative for IT executives to be deeply involved in Top Management Teams (TMTs) and highly rewarded for their essential roles with compensation in order to lead strategic information risk management initiatives. As a result, executive leadership has become a key ingredient in any successful strategic information security initiative (Johnston & Hale, 2009; Raghupathi, 2007). Fair authority and responsibility should be assigned to IT executives, who are able to strategically and operationally conduct liaison activities between the IT group and other business units (Enns, et al., 2003; Mitchell, 2006; Preston, et al., 2008).

Therefore, it is imperative to understand the impact of IT executive involvement in a TMT and compensation on IT internal controls as well as information security, since it helps a firm successfully set compensation strategies for executives as well as delegate authority and responsibility for ensuring confidentiality, integrity and availability of information assets.

2.3 Information Risk Management for a Customer Value Driver

A common motivation for organizations to invest in information risk management is to safeguard firms' confidential data, as well as their customers' personal information. Over the past few years, privacy incidents have been announced frequently enough to attract researchers. Then, there is a significant body of related research. Some previous research investigated the causes of privacy concerns which consumers perceive (Milne

& Boza, 1998; Petrison & Wang, 1993; J. Phelps, Nowak, & Ferrell, 2000; Sheehan & Hoy, 1999). This stream of research primarily contributes a better understanding of the factors that underlie privacy concerns and the ways in how policy and practices can be employed to reduce consumer concerns. Milne and Boza (1998) presented a model of the antecedents of concern and trust. Among the variables tested, their findings indicate that trust and perceived information control are negatively related to concern, while attitude toward a buyer-seller relationship in direct marketing is positively related to trust. Phelps et al. (2000) presented a conceptual model in which consumers' privacy concerns are determined by the type of personal information requested, the amount of information control offered, the potential consequences and benefits offered in the exchange, and consumer characteristics. They proposed these factors not only influence overall concern, but also influence consumer beliefs regarding marketers' information practices and that the outcomes of overall concern and beliefs influence consumers' future behavioral and attitudinal responses. Our paper is different from their study in that it differentiate between the types of information requested over the Internet (e.g., financial versus demographics) and online service types (e.g., Search engines versus Online retailers), while Phelps et al. (2000) and Milne et al. (1999) focused on consumers' purchase decisions upon privacy concerns in interacting with direct marketers. Based on the relationship between privacy concerns and consumer characteristics, this study also involves consumer individual differences (i.e., Internet usage and experiences with information misuse).

Another stream of recent information privacy research is the examination of the consequences of consumer privacy concerns. Understanding the attitudinal and behavioral reactions that stem from privacy concerns is as important as understanding the antecedents (J. E. Phelps, D'Souza, & Nowak, 2001). Without a sense of the consequences, it is impossible to understand how important privacy concerns are for firms and consumers. This is especially important to the potential consequences of privacy concerns and related factors on establishing a long-term relationship, or purchase behavior. Sheehan and Hoy (1999) reported privacy concern makes respondents more likely to provide incomplete information to a website and request removal from mailing lists. Furthermore, as privacy concern increases, respondents were less likely to register at websites that request information. Many researchers demonstrated that consumers are reluctant to provide their personal information or participate in online transactions due to consumers' privacy concerns in a firm's obligations on both transactions and operations (Sipior, Ward, & Rongione, 2003). Internet privacy concerns can result in their willingness, or non-willingness, to participate in the electronic market and disclose consumers' personal information (Ba & Pavlou, 2002; Lee & Turban, 2000; Suh & Han, 2003). If consumers cannot believe their transactions and data are handled safely and securely, they try to switch providers.

The more competitive industry becomes, the more information firms require with various purposes such as personalized services or direct marketing. Providing personalized services or offerings on websites seem quite profitable for firms. However, personalizing consumes' interactions entails gathering considerable amounts of their

information and it can frequently make consumers feel private information has been violated (Kobsa, 2007). Other potential privacy concerns in the context of personalized systems include unsolicited marketing, price discrimination, information being revealed to other users and so on. A number of factors have been identified that play a role in the decision process for information disclosure. They include individuals' characteristics, the type of information to be disclosed, the value of personalization benefits, and websites' privacy protection practices (Diney & Hart, 2006; Kobsa, 2008; Pavlou, Liang, & Xue, 2007; Xu, Dinev, Smith, & Hart, 2008).

2.4 Research Issues

This review of the literature on information risk management in the IS literature and related fields brings to light the breadth and the depth of the extant research on issues related to enterprise-wide business processes by which it can be managed. Though this dissertation focuses on a couple of aspects of information risk management research, the extant literature can provide a rich tapestry of frameworks and models that aid the understanding of the central issues of this dissertation. With these backgrounds, we proceed to the two essays in this dissertation.

The first area of research that we believe deserves further exploration is the development of a more holistic theory or framework that empirically incorporates financial and organizational perspectives related to information risk management. Despite the emphasis on IT executives' roles, few empirical studies have focused on the status of IT executives in a TMT and their compensation. Previous research mainly focused on the technical characteristics of information security such as software design,

databases, and systems architecture and hardware performance (Cavusoglu, Mishra, & Raghunathan, 2005; Muralidhar, Parsa, & Sarathy, 1999; Posthumus & von Solms, 2005; Straub & Welke, 1998). Instead, the managerial approach of this essay allows the study to integrate these technical issues into a social context, taking into account the organization's norms. Since the organizational environment is changing, the multi-disciplinary study would be a beneficial way of exploring the wider issues of information risk management such as patterns of organizational context, roles, responsibility, and practices.

The second area of research studies how privacy concerns affect consumer willingness to form B2C relationship over the Internet and which factors accelerate or alleviate consumer privacy concerns. While the prior research has mainly focused on how privacy concerns negatively affect consumer purchase intention, this essay more specifically examines consumer willingness to provide different types of personal information based upon the website types with privacy-related factors such as awareness of privacy protection and expected benefits exchanged with personal information.

CHAPTER 3. INFORMATION RISK MANAGEMENT AND IT EXECUTIVES' STATUS IN A TOP MANAGEMENT TEAM

3.1 Introduction

As organizational departments of a business become increasingly dependent on Information Technology (IT), accountability for information systems has extended from IT personnel to personnel and managers throughout the firm. With divergent reporting lines and information access, the dissemination of information assurance responsibility can impede coherence in information risk management. This potential lack of coherence increases the possibility of compromising information assets, resulting in direct damage to information assets as well as indirect damage to reputation and competitive advantages (Schultz, Proctor, Lien, & Salvendy, 2001). Accordingly, information risk management has quickly garnered top management's awareness as an enterprise-wide and strategic issue.

Furthermore, legislative compliance requirements such as the Sarbanes-Oxley Act of 2002 (SOX) have made information risk management more critical to good corporate governance by mandating stricter internal controls over information (ITGI, 2006). In the context of information risk management, one of the most significant provisions of SOX is Section 404 which requires public companies to periodically attest to the validity and integrity of IT internal controls for ensuring accurate information in their business procedures. Researchers in information assurance have provided empirical evidence that

SOX has made firms more cognizant of their information risk management activities (Gordon & Loeb, 2002, 2006). The Public Company Accounting Oversight Board (PCAOB), established by SOX, mentions that especially IT internal controls weaknesses should be considered as an enterprise level control, given the extensive and pervasive usage of IT in daily business processes and transactions. IT internal controls are not simply a technical issue since they require enterprise-wide strategic dimensions such as policies and standardization for information processing, roles, and accountability (Basu & Jarnagin, 2008).

Due to these internal and external requirements, researchers and practitioners have argued that successful information risk management can be achieved through executive-level oversight, since top executives can control risks across an entire firm and all employees need to be engaged in risk management activities (McFadzean, et al., 2007). More and more firms have appointed IT executives, such as the Chief Information Officer (CIO), Chief Security Officer (CSO), and Chief Information Security Officer (CISO) (Gartner, 2008). With the increased importance of information systems, IT executives would like to see their role in the organization elevated, giving them more clout, stature and visibility, and IT executives have been key figures responsible for governing and securing IT (Enns, et al., 2003; Mitchell, 2006; Stephens, Ledbetter, Mitra, & Ford, 1992). Their roles have been evolving from a traditional project-oriented focus to a strategic decision-making responsibility.

Despite an increased emphasis on executive-level leadership in information technology, few empirical studies have focused on IT executive status in a Top

Management Team (TMT) (Santalo & Kock, 2009; Smaltz, et al., 2004; Yayla & Hu, 2008). A lack of IT executive strategic decision-making authority prevents IT executives from acquiring peer acceptance and prevents their performance as a liaison between IT and non-IT units (Enns, et al., 2003; Preston, et al., 2008). Given IT executives' cross-functional roles for ensuring enterprise-wide information risk management, we argue that IT executives need to be deeply involved in TMTs and fairly compensated in order to lead strategic initiatives. Since many firms consider information to be an important asset, information system controls have become the common denominator in all areas of risk addressed by corporate governance standards including strategic, financial, technical, operational, and regulatory risks. The final responsibility for information risk management rests with top executives who must delegate fair authority to IT executive management as well as make sure that delegation tasks are communicated and understood clearly (Johnston & Hale, 2009; Raghupathi, 2007).

Given the pervasive and extensive usage of IT, we argue that IT internal controls weaknesses and information breach incidents reflect the level of a firm's strategic and operational performance in information risk management. Effective and efficient information risk management is imperative for firms to gain the trust and support of the community or markets that they service. It can be achieved only if top level executives give it their complete support and commitment across all required functions of a firm (McFadzean, et al., 2007). Thus, it is increasingly necessary for IT executives to provide stewardship for their enterprises in terms of IT internal controls and secured systems.

Therefore, it is vital for researchers to investigate the impact of IT executive status in a TMT on information risk management.

With this purpose, we first need to capture which status IT executives acquire in firms' TMTs. Previous literature explains the status of a position can be revealed from direct engagement in top management levels, compensation levels, and turnover (Fiss, 2006; Harrison, Torres, & Kukalis, 1988; Ton & Huckman, 2008). Based on these factors, we derived the following research questions about the effects of IT executive status on information risk management: Does IT executives' engagement in a TMT have any relationship with the achievement of reducing the firms' information risk exposure? In terms of compensation along with authority and motivation, we can derive two types of compensation levels: the level of IT executives' compensations across firms and the difference between IT and non-IT executives' compensations within a firm. Then, we can ask the following. Do IT executive compensation levels in a firm, compared to those in other firms, have an association with the firm's information risk management outcomes? How does the difference between IT and non-IT executives' compensations within a firm influence its information risk management outcomes? Does IT executive turnover as a proxy of IT strategy continuity affect them? In addition to these primary questions, we investigate which executive compensation contract type has more influence on a firm's achievement in information risk management.

The paper is structured into five main sections. In Section 3.2, we review prior literature and background theories. Then, we provide the research model and theoretical support for the hypotheses in Section 3.3. The methodology section discusses the data

collection processes, the measures, and the descriptive statistics. Then, we follow with a presentation of our empirical analysis results. Finally, the paper discusses the results and the implications for future IT research and managerial practices.

3.2 Theoretical Background

Previous research in information risk management mainly focused on its technical characteristics such as software design, databases, systems architecture and hardware performance (Cavusoglu, et al., 2005; Muralidhar, et al., 1999; Posthumus & von Solms, 2005; Straub & Welke, 1998). However, this paper examines several of the managerial characteristics of information risk management, particularly the IT governance perspective. As a part of IT governance, protecting information assets and ensuring the internal controls of information systems fall under the purview of risk management which addresses the safeguarding of information assets, disaster recovery and continuity of operation (ITGI, 2005; Li, et al., 2007). Information risk management should be an integral part of IT governance, because it requires integrating strategy, policies, implementations and operations.

A firm's achievement in information risk management needs to be assessed by objective criteria. This paper employs the following two data sources. The first one is information derived from Section 404 of SOX, which requires public firms to announce the assessment of the effectiveness of their IT internal controls and forces their controls to be computer-based. The evaluation of IT internal controls involves not only the quality of accounting or financial information systems, but also the quality of a firm's information risk management (ITGI, 2006). According to the SEC, Section 404

procedures are intended to help firms "detect fraudulent information reporting early and deter information fraud, directly improving the reliability of financial statements" (SEC Release. No 33-8128, 2002). Although Section 404 causes costs and disclosure burdens for firms, firms can measure the benefits of successful implementation and maintenance of good internal controls and disclosures in the long term. Some researchers provide evidence that Section 404 compliance is likely to benefit firms' information risk management by adopting anti-fraud controls such as effective monitoring of operations, continuous risk analysis, and follow-up to unusual results (Krishnan, Rama, & Zhang, 2008; Rittenberg & Miller, 2005).

The second source is information breach information, as announced in major media outlets. Information breaches mainly reflect a firm's commitment to ensuring the confidentiality of the data, which is the ability to prevent disclosure of information to unauthorized individuals or systems (K. Campbell, et al., 2003; Kannan, Rees, & Sridhar, 2007). Furthermore, increased information breaches and electronic fraud have driven stricter legal requirements with the Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPPA), and the USA Patriot Act (Turban, Leidner, Mclean, & Wetherbe, 2008), among others.

We developed a research model combining four streams of literature. The first stream consists of works by contingency theorists who try to find organizational structure with decision-making responsibilities under task uncertainty (Drazin & Vandeven, 1986; Schoonhoven, 1981). As task uncertainty increases and it becomes more efficient to decentralize decision making, the organization needs to have a direct

relationship across functional departments to solve potential control problems. The theory states that organizational performance depends on the fit between organization structure and process given task uncertainty (Dubin, 1976). In terms of information risks, they are associated with internally and externally unpredictable attacks on information as well as the use, ownership, operation, involvement, and adoption of IT within an enterprise. It consists of IT-related events and conditions that could potentially impact the business. It can occur with both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives.

Our second stream of literature involves agency theory. Agency theory explains the mechanisms between a principal who delegates work and an agent who performs that work, and focuses on determining the optimal contract governing the principal-agent relationship given risk-natural principals and risk-averse agents. Eisenhardt (1989) emphasizes that the theory gives valid insight into information systems, risks, outcome uncertainty and incentives. She develops the proposition that outcome uncertainty makes behavior-based contracts (e.g., salaries) more efficient than outcome-based contracts (e.g., commissions, bonuses, stock options) (Eisenhardt, 1989). Some researchers have presented evidence of positive links between a manager's compensation contract and the extent of subsequent innovative activity as well as firm performance (Holthausen, Larcker, & Sloan, 1995; Nagar, 2002). A firm’s compensation strategy can be considered as the ex ante effect on its performance, since the authority and motivation created by compensation significantly influence individuals’ large-scale decision makings (Hall & Liedtka, 2005). In light of compensation as the ex ante effect on firm

performance, our paper considers IT executive compensation levels in TMTs as a proxy of authority or influence on IT internal controls and information security in terms of strategic decision making.

The third field of literature addresses the issue of pay difference across managerial team members, which has received attention from organizational theorists. Pay difference may increase effort and provide incentives for high workforce performance levels, but may also inhibit cooperation. There has been considerable research examining the implications of two competing theoretical models: tournament theory and equity fairness. Tournament theory suggests that large pay differences provide strong motivation for highly qualified managers, leading to improved enterprise performance (E. P. Lazear & Rosen, 1981). On the other hand, equity fairness argues that greater pay differences increase dysfunctional behavior among team members, adversely affecting enterprise performance (Pfeffer & Langton, 1993). According to tournament theory, larger pay difference lead to higher performance, regardless of coordination needs, because they elicit stronger individual effort. Some empirical studies have shown that firm performance is higher when TMT pay is more dispersed (Henderson & Fredrickson, 2001; Main, Oreilly, & Wade, 1993). In particular, firms in uncertain environments need to have greater pay differences to overcome the effort-dampening effects of increased risk (E.P. Lazear, 1995; E. P. Lazear & Rosen, 1981). In terms of information risk management, we need to consider the emphasized importance of enterprise-wide collaboration on IT executives' roles and unpredictable variables on information risk management. In addition, organizational researchers argue that pay difference on

outcome-based contracts (e.g., incentives, commissions, stock options) has a larger effect on an employee's performance rather than that of behavior-based contracts (e.g., salaries), since outcome-based contracts are based on relative performance to determine compensation by eliminating environmental effects and focusing on executives' efforts (Minton, Lewicki, & Sheppard, 1994). Thus, we argue that tournament theory more appropriately explains IT executives' performance and pay difference between IT executives and non-IT executives in the context of information risk management.

The last category of literature focuses how turnover in TMTs affect firm performance. Lower rates of turnover result in better performance because turnover might cause discontinuity in an enterprise's operation and strategy as well as increase indirect costs (Huselid, 1995). We can apply Huselid's theory to information risk management and argue IT executive turnover in TMTs creates discontinuity in a firm's operations and strategies. We investigate the impact of IT executive turnover on IT internal controls and information security at the organizational level.

3.3 Conceptual Model and Research Hypothesis

The research model was built by integrating information risk management with theories reviewed in the previous section. Figure 1 shows a graphical summary of our conceptual framework with the specific constructs to answer the research questions.

First, IT executives' actual involvement in TMTs mirrors the direct relationship between IT executives and other top executives. If IT executives are viewed as outsiders by other top executives in TMTs, they may not actually possess strategic influence in TMTs and may lack operational influence across required functions (Strassmann, 1994).

A direct connection from IT executives to executives in TMTs supports cross-functional coordination, giving the issues of information systems greater weight as the corporate agenda is formed (Gartner, 2008). It leads to sound strategic alignment and execution in order to ensure enterprise-wide information assurance and IT internal controls.

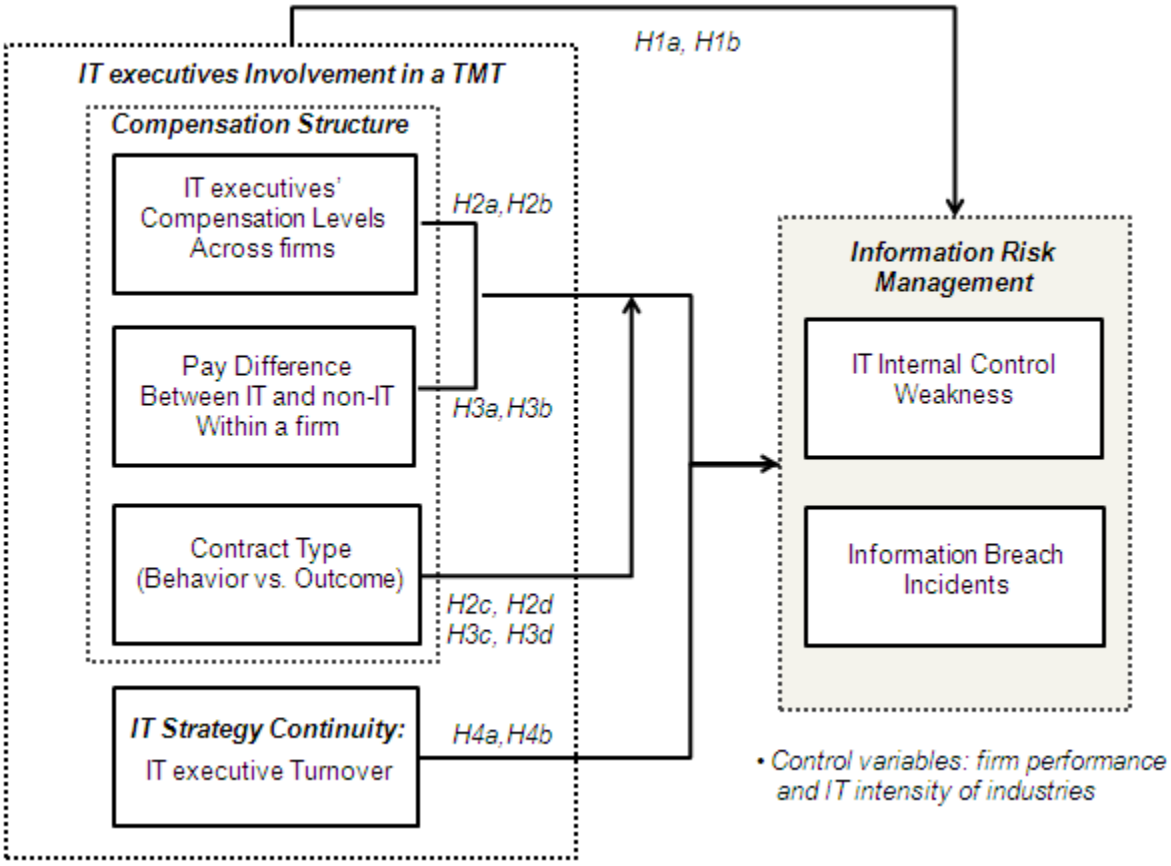


Figure 3.1 Research Model

This study integrates contingency theory to explain the effect of the structure of a TMT on information risk management. In terms of information risk, the organizational structure of a TMT can be represented by whether IT executives are directly engaged with other top executives or not. Then, we hypothesize a firm's performance on information risk management is influenced by whether an IT executive is involved in a

TMT under uncertain and unpredictable information risks. Our contingency approach is to recognize and respond to the situational structuring of IT executives' relationships with other top executives in order to attain effective information risk management. Hence, we suggest the followings:

Hypothesis 1a: *An IT executive's involvement in a TMT decreases the likelihood of a firm's IT internal controls weaknesses.*

Hypothesis 1b: *An IT executive's involvement in a TMT decreases the likelihood of a firm's information breach incidents.*

Although it has been a couple of decades since the realization of the critical role of IT executives in TMTs, the simple presence of IT executives in TMTs does not assure authority for strategic risk management decisions across a firm. Previous research examined a relationship between compensation structures and innovative strategic decisions, and claimed executives with broad oversight authority have higher compensation-performance sensitivity than executives with regional authority (Aggarwal & Samwick, 2003; Hall & Liedtka, 2005). Agency theorists have focused on determining the most efficient contract governing the relationship between one party delegates work and another performing that work (Eisenhardt, 1989). Organizational researchers have also tried to indicate which contract is the most efficient under varying levels of task uncertainty, risk aversion, external environment factors and information asymmetry for the optimal compensation contracts of upper-management position (Santalo & Kock, 2009). It has been widely accepted that common uncertainty in outcome or environment, is positively related to behavior-based contracts and negatively

related to outcome-based contracts (Beatty & Zajac, 1994; Eisenhardt, 1989). The issues of task uncertainty or unpredictability arise because outcomes are only partly a function of effort due to uncontrollable factors. Government policies, economic climate, competitor actions, technological changes, etc. may cause uncontrollable variations in a function of effort and outcomes. If task uncertainty is high, behavior-based contracts are more attractive than outcome-based contracts, since the outcome from efforts for tasks cannot be accurately measured by a function of behaviors or efforts on outcome/performance. Thus, as task uncertainty increases, it becomes increasingly difficult to assess managerial performance in absolute terms. This is because of the difficulties in previously prescribing managerial actions and evaluating the effort-dampening effects due to uncontrollable variations (E.P. Lazear, 1995). Building upon this literature, we study the more specific relationship between IT executives' compensation and their performance on information risk management. Thus, we propose our next set of hypotheses as:

Hypothesis 2a: *A higher level of IT executive compensation across firms decreases the likelihood of a firm's IT internal controls weaknesses.*

Hypothesis 2b: *A higher level of IT executive compensation across firms decreases the likelihood of a firm's information breach incidents.*

Hypothesis 2c: *The effect of IT executives' compensation on IT internal controls weaknesses is stronger with a behavior-based contract than with an outcome-based contract.*

Hypothesis 2d: *The effect of IT executives' compensation on information breach incidents is stronger with a behavior-based contract than with an outcome-based contract.*

Organizational research has emphasized the importance of the pay difference among top executives under uncertain environments which are unpredictable, complex, and difficult to understand and manage (Dess & Beard, 1984). According to tournament theory, a larger pay difference is supposed to be appropriate under highly unpredictable circumstances, because the unpredictability requires relative performance standards rather than absolute ones (E. P. Lazear & Rosen, 1981). Effects of uncontrollable factors from unpredictable circumstances can be teased out from executives' efforts on outcomes with a relative performance evaluation within a firm. Then, a pay difference determined by outcome-based contracts becomes more attractive than that determined by behavior-based contracts among executives with common uncontrollable variations in a firm. Previous literature provides evidence that pay difference enhances motivation and results in higher levels of workforce performance (Shaw, Gupta, & Delery, 2002). The benefits are even larger with the use of outcome-based incentives. Pay difference in the absence of outcome-based incentives is likely to weaken a function of behavior or efforts on performance, and violate rules of consistency and control (Bishop, 1987; Bloom, 1999). Ultimately, when a pay difference is combined with incentive or outcome-based contracts, work performance is likely to be increased. This paper determined a pay difference for each contract type by subtracting the average compensation of non-IT executives from that of IT executives in a firm and dividing it

by IT executive compensation. Then, a positively larger pay difference determined by outcome-based contracts provides incentives for IT executives by relative performance evaluation among top executives in a firm. Therefore our next hypotheses are:

Hypothesis 3a: *The more positive the pay difference between IT executives and non-IT executives on the TMT, the lower the likelihood of a firm's IT internal controls weaknesses.*

Hypothesis 3b: *The more positive the pay difference between IT executives and non-IT executives on the TMT, the lower the likelihood of a firm's information breach incidents.*

Hypothesis 3c: *The effect of the pay difference on IT internal controls weaknesses is stronger with an outcome-based contract than with a behavior-based contract.*

Hypothesis 3d: *The effect of the pay difference on information breach incidents is stronger with an outcome-based contract than with a behavior-based contract.*

We examine the impact of IT strategy continuity by measuring IT executive turnover. Kesner and Sebora (1994) claim that frequent executive turnover may disrupt organizational continuity and hurt enterprise performance (Kesner & Sebora, 1994). By narrowly focusing on IT executive turnover, Perlman (2007) shows that IT executive turnover has been high compared to other executives. Frequent turnover could be disruptive to any organization, but it is particularly damaging to information management processes which encompass an entire organization and undergird so many

governmental services (Perlman, 2007). Although the importance of IT executives has increased in organizations, their positions have continued to be some of the most politically dangerous and operationally difficult executive positions. This is because information technology is expensive, volatile, complex and politically risky. Thus, IT executives need to strategically handle rapidly changing job responsibilities and dynamic information requirements. The frequent turnover of IT executives might result in discontinuity in the organizational and structural operations of IT systems as well as IT strategies for risk management. Therefore, the ratio of IT executives' turnover and non-IT executives' average turnover attests to the severe pressure that is now being placed on individuals at the top IT executive level within the firm. As a result, our next hypotheses are:

Hypothesis 4a*: The higher the ratio of IT executives' turnover to non-IT executives' turnover, the higher the likelihood of IT internal controls weaknesses.*

Hypothesis 4b*: The higher the ratio of IT executives' turnover to non-IT executives' turnover, the higher the likelihood of information breach incidents.*

3.4 Data collection and Research Methodology

Data Collection

The empirical analysis of this study includes two dependent variables, which represent the level of a firm's information risk management outcomes: IT internal control weaknesses and information security breach reports. The first dependent variable is a firm's IT internal controls weakness, which is evaluated by external auditors. IT

internal controls have been one of the most critical issues for public enterprises since SOX has been announced in 2002. Public companies' internal controls weaknesses were collected using Audit Analytics from Wharton Research Data Services (WRDS) between 2004 and 2008. Section 404 of SOX requires all public companies to report on the effectiveness of internal controls for fiscal years ending on or after 2004 as part of their annual filing with the SEC. Audit Analytics is widely used by accounting researchers to capture management assessment of internal control effectiveness (J. Doyle, Ge, & McVay, 2005; J. T. Doyle, Ge, & McVay, 2007; N. Y. Kim, et al., 2008; Li, et al., 2007; Stoel & Muhanna, 2009). Aligning with classification by Audit Analytics, we categorized the types of internal controls weaknesses into IT internal controls weaknesses and non-IT control weaknesses. We only used the IT internal controls weakness data.

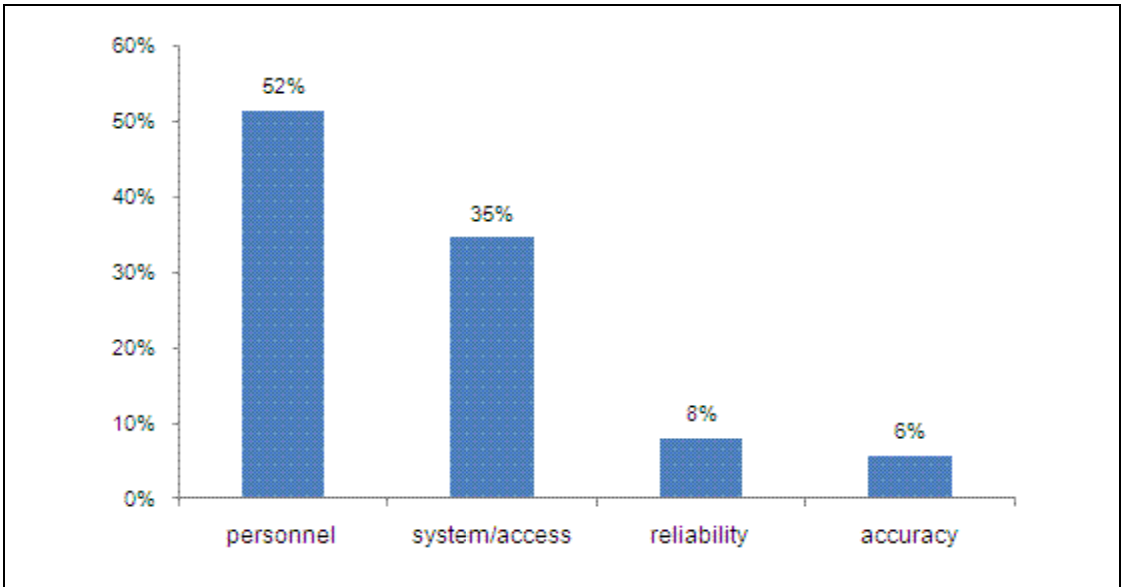
IT internal controls weakness (ITCW): We collected data on IT internal controls weakness using Audit Analytics, which provides a consistent methodology for considering the types of IT internal controls weaknesses. Evaluating internal controls means attesting to the validity and integrity of information systems from the time information enters the company to the completion of the annual report each year. SOX requires that each company's external auditors independently review management's assessment of internal controls. Among internal controls, non-IT internal controls weaknesses such as accounting and financial issues were eliminated by coding as 0. Then, IT internal controls weaknesses were included as an indicator variable which is set as 1. Figure 3.2a shows the number of IT internal controls weakness types.

The second dependent variable includes information security breach reports in publicly traded U.S. firms. We collected data on information breaches using Lexis/Nexis, CNet, and ZDNet, searching newswires for the key words "information breaches", "security breaches", "identify theft", "hacking", "site attack", "virus", "data theft", or "privacy breaches". There have been 1,486 information breaches announced from 2003 to 2008 in Lexis/Nexis, CNet, and ZDNet. We eliminated information breaches from government/military, medical/healthcare, and educational institutions. Finally, 577 incidents from the business sector were collected and 232 incidents among them come from publicly traded firms in Standard and Poor's (S&P) 1500.

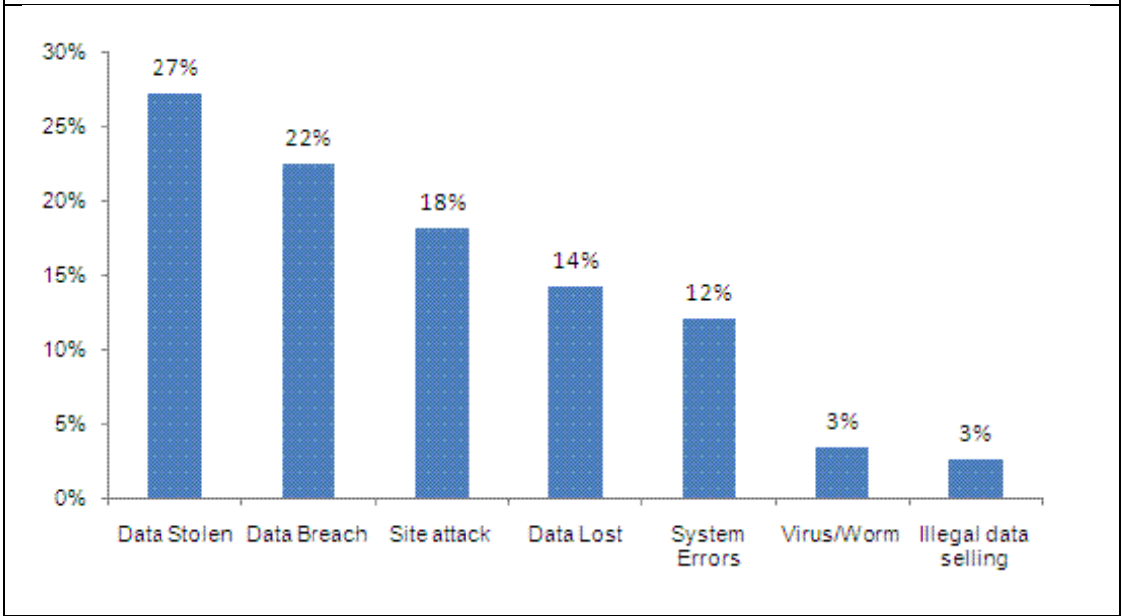
Breaches (BREACH): We examined whether information breach incidents occur at a year t. If a firm has at least one breach incident at time t, then BREACH is equal to 1, otherwise 0. Figure 3.2b shows the number of each breach type publicly announced between 2003 and 2008.

Next, we constructed our independent variables for executive compensation, pay difference and turnover using the ExecuComp distributed by S&P. The ExecuComp database contains all information on total compensation from the top five to nine executives in a TMT at each of the firms in the S&P 1500, and it is used extensively for empirical research. The two main advantages of ExecuComp relative to other data that have been used to examine executive compensation are that it contains a wide cross-section of firms and that it contains data not only for CEOs but other executives as well. We identified that ExecuComp has 1,462 firms reported from 2002 to 2008. However, 283 firms have IT executives under several titles such as the CIO, CSO, and CISO. Our

sample has 158 cases in IT internal controls weaknesses and 232 incidents in information breaches. We extracted controls from 1,462 firms from the ExecuComp database, and conducted case-control studies with breached firms and IT internal weakness, respectively.



a. IT Internal Control Weakness Types



b. Information Breach Incident Types

Figure 3.2 Types of Information Risks

IT Executives (ITEXT): The first independent variable was the involvement of IT executives in each company's TMT. If a company had an IT executive during the previous year *t-1*, when information breach incidents or IT internal controls weaknesses occurred at year *t*, the value equals 1. Otherwise, it equals 0.

Compensation (COMP): We defined each executive's compensation as the sum of behavior-based and outcome-based contracts at year *t*-1, when IT internal controls weaknesses or information breaches occurred at year *t*. Behavior-based contracts included salary, while outcome-based contracts were valued as the sum of bonuses, stock options, performance share awards, performance units/cash awards, and dividend equivalents. The part of compensation with a behavior-based contract (*BEHAVIOR*) represents salaries, while that of an outcome-based contract (*OUTCOME*) includes bonuses, transfer of property rights, and stock options related to market governance.

Contract Type (TYPE): This variable is to indicate behavior-based contract or outcome-based contract. If it is a behavior-based contract, it is equal to 1; otherwise it is equal to 0.

Pay Difference (DIFF): Pay difference represents the disparity of compensation at year *t-1*, when information breaches or IT internal controls weaknesses occurred at year *t*. We derived a firm *i*'s pay difference by the following equation.

$$DIFF_{it} = (COMP_{IT,it} - avg(COMP_{non\text{-}IT,it}))/COMP_{IT,it}$$

A firm *i*'s pay difference ($DIFF_{it}$) at a year *t*, is determined by subtracting the average compensation of non-IT executives ($COMP_{non\text{-}IT,it}$) from IT executives compensation ($COMP_{IT,it}$) and dividing the result by IT executive compensation. A

negative pay difference means IT executives' compensation is smaller than the average of others, and it becomes positive when IT executive compensation is larger than others. In addition, pay difference was subdivided by the contract types and categorized as two types: pay difference in behavior-based contracts (*BDIFF*) and pay difference in outcome-based contracts (*ODIFF*). This categorization was done in order to examine how a contract type changes the effect of pay difference on a firm's information risk management.

Table 3.1 Descriptive Statistics

Variable	Mean	Std Dev	Median	Minimum	Maximum
All firms from the industries which had at least one breach or weakness, n=1,462					
IT intensity	2.386	4.209	1.000	0.110	22.98
Firm Performance	3.825	15.396	4.154	-97.721	1,100
The firms with Information Security Breaches in t year, n=232					
IT intensity	2.408	4.375	0.840	0.110	22.98
Firm Performance	3.863	6.797	3.663	-32.324	21.106
The firms with IT internal controls weaknesses in t year, n=158					
IT intensity	2.577	4.55	1.000	0.110	22.98
Firm Performance	1.408	8.916	1.503	-47.465	42.826
The firms with IT executives (ITEXEC=1) in t-1 year, n=283					
Compensation (Behavior-based)	425.188	263.533	354.329	78.411	2,188.75
Compensation (Outcome-based)	675.89	699.68	440.31	0.00	4,409.17
Pay Difference (Behavior-based)	-0.180	0.323	-0.207	-1.42	0.98
Pay Difference (Outcome-based)	-0.233	0.398	-0.256	-1.894	0.98
Turnover	1.213	0.626	1.000	0.222	4.000
IT intensity	1.746	0.513	1.000	0.170	22.98
Firm Performance	3.312	9.746	4.387	-47.465	39.116

Note. *Compensation is measured in $1,000 unit.*

Turnover (TURNOVER): We examined whether IT internal controls weaknesses or information breaches are more likely to occur if an IT executive departed at year *t-1*. We counted the number of IT executives and non-IT executives at a position; then, the number of IT executives at a position was divided by the average number of non-IT executives at a position.

IT Intensity (ITINT): We needed to control the IT intensity of an industry, because it leads to different interdependencies between IT and non-IT executives (Siegel & Hambrick, 2005). The study adopted the ratio of IT capital to labor which has been generally employed by previous IS literature (Park, Shin, & Sanders, 2007; Zhu & Kraemer, 2002). The Bureau of Economic Analysis (BEA) annual data were used for the data on IT equipment investments and full-time employees in a firm for the period 2002-2007. IT equipment includes computers and peripheral equipment, software, and other information processing equipment (Dumagan & Gill, 2002). We calculated the ratio between IT equipment per Full-Time Employee (FTE) for each industry and the average IT equipment per FTE for all industries. The IT intensity of an industry is derived by the following equation.

$$ITINT_i = \left(\frac{IT\ Equipment_i}{FTE_i}\right) / \left(\frac{IT\ Equipment_{total}}{FTE_{total}}\right)$$

Firm Performance (FVALUE): A firm's performance can influence both pay level and the mixture of different pay components. We also considered enterprise performance, which is positively associated with the relative importance of incentives by

adding each firm's ROA, since more profitable enterprises may be able to pay more (Anderson et al. 2000).

With these data resources, we constructed the measures for our empirical models. Appendix A shows the definitions of all variables in the models. Table 1 provides the descriptive statistics for all samples.

Table 3.2 Correlation Matrix of the Variables and Tolerance Value

	Mean	s.d.	1	2	3	4	5	6	7
1.IT Internal control Weaknesses	0.11	0.10	1.00						
2.Information Breaches	0.16	0.14	0.00	1.00					
3.Compensation	1,101	879.72	-0.19	-0.23	1.00				
4.Pay Difference (Behavior-based)	-0.18	0.33	-0.01	0.07	0.12	1.00			
5. Pay Difference (Outcome-based)	-0.23	0.40	0.01	0.05	0.16	0.16	1.00		
6.Turnover	1.21	0.63	0.06	-0.05	0.02	0.03	-0.34	1.00	
7.ROA	3.31	9.75	-0.11	0.03	0.07	-0.04	-0.06	0.09	1.00
8.IT Intensity	1.75	0.51	0.04	0.12	0.17	-0.12	-0.03	-0.16	0.01

Note. *Compensation is measured in $1,000 unit.*

Data Analysis

Before setting up the models, we needed to conduct a correlation test among all variables. Table 3.2 displays the correlation matrix with the low values. Thus, multicollinearity is not a concern for our models.

Our models employed both conditional and unconditional logistic regressions to test the hypotheses. Suppose we have $i=1,\ldots,n$ firms and each firm is presented with a dichotomous variable for dependent variables (y) (i.e., IT internal controls weakness

and information breaches, j=1 and 2). The model (1) tests H1a and H1b with the probabilities that a firm has IT control weaknesses and information breaches, when it has an IT executive in its TMT. y_{it} equals 1 if a firm i has any IT control weakness ($Pr_1(y_i = 1)$, j=1) or an information breach ($Pr_2(y_i = 1)$, j=2) during year t. X_k represents *ITEXE*, *FVALUE*, and *ITINT* in the model (1) as described in Appendix A.

$$logit\left(Pr_j(y_{it} = 1 | X_{i(t-1)k})\right) = f_j(\alpha_0 + \alpha_1 ITEXE_{i,t-1} + \gamma_1 FVALUE_{it-1} + \gamma_2 ITINT_{it-1}) \quad (1)$$

The model (2) tests the main effects of IT executive compensation, pay difference and IT executive turnover for H2 ~ H4 with conditional logistic analysis. The data set was rearranged and included both charged and uncharged firms with information breaches and IT internal controls weaknesses for representing cases and controls in a conditional logistic model (Hosmer & Lemeshow, 1992). The control groups have the same first 2-digit Standard Industrial Classification (SIC) codes and similar ROA as their case groups. The model (2) adopted 3 matched controls (m) over each case.

$$logit\left(Pr_j(y_{it} = 1 | X_{i(t-1)k}) / \sum_m Pr_j(y_{imt} = 1 | X_{im(t-1)k})\right) = g_j(\beta_1 COMP_{i(t-1)} + \beta_2 BDIFF_{i(t-1)} + \beta_3 ODIFF_{i(t-1)} + \beta_5 TURNOVER_{i(t-1)}) \quad (2)$$

One issue in the model was to test the interaction effect of contract types, since we would like to compare the effects of IT executives' compensation on dichotomous outcome variables in terms of a behavior-based and an outcome-based contract. It is not uncommon for researchers to examine interaction effects by separate logistic regressions for behavior-based contracts and outcome-based contracts (Jaccard 2001). We therefore separately run the model (2) to evaluate the effects of a behavior-based contract, an

outcome-based contract, and a total compensation. It investigates how compensation and its contracts in TMTs influence the probabilities that the firm has IT control weaknesses and information breach incidents.

However, the separate equations have some misleading results because we cannot perform a formal statistical test of the difference between the logistic coefficients for two contract types. Even though they are statistically significant, the coefficients might be comparable in magnitude with trivial differences between them. Formal interaction analysis through product terms in a single equation is preferable because it provides a means of formally testing the difference between logistic coefficients (Jaccard, 2001). Therefore, we included additional product terms which include contract types, compensation, and pay difference to test the hypotheses H2c, H2d, H3c, and H3d. The moderated analysis was conducted by an unconditional logistic regression technique where the model (3) was used (Allison, 1999; Hosmer & Lemeshow, 1992).

$$logit\,(Pr_j(y_{it} = 1 \mid X_{i(t-1)k})) \tag{3}$$
$$= f_j(\beta_0 + \beta_1 COMP_{i(t-1)} + \beta_4 DIFF_{i(t-1)} + \beta_5 TURNOVER_{i(t-1)} +$$
$$\delta_1(COMP_{i(t-1)} * TYPE_{i(t-1)}) + \delta_2(DIFF_{i(t-1)} * TYPE_{i(t-1)}) +$$
$$\gamma_3 FVALUE_{i(t-1)} + \gamma_4 ITINT_{it-1})$$

3.5 Results

Table 3.3 and 3.4 report the results from our models. Controlling for firm overall performance and IT intensity, the model (1) shows that when an IT executive is engaged in a TMT, there is a lower probability of IT internal controls weaknesses and information breaches with the coefficients (α_1), -0.73 and -0.37, respectively. These

support hypotheses 1a and 1b, which argued that IT executive involvement in TMTs, would have positive effects on a firm's information risk management.

Table 3.3 The Results with IT Internal Controls Weakness

	Model 1	**Model 2**			**Model 3**	**Hypotheses**
		Conditional Logit				
	IT executive involvement	Behavior -based	Outcome -based	Total		
IT Executives (α_1)	-0.73** *(0.32)*					*H1a: Supported*
Compensation (β_1)		-7.52*** *(1.890)*	-6.18** *(2.062)*	-3.44** *(1.175)*	-5.47*** *(1.492)*	*H2a: Supported*
Pay Difference in behavior-based contracts (β_2)		-0.08 *(0.126)*	-0.02 *(0.158)*	-0.14 *(0.134)*		
Pay Difference in outcome-based contracts (β_3)		-15.04** *(4.181)*	-18.24* *(8.965)*	-17.78* *(8.571)*		*H3a: Supported*
Pay Difference (β_4)					-6.76** *(3.648)*	
Turnover (β_5)		2.29*** *(0.530)*	3.22*** *(1.244)*	2.9** (0.900)	1.47** *(0.505)*	*H4a: Supported*
Compensation * Contract Type (δ_1)					-6.37*** *(1.737)*	*H2c: Supported*
Pay Difference * Contract Type (δ_2)					6.81** *(3.663)*	*H3c: Supported*
Control Variables						
Firm Value (γ_1)	-1.23*** *(0.14)*				-2.32*** *(0.46)*	
IT Intensity (γ_2)	-0.25 *(0.11)*				0.35 *(0.33)*	

Note. *Standard errors are in parentheses. p-values are represented by * Significant at 10%, ** Significant at 5%, *** Significant at 1%.*

In order to test hypotheses 2a and 2b, the model (2) was conducted. We found IT executives' compensation levels across firms are negatively associated with the possibilities of both IT internal control weaknesses with -3.44 and information breaches with -7.29. Furthermore, IT executive compensation with a behavior-based contract (β_1= -7.52) decreases the possibility of IT internal control weaknesses more than with the

outcome-based contracts (β_1= -6.18). Similarly, in terms of information breaches, the magnitude of a behavior-based contract (β_1= *-21.16*) is larger than that of the outcome-based contracts (β_1= *-8.57*). This result shows that the unpredictability of information breach incidents has significantly increased the impact of behavior-based contracts on IT executives' performance in information risk management.

Therefore, we can conclude that the outcome uncertainty of information risk management has made the impact of the behavior-based contracts larger than that of the outcome-based contract on IT executives' compensation. Next, we examined how the pay difference between IT and non-IT executives within a firm, affects its information risk management outcomes with hypotheses 3a and 3b. This study also focuses on investigating the magnitude of a pay difference from both positive and negative directions. A positive difference means IT executives' compensation becomes larger than the average of others and vice versa.

As Table 3.2 displays, the means of each pay difference of two contracts have generally negative values indicating non-IT executives are normally largely paid than IT executives. Based on the sample, the model (2) provides the evidence that the pay differences with both a behavior-based and an outcome-based contract are negatively associated with the likelihoods of IT internal controls weaknesses and information breaches by all negative coefficients of β_2 and β_3 in Table 3.3 and 3.4. Consistent with tournament theory, the magnitudes of pay differences in behavior-based contracts (β_2= -0.14 and -0.06) are smaller on the likelihood of IT internal controls weaknesses and information breaches than those in the outcome-based contracts (β_3= -17.78 and -64.69).

Table 3.4 The Results with Information Breach Incidents

	Model 1	**Model 2**			**Model3**	**Hypotheses**
	IT executive involvement	Conditional Logit				
		Behavior-based	Outcome-based	Total		
IT Executives (α_1)	-0.37* *(0.215)*					*H1b: Supported*
Compensation (β_1)		-21.16*** *(5.38)*	-8.57*** (1.91)	-7.29** (1.58)	-4.72** (1.43)	*H2b: Supported*
Pay Difference in behavior-based contracts (β_2)		-0.04* *(0.05)*	-0.02 *(0.04)*	-0.06* *(0.04)*		*H3b: Supported*
Pay Difference in outcome-based contracts (β_3)		-46.97*** *(12.22)*	-63.17*** *(14.35)*	-64.69*** *(14.55)*		
Pay Difference(β_4)					-45.25*** *(15.57)*	
Turnover (β_5)		1.19*** *(0.43)*	1.66*** *(0.45)*	1.53*** *(0.44)*	1.15*** *(0.34)*	*H4b: Supported*
Compensation * Contract Type (δ_1)					-12.36** *(5.29)*	*H2d: Supported*
Pay Difference * Contract Type (δ_2)					45.20*** *(14.56)*	*H3d: Supported*
Control Variables						
Firm Value (γ_1)	-0.33** *(0.105)*				-0.13 *(0.18)*	
IT Intensity (γ_2)	-0.15 *(0.097)*				-0.41** *(0.23)*	

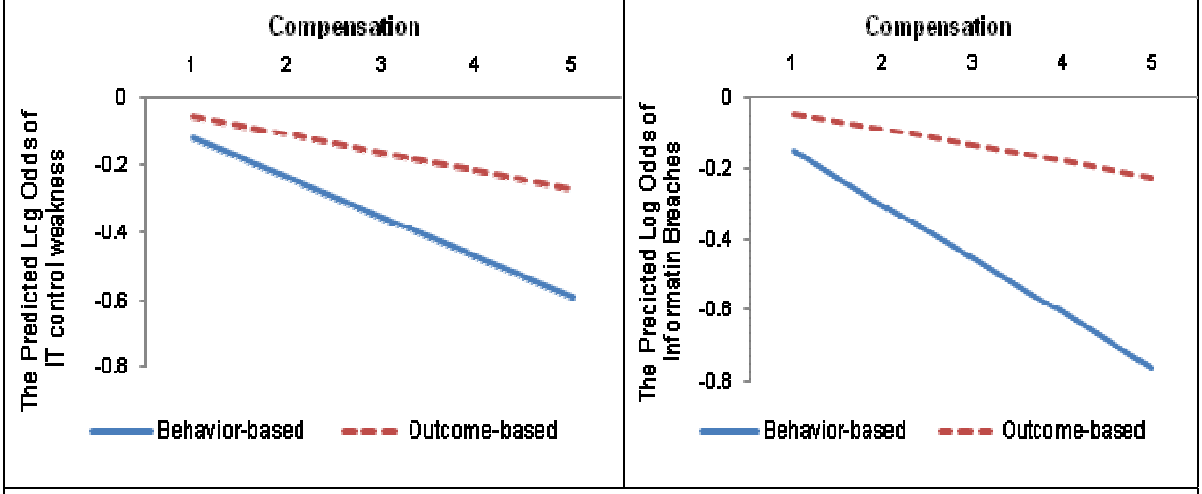
Note. *Standard errors are in parentheses. p-values are represented by * Significant at 10%, ** Significant at 5%, *** Significant at 1%.*

To further explore the moderating effects of two contract types, the model (3) conducts interaction analysis through product terms to formally investigate a magnitude between them for hypotheses 2c, 2d, 3c, and 3d. While the model (2) separately tests compensation levels and a pay difference in two contract types, the model (3) adds the product terms to examine the interaction effects of compensation and pay difference in

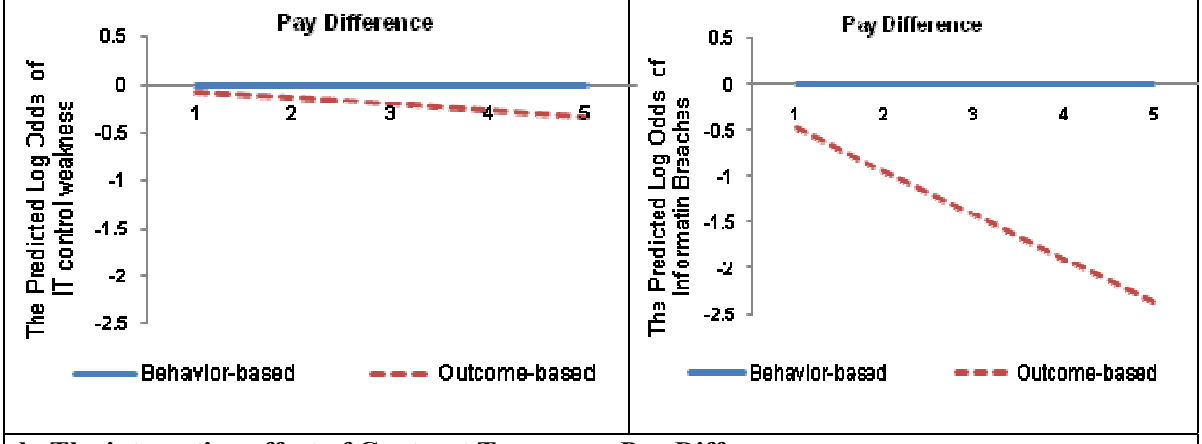
contract types on two dependent variables. The result indicates that a product term (δ_1) with a behavior-based contract and IT executive compensation, negatively affects both IT internal controls weaknesses and information breaches by -6.37 and -12.36, respectively. On the other hand, the product term (δ_2) with a behavior-based contract and a pay difference, increases the likelihood of IT internal controls weaknesses and information breaches by 6.81 and 45.20. This implies the contrary effect of two contracts on compensation and pay difference. While IT executive compensation with a behavior-based contract, decreases the likelihoods of IT internal controls weaknesses and information breaches, a pay difference with a behavior-based contract does not have any effect on their likelihoods. However, a pay difference with an outcome-based contract significantly lowers the likelihoods of IT internal controls weaknesses and information breaches.

Figure 3.3 plots the predicted log odds of the dependent variables (i.e., IT internal controls weaknesses and information breaches) and the focal independent variables (i.e., IT executives' compensation levels and pay differences) in two contract types (i.e., behavior-based and outcome-based). The nonparallel slopes are indicative of the interaction, and their degrees give some appreciation of the magnitude of the interaction effects. The slopes of Figure 3.3 present how differently two contract types moderate the effects of compensation levels and pay differences on outcome variables. Figure 3.3a reveals that the solid lines of a behavior-based contract in IT executive compensation punctually drop, while the dotted lines of an outcome-based contract gently decrease. As

IT executive compensation levels increase, the difference between the effects of two contracts becomes larger.



a. The interaction effect of Contract Types on Compensation



b. The interaction effect of Contract Types on a Pay Difference

Figure 3.3 The Plot of Interaction

Contrary to the results of Figure 3.3a, Figure 3.3b suggests the solid lines of a pay difference with a behavior-based contract show the flat slopes with IT internal controls weaknesses and information breaches. On the other hand, the dotted lines of an outcome-based contract have the sharply decreasing slopes. These are consistent with organizational researchers' arguments that the effects of relative pay differences become

larger when outcome-based contracts are in use within a firm, as well as that the effects of absolute executive compensation across firms become larger with behavior-based contracts rather than outcome-based contracts under highly uncertain outcomes and circumstances (Bishop, 1987; Frederickson, 1992).

Lastly, we define IT executive turnover as a proxy of IT strategy discontinuity in information risk management. IT executives' roles cover information management policies, risk analysis, risk management, and disaster recovery. The results from our models indicate that IT executive turnover led to a high possibility of IT internal controls weaknesses and information breach incidents, supporting Hypotheses 4a and 4b (β_5 = 1.47 and 1.15). The frequent turnover of IT executives could be disruptive to a firm, but it is also particularly damaging to information risk management efforts.

3.6 Discussions

This paper provides the first comprehensive analysis of the impact of IT executive status in TMTs on information risk management. First, IT executive involvement in TMTs results in more effective information risk management by reducing the likelihood of IT internal controls weaknesses and information breaches. This implies that IT executive engagement in TMTs helps a firm better govern information risks with initiatives for strategic alignment and execution (Preston, et al., 2008). Second, IT executive compensation levels positively affect information risk management. To formally investigate the effects of contract types on compensation, we categorized IT executive compensation into behavior-based and outcome-based contracts. Task uncertainty and difficulties in outcome measurability are positively related to behavior-

based contracts more than outcome-based contracts in IT executives' compensation across firms. Third, a pay difference in an outcome-based contract significantly reduces a firm's information risk exposures, while the study failed to provide evidence for any significant effect of a pay difference in a behavior-based contract on them. It implies that information risk management magnifies the effect of pay difference with outcome-based contracts in relative performance evaluation within a firm under task uncertainty and environmental dynamism. Fourth, this paper demonstrates IT executive turnover has a significantly negative effect on information risk management issues, which include information security policy, risk analysis, risk management, contingency planning and disaster recovery. Although general executive turnover has compound effects from various environmental factors, IT executive turnover is more related to IT strategic issues, which leads to discontinuity in operation and strategy (Roepke, Agarwal, & Ferratt, 2000).

Furthermore, it is also meaningful to compare the results of IT internal controls weaknesses and information breaches in terms of task programmability. Task programmability can be defined as the degree to which appropriate behavior by the agent can be specified in advance (Eisenhardt, 1989). In our context, a firm's IT internal control activities are previously much more programmed through check or audited lists than information breach preventing activities, because IT internal controls are evaluated by external auditors who work through a standardized framework (i.e., Cobit[1]) to access a firm's legislative compliance (ITGI, 2006). Hence, IT executives' outcome

[1] *the IT Governance Institute's Control Objectives for Information and Related Technology (CobiT)*

performance in IT internal controls weaknesses can be more easily observed and evaluated according to relatively standardized guidelines. Thus, the more previously programmed the task, the more attractive are behavior-based contracts of compensation because information about the agent's behavior is more readily determined. This proposition is also consistent with our results.

In summary, our study provides firms with a benchmark for compensation strategies that can be helpful to assess enterprise-wide performances in information risk management. The results suggest IT executives with enough strategic decision-making authority and peer acceptance in organization cultural practices are positively associated with protecting information systems. Firms can use our findings to maximize executives' performance on their specific tasks with fair compensation structure.

3.7 Conclusions and Implications

Due to litigation and governmental investigation, organizations today are regularly compelled to produce electronically stored information, which massively exposes them to risks. It is imperative for executive-level leadership to exercise controls over such highly variable processes fraught with risk and uncertainty, which lead to difficulty in measuring outcome, rendering outcome-based contracts less attractive (Anderson, 2008; Eisenhardt, 1985). In this circumstance, this paper explores how IT executive involvement in a TMT and their compensation structures affect organizational performance in information risk management, which requires interdependency across all departments as well as a degree of maturity in an organization's capability to manage risks through continuous improvement in all daily information processes.

The majority of executive compensation research emanates from the management and finance areas. Their results have been very expansive regarding market-based measures or accounting-based measures of firm performance, and ambiguous conclusions were frequently suggested. Although many researchers from a number of disciplines have examined executive compensation through a wide variety of theoretical lenses, few have attempted to integrate compensation structures within specific tasks or circumstance. This paper incorporated the contributions and insights from information risk management into compensation research, which involves more specific tasks such as ensuring IT internal controls and preventing information breaches. While previous research suffered from the use of comprehensive or compound measures of firm performance, we employed explicitly coded IT internal controls weaknesses across firms and publicly announced newswires which directly affects firms' market values.

This study presents the first in-depth, cross-level empirical analysis of compensation for IT executives. It contributes to the literature on executive compensation in several ways. First, it provides a deeper understanding of how an effort/outcome uncertainty of tasks for which executives should take responsibility affects their compensation structure. The results indicate task uncertainty of an effort/outcome function influences compensation structure. Second, it provides the first insight into both cross-sectional IT executive compensation and the distribution of compensation among executives within a firm. The findings have important implications for top executives and compensation policy makers. The importance of task-specific factors in setting compensation levels suggests that IT executives should pay considerable attention to task characteristics in

their career planning. The questions and issues addressed in the current study will continue to be important to firms' information risk management, especially as the IT executives are influential in handling the interdependence between business units.

Nevertheless, it also presents a mixed blessing with unanswered questions offering some opportunities for future research. First, one of the unanswered questions is due to the limitation in measuring executives' individual factors such as education, age, and experience in information systems. These idiosyncratic factors can also differentiate individuals' risk propensity and capabilities. Second, the paper does not directly deal with IT executives' explicit reporting relationship, which might be one of the significant factors in organizations by adding strength to an employee's position. Since IT executives are attempting to influence corporate strategy, it would seem apparent that they need to report to a president or CEO rather than a controller or other executive. However, this study focuses on the compensation structures which represent an interrelationship among top executives in TMTs rather than a hierarchical relationship. Lastly, it is very important to explore IT executive compensation determinants in various geographical contexts as IT employment becomes global. Due to political, economic, and technological climates, a country's risk propensity and IT maturity will influence the determinants of IT professional compensation.

CHAPTER 4. ENHANCING CONSUMER WILLINGNESS TO PROVIDE PERSONAL INFORMATION DESPITE PRIVACY CONCERNS

4.1 Introduction

The Internet has greatly expanded opportunities for firms to communicate with their customers. Firms have collected information about customers through websites to capture their needs and to adopt the information for high-quality marketing techniques. Communication with customers through websites has become increasingly important as consumers rely more on the Internet for information and purchases and become more loyal online (Shankar, Smith, & Rangaswamy, 2003). Firms now compete to build vast quantities of information to increase existing customers' loyalty and attract potential customers. However, the excessive use of personal information hurts consumer privacy in various ways, such as by unsolicited emails, credit card fraud, or identity theft. For instance, Sears faced a class-action lawsuit after making its consumers' purchase history public via a business partner web site[2]. Also, in May 2008 Charter Communications, one of the nation's largest Internet service providers, announced enhanced service plans by installing software to map its Internet consumers' browsing behavior in order to sell ads tailored to consumers' interests. Consumers immediately protested to protect their privacy, and the plan was cancelled[3].

---

[2] *See http://www.infoworld.com/article/08/01/08/Sears-sued-over-privacy-breach_1.html*
[3] See *http://www.slate.com/id/2198119/*

Consumer privacy has many different meanings based on different contexts, from a right or entitlement in law (Smith, 2001; Vail, Earp, & Anton, 2008), to a state of limited access or isolation in social psychology (D. J. Kim, Ferrin, & Rao, 2008; Schwartz, 1968), and to a control in information systems (Chellappa & Shivendu, 2007; Culnan & Armstrong, 1999; Diney & Hart, 2006). In this study, privacy concerns are limited to the concerns consumers have in regard to fairness and control over personal information in information systems (A. J. Campbell, 1997).

Information sharing is necessary to establish a long-term relationship between a website and consumers. However, negative perception on the behalf of consumers regarding the commitment of the form to their private information may impede such relationship (Eastlick, Lotz, & Warrington, 2006). As more and more consumers have become anxious about protecting their information, it has been critical to identify which factors can outweigh the effect of privacy concerns on consumer willingness to provide their personal information (Diney & Hart, 2006). Although market researchers claim that the benefits of *e*-Commerce are numerous for consumers as well as organizations, many consumers use Internet channels for just seeking information and still make their actual purchase through traditional channels (Barua, Konana, Whinston, & Yin, 2001). Wang and Emurian (2005) demonstrated information privacy concerns build "a most formidable barrier to people engaging in e-commerce" (Wang & Emurian, 2005) (pp. 105-121). Indeed, in the electronic markets with limited legal protection and numerous competitors with low switching costs, alleviating consumer privacy concerns is considered as a necessity for building trust and satisfaction in establising B2C

relationships over the Intenet. (Luo, 2002; Schlosser, White, & Lloyd, 2006; Selnes, 1998; Steenkamp & Geyskens, 2006). However, collecting personal information also lays a heavy burden on firms to ensure adequate privacy protection, while the utilization of the information has been imperative to meet consumers' needs and build their loyalty (Bowie & Jamal, 2006). Therefore, it becomes more critical for firms to resolve consumers' privacy concerns so that they are willing to provide their information.

While many researchers examined privacy-related factors and benefits (Jarvenpaa & Ives, 1991; Jarvenpaa & Tiller, 2001; Pavlou & Gefen, 2004), few studies incorporated specified types of requested personal information and website types which request the information over the Internet (J. Phelps, et al., 2000). Therefore, the purpose of this paper is to understand how information privacy concerns influence the extent of consumer willingness to provide several types of personal information (i.e., contact, demographic, browsing habit, and finance information) with website types (i.e., search engine and online retailer) and how expected benefits influence the extent of consumer willingness to provide such information. To our knowledge, this study is the first to have linked these variables to information sharing over the Internet. Incorporating the types of website and requested information in the model represents contributions that help to explain consumer willingness to provide information in detail. The results can give firms new insights into how to provide privacy protection, benefits, and specific information practices to motivate consumers to disclose personal information based on its website type.

We first synthesize background theories for developing a research model in Section 4.2. Then, we propose a research model in Section 4.3 and explain the constructs in Section 4.4. Section 4.5 reports the results of the empirical analysis. Last, we discuss the implications of the results for practice and theory in Section 4.6.

4.2 Theoretical Background

We build a conceptual model that examines how privacy concerns, awareness of firms' privacy protection, and expected benefits influence consumer willingness to disclose personal information. The study focuses on investigating how expected benefits, website types and the type of information disclosed moderate the main effects of privacy concerns, awareness of firms' protection policy, and expected benefits on consumer willingness. The model is woven by joining two theories: information boundary theory and social exchange theory.

First, the Information Boundary Theory (IBT) builds an individual informational space of information disclosure with her/his own boundary, which depends on the nature of disclosed information and individual and environmental characteristics (Petronio, 2002). The theory predicts that individuals' reactions to information collection about them follow dynamic, psychological processes, by which they attempt to control boundary opening and boundary closure for their personal information (Stanton & Stam, 2003). Depending on individual and environmental characteristics, an attempt by an external organization to penetrate these boundaries may be differently perceived by the individual as privacy intrusion (Xu, et al., 2008). IBT has been applied for building a reasonable foundation for understanding privacy management in IT intensive

organizations (Stanton & Stam, 2003; Xu, et al., 2008; Zakaria, Stanton, & Stam, 2003). They argued that when the individual detects a request for information disclosure by an organization (e.g., an online retailer), the individual initiates her/his own privacy calculus with the risks the benefits of disclosure and decides the disclosure as acceptable or unacceptable based on privacy calculus. In terms of influential factors on individuals' boundaries, Phelps et al. (2000) presented a conceptual model in which consumers' privacy concerns are determined by the type of personal information requested, the amount of information control offered, the potential consequences and benefits offered in the exchange, and consumer characteristics. They proposed these factors not only influence consumer concerns regarding marketers' information practices and overall concerns affect consumers' future behavioral and attitudinal responses to marketing strategies.

Second, the Social Exchange Theory (SET) asserts that individuals weigh the costs and benefits to decide whether to engage in social exchanges. If the benefits outweigh the costs, then the individual is willing to enter into an exchange relationship. Indeed, SET concepts has been applied for conceptualizing a wide range of relationship-marketing paradigms, which have developed over the past few decades in consumer to business as well as business to business sectors (Hald, Cordon, & Vollmann, 2009; Luo, 2002; Pappas & Flaherty, 2008; Ross & Robertson, 2007; Stanton & Stam, 2003). Relationship marketing involves relational exchanges, which take place not only for money as discounts but also for non-monetary benefits such as high quality service, or personalized offers (Awad & Krishnan, 2006; Chellappa & Shivendu, 2007; Chellappa

& Sin, 2005; Kobsa, 2007; Mabley, 2000). This is especially important to understand how to alleviate the effect of privacy concerns on disclosing personal information for establishing a B2C relationship. When given more benefits and mitigating privacy concerns by awareness of a firm's privacy protection practices in *e*-Commerce, consumers are willing to provide their private data because they are not concerned about improper information collection, or improper monitoring (H. Q. Wang, Lee, & Wang, 1998). On the other hand, if consumers cannot believe their transactions and data are handled safely and securely, they try to switch providers. In particular, the more competitive industry becomes, the more information firms require with various purposes such as personalized services or direct marketing. However, it can make consumers feel private information has been violated, while a firm believes it provides better services to consumers.

4.3 Research Model and Hypotheses

The research model was built by integrating information privacy with theories reviewed in the previous section. Figure 4.1 shows a graphical summary of our conceptual framework with the specific constructs to answer the research questions. The research model is depicting measured variables (i.e., web type and the type of personal information) as rectangles and latent or unmeasured variables as ovals.

Consumer willingness to provide personal information over the Internet involves weighing privacy concerns, a website's privacy protection, and the benefits exchanged with their information. Hence, consumers should determine the degree to which they will provide their personal information based on those factors. Previous literature has

investigated this consumer decision including privacy calculus from an economic perspective (Diney & Hart, 2006; Hann, Hui, Lee, & Png, 2008). However, consumers tend to involve a cognitive decision process, comprising privacy risk, privacy protection and benefits rather than making an economic cost-benefit analysis with unpredictable outcomes.

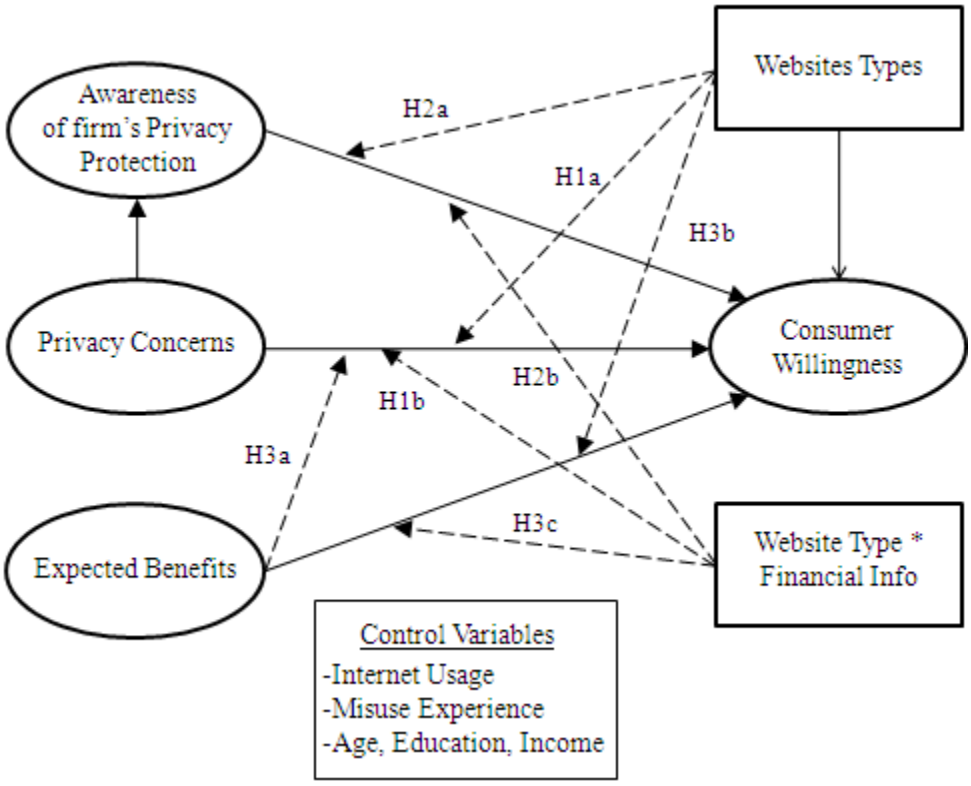


Figure 4.1The Conceptual Model

This essay studies a cognitive decision process that consumers make when personal information was requested by each type of websites. A type of personal information being exposed is critical in this decision process, because it makes consumers have a different level of perceived privacy risks (Belanger, Hiller, & Smith, 2002). Many researchers indicate that consumer willingness to disclose information depends on the

type of requested information (Metzger, 2006, 2007; J. Phelps, et al., 2000). Phelps (2000) found that consumers are more willing to provide demographic and lifestyle information than financial and contact information. Metzger (2006) claimed that consumers are more willing to provide basic demographic information than browsing, contact, and financial information. Also, the type of websites poses different types of risks such as financial risks (i.e., credit card frauds or price discrimination) and information risks (i.e., personal identifiers to be disclosed to unauthorized others) (Bart, Shankar, Sultan, & Urban, 2005) in consumers' perception of privacy concerns. For example, online retailers hold both types of risks, while search engines bear information risks about personal identifiers and browsing habits rather than financial risks. Thus, this essay focuses on examining how the strength of the relationship between privacy-related factors and consumer willingness varies with the type of information to be disclosed and the type of websites.

First, we examine the degree to which the type of information to be disclosed and website types moderate the main effect of privacy concerns on consumer willingness to be profiled in a website. Although many studies have found that most consumers have refused to provide some personal information, this study has delved deeper into consumer willingness to share their information with different types of both websites and requested information. A few marketing studies suggested that consumers are more protective of financial data and personal identifiers rather than habit and lifestyle information(J. Phelps, et al., 2000; J. E. Phelps, et al., 2001).

In addition, the type of websites (i.e., search engines or online retailers) changes the relevance of those types of personal information requested, and then the effect of privacy concerns on consumer willingness would be altered. For instance, financial information is necessary to purchase a product in an online retailer's website, while it is not in a search engine site. On the other hand, browsing habits might be relevant for both of web sites types for personalized services and offerings (Awad & Krishnan, 2006). Given the evidence, we predict that

Hypothesis 1a: *An online retailer that requests overall personal information negatively moderates the effect of privacy concerns on consumer willingness to disclose the information more than a search engine.*

Hypothesis 1b: *An online retailer that requests financial information negatively moderates the effect of privacy concerns on consumer willingness to disclose the information more than a search engine.*

Firms attempt to address consumers' privacy concerns regarding online profiling by posting their privacy policy online or adopting privacy seals such as TRUSTe, WebTrust, or BBBOnline (Moores & Dhillon, 2003; Vail, et al., 2008). Privacy policies are written statements, usually posted on a firm's web site, and describe all the types of personally identifiable information that may be collected, how it is collected, and how it will be used and/or shared. Previous studies suggest that policy decisions as well as the development of protection technology tools reduce information privacy concerns in protecting consumers' privacy (Culnan, 2000; Vail, et al., 2008). Thus, if consumers are well aware of a website's a privacy protection practices such as privacy policy and

privacy seals, they would be more likely to provide their information (Hui, Teo, & Lee, 2007). The effect of their awareness on willingness could be changed based on a type of a website and types of requested information by the website. While many studies have measured an overall influence of firms' privacy protection, it is still critical to study their influence in detail. Therefore, we hypothesized that

Hypothesis 2a: *A search engine that requests overall personal information positively moderates the effect of consumer awareness of a firm's privacy protection on consumer willingness to disclose the information more than an online retailer.*

Hypothesis 2b: *An online retailer that requests financial information positively moderates the effect of consumer awareness of a firm's privacy protection on consumer willingness to disclose the information more than a search engine.*

From the theoretical standpoint of SET, expected benefits such as personalized services and offerings affect consumer willingness associated with privacy concerns about information disclosure. Awad and Krishnan (2006) argued that consumers with a higher level of privacy concern will likely perceive personalized services and offerings to be of less value than consumers with a lower level of privacy concern (Awad & Krishnan, 2006). Given this evidence, this study investigates whether expected benefits in exchange for personal information can motivate consumers who express concern over their own privacy, to share such information in the online. Also, it examines how the effect of expected benefits could be altered by a type of a website and the type of

requested information. Thus, we hypothesize that greater expected benefits is associated with being more willing to be profiled online despite privacy concern.

Hypothesis 3a: *Consumers' expected benefits positively moderates the effect of privacy concerns on consumer willingness to disclose personal information.*

Hypothesis 3b: *An online retailer that requests overall personal information positively moderates the effect of expected benefits on consumer willingness to share the information more than a search engine.*

Hypothesis 3c: *An online retailer that requests financial information positively moderates the effect of expected benefits on consumer willingness to share the information more than a search engine.*

4.4 Data Collection

The Internet survey was conducted among Internet users in the US from March 2009 to May 2009. The sample consisted of an Internet panel put together by Survey Sampling International LLC [4]. Compared with postal mail or telephone surveys, Internet surveys are a faster and cheaper way to collect a great amount of data than the postal mail or telephone surveys. The written questionnaire contained the four latent constructs including privacy concerns, consumer willingness to share personal information, awareness of firms' privacy protection, and expected benefits exchanged with information. They were assessed using a five-point Likert scale. Items were adapted

[4] See *www.surveysampling.com :Survey Sampling International LLC provides sampling solutions for survey research. It offers access to consumer and business-to-business respondents through Internet, telephone, and mobile.*

from past research privacy concerns (Eastlick, et al., 2006; Milne & Boza, 1998). Internet usage and experience of misused information were added as single-item instruments. The total number of responses was 685, of which 615 were valid. Table 4.1 provides a summary of respondent characteristics. We controlled for consumer demographics, including income, and education, when testing this model, because it is likely that the effects of the constructs described in the model may vary with certain demographic variables.

Table 4.1 Socioeconomic and Demographic Characteristics

	# of respondents		# of respondents
Income:	n=618	**Education:**	n=665
Less than $15,000	50	High school degree	211
$15,000 to under $25,000	61	Some college	251
$25,000 to under $35,000	78	College degree	150
$35,000 to under $50,000	109	Graduate school or degree	53
$50,000 to under $75,000	161		
$75,000 to under $100,000	73	**Marital Status:**	n=685
More than $100,000	86	Married	447
		Never Married	110
Age:	n=677	Widowed/divorced	128
18 to 24	24		
25 to 34	87	**Location of Residence:**	n=656
35 to 44	232	Urban	144
45 to 54	240	Suburban	317
55 and others	94	Rural	195
		Gender:	n=666
Employ Status:	n=673	Female	530
Full time	272	Male	136
Part time	115	**Ethnicity:**	n=661
Others	286	Caucasian	546
		Other	115

Privacy Concerns. Five items were designed to evaluate consumers' privacy concerns about firms' obligation and how consumers value privacy (Eastlick, et al., 2006; Milne & Boza, 1998). Although privacy has many different meanings based on different contexts, this study defined privacy concerns as consumers concern about

fairness and control over personal information in information systems (A. J. Campbell, 1997).

Awareness of privacy protection. Privacy awareness reflects the extent to which a customer is informed about privacy practices and policies, and third-party institutional mechanisms such as TRUSTe, BBB Online, WebTrust, and PWC Privacy (Olivero & Lunt, 2004). A five-item scale was employed to assess consumers' privacy awareness of privacy protection.

Expected Benefits. When profiled online by sharing personal information, consumers face many costs associated with perceived risks. Consumers' expected benefits exchanged with the risks include convenience, easiness, and saving time due to personalized services and offerings. Economic theories suggest that individuals would disclose personal information for sufficient benefits (Chellappa & Shivendu, 2007; Dinev et al., 2006; Diney & Hart, 2006). We measure expected benefits exchanged with personal information in terms of preference of personalized services, convenience, and time saving.

Website Type. This study categorized online services into two categories: Search engines and Online Retailers. This measure examines how the inherent functions of a website influence consumer willingness to provide each type of personal information (Bart, et al., 2005; J. Phelps, et al., 2000). To eliminate brand reputation, the survey gave specific examples which include Google and Yahoo for Search engines and Amazon.com for Online Retailers.

Personal Information. The privacy literature suggests that personal information falls into the four categories (Olivero & Lunt, 2004; J. Phelps, et al., 2000). Table 4.2 lists the types and items that each type includes. This study measured consumer willingness to disclose each type of information requested by different types of websites.

Table 4.2 The Type of Personal Information Requested by a Firm

Categories	Personal Information
Contact Information	Name, E-mail address, Mailing address, Telephone
Demographic Information	Gender, Age, Education, Income, Personal interests, Hobbies
Behavioral Information	Browsing habits
Financial Information	Credit card numbers, Bank account

Consumer Willingness. Regardless of industries, firms collect and use specific consumer information to acquire competitive advantages by capturing consumers' needs in a tough market. Consumer personal information, requested by a firm, can be generally classified as contact, behavioral, demographic, and financial information (Meinert, Peterson, Criswell, & Crossland, 2006). The types of personal information have various degrees to which each type draws consumer privacy concerns (Milne 1997; Nowak and Phelps, 1992).

Consumer Type. Previous literature established that age, education, and income are positively associated with the degree of stated Internet privacy concern (Diney & Hart, 2006; Kobsa & Teltzrow, 2005). Gender effects on Internet privacy concerns have yet to be clearly established. So, our study just includes age, education, and income into consumer type.

4.5 Research Methodology and Results

A Structural Equation Model (SEM) approach using Partial Least Squares (PLS) was employed to test the hypotheses of this study. The PLS algorithm iteratively maximizes the strength of the relation of successive predictors and the dependent component scores by maximizing the covariance of each predictor-score with the dependent variables. PLS is robust in the face of violation of the usual statistical assumptions of latent variable modeling such as multicollinearity and multivariate normality (Cassel et al., 1999, 2000). Most of all, PLS has been found to be an effective analytical tool to test interaction effects (Chin, Marcolin, & Newsted, 2003). Also, given that model complexity is naturally exacerbated when adding these interaction terms with distributional problems, PLS provides a flexible means for addressing these concerns (Wicks & Chin, 2008).

Table 4.3 Descriptive Statistics and Correlation Matrix

Construct Scale	#Items	Descriptive		Correlations			
		M	SD	1	2	3	4
1.Privacy concerns	4	3.07	1.56	**.69**			
2.Awareness	3	2.63	1.55	.42**	**.70**		
3.benefits	4	3.57	1.93	.21*	.26**	**.73**	
4.willingness	4	1.15	.95	-.33*	-.15	.07*	**.67**

Note1. *The average variance extracted is presented in bold characters in the correlation matrix*
Note2. *p-values are represented by * p<.05,**<.01, *** p<.001*

This study investigates the interaction effects by the type of websites and the type of personal information by incorporating latent multiplicative variables in the structural model by employing SmartPLS, which is software to implement PLS for SEM. SmartPLS can easily handle interaction effects to implements the product terms provided by Chin et al (2003). The measures for interaction term are created by creating

all possible products of standardized indicators of predictor and moderator variables (Chin, et al., 2003).

Table 4.4 Measurement Properties of the PLS Model

Construct	Statement	Factor loading	Reliability
Willingness to provide personal information			.830
	Willingness to provide Contact information	.810	
	Willingness to provide Demographic information	.819	
	Willingness to provide Browsing habits	.841	
	Willingness to provide Financial information	.828	
Privacy Concerns			.734
	Concerned about firms' intention in collecting personal information	.821	
	Concerned about firms' fulfillment in privacy statements	.794	
	Concerned about secondary use of personal information	.778	
	Concerned about information security and accuracy	.824	
Awareness			.712
	Awareness of third-party institutional mechanisms	.802	
	Awareness of privacy policy	.823	
	Awareness of cookies	.635	
Benefits			.894
	I can provide personal information for easiness in online	.855	
	I can provide personal information for convenience	.857	
	I can provide personal information for saving time	.871	
	I can provide personal information for personalized services (i.e., recommendation, offerings)	.856	

We evaluated the measurement model by examining the reliability of the individual items and the discriminant/convergent validity of the constructs for proving the adequacy of the measures. First, we compared the average variance extracted (AVE) from each construct with its correlations with the other constructs as a test of discriminant/ convergent validity. As indicated in Table 4.3, all values representing the square root of AVE are greater than all the other correlations. In addition, principal component factor analysis was employed to test the construct reliability and validity.

The results are presented in Table 4.4. The validity of the construct was assessed by examining the cross-loadings, which shows that no item loads more highly on another construct than it does on the construct it is intended to measure. The results provide evidence that the indicators and their underlying constructs were acceptable.

Table 4.5 Structural Model 1: No Multiplicative Variable

Path	Overall	Contact	Demo	Browsing	Finance
Privacy Concerns → Consumer Willingness	-.374*** (11.85)	-.283*** (9.53)	-.293*** (9.68)	-.255*** (9.19)	-.271*** (11.55)
Awareness of Protection → Consumer Willingness	.014 (0.45)	-.028 (0.89)	-.031 (0.99)	.020 (0.67)	.086** (2.96)
Privacy Concerns→ Awareness of Protection	.486*** (17.11)	.488*** (15.83)	.489*** (17.63)	.488*** (15.69)	.487*** (18.98)
Expected Benefits → Consumer Willingness	-.008 (0.56)	.001 (0.04)	-.017 (0.69)	-.007 (0.26)	.035 (1.04)
WebType → Consumer Willingness	.133*** (5.79)	.190*** (7.47)	.006 (0.22)	-.036 (1.31)	.265** (11.09)
Consumer Type → Privacy Concerns	.283*** (7.06)	.262*** (6.17)	.242*** (6.89)	.242*** (6.41)	.249*** (6.47)
Misuse Experience → Privacy Concerns	.199*** (6.81)	.182*** (6.77)	.200*** (6l37)	. 201*** (7.90)	. 202*** (7.51)
Internet Usage → Awareness of Protection	.113*** (2.87)	.097** (2.76)	.095*** (2.69)	.095*** (3.19)	.095** (2.86)
R-squares	.15	.11	.10	.06	.13

***Note**. t-values are in parentheses. p-values are represented by * p<.05,**<.01, *** p<.001*

After establishing the validity of the measures, we tested the structural paths in the research model using PLS. Table 4.5 and 4.6 report the standardized path coefficients and t-values for the models we tested. The significance level was assessed with a two-tailed distribution. Consistent with the procedure suggested by Chin et al. (2003), the PLS models which both did not include (Model 1) multiplicative variables and included them (Model 2) were performed. The inclusion of the multiplicative variables explains

an additional about 4% of the variance in consumer willingness to provide both overall and financial information. Then, we emphasize the presentation of Model 2.

Table 4.6 Structural Model 2: Multiplicative Variables

Path	Overall	Contact	Demo	Browsing	Finance	Hypotheses
Privacy Concerns → Consumer Willingness	-.387*** (11.02)	-.289*** (8.57)	-.153*** (9.53)	-.251*** (7.18)	-.269*** (8.07)	
Awareness of Protection → Consumer Willingness	-.005 (0.95)	-.031 (1.12)	-.037 (1.27)	-.006 (0.20)	.025 (0.67)	
Privacy Concerns→ Awareness of Protection	.460*** (15.79)	.488*** (18.21)	.489*** (16.77)	.488*** (16.89)	.487*** (17.12)	
Expected Benefits → Consumer Willingness	.010 (0.74)	-.016 (0.45)	.006 (0.26)	.001 (0.05)	.053 (0.93)	
WebType → Consumer Willingness	.133*** (4.88)	.134* (1.62)	.109 (0.23)	-.036* (1.82)	.125*** (3.40)	
WebType * Privacy Concerns → Consumer Willingness	-.041** (2.59)					***H1a: Supported***
		-.065 (1.04)	-.030 (0.60)	.027 (0.53)	-.144*** (4.61)	***H1b: Supported***
WebType * Awareness of Protection → Consumer Willingness	-.042** (2.36)					***H2a: Supported***
		-.035* (1.67)	-.034 (0.74)	-.026 (0.50)	.152* (1.98)	***H2b: Supported***
Expected Benefits * Privacy Concerns → Consumer Willingness	.050*** (3.53)	.019* (1.81)	.013 (0.57)	.024 (0.86)	.027* (2.25)	***H3a: Supported***
WebType * Expected Benefits → Consumer Willingness	.028 (1.51)					***H3b:Not Supported***
		.061* (1.67)	-.010 (0.58)	.024 (0.52)	.050* (1.97)	***H3c: Supported***
Consumer Type → Privacy Concerns	.258*** (8.68)	.242*** (6.74)	.242*** (7.05)	.249*** (6.89)	.276*** (6.86)	
Misuse Experience → Privacy Concerns	.201*** (7.09)	.201*** (7.78)	.200*** (2.41)	.201*** (7.07)	.202*** (8.69)	
Internet Usage → Awareness of Protection	.092*** (3.89)	.095*** (3.11)	.095*** (4.09)	.095*** (3.31)	.119*** (3.71)	
R-squares	.19	.15	.12	.11	.17	

Note. *t-values are in parentheses. p-values are represented by * p<.05,**<.01, *** p<.001*

In addition, separate analyses were run for consumer willingness to provide overall personal information and four types of personal information (i.e., contact, demographic, browsing, and financial information). Path coefficients were generated for each sub sample, and then were compared to determine whether the relationship between a set of predictors (i.e., Privacy Concerns, Awareness of Privacy Protection, and Expected Benefits) and consumer willingness to provide personal information depended on Web site types.

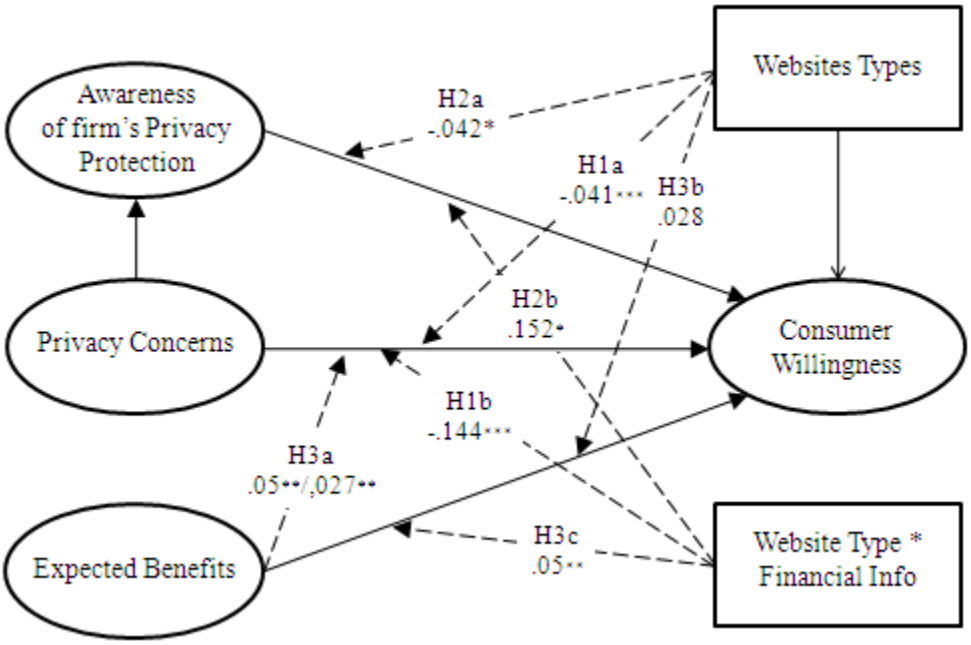


Figure 4.2 PLS Completely Standardized Path Coefficients

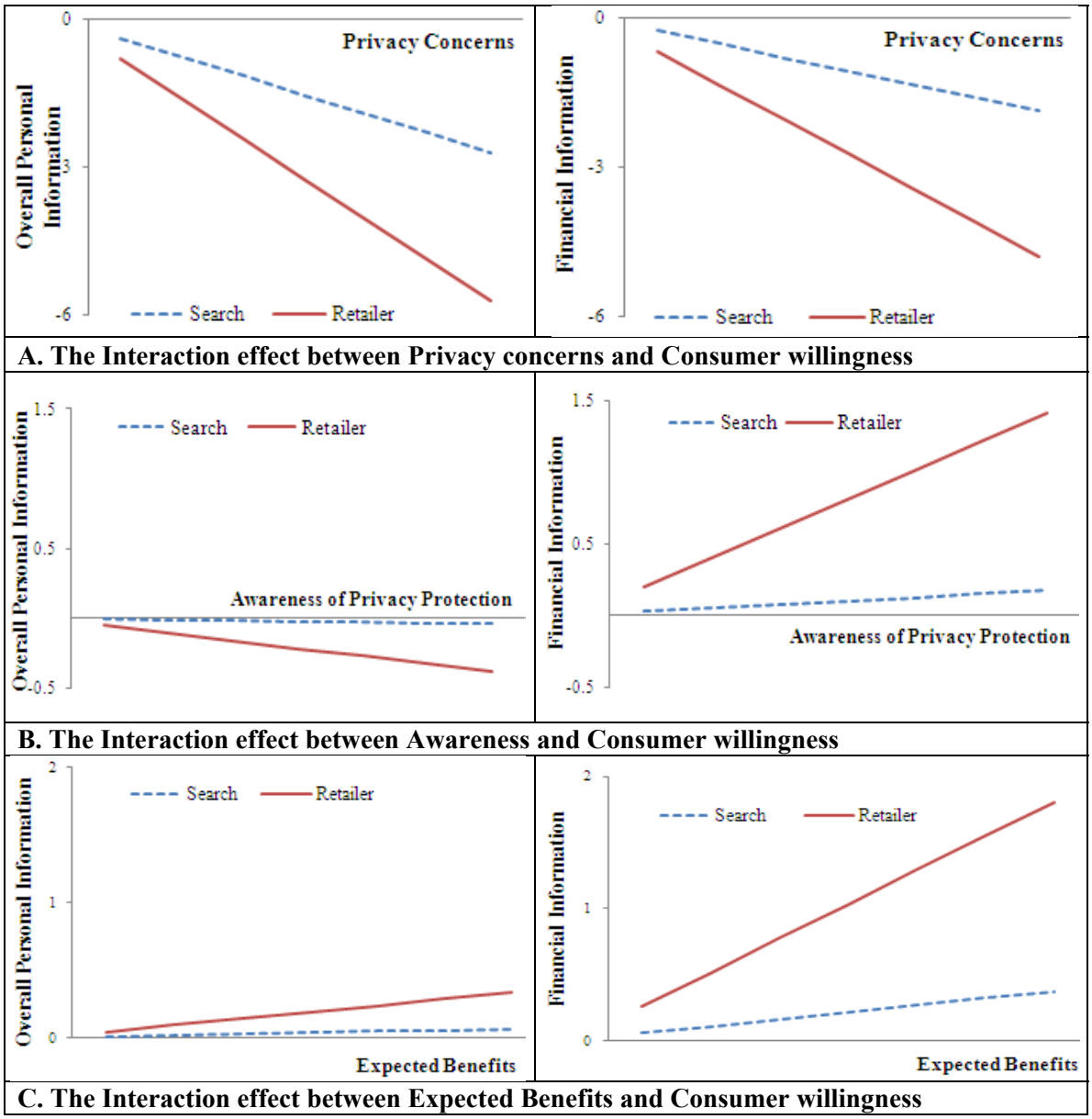
The results from separate analyses tells overall, contact and financial information, which have the possibility of personal identifier disclosure and incurring monetary losses, have higher R-squares and more significant coefficients than those of demographic and browsing information. Furthermore, this study investigated other combinations of contact, demographic, and browsing information. Appendix B shows

the results from these combinations. The outcomes suggested they have much lower R-squares and their coefficients are less significant than those of separate types and overall personal information. Therefore, this study mainly discusses the results the overall and financial information.

First, in terms of control variables, the consumer type, which include age, education, and income, is positively related to privacy concerns (*path coefficient* =.283 in Model 1 and .258 in Model 2). The finding is consistent with those of privacy literature (Dommeyer and Gross, 2003). Misuse Experience also has a positive relationship with privacy concerns (*path coefficient* =.199 and .201) and Internet usage significantly increases their awareness of privacy protection (*path coefficient* =.113 and .092). Similarly, in the separate analyses of sub-personal information, Consumer Type and Misuse Experience have also positive main effects on privacy concerns and Internet usage is positively related to consumer awareness of privacy protection.

Second, the main effects of privacy concerns, awareness of privacy protection, and expected benefits on consumer willingness are intertwined. Privacy concerns show significantly negative effect, while awareness of privacy protection and expected benefits statistically do not have any significant effect on consumer willingness in both Model 1 and Model 2. However, the effects of awareness of privacy protection and expected benefits have amplified with the type of websites in terms of interaction effects. To test the hypotheses based on the interaction effects, we investigated the effects of a website type by multiplicative variables in Model 2. The completely standardized path coefficients of the structural model provide evidence for the hypothesized interaction

effects by examining the role of a website type on the strength of the relationships between privacy concerns, awareness, expected benefits and willingness.



A. The Interaction effect between Privacy concerns and Consumer willingness

B. The Interaction effect between Awareness and Consumer willingness

C. The Interaction effect between Expected Benefits and Consumer willingness

Figure 4.3 The Interaction Effects of a Website Type

The results of our hypotheses tests are shown on Figure 4.2, and the comparisons of the separate analyses were illustrated in Figure 4.3. Model 2 shows the larger magnitude of the effect of privacy concerns on consumer willingness (H1a) were supported with a

path coefficient, -.041 at level $p<0.05$. Similarly, a website type also significantly increases the effect of privacy concerns on consumer willingness to provide financial information with -.144 at level $p\leq0.01$ (H1b). Figure 4.3A also shows the similar patterns of the interaction effects of websites on privacy concerns.

Kobsa and Teltzrow (2005) demonstrated that website visitors disclosed significantly more information about themselves when the website explained the user benefits and the site's privacy protection practices in connection with the requested data for every requested piece of personal information. However, our study failed to statistically demonstrate any significant effect of awareness of privacy protection as a main effect. Consumer awareness decreases consumer willingness to provide overall personal information with a path coefficient, -.005, while it increases consumer willingness to provide financial information with coefficient, .025, although neither are significant effects. This would be why awareness of privacy protections mitigates the effect of privacy concerns, as they were shown in Figure 4.1. Consumer awareness of privacy protection results from privacy concerns, which directly and negatively affect consumer willingness, and consumer awareness results in consumer willingness to provide personal information. Thus, the study more deeply investigated the effect of consumer awareness as mitigating effect, and then it suggests consumers' awareness of privacy protection should make them more willing to provide financial information for online retailers, while awareness would not have any effect in other information such as contact, demographic, and browsing information.

Due to these conflicting results, this study focused on examining whether a website type significantly reinforces or mitigate the effect of consumer awareness of privacy protection on consumer willingness to provide personal information. The outcome showed that a website type has significantly contrary influences in the effect of awareness of privacy protection on consumer willingness to provide the overall and financial information with path coefficients, -.042 ($p \leq .01$) and .152 ($p \leq .05$), which are statistically significant. However, H2a was supported with a negative coefficient in the overall information, while H2b was supported with a positive coefficient in financial information. This implies that consumer awareness significantly mitigates the effect of privacy concerns on consumer willingness to provide financial information for online retailers more than other information. Figure 4.3B compares the interaction effects of website types on consumer awareness.

Last, we investigated how a website type changes the effect of consumers' expected benefits on consumer willingness to provide personal information. Although the main effects of expected benefits statistically do not have any significant effect in all analyses, the interaction effects of expected benefits on the relationship between privacy concerns and consumer willingness to provide overall and financial information have a significant influence with a path coefficient, .05 ($p < .001$). However, the interaction effect of a website on the relationship between expected benefits and consumer willingness to provide overall personal information does not have a significant effect. Thus, we failed to provide any evidence for supporting H3b with coefficient, .028 at *t-value,* 1.51. On the other hand, in terms of financial information, consumer willingness was significantly

increased when consumers work with online retailers more than with search engines, with a path coefficient, .05 at level $p < .05$, by which H3c was supported. Figure 4.3C displays the comparison of the interaction effects of website type on expected benefits.

Overall, this result shows consumers' privacy concerns make them less willing to provide their information. However, if a website provides more information about its privacy protection and benefits exchanged with personal information for consumers who visit the website, consumers become more willing to provide their information. These effects of awareness of privacy protection and expected benefits especially become larger when consumers need to provide financial information for online retailers than search engines. In terms of overall personal information including all types of information, the effect of awareness of privacy protection decreases consumer willingness, while expected benefits significantly make consumers more willing to provide their overall personal information.

4.6 Discussions and Conclusions

This study empirically examines how the effects of privacy concerns, awareness of privacy protection, and expected benefits on willingness, are influenced by different types of information and website types. The primary goal of this paper was to develop and empirically test an extended model of the privacy calculus in which a set of the interaction effects of various environmental factors (i.e., types of requested information and website types) was hypothesized to affect consumer willingness to provide personal information.

The analyses indicated that all the constructs' properties exceeded the established criteria for instrument reliability and discriminant validity (Table 4.3 and 4.4). To prove the significant interaction effect of types of requested information and websites, we run PLS and compared R-squares from Model 1 with no multiplicative variables and Model 2 with multiplicative variables. The latter model explains an additional 4~5% of the variance in consumer willingness (Table 4.5 and 4.6). The results supported 6 out of 7 hypotheses (Table 4.6).

The factors examined in the model comprise a set of factors in a decision process in which competing privacy concerns and benefits are weighed and where the mitigating effect of awareness of privacy protection and the direct effect of privacy concern may outweigh the influence of each other. This study focuses on investigating the interaction effects of environmental factors in the decision process. Overall, a type of which website consumers deal with strongly influences the effects of privacy concerns, awareness of privacy protection, and expected benefits exchanged with personal information. In addition, the magnitude and direction of the effects vary with types of requested personal information.

The theoretical model is based on the notions of Information Boundary Theory and Social Exchange Theory, which the individual initiates her own privacy calculus with the risks the benefits of disclosure and decides the disclosure based on privacy calculus, when the individual detects a request for information disclosure by a website. The pattern of these results provides insight into the complex process that leads to the decision to provide personal information. A high level of consumer willingness to

provide financial information must be preceded by higher levels of awareness of privacy protection and expected benefits, despite consumer resistance to personal information disclosure due to privacy concerns. Furthermore, consumer willingness for financial information disclosure increases when consumers deal with online retailers more than search engines. On the other hand, consumer willingness for all four types of personal information disclosure is increased only by expected benefits, and awareness of privacy protection does not have any statistically significant effect. These findings suggest that expected benefits such as personalized systems should be able to explain to consumers which information about them are being stored and how these are going to be used, while awareness of privacy protection indirectly is increased by privacy concerns, which significantly decrease consumer willingness, and at the same time awareness directly increases consumer willingness.

While prior studies incorporated privacy concerns and benefits as predictors of consumer willingness to provide personal information (Jarvenpaa & Tiller, 2001; Pavlou & Gefen, 2004), the model we tested incorporated specified types of requested personal information and website types which request the information over the Internet as the moderators, as well as the predictors which prior studies included. Our model explains the drivers of consumer willingness to provide various types of personal information in the context of privacy-related factors, such as expected benefits and awareness of privacy protection with different types of website. From the models, the study observed the potential value of generating awareness and informing consumers of the relevant usage of each type of collected personal information and benefits based on each website.

These activities can make consumers more willing to provide their information despite privacy concerns.

In conclusion, this paper provides insight into the argument made by practitioners and economists about the privacy calculus (e.g., Ackerman et al. 1999; Sweat 2000), namely that privacy concern contradicts consumers' expected benefits exchanged with personal information. Consumer willingness with regard to information disclosure is the result of a combination of factors that indirectly and directly affects privacy concerns when there is a decision in favor of information disclosure. These results would suggest practitioners and economists should not assume that personal information disclosure reflects simply a lack of privacy concerns, but should recognize that consumer willingness to personal information disclosure could have grown despite consumers' privacy concerns if a website makes consumers more aware of its privacy protection and benefits based on its service types and types of requested information. Then, website providers need to be vigilant in seeking ways to promote benefits exchanged with personal information and their privacy protection practices.

For future research, we need to incorporate the characteristics of specific firms, such as their reputation, website designs, and brand image, since the direct and indirect effect of firm heterogeneity are strong influences on consumer willingness. As the measures for this, the page view raking and brand equity can be considered. Further, future research could be undertaken to understand the multi-dimensions of consumer privacy concerns such as confidentiality, integrity, and availability, in order to clarify how each

dimension might be related to established legal issue and potential differential effects of each on consumer behavior.

CHAPTER 5. CONCLUSIONS

This dissertation provides two different perspectives in investigating information risk management: from an internal perspective, performance measurement related to information breaches and IT internal control weaknesses, and from an external perspective, consumer value drivers to provide high-quality products or services.

The first essay examines how IT executive involvement in a TMT and their compensation structures affect organizational performance in information risk management, which requires interdependency across all departments as well as a degree of maturity in an organization's capability to manage risks through continuous improvement in all daily information processes. Litigation and governmental investigation have forced firms to produce electronically stored information across a firm's all functional departments, which are exposed to internal and external risks. Then, it is imperative for executive-level leadership to exercise information risk management activities over such highly variable processes fraught with risk and uncertainty across a firm. Although many researchers have examined executive compensation through a wide variety of theoretical lenses, a few studies have attempted to integrate compensation structures within specific tasks such as information risk management or highly uncertain circumstances. The first essay synthesized information risk management and compensation research, which involves more specific tasks such as ensuring IT internal controls and preventing information breaches. To our knowledge,

this study provides the first in-depth, cross-level empirical analysis of compensation for IT executives. It contributes to the literature on executive compensation in several ways. First, it provides a deeper understanding of how an effort/outcome uncertainty of tasks for which executives should take responsibility affects their compensation structure. The results indicate task uncertainty of an effort/outcome function influences compensation structure. Second, it provides the first insight into both cross-sectional IT executive compensation and the distribution of compensation among executives within a firm. The findings have important implications for top executives and compensation policy makers. The importance of task-specific factors in setting compensation levels suggests that IT executives should pay considerable attention to task characteristics in their career planning. The questions and issues addressed in the current study will continue to be important to firms' information risk management, especially as the IT executives are influential in handling the interdependence between business units.

The second essay examines how the privacy concerns, awareness of privacy protection, and expected benefits are influenced by the disclosure of different types of information and website types. To prove the significant interaction effect of types of requested information and websites, we run PLS and compared R-squares from two models with/without multiplicative variables. The model with multiplicative variables explains an additional 4~5% of the variance in consumer willing nesses and supports 6 out of 7 hypotheses. The factors examined in the model comprise a set of constituent in decision process in which competing privacy concerns and benefits are weighed and where the effects of awareness of privacy protection and the direct effect of privacy

concerns on consumer willingness may outweigh the influence of each other. Overall, types of which website consumers transact with strongly influence the effects of privacy concerns, awareness of privacy protection, and expected benefits exchanged with personal information. In addition, the magnitudes and directions of the effects vary with the types of requested personal information. The second essay first has linked these variables to information sharing over the Internet. These results show that consumer willingness to personal information disclosure could have grown if consumers can recognize a website's privacy protection and benefits exchanged with information sharing despite their privacy concerns. Thus, we suggest practitioners and economist should not assume that personal information disclosure reflects simply a lack of privacy concerns, but should recognize consumer willingness could have grown by making consumers more aware of its privacy protection and benefits based on its service types and types of requested information. This study observed the potential value of generating awareness and informing consumers of the relevant usages of collected each type of personal information and benefits based on each website. These activities can make consumers more willing to provide their information despite privacy concerns. Then, a website providers need to be vigilant in seeking ways to promote benefits exchanged with personal information and their privacy protection practices.

In conclusion, we can expect that organizations will increasingly rely on information technology and information risk management will continue to receive a great deal of attention. Failure to manage information risk could create a loss of customer confidence and lost sales. This dissertation lends support to the inclusion of information risk

management as part of the enterprise governance process, thereby aligning information risk management with other core business assets and processes critical to the success of the firm. When information risks are seen only as an operational component of information technology it may be difficult for management outside of IT to contribute to or support information assurance initiatives or to build a case for information risk management. This wider view and participation in information risk management strategies and activities must be an essential component as internally part of the enterprise governance process as well as externally part of establishing customer relationship on the adoption of electronic channels.

BIBLIOGRAPHY

BIBLIOGRAPHY

Aggarwal, R. K., & Samwick, A. A. (2003). Performance incentives within firms: The effect of managerial responsibility. *Journal of Finance, 58*(4), 1613-1649.

Allison, P. D. (1999). *Logistic regression using the SAS system: theory and application*.

Anderson, E. (2008). The salesperson as outside agent or employee: A transaction cost analysis. *Marketing Science, 27*(1), 70-84. doi: 10.1287/mksc.1070.0333

Armstrong, C. P., & Sambamurthy, V. (1996, Dec 15-18). *Information technology assimilation in firms: The influence of senior leadership and IT infrastructures.* Paper presented at the 17th International Conference on Information Systems, Cleveland, Ohio.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13-28.

Ba, S. L., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243-268.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all Web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing, 69*(4), 133-152.

Barua, A., Konana, P., Whinston, A. B., & Yin, F. (2001). Driving E-business excellence. *Mit Sloan Management Review, 43*(1), 36-+.

Basu, A., & Jarnagin, C. (2008). How to Tap IT's Hidden Potential. *The Wall Street Journal.Com*. Retrieved from http://online.wsj.com/article/SB120467900166211989.html

Beatty, R. P., & Zajac, E. J. (1994). Managerial Incentives, Monitoring, and Risk Bearing - A Study of Executive-Compensation, Ownership, and Board Structurae in Initial Public Offerings. *Administrative Science Quarterly, 39*(2), 313-335.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3-4), 245-270.

Bishop, J. (1987). The Recognition and Reward of Employee Performance. *Journal of Labor Economics, 5*(4), S36-S56.

Bloom, M. (1999). The performance effects of pay dispersion on individuals and organizations. *Academy of Management Journal, 42*(1), 25-40.

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the Internet: Self-regulation or government regulation? *Business Ethics Quarterly, 16*(3), 323-342.

Cai, C. X., Keasey, K., & Short, H. (2006). Corporate governance and information efficiency in security markets. *European Financial Management, 12*(5), 763-787.

Campbell, A. J. (1997). Relationship Marketing in Consumer Markets. *Journal of Direct Marketing, 11*, 46-48.

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28-46. doi: 10.1287/isre.1050.0041

Chellappa, R. K., & Shivendu, S. (2007). An economic model of privacy: A property rights approach to regulatory choices for online personalization. *Journal of Management Information Systems, 24*(3), 193-225. doi: 10.2753/mos0742-1222240307

Chellappa, R. K., & Sin, R. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management, 6*, 181-202. doi: 10.1007/s10799-005-5879-y

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research, 14*(2), 189-217.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing, 19*(1), 20-26.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115.

Dameri, R. P. (2008). Using an Enterprise Information Management System to Enhance IT Compliance and Information Value. *Proceedings of the 2nd European Conference on Information Management and Evaluation*, 111-121.

Dess, G. G., & Beard, D. W. (1984). Dimensions of Organizational Task Environments. *Administrative Science Quarterly, 29*(1), 52-73.

Dhar, V., & Sundararajan, A. (2007). Information technologies in business: A blueprint for education and research. *Information Systems Research, 18*(2), 125-141.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce - a study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389-402. doi: 10.1057/palgrave.ejic.3000590

Diney, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*(1), 61-80. doi: 10.1287/isre.1060.0080

Doyle, J., Ge, W., & McVay, S. (2005, Oct 01-02). *Determinants of weaknesses in internal control over financial reporting.* Paper presented at the Conference on Corporate Governance - Financial Report, Internal Control and Auditing, Cambridge, MA.

Doyle, J. T., Ge, W., & McVay, S. (2007). Accruals quality and internal control over financial reporting. *Accounting Review, 82*(5), 1141-1170.

Drazin, R., & Vandeven, A. H. (1986). Alternative Forms of Fit in Contingency Theory *Administrative Science Quarterly, 30*(4), 514-539.

Dubin, R. (1976). *Theory building in applied areas*: Chicago: Rand McNally.

Dumagan, J., & Gill, G. (2002). Industry-Level Effects of Information Technology Use on Productivity and Inflation *U.S. Department of Commerce*. Washington DC.: Digital Economy.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877-886. doi: 10.1016/j.jbusres.2006.02.006

Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science, 31*(2), 134-149.

Eisenhardt, K. M. (1989). Agency Theory - An Assessment and Review. *Academy of Management Review, 14*(1), 57-74.

Enns, H. G., Huff, S. L., & Higgins, C. A. (2003). CIO lateral influence behaviors: Gaining peers' commitment to strategic information systems. *MIS Quarterly, 27*(1), 155-176.

Ernst, & Young. (2008). Moving Beyound compliance, Global Information Security Survey. Retrieved from http://www.ey.com/AU/en/About-us/Our-alumni/Moving-beyond-compliance

Fiss, P. C. (2006). Social influence effects and managerial compensation evidence from Germany. *Strategic Management Journal, 27*(11), 1013-1031. doi: 10.1002/smj.558

Frederickson, J. R. (1992). Relative Performance Information - The Effects of Common Uncertainty and Contract type on Agent Effort. *Accounting Review, 67*(4), 647-669.

Gartner. (2008). The evolving role of CISO in the New security Order. Retrieved from www.thectoforum.com/content/evolving-role-ciso

Gordon, L., & Loeb, M. (2002). The Economics of Information Security Investment. *ACM Transactions On Information and System Security, 5*(4), 438.

Gordon, L., & Loeb, M. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy, 25*(5), 503-530.

Hald, K. S., Cordon, C., & Vollmann, T. E. (2009). Towards an understanding of attraction in buyer-supplier relationships. *Industrial Marketing Management, 38*(8), 960-970. doi: 10.1016/j.indmarman.2008.04.015

Hall, J. A., & Liedtka, S. L. (2005). Financial performance, CEO compensation, and large-scale information technology Outsourcing decisions. *Journal of Management Information Systems, 22*(1), 193-221.

Hann, H., Hui, K. L., Lee, S. Y. T., & Png, I. P. L. (2008). Consumer privacy and marketing avoidance: A static model. [Article]. *Management Science, 54*(6), 1094-1103. doi: 10.1287/mnsc.1070.0837

Harrison, J. R., Torres, D. L., & Kukalis, S. (1988). The Changing Of The Guard - Turnover and Structural-Change in The Top-Management Positions. *Administrative Science Quarterly, 33*(2), 211-232.

Henderson, A. D., & Fredrickson, J. W. (2001). Top management team coordination needs and the CEO pay gap: A competitive test of economic and behavioral views. *Academy of Management Journal, 44*(1), 96-117.

Holthausen, R. W., Larcker, D. F., & Sloan, R. G. (1995). Business Unit Innovation The Structure Of Eexecutive- Compensation. *Journal of Accounting & Economics, 19*(2-3), 279-313.

Hosmer, D. W., & Lemeshow, S. (1992). *Applied Logistic Regression*: WILEY Inter-Science.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19-33.

Huselid, M. A. (1995). The Impact Of Human-Resource Management-Practices On Turnover, Productivity, and Corporate Financial Performance. *Academy of Management Journal, 38*(3), 635-672.

ITGI. (2005). *Board Briefing on IT Governance*. http://www.isaca.org/sox/.

ITGI. (2006). *IT Control Objectives For Sarbanes-Oxley*. http://www.isaca.org/sox/.

Jaccard, J. (2001). *Interaction effects in logistic regression*: A SAGE University Paper.

Jarvenpaa, S. L., & Ives, B. (1991). Executive Involvement and Participation in the Management of Information Technology. *MIS Quarterly, 15*(2), 205-227.

Jarvenpaa, S. L., & Tiller, E. H. (2001). Customer trust in virtual environments: A managerial perspective. *Boston University Law Review, 81*(3), 665-686.

Johnston, A. C., & Hale, R. (2009). Improved Security through Information Security Governance. *Communications of the Acm, 52*(1), 126-129. doi: 10.1145/1435417.1435446

Kalikiri K., H. (2009). How can IT be a key business differentiator? *CTO Forum*. Retrieved from http://www.thectoforum.com/content/how-can-it-be-key-business-differentiator

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. [Article]. *International Journal of Electronic Commerce, 12*(1), 69-91. doi: 10.2753/jec1086-4415120103

Kesner, I. F., & Sebora, T. C. (1994). Executive Succession - Past, Present and Future. *Journal of Management, 20*(2), 327-372.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. [Article]. *Decision Support Systems, 44*(2), 544-564. doi: 10.1016/j.dss.2007.07.001

Kim, N. Y., Robles, R. J., Cho, S. E., Lee, Y. S., & Kim, T. H. (2008). SOX Act and IT Security Governance. *International Symposium on Ubiquitous Multimedia Computing, Proceedings*, 218-221.

Kobsa, A. (2007). Privacy-enhanced personalization - Multi-pronged strategies are needed to reconcile the tension between personalization and privacy. *Communications of the Acm, 50*(8), 24-33.

Kobsa, A. (2008). Privacy-Enhanced Personalization. *New Directions in Intelligent Interactive Multimedia, 142*, 31-31.

Kobsa, A., & Teltzrow, M. (2005). Contextualized communication of privacy practices and personalization benefits: Impacts on users' data sharing and purchase behavior. *Privacy Enhancing Technologies, 3424*, 329-343.

Kokolakis, S. A., & Kiountouzis, E. A. (2000). Achieving interoperability in a multiple-security-policies environment. *Computers & Security, 19*(3), 267-281.

Krishnan, J., Rama, D., & Zhang, Y. (2008). Costs to comply with SOX Section 404. *Auditing-a Journal of Practice & Theory, 27*(1), 169-186.

Lazear, E. P. (1995). Personnel economics. Cambridge, MA: MIT Press.

Lazear, E. P., & Rosen, S. (1981). Rank-Order Tournaments As Optimum Labor Contracts. *Journal of Political Economy, 89*(5), 841-864.

Lee, M. K. O., & Turban, E. (2000, Aug 24). *A trust model for consumer Internet shopping.* Paper presented at the Meeting of the International Conference on Electronic Commerce 2000 (ICEC2000), Seoul, South Korea.

Li, C., Lim, J.-H., & Wang, Q. (2007). Internal and external influences on IT control governance. *International Journal of Accounting Information Systems, 8*, 225-229.

Luo, X. M. (2002). Trust production and privacy concerns on the Internet - A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, 31*(2), 111-118.

Mabley, K. (2000). Privacy vs. Personalization. www.cyberdialogue.com.

Main, B. G. M., Oreilly, C. A., & Wade, J. (1993). Top Executive Pay - Tournament or Teamwork. *Journal of Labor Economics, 11*(4), 606-628.

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*, 622-660. doi: 10.1108/14684520710832333

Meinert, D., Peterson, D., Criswell, J., & Crossland, M. (2006). Would Regulation of Web Site Privacy Policy Statements Increase Consumer Trust? *Informing Science, 9*, 123-142.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research, 33*(3), 155-179. doi: 10.1177/0093650206287076

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2).

Milne, G. R., & Boza, M.-E. (1998). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing, 13*(1), 5-24.

Minton, J., Lewicki, R., & Sheppard, B. (1994). Unjust Dismissal in the Context of Organizational Justice. *Annals of the American Academy of Political and Social Science, 536*(135-148).

Mitchell, V. L. (2006). Knowledge integration and information technology project performance. *MIS Quarterly, 30*(4), 919-939.

Moores, T. T., & Dhillon, G. (2003). Do privacy seals in e-commerce really work? *Communications of the ACM, 46*(12), 265-271.

Muralidhar, K., Parsa, R., & Sarathy, R. (1999). A general additive data perturbation method for database security. *Management Science, 45*(10), 1399-1415.

Nagar, V. (2002). Delegation and incentive compensation. *Accounting Review, 77*(2), 379-395.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology, 25*(2), 243-262. doi: 10.1016/s0167-4870(02)00172-1

Pappas, J. M., & Flaherty, K. E. (2008). The effect of trust on customer contact personnel strategic behavior and sales performance in a service environment. *Journal of Business Research, 61*(9), 894-902. doi: 10.1016/j.jbusres.2007.09.017

Park, J., Shin, S. K., & Sanders, G. L. (2007). Impact of international information technology transfer on national productivity. *Information Systems Research, 18*(1), 86-102. doi: 10.1287/isre.1070.0116

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37-59.

Pavlou, P. A., Liang, H. G., & Xue, Y. J. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105-136.

Perlman, E. (2007). Topside Turnover. *Governing*. Retrieved from http://www.governing.com/topics/public-workforce/Topside-Turnover.html

Petrison, L. A., & Wang, P. (1993). From Relationships To Relationship Marketing - Applying Database Technology To Public-Relations. *Public Relations Review, 19*(3), 235-245.

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*: State University of New York Press, Albany, NY.

Pfeffer, J., & Langton, N. (1993). The Effect Of Wage Dispersion On Satisfaction, Productivity, and Working Collaboratively - Evidence From College and University-Faculty. *Administrative Science Quarterly, 38*(3), 382-407.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and Consequences of Consumer Privacy Concerns : An Empirical Investigation. *Journal of Interactive Marketing, 14*(4).

Posthumus, S., & von Solms, R. (2005). A responsibility framework for information security. *Security Management, Integrity, and Internal Control in Information Systems, 193*, 205-221.

Preston, D. S., Chen, D., & Leidner, D. E. (2008). Examining the Antecedents and Consequences of CIO Strategic Decision-Making Authority: An Empirical Study. *Decision Sciences, 39*(4), 605-642. doi: 10.1111/j.1540-5915.2008.00206.x

Raghupathi, W. (2007). Corporate governance of IT: A framework for development. *Communications of the Acm, 50*(8), 94-99.

Ransbotham, S., & Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. [Article]. *Information Systems Research, 20*(1), 121-139. doi: 10.1287/isre.1080.0174

Rittenberg, L. E., & Miller, P. K. (2005). Sarbanes-Oxley Section 404 Work Looking at the Benefits. *The IIA Research Foundation*. Retrieved from www.theiia.org/download.cfm?file=343

Roepke, R., Agarwal, R., & Ferratt, T. W. (2000). Aligning the IT human resource with business vision: The leadership initiative at 3M. *MIS Quarterly, 24*(2), 327-353.

Ross, W. T., & Robertson, D. C. (2007). Compound relationships between firms. *Journal of Marketing, 71*(3), 108-123.

Sale, H. A. (2006). Independent directors as securities monitors. *Business Lawyer, 61*(4), 1375-1412.

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *Mis Quarterly, 23*(2), 261-290.

Santalo, J., & Kock, C. J. (2009). Division Director Versus CEO Compensation: New Insights Into the Determinants of Executive Pay. [Article]. *Journal of Management, 35*(4), 1047-1077. doi: 10.1177/0149206308329965

Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors into buyers: How web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing, 70*(2), 133-148.

Schoonhoven, C. B. (1981). Problems With Contingency Theory - Testing Assumptions Hidden Within The Language OF Contingency Theory. *Administrative Science Quarterly, 26*(3), 349-377.

Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computers & Security, 20*(7), 620-634.

Schwartz, B. (1968). Social Psychology Of Privacy. *American Journal of Sociology, 73*(6), 741-752.

SEC Release. No 33-8128, S. (2002). *Acceleation of periodic report filing dates and disclosure concerning website access to reports*.

Selnes, F. (1998). Antecedents and consequences of trust and satisfaction in buyer-seller relationships. *European Journal of Marketing, 32*(3/4), 305-322.

Shankar, V., Smith, A. K., & Rangaswamy, A. (2003). Customer satisfaction and loyalty in online and offline environments. *International Journal of Research in Marketing, 20*(2), 153-175. doi: 10.1016/s0167-8116(03)00016-8

Shaw, J. D., Gupta, N., & Delery, J. E. (2002). Pay dispersion and workforce performance: Moderating effects of incentives and interdependence. *Strategic Management Journal, 23*(6), 491-512. doi: 10.1002/smj.235

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising, 28*(3), 37-51.

Siegel, P. A., & Hambrick, D. C. (2005). Pay disparities within top management groups: Evidence of harmful effects on performance of high-technology firms. *Organization Science, 16*(3), 259-274. doi: 10.1287/orsc.1050.0128

Sipior, J. C., Ward, B. T., & Rongione, N. M. (2003). Ethics of collecting and using consumer Internet data. *Information Systems Management, 21*(1), 58-66.

Smaltz, D. H., Sambamurthy, V., & Agarwal, R. (2004, Oct). *The antecedents of CIO role effectiveness in organizations: An empirical study in the healthcare sector.* Paper presented at the Conference on Information Systems and Technology, Denver, CO.

Smith, H. J. (2001). Information privacy and marketing: What the US should (and shouldn't) learn from Europe. *California Management Review, 43*(2), 8-+.

Stanton, J. M., & Stam, K. (2003). Information Technology, Privacy, and Power within Organizations: A Merger of Boundary Theory and Social Exchange Perspectives. *Surveillance and Society, 2*(Spring), 152-190.

Staw, B. M. (1980). The Consequences Of Turnover. *Journal of Occupational Behaviour, 1*(4), 253-273.

Steenkamp, J., & Geyskens, I. (2006). How country characteristics affect the perceived value of web sites. *Journal of Marketing, 70*(3), 136-150.

Stephens, C. S., Ledbetter, W. N., Mitra, A., & Ford, F. N. (1992). Executive or Fuctional Manager-The Nature of the CIOs Job. *MIS Quarterly, 16*(4), 449-467.

Stoel, D., & Muhanna, W. A. (2009). *IT Internal Control Weaknesses and Firm Performance: An Empirical Investigation*.

Strassmann, P. A. (1994). CIOs should get back to Basics. *Datamation, 40*(18), 70-72.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce, 7*(3), 135-161.

Ton, Z., & Huckman, R. S. (2008). Managing the impact of employee turnover on performance: The role of process conformance. *Organization Science, 19*(1), 56-68. doi: 10.1287/orsc.1070.0294

Turban, E., Leidner, D., Mclean, E., & Wetherbe, J. (2008). *Information technology for management : transforming organizations in the digital economy*.

Vail, M. W., Earp, J. B., & Anton, A. I. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *Ieee Transactions on Engineering Management, 55*(3), 442-454. doi: 10.1109/tem.2008.922634

von Solms, S. H. (2005). Information Security Governance - Compliance management vs operational management. *Computers & Security, 24*(6), 443-447. doi: 10.1016/j.cose.2005.07.003

Wang, & Emurian, H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior, 21*(1), 105-125. doi: 10.1016/j.chb.2003.11.008

Wang, H. Q., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63-70.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research, 19*(1), 106-120. doi: 10.1287/isre.1070.0143

Wicks, A. M., & Chin, W. W. (2008). Measuring the three process segments of a customer's service experience for an out-patient surgery center. *Int J Health Care Qual Assur, 21*(1), 24-38.

Xu, H., Dinev, T., Smith, J. H., & Hart, P. (2008). *Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View.* Paper presented at the International Conference on Information Systems (ICIS), Paris.

Yayla, A., & Hu, Q. (2008). *Determinants of CIO Compensation Structure and Its Impact on Firm Performance*. Paper presented at the Hawaii International Conference on System Sciences, Proceedings of the 41st Annual.

Zakaria, N., Stanton, J., & Stam, K. (2003). Exploring security and privacy issues in hospital information system: an Information Boundary Theory perspective. *AMIA Annu Symp Proc*, 1059.

Zhu, K., & Kraemer, K. L. (2002). e-Commerce metrics for net-enhanced organizations: Assessing the value of e-commerce to firm performance in the manufacturing sector. *Information Systems Research, 13*(3), 275-295.

APPENDICES

Appendix A. The Breached Firms

No	Event Date	Company Name	Type of Incident	Type of Breaches
1	1/24/2003	SIEBEL SYSTEMS INC	worm	Availability
2	1/28/2003	BOEING CO	worm	Availability
3	1/28/2003	COUNTRYWIDE FINANCIAL CORP	Site attack	Availability
4	1/30/2003	IBM	Data Lost	Confidentiality
5	2/6/2003	BANK OF AMERICA CORP	worm	Integrity
6	2/6/2003	WASHINGTON MUTUAL INC	worm	Availability
7	2/19/2003	AMERICAN EXPRESS CREDIT CORP	Hacking	Confidentiality
8	2/20/2003	MASTERCARD INC	Hacking	Confidentiality
9	4/30/2003	DIRECTV GROUP INC	Hacking	Confidentiality
10	5/8/2003	MICROSOFT CORP	Hacking	Availability
11	6/18/2003	GUESS INC	Program Errors	Confidentiality
12	8/11/2003	ACXIOM CORP	Hacking	Confidentiality
13	8/15/2003	MICROSOFT CORP	worms	Integrity
14	8/21/2003	CSX CORP	virus	Integrity
15	9/10/2003	KNIGHT-RIDDER INC	Site attack	Availability
16	10/1/2003	BEST BUY CO INC	Hacking	Integrity
17	11/22/2003	WELLS FARGO & CO	Data Stolen	Confidentiality
18	11/27/2003	WELLS FARGO & CO	Hacking	Confidentiality
19	12/18/2003	Acxiom Corp.	Data Breach	Confidentiality
20	2/2/2004	GATEWAY INC	System Errors	Confidentiality
21	2/2/2004	IOMEGA CORP	System Errors	Confidentiality
22	2/2/2004	KOHL'S CORP	System Errors	Confidentiality
23	2/2/2004	OPEN SOLUTIONS INC	System Errors	Confidentiality
24	2/2/2004	SAKS INC	System Errors	Confidentiality
25	2/2/2004	TIFFANY & CO	System Errors	Confidentiality
26	2/13/2004	MICROSOFT CORP	Data Lost	Confidentiality
27	3/16/2004	EBAY INC	Hacking	Integrity
28	3/19/2004	BJ'S WHOLESALE CLUB INC	System Errors	Confidentiality
29	4/14/2004	MICROSOFT CORP	Data Breach	Integrity
30	5/18/2004	CISCO SYSTEMS INC	Code Theft	Integrity
31	6/7/2004	LOWE'S COMPANIES INC	Hacking	Confidentiality
32	6/16/2004	AKAMAI TECHNOLOGIES INC	Site attack	Availability
33	6/26/2004	MICROSOFT CORP	Data Stolen	Confidentiality

34	7/14/2004	INTUIT INC	Data Stolen	Confidentiality
35	7/27/2004	GOOGLE INC	Virus	Integrity
36	7/27/2004	YAHOO INC	Virus	Integrity
37	9/28/2004	SUNTRUST BANKS INC	Site attack	Availability
38	10/27/2004	GOOGLE INC	Hacking	Confidentiality
39	11/3/2004	WELLS FARGO & CO	Data Stolen	Confidentiality
40	11/11/2004	AFFILIATED COMPUTER SERVICES	Hacking	Confidentiality
41	12/8/2004	SUNTRUST BANKS INC	Phising	Availability
42	12/27/2004	LYCOS INC	Site attack	Availability
43	2/14/2005	ChoicePoint	Data Breach	Confidentiality
44	2/25/2005	Bank of America	Data Lost	Confidentiality
45	3/5/2005	Automatic Data Processing	Program Errors	Confidentiality
46	3/23/2005	Bank of America,Columbia Funds	Data Breach	Confidentiality
47	3/23/2005	City National Bank	Data Breach	Confidentiality
48	3/23/2005	Nuveen Investments	Data Breach	Confidentiality
49	3/23/2005	Pimco	Data Breach	Confidentiality
50	3/23/2005	U S BANCORP	Data Breach	Confidentiality
51	4/5/2005	MCI	Data Stolen	Confidentiality
52	4/13/2005	Polo Ralph Lauren	Hacking	Confidentiality
53	4/14/2005	COMCAST CORP	illegal data exposed	Confidentiality
54	4/26/2005	Foster Wheeler, Clinton, N.J	Hacking	Confidentiality
55	4/28/2005	Bank of America	Illegal data selling	Confidentiality
56	4/28/2005	Commerce Bank	Illegal data selling	Confidentiality
57	4/28/2005	PNC Bank of Pittsburgh	Illegal data selling	Confidentiality
58	4/28/2005	Wachovia	Illegal data selling	Confidentiality
59	5/2/2005	Time Warner	Data Lost	Confidentiality
60	5/8/2005	IRON MOUNTAIN INC	Data Lost	Confidentiality
61	5/28/2005	Motorola	Data Stolen	Confidentiality
62	6/7/2005	UNITED PARCEL SERVICE INC	Data Lost	Confidentiality
63	6/17/2005	MasterCard International	Hacking	Confidentiality
64	6/21/2005	CVS CAREMARK CORP	System Errors	Confidentiality
65	7/8/2005	IRON MOUNTAIN INC	Data Lost	Confidentiality
66	7/29/2005	EBAY INC	Program Errors	Availability
67	8/8/2005	Huntington National Bank, Toledo, Ohio	Data Stolen	Confidentiality
68	8/8/2005	J.P. Morgan Private Bank.	Data Breach	Confidentiality

69	8/12/2005	VERIZON COMMUNICATIONS INC	Program Errors	Integrity
70	9/22/2005	ChoicePoint	Program Errors	Confidentiality
71	9/23/2005	Bank of America	Data Stolen	Confidentiality
72	10/8/2005	BLOCKBUSTER INC	Data Lost	Confidentiality
73	11/5/2005	SAFEWAY INC	Data Stolen	Confidentiality
74	11/7/2005	PAPA JOHNS INTERNATIONAL INC	Program Errors	Confidentiality
75	11/18/2005	Boeing Co	Data Stolen	Confidentiality
76	12/6/2005	SAM'S CLUB	Program Errors	Integrity
77	12/21/2005	Ford Motor Co	Data Stolen	Confidentiality
78	12/22/2005	H&R Block	Program Errors	Confidentiality
79	12/25/2005	Convergys	Program Errors	Integrity
80	12/27/2005	Marriott International	Data Lost	Confidentiality
81	1/1/2006	Progressive Casualty Insurance	Data Breach	Confidentiality
82	1/2/2006	H&R Block	Program Errors	Integrity
83	1/11/2006	UNITED PARCEL SERVICE INC	Data Lost	Confidentiality
84	1/20/2006	Honeywell International	Data Breach	Confidentiality
85	1/25/2006	Ameriprise Financial	Data Stolen	Confidentiality
86	1/31/2006	FedEx Freight West.	System Errors	Integrity
87	2/1/2006	Automatic Data Processing	Data Breach	Confidentiality
88	2/6/2006	Regions Bank	System Errors	Confidentiality
89	2/14/2006	BANK OF AMERICA CORP	Data Stolen	Confidentiality
90	2/14/2006	OFFICEMAX INC	Hacking	Confidentiality
91	2/14/2006	WASHINGTON MUTUAL INC	Hacking	Confidentiality
92	2/14/2006	WELLS FARGO & CO	Hacking	Confidentiality
93	2/17/2006	McAfee	Data Lost	Confidentiality
94	2/20/2006	Verizon Communications Inc.(Alltel Corporation)	Data Lost	Confidentiality
95	3/1/2006	American Insurance Group (AIG)	Hacking	Confidentiality
96	3/1/2006	MEDCO HEALTH SOLUTIONS INC	Data Stolen	Confidentiality
97	3/1/2006	Verizon Communications	Data Stolen	Confidentiality
98	3/13/2006	General Motors	Hacking	Confidentiality
99	4/3/2006	AUTHORIZE.NET HOLDINGS INC	Data Stolen	Confidentiality

100	4/6/2006	Iron Mountain / Long Island Railroad	Data Lost	Confidentiality
101	4/7/2006	Fifth Third Bank	Data Breach	Confidentiality
102	4/26/2006	MASTERCARD INC	Hacking	Availability
103	4/26/2006	MORGAN STANLEY	Data Breach	Confidentiality
104	4/29/2006	Union Pacific Corporation	Data Stolen	Confidentiality
105	5/1/2006	Equifax	Data Stolen	Confidentiality
106	5/5/2006	Wells Fargo	Data Stolen	Confidentiality
107	5/6/2006	Mercantile Bank shares	Data Stolen	Confidentiality
108	6/2/2006	ELECTRONIC DATA SYSTEMS CORP	Data Stolen	Confidentiality
109	6/27/2006	AAAAA Rent-A-Space	Data Breach	Confidentiality
110	6/29/2006	AllState Insurance	Data Breach	Confidentiality
111	7/5/2006	BISYS GROUP INC	Data Lost	Confidentiality
112	7/6/2006	AUTOMATIC DATA PROCESSING	Data Breach	Integrity
113	7/26/2006	Netscape.com	Hacking	Availability
114	8/1/2006	Affiliated Computer Services, Inc	Program Errors	Confidentiality
115	8/1/2006	DOLLAR TREE INC	System Errors	Integrity
116	8/1/2006	U S BANCORP	Data Breach	Confidentiality
117	8/1/2006	Weyerhaeuser	Data Breach	Confidentiality
118	8/1/2006	Williams Sonoma, Inc	Data Stolen	Integrity
119	8/8/2006	LINENS N THINGS INC	Data Breach	Integrity
120	8/14/2006	Chevron	Data Stolen	Confidentiality
121	8/21/2006	Sovereign Bank	Data Stolen	Confidentiality
122	8/23/2006	Xerox	Data Stolen	Confidentiality
123	8/25/2006	Verizon Wireless	Data Breach	Integrity
124	8/27/2006	AT&T	Hacking	Availability
125	8/28/2006	Wells Fargo	Data Stolen	Confidentiality
126	9/7/2006	Chase Card Services	Data Lost	Confidentiality
127	9/24/2006	General Electric Co	Data Stolen	Confidentiality
128	10/1/2006	Gymboree	Site attack	Availability
129	10/1/2006	TD Ameritrade Holding Corp	Hacking	Integrity
130	10/26/2006	Aetna	Data Stolen	Confidentiality
131	11/3/2006	Starbucks	Data Stolen	Confidentiality
132	12/12/2006	Money Gram International	Data Breach	Availability
133	12/14/2006	Bank of America	Data Breach	Integrity
134	12/14/2006	Boeing	Data Stolen	Confidentiality
135	12/20/2006	TJX	Data Breach	Confidentiality

136	12/29/2006	KEYCORP	Data Stolen	Confidentiality
137	1/12/2007	KB Home	Data Stolen	Confidentiality
138	1/19/2007	Electronic Data Systems-EDS	Data Stolen	Confidentiality
139	1/23/2007	XEROX CORP	Data Stolen	Confidentiality
140	1/26/2007	Chase/Bank One	Illegal data selling	Confidentiality
141	2/1/2007	Washington Mutual	Hacking	Integrity
142	2/23/2007	IBM	Data Lost	Confidentiality
143	3/14/2007	WELLPOINT INC	Data Stolen	Confidentiality
144	3/28/2007	RadioShack	Data Lost	Confidentiality
145	4/1/2007	Bank of America	Data Stolen	Confidentiality
146	4/1/2007	Caterpillar Inc.	Data Stolen	Confidentiality
147	4/1/2007	Life Time Fitness	Data Stolen	Confidentiality
148	4/7/2007	AOL	Hacking	Integrity
149	4/15/2007	JP Morgan Chase	Data Breach	Confidentiality
150	4/17/2007	CVS CAREMARK CORP	Data Breach	Confidentiality
151	4/27/2007	Google	Hacking	Integrity
152	5/15/2007	Columbia Bank	Hacking	Integrity
153	5/19/2007	Texas First Bank- S1 Corp	Data Stolen	Confidentiality
154	5/25/2007	Pfizer	Data Stolen	Integrity
155	5/28/2007	Dollar General	Data Breach	Integrity
156	5/29/2007	GfK Custom Research North	Data Stolen	Availability
157	5/29/2007	SAIC	Data Breach	Integrity
158	6/3/2007	Fidelity National Information	Data Breach	Confidentiality
159	6/11/2007	PFIZER INC	Data Stolen	Confidentiality
160	6/21/2007	AMERICAN AIRLINES INC	Data Breach	Confidentiality
161	7/6/2007	Western Union	Hacking	Confidentiality
162	7/25/2007	Merrill Lynch	Data Stolen	Confidentiality
163	7/27/2007	AT&T	Data Stolen	Integrity
164	7/31/2007	Textron	Data Stolen	Confidentiality
165	8/6/2007	VERISIGN INC	Data Stolen	Confidentiality
166	8/7/2007	Electronic Data Systems	Data Breach	Integrity
167	9/10/2007	Wachovia Bank	Data Breach	Integrity
168	9/12/2007	UNITEDHEALTH GROUP INC	Data Lost	Confidentiality
169	9/14/2007	TD AMERITRADE HOLDING CORP	Hacking	Confidentiality
170	9/19/2007	Gap Inc.	Data Stolen	Confidentiality
171	9/20/2007	Semtech	Data Lost	Confidentiality
172	9/25/2007	E-Bay	Site attack	Availability

173	9/25/2007	Pfizer- Wheels, Inc.	Program Errors	Confidentiality
174	10/1/2007	Citibank	Hacking	Availability
175	10/10/2007	Commerce Bank	Hacking	Integrity
176	10/15/2007	Home Depot, Massachusetts	Data Stolen	Confidentiality
177	10/16/2007	ADMINISTAFF INC	Data Stolen	Integrity
178	10/22/2007	Blockbuster	Data Lost	Confidentiality
179	10/30/2007	HARTFORD FINANCIAL SERVICES	Data Breach	Availability
180	11/28/2007	Oracle Corporation	Data Lost	Confidentiality
181	12/1/2007	WA Bank of America	Data Breach	Confidentiality
182	12/3/2007	Wendy's International	Data Stolen	Confidentiality
183	12/21/2007	GENERAL ELECTRIC CO	Data Lost	Confidentiality
184	12/21/2007	IRON MOUNTAIN INC	Data Lost	Confidentiality
185	12/21/2007	Iron Mountain-GE Money-Americas	Data Lost	Confidentiality
186	1/1/2008	People's United Bank	Data Lost	Confidentiality
187	1/8/2008	Google Website	Hacking	Confidentiality
188	1/15/2008	Kraft Foods	Data Stolen	Confidentiality
189	1/31/2008	Marriott International - Hewitt	Data Lost	Confidentiality
190	2/10/2008	Old Navy	Data Breach	Integrity
191	2/16/2008	Genworth Life and Annuity Insurance Co	Data Breach	Confidentiality
192	2/18/2008	Stryker Instruments	Hacking	Confidentiality
193	2/20/2008	3M Company	Data Stolen	Confidentiality
194	3/1/2008	Agilent -Stock & Option Solutions	Data Stolen	Confidentiality
195	3/5/2008	SunGard Availability Services (SAS) #2	Data Lost	Confidentiality
196	3/8/2008	Viacom Inc.(MTV Network)	Data Breach	Confidentiality
197	4/1/2008	Pfizer Inc	Data Stolen	Integrity
198	4/8/2008	WELLCARE HEALTH PLANS INC	Program Errors	Confidentiality
199	4/8/2008	WELLPOINT INC	Data Breach	Confidentiality
200	4/10/2008	Community Bank	Data Breach	Confidentiality
201	4/10/2008	H&R Block	Data Breach	Integrity
202	4/22/2008	Verizon Wireless	Data Breach	Confidentiality
203	4/23/2008	First Bank and Trust	Data Breach	Confidentiality
204	4/29/2008	Merrill Corporation	Program Errors	Confidentiality
205	5/1/2008	Adobe Systems Inc	Data Breach	Integrity
206	5/1/2008	BB&T CORP	Data Stolen	Confidentiality

207	5/11/2008	SunGard Data Systems/ Newedge	Data Breach	Confidentiality
208	5/15/2008	AT&T	Data Stolen	Confidentiality
209	5/16/2008	Wells Fargo	Data Breach	Integrity
210	5/27/2008	Charter Communications	Data Breach	Availability
211	6/9/2008	United Transportation Union	Data Lost	Confidentiality
212	7/1/2008	Wells Fargo	Data Breach	Integrity
213	7/15/2008	Charter Communications	Data Stolen	Confidentiality
214	7/17/2008	BRISTOL-MYERS SQUIBB CO	Data Breach	Confidentiality
215	7/25/2008	Delphi	Data Lost	Confidentiality
216	7/30/2008	United Bancorp of WY-Parent Company	Data Lost	Confidentiality
217	8/1/2008	American Greetings / UPS	Data Breach	Integrity
218	8/7/2008	Bank of America	Data Stolen	Confidentiality
219	8/23/2008	Wells Fargo #2	Data Lost	Confidentiality
220	8/28/2008	Cape Coral Wachovia Bank	Data Lost	Confidentiality
221	8/29/2008	Bear, Stearns Corp, JP Morgan Chase	Program Errors	Confidentiality
222	9/2/2008	Keizer Lowe's	Data Breach	Confidentiality
223	9/10/2008	COUNTRYWIDE FINANCIAL CORP	Data Breach	Confidentiality
224	9/21/2008	Bank of America	System Errors	Integrity
225	9/24/2008	Rite Aid	Data Lost	Confidentiality
226	10/17/2008	Community Bank	Program Errors	Confidentiality
227	10/18/2008	Symantec	Data Stolen	Confidentiality
228	10/29/2008	Starbucks Corp	Data Stolen	Confidentiality
229	11/13/2008	Pulte Homes Las Vegas	Data Breach	Confidentiality
230	12/3/2008	Hewlett Packard	Data Stolen	Confidentiality
231	12/8/2008	Bank of America	Hacking	Integrity
232	12/10/2008	Regions Bank	Data Stolen	Confidentiality

Appendix B. The Comparison of Other Combinations of Personal Information

Model 3: No multiplicative Variable

Path	Contact+ Demo	Contact + Browsing	Demo + Browsing	Contact + Demo + Browsing
Privacy Concerns → Consumer Willingness	-.325*** (10.47)	-.313*** (10.69)	-.315*** (10.00)	-.343*** (11.23)
Awareness of Protection → Consumer Willingness	-.033 (1.06)	.001 (0.03)	-.005 (0.18)	-.015 (0.51)
Privacy Concerns→ Awareness of Protection	.488*** (18.64)	.487*** (15.59)	.488*** (16.56)	.488*** (17.33)
Expected Benefits → Consumer Willingness	-.008 (0.27)	-.009 (0.37)	-.012 (0.42)	.-007 (0.28)
WebType → Consumer Willingness	.111*** (4.37)	.057** (2.19)	-.017 (0.60)	.065* (2.37)
Consumer Type → Privacy Concerns	.242*** (6.45)	.242*** (7.19)	.242*** (6.51)	.242*** (5.80)
Misuse Experience → Privacy Concerns	.201*** (8.09)	.201*** (7.20)	.201*** (7.86)	.201*** (7.69)
Internet Usage → Awareness of Protection	.095*** (2.76)	.095*** (2.59)	.095*** (2.96)	.095** (2.95)
R-squares	.13	.10	.10	.11

Model 4: Multiplicative Variables

Path	Contact+ Demo	Contact + Browsing	Demo + Browsing	Contact + Demo + Browsing
Privacy Concerns → Consumer Willingness	-.333*** (9.54)	-.322*** (9.83)	-.321*** (10.75)	-.351*** (10.17)
Awareness of Protection → Consumer Willingness	-.037 (1.30)	-.005 (1.15)	-.009 (1.30)	-.019* (1.63)
Privacy Concerns→ Awareness of Protection	.488*** (17.19)	.487*** (15.28)	.488*** (15.72)	.488*** (16.83)
Expected Benefits → Consumer Willingness	-.006 (0.28)	-.007 (0.27)	-.011 (0.30)	-.005 (1.19)
WebType → Consumer Willingness	-.011*** (4.85)	-.057* (2.03)	-.017 (0.65)	.065* (2.32)
WebType * Privacy Concerns → Consumer Willingness	-.047* (1.86)	-.049* (1.76)	-.030* (1.60)	-.045* (1.84)
WebType * Awareness of Protection → Consumer Willingness	-.028 (1.59)	-.038 (0.75)	-.029 (0.72)	-.032* (1.73)
Expected Benefits * Privacy Concerns → Consumer Willingness	.024* (1.94)	.028* (1.61)	.001* (1.69)	.024* (1.98)
WebType * Expected Benefits → Consumer Willingness	-.001 (1.46)	.019 (1.03)	.016 (1.07)	.019 (1.51)
Consumer Type → Privacy Concerns	.242*** (7.29)	.242*** (7.25)	.242*** (6.38)	.242*** (7.27)
Misuse Experience → Privacy Concerns	.201*** (7.37)	.201*** (7.18)	.201*** (6.61)	.201*** (7.13)
Internet Usage → Awareness of Protection	.095** (2.90)	.095*** (3.15)	.095** (2.67)	.095** (2.81)
R-squares	.14	.10	.11	.13

Note. *t-value are in parentheses. p-values are represented by * p<.05,**<.01, *** p<.001*

VITA

VITA

EDUCATION

Doctor of Philosophy 2006 ~ 2010
(Major: Management Information Systems/ Minor: Marketing)
Krannert Graduate School of Management, ***Purdue University***
Dissertation title: Essays on Information Assurance in Electronic Markets

Master of Science (Information Systems Management) 2002 ~ 2003
H. John Heinz III School of Public Policy and Management,
Carnegie Mellon University

Bachelor of Science (Microbiology) 1991 ~ 1995
College of Natural Sciences, Kyungpook National University, Korea

REFEREED PROCEEDINGS AND PRESENTATIONS

Juhee Kwon and Jacquelyn M. Rees, "Risk Management, Policy and Laws", The CERIAS (The Center for Education and Research in Information Assurance and Security) Symposium, Purdue, Indiana, 2010.

Juhee Kwon, Jacquelyn M. Rees, and Tawei Wang, "Information Risk Management and IT Executives' Status in a Top Management Team", *Web 2009 proceeding*, Arizona, 2009.
:Under the 1st round review at MIS Quarterly

Juhee Kwon and Jacquelyn M. Rees, "Consumer Privacy Concerns with Internet Service Types, the types of Information requested, and Consumer Characteristics", The Marketing Workshop, Purdue, Indiana, 2009.

Juhee Kwon and Manohar U. Kalwani, "The Impacts of Product Bundling on Price Dispersion in the Online Travel Market", The Annual Big-Ten IS Symposium, Notre Dame, Indiana, 2008.

WORKING PAPERS

Juhee Kwon and K. Altinkemer, "Triple Play: Strategies and Business Models"

Juhee Kwon and Jungpil Hahn, "Online Bidding Behavior across Product categories: An Empirical Exploration" !

Juhee Kwon and Jacquelyn M. Rees, "Detecting Participants' Frauds in Online Auctions"

COURSES TAUGHT

Instructor for MGMT 382 Introduction to Management Information Systems 2008
Awarded the Certificate for Outstanding Teaching, Purdue University

Teaching Assistant for MIS & Principles of Information Systems (MBA) 2006 - 2009

WORKING EXPERIENCE

SAMSUNG ELECTRONICS, Seoul Korea 2003-2006
Information Strategist, Information Strategy Planning Group,

YAHOO! KOREA, Seoul Korea 2000-2001
System/Business Analyst

LG CNS, Seoul Korea 1995-2000
System/Business Analyst,

SPECIAL AWARDS and HONORS

Outstanding Teaching Award at Purdue University 2008
Full Assistantship from Purdue University 2006-2010
Graduation with Distinction at Carnegie Mellon University May 2003
W.W. Cooper Scholarship at Carnegie Mellon University 2002-2003
Merit-based Scholarship at Kyungpook National University 1992-1995

ACADEMIC SERVICES

Ad Hoc Reviewer for International Conference on Information Systems (ICIS 2009) !
Ad Hoc Reviewer for Electronic Commerce Research and Applications (2009 -2010)