Effects Of It Governance On Information Security

2007

Yu Wu
University of Central Florida

EFFECTS OF IT GOVERNANCE ON INFORMATION SECURITY

by

YU WU
B. Econ. Xiamen University, 1991
M.S. Golden Gate University, 1995
M.S. University of Central Florida, 2003

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Management Information Systems
in the College of Business Administration
at the University of Central Florida
Orlando, Florida

Fall Term
2007

Major Professor: Carol S. Saunders

ABSTRACT

This dissertation is composed by three essays that explore the relationship between good IT governance and effective information security services. Governance steers and verifies performance of fiduciary duties, through the implementation of proper governance mechanisms. With a focus on information security, this essay presents three categories of governance mechanisms – process-based, structural, and relational. When properly instituted, they work together to ensure that IT understands business requirements for information security and strives to fulfill them. An explanation is offered about the efficacy of those mechanisms, based on an agency theory perspective that views IT as an agent for business. The two underlying causes for agency problems are goal incongruence and information asymmetry between the agent and the principal. Governance mechanisms help to reduce both goal incongruence and information asymmetry. Hence, they lead to desired outcomes. A theoretical framework is presented and empirical tested.

ACKNOWLEDGMENTS

First, I would like to express my enormous gratitude to my advisor, Dr. Carol Saunders, for her patience, guidance, encouragement, and invaluable advice throughout the entire dissertation process. I am also in debt to the members of my dissertation committee, for their insightful suggestions and the time and effort they spent reviewing the various renditions of this dissertation before it takes its current shape:

Dr. Peggy Drywer, University of Central Florida
Dr. Ross Hightower , University of Central Florida
Dr. Detmar Straub, Georgia State University
Dr. Craig Van Slyke, Saint Louis University

I also benefited from the reviews, comments, and suggestions provided by a number of anonymous academic reviewers. I am thankful for their input. In addition, I want to thank two academic reviewers for going over the ideas with me in detail:

Dr. Qing Hu, Florida Atlantic University
Dr. Huigang Liang, Temple University

The empirical test of theories put forth in this dissertation would have been impossible without data collected through a survey conducted in the summer of 2007. I received responses from security and business managers at more than 100 organizations. As a way to show my appreciation, I will make a donation on behalf of all responding organizations to the graduate study scholarship fund at $(ISC)^2$, a non-profit organization dedicated to information security education and certification. Although many responding organizations chose to remain anonymous, I am glad to be able to at least express my appreciation to those who informed me of their participation (listed separately).

In particular, I feel very much indebted to the following people without whose generous and timely support this survey would have been fruitless:

Tom Lamm, Director of Research, Standards and Academic Relations, ISACA
Ron Hale, Director of Information Security Practices, ISACA
Dan LoPresto, CISSP, Marketing Officer, ISSA Central Florida Chapter
Brett Osborne, CISSP, CISM, President, ISSA Central Florida Chapter
Tony Valentino, CISA, PMP, President, ISACA Central Florida Chapter
Lisa Young, President, ISACA West Florida Chapter

Members on the advisory boards for the Department of MIS at University of Central Florida and the Department of Information Technology and Decision Sciences at University of North Texas also participated in the survey and I want to thank both boards.

Given the exploratory nature of this dissertation, input from domain experts in the field is very essential. I am grateful to all those information security and IT audit practitioners who participate in the process of survey instrument development:

Kelvin Arcelay, Citas Group, LLC, Atlanta, GA
Ngy Ea, AIT Consulting, LLC, Atlanta, GA
George Grachis, CISSP, Brevard County Public Schools, Viera, FL
Terri Khalil, CISSP, PriceWaterhouseCoopers, Tampa, FL
Randy Khun, CISA, University of Central Florida, Orlando, FL
Dan LoPresto, CISSP, Bright House, Orlando, FL
Randy Reily, CISSP, CISA, American Automobile Association, Heathrow, FL
Lance Turcato, CISA, CISM, City of Phoenix, AZ
Chris Vakhordjian, CISSP, University of Central Florida, Orlando, FL
Wei Zhang, Rotech Corporation, Orlando, Florida
Gary Wunrow, Sentry Insurance, Stevens Point, WI

Many thanks to my fellow CBA doctoral students who helped me with the instrument creation process: Lascelles Adams, Jack Hsu, Maribeth Kuenzi, Yuzhu (Julia) Li, Lars Linden, Chad Milewicz, James Parrish, Rajani Pillai, J.T. Shim, and Zhe Zhang. Thanks to Maribeth Kuenzi also for sharing her experience and advices in conducting a mail survey.

Last and definitively not the least, my wife, Minhua Yang, for her encouragement, patience, and enormous amount of work she has done for the survey administration process.

Security and business managers at more than 100 organizations participated in the survey to support this dissertation. I want thank them and their organizations. For those who chose to inform me of their participation, I am also glad to acknowledge them here:

Acuity
APL Limited
Aramark
Attorney's Title Insurance Fund
Ametek, Inc.
Babson Capital Management
BNY Mellon
Brown-Forman Corp.
Campus Crusade for Christ
City of Orlando
City of Phoenix
Clear Channel Communications
Cummins, Inc.
Darden Restaurants
Edward Don & Co.
Ernst & Young
FedEx
Fiserv
General Mills
Harley-Davison
Hewitt Associates
Highmark
HSN
Ingenix, Inc.
Intuit
LAN International Orlando
MeadWestvaco
Network Services Company
Oregon Cutting Systems
Orlando Sentinel
RealTime Services, Inc.
PriceWaterhouse Coopers
Prudential Financial, Inc.
Service Insurance Company
Standex
State Street Corp.
The Holy Land Experience Ministries
Tampa General Hospital
Tampa International Airport
TD Banknorth, Inc.
Tribridge, Inc.
U. Texas MD Anderson Cancer Center

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

CIA	Confidentiality, Integrity, and Availability
CISA	Certified Information System Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CobiT	Control Objectives for Information and related Technology
ISACA	Information Systems Audit and Control Association
ISSA	Information Systems Security Association
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Standards and Technology
SLA	Service level agreement
SOX	Sarbanes-Oxley Act

CHAPTER 1 WHAT COLOR IS YOUR ARCHETYPE? GOVERNANCE PATTERNS FOR INFORMATION SECURITY

Security managers have long lamented the lack of top management support, insufficient budget for tooling up security, the proverbial user who just can't refrain from opening the suspicious email attachment, and so on. But now senior managers are taking their refrains more seriously. Among other things, the Sarbanes-Oxley Act has catapulted discussion about accountability for information security onto the agenda of boards of directors meetings. These boards are recognizing the importance of IT governance for ensuring information security and enhancing accountability. It is not a matter of whether, but when and how, companies should bring information security under the umbrella of IT governance. This paper provides a perspective on making governance decisions about information security.

IT governance aligns the actions of IT staff with business goals through monitoring and empowerment. Empowerment comes from granting the right to make decisions. However, it should not be done randomly or on a whim. It requires carefully allocating decision rights for given areas of responsibilities.

Herbert Simon (1960) suggests that the nature of decisions dictates where each important class of organizational decisions should be made. Neither centralizing nor decentralizing decision

making is always a good thing. Rather a company must delegate the "natural subdivision" for each major decision.

Weill and Ross (2004) revisit Simon when they define IT governance as "specifying the decision rights and accountability framework to encourage desirable behavior in using IT (p. 2)." Weill and Ross categorize IT decisions into five major classes: IT principles, IT architecture, IT infrastructure, business application needs, and IT investment and prioritization. Their study of 256 enterprises shows that high performing companies use the proper decision right allocation pattern for each major class of IT decisions.

Weill and Ross use political archetypes to accentuate differences among allocation patterns. Table 1.1 summarizes prescribed decision rights allocations for each archetype. Business monarchy and feudal archetypes place business executives or business unit heads, respectively, at the helm when it comes to security decisions. With the federal archetype both the business unit and corporate management hold decision rights. In contrast, the IT monarchy puts information security decisions squarely on the shoulders of the IT professionals. In the IT duopoly decisions are made by both IT executives and business executives/leaders, while no IT governance is practiced with anarchy.

For security professionals looking for solutions to problems they encounter, this framework provides a new perspective – a mismatch between decision rights and decision class. For example, one common sin is treating information security solely as a technical issue and forcing

security-related organizational or human decisions upon reluctant IT "techies" who are ill-equipped for making such decisions.

Table 1.1 Weill and Ross IT Governance Archetypes

Archetype	Decision Right Distribution	Explanation about the Role of IT
Business monarchy	Senior business executives make IT decisions for the entire enterprise. The IT executive is considered as one voice in the decision making.	Business executives make the decisions about with security with the corporate IT head, the CIO, as an equal partner with other executives.
IT monarchy	IT professionals make the IT decisions.	IT can be implemented in many different flavors, involving IT professionals at corporate IT or business unit IT to variable degrees.
Feudal	Business unit management makes IT decisions.	Either corporate IT or business unit IT or both can be involved in decision making as well.
Federal	Involving both the corporate center and business units.	Either corporate IT or business unit IT or both can be involved in decision making as well.
IT duopoly	Decisions are made by the duo of IT executives and either corporate business executives or business unit leaders.	This archetype also incarnate in one of these two forms: (a) "Bicycle wheel" with the corporate IT at the hub. Sitting at the rim are the business units, each of which forms a spoke together with the hub; or (b) "T" arrangement, with the IT executive having overlapping memberships in an executive committee and an IT committee.
Anarchy	No IT governance.	

No single governance archetype provides a one-size-fits-all pattern for security decision making. Weill and Ross' framework treats "security and risk" merely as a cluster in "IT infrastructure services." We think this classification is too narrow and instead propose that IT security affects the entire IT gamut. We illustrate our point by discussing six critical success factors (CSF) for

information security that are frequently discussed in the security literature. We identify the most suitable governance archetype for each CSF class.

1.1 CSF 1: Information Security Strategy – IT Principles

A company's information security strategy "is a related set of high-level statements about how IT is used in the business (Weill and Ross, 2004, p. 27)." It is built upon such IT principles as protecting the confidentiality of customer information, strict compliance with regulations, maintaining a security baseline that is above the industry benchmark, etc. (Egan, 2005).

Security strategies of companies in the same line of business may differ dramatically. For instance, a software company's strategy may aggressively value time-to-market over security when building its products. It may alternatively be paranoid about secure coding. Microsoft had adopted the first strategy for a long time. After enough criticisms were leveled, it decided to adopt a different strategy with its Trustworthy Computing initiative that aims to be "secure by design, secure by default, secure in deployment" (Wylder, 2004). While Microsoft Windows has long been associated with lax security, Java's security record is impressive and seems to be an outcome of Sun's strategy to bake security into the product from day one.

Security strategy is hardly a technical decision. It is often defined based on the company's mission, overall strategy, business model, and the demands of its business environment. Deciding on the security strategy, therefore, requires decision makers who thoroughly

understand the company's strategic view and management system (LeVeque, 2006). In contrast, decision makers need not be well-versed in information security implementation. Thus, a business monarchy is a good match for such situations in which the top business executives set the tone for the company's security. As part of the business monarchy's "ruling class," the CIO handles the reality check of the decided security strategy. If necessary, the IT function provides the required technical input for supporting the decision.

1.2 CSFs 2 & 3: Security Policies and Technical Architecture – IT Architecture

These two CSF deal with IT architecture, or "the organizing logic for data, applications, and infrastructure, captured in a set of policies, relationships, and technical choices to achieve desired business and technical standardization and integration (Weill and Ross, 2004, p. 30)."

CSF 2 is concerned with logical, business-oriented architecture. Architecture supports the standardization and integration requirements based on a company's business strategy (Ross, Weill, and Robertson, 2006; Weill and Ross, 2004). Standardization ensures the uniformity that encourages efficient business processes. Integration builds on uniform data definition to allow sharing of data across business processes, thus enhancing efficiency, coordination, and agility (Ross et al, 2006).

Security policies, a critical success factor, encourage standardization and integration. Following best practices, they broadly define the scope of and overall expectations for the company's

information security program. From these, lower-level policies are derived to control specific security areas (e.g., Internet use, access control, etc.) and/or individual applications (e.g., payroll systems, telecom systems, etc.) (Peltier, 2004). A goal of security policies is standardizing behavior. Supplemented by security standards, guidelines, and procedures, policies maintain standardized employee behaviors where security is concerned (Tudor, 2001).

Among the various policies, information asset classification policy particularly helps integration. Asset classification is an important first step for security programs because it informs company decisions about which information assets to protect. Although it does not target integration directly, the exercise of identifying, categorizing, and entrusting information assets with responsible parties greatly facilitates data standardization and sharing.

Weill and Ross (2004) observe that in many companies senior management relegates architecture decisions to IT even though many high-level architecture decisions have substantial business significance. Business leaders are needed to maintain a strategic business view (Ross et al, 2006). Still, IT leaders should not be excluded for two reasons. First, their judgment prevents unrealistic goals for standardization and integration. Second, policy decisions require the ability to analyze the technical and security implications of user behaviors and business processes. Thus, for high-level security architecture decisions, IT duopoly is a good fit.

CSF 3 is the 'technical security architecture' (e.g., Panko, 2004). It provides the organizing logic for security infrastructure components and focuses on designing a company's network and

security topology. For instance, a very widely used security typology is demilitarized zones (DMZs). DMZs provide a buffer between the public, presumably hostile, Internet and the company's internal networks. DMZ design calls for a series of decisions on firewall setup and server configuration so that they can be placed strategically to form a DMZ. In a larger picture, DMZs are part of a layered protection architecture whose design involves numerous technical decisions. DMZs require a high level of technical expertise.

The matching archetype for this CSF is fairly straightforward. Having business leaders make technical architecture decisions is not only micromanagement, but also infeasible because they lack the technical know-how. IT monarchy fits these decisions well because only IT managers have the technical expertise to design and implement such systems.

1.3 CSF 4: Information Security Infrastructure – IT Infrastructure

"IT infrastructure is the shared and reliable services used by multiple applications (Weill and Ross, 2004)." Security infrastructure provides protection by arranging security mechanisms according to the security architecture specifications.

The most conspicuous mechanisms are those directly related to security. Firewalls, intrusion detection systems (IDSs), encryption devices are the most popular examples. Many mechanisms are either hardware or software solutions. The hardware often has some performance advantage, while software offers richer functionality. The other major part of infrastructure is built by

hardening existing network infrastructure components and computing platforms. For instance, the primary function of routers and switches is to provide network connectivity. However, they can act as the first line of defense with their security-related configuration such as access lists, virtual LANs, etc.

Decisions in this class are concerned with technology selection and configuration. Common objectives are to achieve consistency in protection, economy of scale, and synergy among the components. For these reasons, corporate IT typically is responsible for managing the dedicated security mechanisms. Also, general IT infrastructure such as enterprise network devices (the second component above) often is centrally controlled by corporate IT. Thus, to use Simon's terminology, corporate IT is the "natural subdivision" for security infrastructure decisions. In other words, the fitting governance pattern for these decisions is IT monarchy, where corporate IT takes the lead.

1.4 CSF 5: Business Requirements for Security – Business Application Needs

IT architecture and infrastructure would be castles in the air if they did not serve business needs and create value. Two conflicting objectives must be balanced when identifying a firm's needs – creativity and discipline. Creativity aims at new and more effective ways of delivering customer value using IT. However, when necessary, a company should be ready to sacrifice creativity for discipline (e.g. enforcing hardware or software standardization) so that architectural integrity can be preserved (Weill and Ross, 2004).

Similarly, companies often must balance the enhanced information security gained from adhering to security policies against productivity losses and user inconvenience. As security attacks become more sophisticated, obeying security measures to deflect those attacks places increased cognitive demands on users (e.g., long passwords with special characters for system logon) and sacrifices productivity (e.g., the daily chore of scanning emails to spot phishing attempts).

Identifying and fulfilling business users' security requirements are essential for legitimate, successful information security programs. Business requirements are the basis for writing security policies. They also impact what security managers see as critical, but tough, challenges: security training and user awareness. This is because when a training program is tied to the unique requirements of individual business processes, it stands a better chance for effectiveness and post-training retention.

Security requirements are determined by evaluating risks. This evaluation requires two key inputs – the computing infrastructure and the way in which people use it to perform their jobs. Perspectives from both IT and business are important in understanding the risks a company faces and how to mitigate them (Alberts and Dorofee, 2003). This is a critical process during which business users express what they want out of the information security program and how they expect the security function to support their business activities. These requirements have resounding effects as they will be incorporated into security policies and fulfilled with security

mechanisms. On the other hand, IT understands issues related to the IT infrastructure and what are needed to keep it running. IT duopoly thus fits business application needs decisions best. Such a governance pattern reconciles rivaling needs for security and achieves the delicate security-productivity trade-off.

1.5 CSF 6: Information Security Investments – IT Investment and Prioritization

The "FUD factor" (fear, uncertainty, and doubt) used to be all that was needed to get top management to plunk down money on information security. As information security becomes a routine concern in daily operations, increasingly security managers need to justify their budget requests financially. A recent empirical study (Gordon and Loeb, 2006) finds that companies are starting to use the Net Present Value (NPV) method to make decisions about security spending. According to the CSI/FBI (Gordon, Loeb, Lucyshyn, and Richardson, 2005) survey, 38% of the respondents use Return on Investment (ROI) analysis, 18% use Net Present Value (NPV), and 19%, Internal Rate of Return (IRR) for IT security investments.

Of course, many more factors are at play when a company evaluates information security investments. Qualitative cost-benefit assessments often supplement, or even substitute for, more quantitative financial analytical methods. As when determining business needs, different units within the company may have rival or conflicting "wishlists" for information security-related purchases that benefit their unique needs. The IT function also should have a significant say in

these decisions as it is in the best position to assess whether and how the investments may fit with the company's current IT infrastructure and application portfolio.

Thus, the most suitable governance pattern for investment and prioritization decisions is IT-business duopoly. In particular, the T-arrangement duopoly pattern (see Table 1.1) fits this type of decision well. The most typical governance mechanism for this archetype is executive committees/councils composed of business and IT executives, such as the IT steering committee and budget committee, with the CIO having overlapping memberships in both. These committees are the venue at which IT and business leaders make business cases for their proposed investments and debate the merit and priorities of the investments. Decisions then are made with the company's best interest in mind.

1.6 Matching Archetypes with Decision Classes

We discussed six critical success factors for information security. For each, we suggested a governance pattern that best suits decisions in that area (see Table 1.2 for a summary). These decision class-archetype matches, however, are by no means etched in stone. Unique organizational and environmental factors may require some deviation. For instance, it is easy to imagine that business monarchy governs security investments decisions if a company emphasizes stringent budget review and control from a pure business/financial perspective. At enterprises with many relatively independent business units, a federal archetype that involves the corporate center, business unit leaders, and IT leaders may be the proper archetype for business

requirement decisions. Alternatively, the corporate culture may even render a feudal archetype the only choice.

That said, because of the nature of different IT decisions, each decision class lends itself best to governance under a certain archetype. Wise companies know this and vary the governance patterns for different decision classes. That is why Weill and Ross (2004) studied those 236 enterprises to identify the archetypes used by some of corporate America's most successful companies for governing IT decisions in the five classes. Their empirical data show that organizations differ significantly in their selected archetypes for allocating decision rights for different decision classes. For instance, duopoly is used by the largest portion (36%) of organizations for IT principles decisions; for IT infrastructure decisions, IT monarchy (59%) is the most popular.

Mismatched archetypes have negative security consequences. An example is the state government described by Tudor (2001). The government includes 11 agencies and departments and has adopted a feudal archetype for IT infrastructure decisions. This is an obvious mismatch because IT monarchy typically is most proper for infrastructure decisions. Since decisions regarding the infrastructural components are made in the 11 departments locally, duplications abound; efficiency, cost-effectiveness, and communication suffer; and these create an environment that makes efficient management of security infrastructure difficult. Tudor's prescription for this problem clearly targets the governance pattern: educate the department

management on security; do not force security decisions on them; and provide incentive for the departments to follow.

Governance patterns thus have significant implications for companies when assigning security responsibilities and accountabilities. The taxonomy of decision classes lays out a logical way to group key security decisions and ensure that all important bases are covered. The archetypes clearly define the responsibilities of the major players in the company – business executives, business unit leaders, corporate IT, business unit IT, etc. By matching the proper archetypes to the key security decisions, the board of directors in effect puts the decisions in the hands of those who are in the most appropriate positions for making quality decisions. In addition, decision makers are truly empowered when they are bestowed the authority to make decisions that (1) are suitable for their positions in the organizational hierarchy; (2) make the best use of their expertise and knowledge; and (3) cater to the needs and specialization of the organization units to which they belong.

Common, recurrent security problems (patchwork, shotgun approaches to security programs, security policies copied from *Information Security for Dummies*, improper security mechanisms, cookie-cutter security training programs, insufficient or lavish security investments, etc.) can all be traced to not having the right decision makers. Therefore, for information security, application of proper archetypes increases the chance that critical success factors are facilitated with good decisions. Just as nations with healthy political systems grow and prosper, information security programs under the governance of proper archetypes thrive. When security

managers present their cases to the board, citing *IT Governance* not only is easier for the audience to understand but also may create more lasting effects than if they cite *Hacking Exposed*.

Table 1.2 Matching Information Security Decisions and Archetypes

Decision Class	Information Security CSF	Symptoms of Improper Decision Right Allocation	Recommended Archetype	Rationale
IT Principles	Security strategy	Security is afterthought and patched on to processes and products.	Business monarchy	Business leaders have knowledge of company's strategies, which security strategy should support. No detailed technical knowledge required.
IT Architecture	Security policies	Security policies are written based on theory and generic templates. Unenforceable due to misfit with company's IT particularities.	IT duopoly	Requires ability to analyze technical and security implications of behaviors and processes. Need to know the particularities of company's IT infrastructure.
	Technical security architecture	Mis-specification of security and network typologies.	IT monopoly	Technical know-how is needed.
IT Infrastructure	Security infrastructure	Selection of wrong, ineffective security mechanisms. Mis-configuration. Ineffective technical control.	IT monarchy	In-depth knowledge and expertise needed.
Business Application Needs	Business requirements for security	Business needs not supported by the security program. Users feel inconvenienced and bypass or undermine security measures. Poor result from user training and awareness programs.	IT duopoly	Security should provide services to business users. Needs to achieve balance between security and productivity. Business inputs critical to user training.
IT Investment and Prioritization	Investments in information security	Under- or over-investment in information security. Waste or insufficiency in human or technical resources for security.	IT duopoly	Requires financial (quantitative) and qualitative evaluation of business impacts of security investments. Business case has to be presented and debated for rivaling projects.

1.7 Chapter 1 List of Reference

1. Alberts, C., & Dorofee, A. (2003). *Managing Information Security Risks: The OCTAVE Approach*. Boston, MA: Addison-Wesley.

2. Egan, M. (2005). *The Executive Guide to Information Security: Threats, Challenges, and Solutions*. Indianapolis, IN: Addison-Wesley.

3. Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM,* 49(1), 121-125.

4. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

5. LeVeque, V. (2006). *Information Security: A Strategic Approach*. Hoboken, NJ: Wiley-Interscience.

6. Panko, R. R. (2004). *Corporate Computer and Network Security*. Upper Saddle River, NJ: Prentice Hall.

7. Peltier, T. R. (2004). *Information Security Policies and Procedures: A Practitioner's Reference* (2nd ed.). Boca Raton, FL: Auerbach Publications.

8. Ross, J. W., Weill, P., & Robertson, D. C. (2006). *Enterprise Architecture as Strategy*. Boston, MA: Harvard Business School Press.

9. Simon, H. A. (1960). *The New Science of Management Decision*. New York, NY: Harper & Brothers Publishers.

10. Tudor, J. K. (2001). *Information Security Architecture*. Boca Raton, FL: Auerbach Publications.

11. Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA: Harvard Business School Press.

12. Wylder, J. (2004). *Strategic Information Security*. Boca Raton, FL: Auerbach Publications.

CHAPTER 2 AN AGENCY THEORY PERSPECTIVE ON IT GOVERNANCE AND INFORMATION SECURITY SERVICES

2.1 Introduction

Information security (InfoSec) "is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information (Whitman and Mattord, 2005, p. 8)." It is receiving greater attention recently, as the complexity of information systems, the sophistication of security attacks, and the legal and financial consequences of security breaches increase. Another reason is tightened regulations. For example, the enactment of Sarbanes-Oxley Act (SOX) raises the bar for accountability related to information security. To comply with SOX, public corporations need to manage information security to ensure that financial, transactional, and audit data are accurate, securely stored, free of corruption, protected from malicious access and modifications, and available for legitimate access (Symantec, 2004; Volonino, Gessner, and Kermis, 2004). Failure to do so can result in prison terms and fines for top executives, primarily the CEO and the CFO.

To protect business information, executives and business users rely on a number of information security services (Grance, Hash, Stevens, O'Neal, and Bartol, 2003). For most firms, to date internal IT has been the primary provider of these services, as the results from various surveys show (BSA and ISSA, 2004; Gordon, Loeb, Lucyshyn, and Richardson, 2005, 2006; McKenna, 2002). If IT cannot provide effective information security services, the results can be costly, as

evidenced by SOX's penalties for non-compliance. This is because information security impacts not just IT but also every facet of an organization. The board of directors and executive management, therefore, should take the lead in ensuring that information security is managed strategically. The information security function should be directed and controlled with a proper governance framework (Posthumus and von Solms, 2004; Williams, 2007).

Information security governance is an integral part of IT governance (ITGI, 2006; Posthumus and von Solms, 2004; S. H. Von Solms, 2005). A natural question to ask is: how do we implement IT governance so that IT is effective in providing information security services? However, to date, the question is still largely unanswered by both the academic and practitioner literature.

Academic research on security governance largely follows the traditional centralized-decentralized-federal trichotomy of governance forms (e.g.,Warkentin and Johnston, 2006a, 2006b). We have yet to see security governance addressed from the angle of dynamic governance mechanisms "such as sourcing arrangements, strategic alliances, roles, teams, processes, and informal relationships (Sambamurthy and Zmud, 2000, p. 106)." The practitioner's literature on this topic tends to adopt a "checklist" (Dhillon and Backhouse, 2001) approach.

Thus, this essay tries to answer a set of questions that are of significance for both academic and practitioner researchers:

Does implementation of various IT governance mechanisms improve the effectiveness of information security services? Which type(s) of mechanisms are more critical for improving information security?

To answer this question, this essay presents a trio of governance mechanism types and uses agency theory to explain their efficacy in governing information security. Agency theory is chosen as the theoretical basis because, in essence, the information security function acts as an agent and provides security services to business departments, the principal. When agency problems occur, the principal's welfare suffers. In the context of information security, that means the principal's information assets are not sufficiently protected and the principal receives suboptimal services. The various IT governance mechanisms tackle the two root causes for agency problems: goal incongruence and information asymmetry between the principal and the agent. This, in turn, leads to more effective information security services.

The rest of the essay proceeds as follows. First, IT's role as provider of information security services and effectiveness of InfoSec services are discussed. This is followed by a discussion of agency relationship and agency problems in the context of information security function. Next, IT governance and three types of governance mechanisms are presented. The last section discusses how each type of these mechanisms can tackle the two root causes of agency problem hence increasing the effectiveness of information security services.

2.2 IT as InfoSec Service Provider

This essay studies information security governance through the perspective that IT is the provider of information security service thus an agent for business users. IT is a staff function that provides services to internal "customers" – other departments throughout the organization (Pitt, Watson, and Kavan, 1995). It is particularly so when information security is concerned, because the outcomes of InfoSec activities fit the characteristics of services as described by Clark (1993):

(a) ***Intangibility*** – InfoSec tasks do not usually produce physical goods. Although some measures such as firewalls or intrusion detection systems often are implemented as hardware thus visible, the absence of security breaches, rather the hardware itself, is the true desired outcome;

(b) ***Inseparability*** – InfoSec services are "sold" and then produced and consumed simultaneously. The moment IT starts a protection measure, it is simultaneously used by the internal customers.

(c) ***Heterogeneity*** – because of the enormous array of technological platforms, applications, data, threats, vulnerabilities, etc. and the variation in security personnel's training and experiences, each instance of security service is unique;

(d) ***Perishability*** – InfoSec service cannot be stored; and

(e) ***Non-transferability*** – When the service is rendered, there is no transfer of ownership.

Furthermore, IT can be construed as providing a subcategory of service (Clark, 1993), one that adds value (security) to a tangible product (information assets). IT implements security measures to protect both the information and the information systems on which information is stored (for conciseness, this essay uses the term "information security" to refer to the protection of both).

IT provides a variety of information security services (Grance et al, 2003). In its various special publications (e.g., Grance et al, 2003), the National Institute of Standards and Technology (NIST) suggests a wide range of InfoSec services that address the following three aspects of InfoSec protection:

(a) ***Management*** – Services in this category aims to develop and maintain an organization-wide security program, formulate security policies, design the security architecture, evaluate the effective security products, etc.

(b) ***Operation*** – Services in this category handles important InfoSec operations such as contingency planning, incident response, security testing, user training, etc.

(c) ***Technical*** – Services in this category are most often associated with IT when information security is discussed, such as firewall configuration and management, intrusion detection system design and monitoring, public key infrastructure (PKI) implementation, etc.

In theory, information security services can be offered by internal IT or external vendors (Grance et al, 2003). In practice, however, industry surveys continuously show that only a very small percentage of firms actually outsource their information security services and, even then, usually only to a limited extent (BSA and ISSA, 2004; Gordon et al, 2005, 2006; McKenna, 2002). Thus, internal IT is the primary provider of a firm's information security services.

The information security function normally is rested upon the IT department or IT personnel. Or it can be a separate security organization, which often reports to the CIO or head of IT (Gentile, Collette, and August, 2006). This essay uses the terms "IT", "information security function," and "security organization" interchangeably to refer to the organizational unit or group that acts as the provider of information security services. The terms "users," "business," and "user departments" refer to other organizational units, users, managers, and executives that depend on IT for protection of information assets.

2.3 Effectiveness of Information Security Services

The effectiveness of information security services is the extent to which the services are delivered successfully. Its evaluation should have three focus points – business function,

customers, and effective security. Thus, any metrics of effectiveness should include business impact, service delivery, and the efficacy of implementation (Grance et al, 2003).

First, they ensure that the firm's information assets are protected in terms of the widely accepted criteria of security that are commonly referred to as the confidentiality-integrity-availability (CIA) triad (Posthumus and von Solms, 2004; B. Von Solms, 2005). Each of the attributes in the CIA triad is defined as:

(a) ***Confidentiality*** is the absence of unauthorized access, disclosure, and use of information (Alberts and Dorofee, 2003; Avižienis, Laprie, Randell, and Landwehr, 2004; Snedaker, 2006; Wylder, 2004).

(b) ***Integrity*** means that information is trustworthy and reliable because it has not been altered or corrupted by unauthorized users or computer processes (Alberts and Dorofee, 2003; Avižienis et al, 2004; Snedaker, 2006; Wylder, 2004). The unauthorized modification and corruption can be either accidental or malicious (Gollmann, 2006).

(c) ***Availability*** is the authorized users' ability to have timely and reliable access to information assets (Alberts and Dorofee, 2003; Avižienis et al, 2004; Snedaker, 2006; Wylder, 2004). It is provided by fault-tolerant design and security measures preventing malicious attackers from blocking legitimate access (Gollmann, 2006). Whereas confidentiality and integrity usually concerns information or data, the scope of availability is more encompassing. It is

also pertinent to other information assets such as servers, Internet connection, networks, etc. (Snedaker, 2006).

Second, an important measurement of IT's effectiveness is the quality of service it provides (Pitt et al, 1995). Along the same line, internal "customers" of InfoSec services expect IT to provide high quality services. IT should deliver reliable services, be responsive to users' service requests, be considerate with user requirements, perform services in a professional manner, etc. It is suggested that quality is an important but overlooked aspect of information security (Snedaker, 2006).

Third, the security assurance provided by IT should support business users in their job function. The increasing importance of information security in fact reflects firms' high reliance on reliable information. Any security breaches affect the reliability of information hence users' productivity.

For information security services to be effective, ways are needed to ensure that IT performs them with diligence. As "a theory of performance outcome (Nilakant, 1994 #103, p. 651," agency theory often is used as the theoretic foundation for analyzing quality of service providers {e.g., Mills, 1990; Pontes, 1995; Singh and Sirdeshmukh, 2000). Therefore, to explain how IT governance can improve InfoSec service effectiveness, this essay treats the relationship between IT and users as that between an agent (IT) and a principal (users). Effectiveness is enhanced when agency problems are reduced. IT governance is introduced as a means to achieve that end

because governance is considered instrumental to controlling agency problems (Baiman, 1990; Levinthal, 1988).

2.4 Agency Relationship in Information Security

When providing security services to the internal "customers," the information security function in essence acts as an agent for the principal, i.e., the business departments. An agency relationship is present whenever "one or more persons (the principal(s)) engage another person (the agent) to perform some service on their behalf which involves delegating some decision making authority to the agent (Jensen and Meckling, 1976, p. 308)." The principal delegates the task because of lack of time or ability to do the task (Nilakant and Rao, 1994). Similarly, user departments need to delegate the provision of InfoSec services to IT because IT usually is the only organizational unit that has the expertise and skills for it.

In an agency relationship, loss of principal's welfare, or agency problems, often occurs. In other words, the principal's objectives may not be implemented in the principal's best interest, due to two agency problems: adverse selection and moral hazard. Adverse selection refers to the agent's exerting the inappropriate type of effort (Nilakant and Rao, 1994). In this situation, the principal is unable to determine the agent's qualifications and abilities (Eisenhardt, 1989; Levinthal, 1988) and whether the agent's decisions and actions are in the principal's best interest (Adams, 1994). For example, a security administrator may dismiss abnormal activities on corporate network as transient peaks in traffic while the reality is that an attacker is scanning the

network. Moral hazard means that the agent exercises inadequate effort. In this situation, the principal is unable to verify the quantity and quality of the agent's efforts (Mills, 1990). As an example of moral hazard, a security administrator may dislike the mundane task of reviewing logs from firewalls, intrusion detection systems, Windows operating systems, etc. She thus only performs a cursory daily review of the log entries and sometimes skips the review altogether. In both adverse selection and moral hazard scenarios, it is unlikely that business managers would notice the security administrator's suboptimal behaviors.

Agency problems stem from goal incongruence between the agent and the principal and the principal's difficulty in verifying the agent's abilities and efforts due to asymmetric information (Eisenhardt, 1989). Differences in training, experiences, work environment, and compensation structure all contribute to the agent having different objectives than the principal's when tackling a task. Goal incongruence between the agent and the principal can result in reduction in principal's welfare (Nilakant and Rao, 1994).

The difficulty in verification is mostly the result of information asymmetry. Information asymmetry refers to the agent "having private information to which the principal cannot costlessly gain access. This private information may be with respect to the agent's action choice and/or state information (Baiman, 1990, p. 343)." First of all, there is expertise-based asymmetry in that the agent possesses some domain knowledge, skills, and abilities that the principal lacks. This asymmetry is in fact the raison d'être for agency relationships. Also, as the agent works on the task, another type of asymmetry develops with respect to the knowledge

about the agent's actions, resources needed for the tasks, the state of the task, etc. (cf., Arrow, 1985; Baiman, 1990). This can be termed performance-based asymmetry. Expertise- and performance-based asymmetries afford the agent the ability to hide information and actions from the principal.

Because of goal incongruence and information asymmetry, possibility always exists for the agent to act opportunistically. Governance is necessary to control the agent's behaviors that are not explicitly stipulated in the employment contract (Baiman, 1990). Finance and accounting researchers have long focused on governance of the management (as shareholders' agent) via compensation structure for the agent (e.g., Indjejikian, 1999; Jensen and Murphy, 1990; Morgan and Poulsen, 2001; Yermack, 2004). Management accounting literature primarily focuses on the reduction of information asymmetry through monitoring (Baiman, 1990). Baiman (1982; 1990) proposes the creation, through monitoring, an "information system" that the principal can utilize to reduce the performance-based asymmetry and become more informed when evaluating and controlling the task outcomes. This essay draws upon the IT governance literature for mechanisms that reduce goal incongruence and information asymmetry between the agent and the principal.

2.5 IT Governance

As an integral part of the enterprise governance, IT governance is the organizational capacity to ensure that IT sustains and extends the organization's strategy. IT Governance Institute (2003)

defines it as the responsibility of the board of directors and executive management. De Haes and Van Grembergen (2004) extend it and suggest that IT management also should be involved in the process of governance.

Research on IT governance has long focused on a trichotomy of organizing logic for IT decision making loci: centralization, decentralization, and federation, and on the antecedents that determines the selection of a particular organizing logic over others (Brown and Grant, 2005; Sambamurthy and Zmud, 2000). Of more practical importance and research interest, however, are the governance mechanisms "such as sourcing arrangements, strategic alliances, roles, teams, processes, and informal relationships (Sambamurthy and Zmud, 2000, p. 106)." Thus, this essay studies various types of governance mechanisms rather than the traditional patterns such as centralization and decentralization. The categorization of the governance mechanisms is based on the work by Peterson (2004), Van Grembergen and colleagues (De Haes and Van Grembergen, 2004; Van Grembergen, De Haes, and Guldentops, 2004), and Weill and Ross (2004).

Process-based governance mechanisms are IT management techniques that ensure that daily behaviors are consistent with IT policies and that all stakeholders are involved in the effective management and use of IT (Weill and Ross, 2004). It is the formal institution of strategic IT decision making or IT monitoring procedures. With varying degrees of comprehensiveness, such standard procedures often are embedded in formalized decision-making methodologies and

management frameworks, e.g., IT investment approval process, balanced scorecard tools, cost-benefit analysis, service level agreements, etc.

An important function provided by process-based mechanisms is the monitoring and tracking of IT performance in terms of service delivery and business benefit realization (De Haes and Van Grembergen, 2004; Peterson, 2004; Van Grembergen et al, 2004; Weill and Ross, 2004). Examples include Control Objectives for Information and related Technology (CobiT), IT Infrastructure Library (ITIL), and ISO17799.

A few process-based IT governance tools are available for organization to choose. For compliance with SOX in terms of IT control, a de facto standard tool is the Control Objectives for Information and related Technology (CobiT), created by IT Governance Institute (ITGI, 2000). CobiT is computing platform agnostic and highly process focused. It serves as a framework for evaluating security and controls over information (Kairab, 2005). CobiT covers all IT-related processes with strong control over InfoSec-related activities in an organization. Out of the 54 control objectives in CobiT 3, 46 have detail control objectives ("sub-CO" of those 54 higher level COs) related to InfoSec and are baselined. Among other functionalities, CobiT ensures that specific responsibilities for the management of security is properly defined; that IT is properly staffed; that security are kept current and compliant with external regulations; that IT's compliance of internal SLAs is regularly examined; that proper security procedures are being followed; and that the adequacy of security controls are regularly assessed (ITGI, 2004).

Another framework that has substantial adoption is the IT Infrastructure Library (ITIL). ITIL is also technology neutral and very focused on IT processes. One of ITIL's underpinnings is embedding InfoSec into everyday processes (Kairab, 2005). A more InfoSec-specific framework is the ISO17799, the international standard for information security management. The ISO 17799 is a high-level standard for different InfoSec aspects, which are grouped into ten major domains. It stresses InfoSec best practices and can serve as a benchmark for security management (Kairab, 2005)

Structural governance mechanisms are the organizational units and roles that are instituted to properly locate decision-making responsibilities, to promote horizontal connection between IT and business functions, and ultimately, to achieve their IT governance goals (Peterson, 2004; Peterson, O'Callaghan, and Ribbers, 2000; Weill and Ross, 2004).

Formal groups such as executive teams, committees, councils, task forces are an important horizontal integration structures for coordinating IT decision making across business and IT. They may be formed temporarily on a task or can be instituted permanently as an overlay structure in the organization (Peterson, 2004; Peterson et al, 2000; Weill and Ross, 2004).

For instance, senior executive committees play a governance role in 90 percent of the organizations surveyed by Weill and Ross (2004). When shared data and IT infrastructure is desired, organizations often form various types of committees whose membership typically includes the CEO, CFO, CIO, and heads of major business units. The decision makers'

combined expertise provides a holistic view that is beneficial to the governance goal – shared data and infrastructure. For matters whose decision right typically falls upon IT, such as IT architecture, organizations with an IT leadership team or committee made up by corporate and business-unit IT leaders perform better than those without. Linkages between business and IT can also be fostered with mechanisms such as joint decision councils (Weill and Ross, 2004).

These structural mechanisms vary in their design and the degree to which they act as an advisory function or exercise formal decision-making authority (Peterson, 2004; Weill and Ross, 2004).

Relational governance mechanisms are the organizational practices that encourage voluntary two-way communication and collaboration between business and IT (De Haes and Van Grembergen, 2004; Peterson, 2004; Van Grembergen et al, 2004).

The major desired outcomes of such mechanisms are better mutual understanding and effective communication channels among the various stakeholders in the organization, such as corporate management, business unit management, IT management, among others (Peterson, 2004). When business and IT understand each other's perspectives, they can accurately interpret and anticipate others' actions and coordinate adaptively. Better understanding and collaboration lead to an integration of domain-specific expertise and tacit knowledge among people with different mental models, insights, and perspectives (Peterson, 2004; Peterson et al, 2000).

Mechanisms that facilitate the mutual understanding and better communication among various stakeholders include direct (informal) contacts, lobbying, joint performance incentives and rewards, collocation of business and IT managers, cross-functional training, job rotations, continuous education, etc.

2.6 Governance Mechanisms and Agency Problem Reduction

IT governance holds the potential to improve InfoSec outcomes by tackling the two root causes of agency problems. Reduction of the two root causes, in turn, leads to more effective InfoSec services.

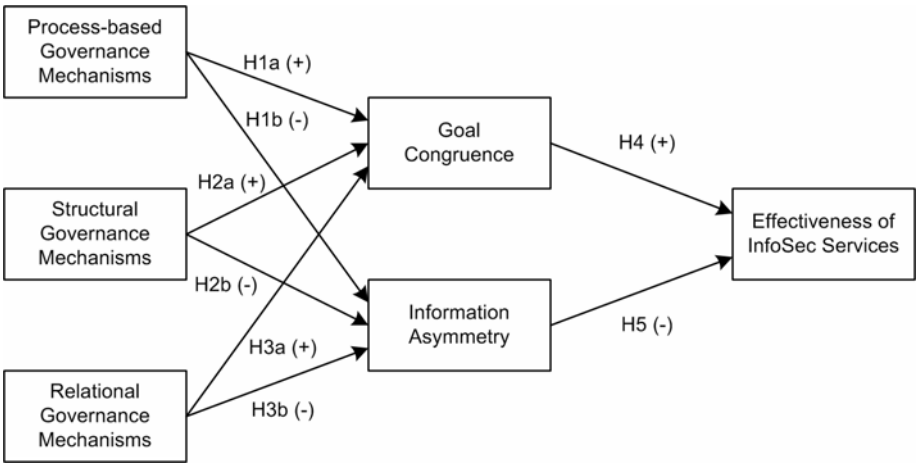


Figure 2.1 Theoretical Model

In this section, the three types of governance mechanisms are discussed with regard to two important activities that are critical to reducing goal incongruence and information asymmetry between IT and users. The first activity is the definition of security requirements, which can be enhanced by service level agreements. Clear definition of security requirements reduces the

incongruence in goals. The second activity is security audit, which generates assessment and feedback information on the effectiveness of information security implementation. In addition, mutually-agreed security requirements also provide a common language of communication, which aids the interpretation of results from security audits.

2.6.1 Goal Congruence

Goal congruence has been defined as the extent to which the relative importance of key performance criteria (Neely and Wilson, 1992; Wickramasinghe and Ginzberg, 2001), including the achievability of goals (Jap, 1999; Jap and Anderson, 2003), are understood between/among parties. For information security services, agreement on key performance criteria can be achieved through a well-implemented process of defining security requirements. In addition, the most important criteria may be solidified in the form of service level agreements.

Security requirements can be categorized into a three-tier structure (Gentile et al, 2006; Snedaker, 2006): business, functional, and technical requirements. The business (or user) requirements are high-level statements that capture the essence of what InfoSec will achieve for the business (Gentile et al, 2006; Snedaker, 2006). Functional requirements are the characteristics that describe how an InfoSec solution or a system, when properly protected, meets the business requirements (Gentile et al, 2006; Snedaker, 2006). Business and functional requirements, once determined, become the basis for technical requirements. Technical requirements are statements

of parameters or measurements that specify the InfoSec measures to be implemented (Snedaker, 2006).

Input from user departments is important to the processes of defining business and functional requirements. Since they are the users of information assets, they have the best understanding of what needs to be protected and to what extent (ITSMF, 2005). The process of soliciting business requirements thus often starts with user identifying the relevant information assets to protect (Alberts and Dorofee, 2003). Asset/data classification is commonly used as the basis for determining the security requirements for information assets. Proper users are assigned the stewardship of the asset and specify their security requirements (Wylder, 2004).

After the business and functional requirements are defined, IT uses them as the basis and specify the technical requirements for information security. After the technical requirements are defined, they serve as the yardstick by which IT evaluates the firm's existing security baseline and decides what additional security measures need to be implemented (Alberts and Dorofee, 2003; ITSMF, 2005).

To ensure proper protection, technical requirements should support the functional requirements, which, in turn, should serve the business requirements properly (Snedaker, 2006). In other words, the technical measures and operations IT implements should meet users' specifications of desired results (functional requirements) and ultimately support users' business needs (business requirements). Therefore, for IT to provide quality InfoSec services to the users, it is essential

that IT and users obtain mutual understanding on what services IT should provide and what criteria to use for gauging IT's effectiveness in providing the services. Such understanding, in addition, may be formalized and articulated in service level agreements (SLAs).

A service level agreement "is an agreement between the provider of a service and its customers which quantifies the minimum quality of service which meets the business need (Hiles, 1994, p. 14)." Besides the regular items to be seen in an agreement, e.g., parties to the agreement, administration, revision, etc., it defines: (a) what the service is, (b) specifics of the service such as timeframe and location within which it is rendered, (c) users' expected level of service, (d) performance indicators, (e) constraints that delineate service attainability beyond which service levels are not guaranteed, and (f) reporting procedure and remedies for nonperformance (Larson, 1998; Rittinghouse and Hancock, 2003; Singleton, McLean, and Altman, 1988; Sturm, Morris, and Jander, 2000). A key benefit of SLAs is that they clarify precisely what the customers' needs are and which elements are the most important (Hiles, 1994). Thus they establish a common language of communications for the parties involved and set mutually-agreed standards for measuring performance (Sturm et al, 2000). These commonalities are even more important for the evaluation of qualitative aspects of IT (Singleton et al, 1988).

In short, collaboration and communications between IT and user departments during the definition process of security requirements is essential to enhancing goal congruence between the two. SLAs, if implemented, also promote goal congruence because they clearly define expected achievable service levels, goal attainability, and performance criteria.

2.6.1.1 Process-based mechanisms and goal congruence

Process-based IT governance frameworks, techniques, and methodologies abound for firms to align the process of InfoSec planning with its business objectives, including capturing user security requirements correctly. For instance, in CobiT 3's Plan and Organize (PO) domain, Control Objectives PO1 governs the processes of identifying critical information and services and considering security requirements. PO6 promotes consistent communication and regular discussion of the basic rules for implementing security requirements and responding to security incidents. Quality management issues are covered in PO11. Control objective DS1 in the Deliver and Support (DS) domain governs the various aspects of both in-house and external SLAs (ITGI, 2004; Lahti and Peterson, 2005). In ITIL, SLAs are addressed as the first book on the subject of Service Delivery. Security Management is one of the major subjects in the ITIL library. The Control process in Security Management stresses the importance of operational level agreement via the use of SLAs (ITSMF, 2005).

Both CobiT and ITIL have a strong InfoSec focus. Firms can also implement InfoSec-specific frameworks such as ISO17799 for InfoSec management or the OCTAVE method for security requirement determination. Regardless of the specific mechanism(s) used and the degree of formality of SLAs, the key is that the mechanisms engender the process of establishing security requirements and service expectations between IT and users.

During this process, IT has the opportunity to discuss with users the technical feasibility or difficulty of fulfilling their security requirements, given the current state of security technologies and the firm's resources. The process also explicates both parties' outlook and stance on risks. When an agreement is achieved, conflicts in expectations and risk stance should have been resolved or at least documented in a proviso. The resultant expectations for security services thus are something IT will buy into. Therefore,

H1a: Process-based governance mechanisms enhance goal congruence between IT and users.

2.6.1.2 Structural mechanisms and goal congruence

In addition to the process-based mechanisms, various structural mechanisms also allow IT and business objectives and priorities to be discussed openly and formally. Formal groups such as executive teams, committees, councils, and task forces are important structures for coordinating IT decision making across business and IT. They may be formed temporarily on a task or instituted permanently as an overlay structure in the organization (Peterson, 2004; Peterson et al, 2000; Weill and Ross, 2004).

Structural mechanisms such as IT steering committee, IT budget committee, IT strategy committee and similar organizational councils and committees are the venue in which IT and user departments present their cases and view points regarding information security. Competing ideas and projects are debated and consensus is built. In addition, formal liaison roles expedite communication between IT and users. As the result, IT achieves a better understanding of users'

requirements for InfoSec and is better prepared to devise security plans in accordance with such goals and priorities. Therefore,

H2a: Structural governance mechanisms enhance goal congruence between IT and users.

2.6.1.3 Relational mechanisms and goal congruence

People inside a firm interact with each other daily and spontaneous cooperative relationships develop as a by-product of seemingly random, uncontrollable actions. Such voluntary relationships help people build network of contracts and communication channels that they can use for job performance. With proper organizational practices, firms can consciously reduce the randomness and increase the chances that these voluntary contacts occur in pursuit of the firm's goals (Galbraith, 1993). They can implement relational mechanisms by encouraging or instituting practices that foster the relationship between IT and user departments. These mechanisms are characterized by their participative and shared nature (Nilakant and Rao, 1994; Peterson, 2004). Examples include direct (informal) contacts, lobbying, joint performance incentives and rewards, collocation of user departments and IT, cross-functional training, job rotations, etc. Firms may also implement initiatives such as strategic dialogs (Nordblom, 2006) or relationship management (Martin, Hatzakis, Lycett, and Macredie, 2004). Or they can be as simple as daily procedures and actions such as keeping each other updated of new developments in the department.

An amiable relationship between IT and business promotes better communications and understanding between the two. In addition to positive effects on IT morale and motivation, these mechanisms also furnish IT with information about with whom to communicate and when communication with business departments is necessary. These, in turn, encourage IT to be more interested in and sensitive to users' security requirements. They are also conducive to the creation of SLAs. IT thus will have a better grasp of the users' goals in terms of InfoSec protection and be more motivated to exercise efforts in delivering good service to user departments. Therefore,

H3a: Relational governance mechanisms enhance goal congruence between IT and users.

2.6.2 Information Asymmetry

An important way to reduce information asymmetry between the agent and the principal is monitoring (Adams, 1994; Baiman, 1990). Monitoring of InfoSec effectiveness usually is performed through security assessments and IT audits.

A security assessment is the process of determining whether the existing information security program is adequately addressing the firm's security risks and is promptly updated for changes in business (Kairab, 2005; Snedaker, 2006).

The scope of assessments can range from focused to comprehensive, depending on the situation. An example of the former is a vulnerability assessment. Also termed "vulnerability scan," it

identifies known vulnerabilities in the firm's operating systems and system-level software. Analysis of vulnerability assessment results points to possible weakness in the IT infrastructure. The vulnerability assessment can be taken one step further by performing a penetration test, or "pen test" for short. A pen test exploits the know vulnerabilities uncovered through the vulnerability scan and tries to penetrate systems and gain access to critical system files, functions, and information. If such an attempt fails, the security measures in place are validated. Finally, at the other end of the spectrum of testing scope, a comprehensive assessment can take the form of a risk assessment that considers more than just technical vulnerabilities but also security threats in the environment as well. Vulnerability scan and pen test often are performed as part of the risk assessment. Results from risk assessments contain a wealth of information about the security of the firm's information and information systems (Maiwald and Sieglein, 2002).

An audit typically is less technical than an assessment but broader in scope (Kairab, 2005). Internal IT auditors usually start their audit with a system. They try to decide the sensitivity of the information the system processes and the criticality of the system to the business operations. They then evaluate the types and sufficiency of security measures that are in place. External audits are more comprehensive and often have the additional objective of validating policy or legal compliance (Maiwald and Sieglein, 2002). Audits may spot weak areas that prompt the firm to conduct a more technical security assessment.

The difference between security assessments and audits is actually quite subtle (Kairab, 2005). For conciseness, the term "security audit" is used to refer to these monitoring methods

collectively. Security audits can be performed by either internal auditors or a third party. Although self-assessments can be performed by IT itself, for unbiased opinions assessments also should be performed by external auditors and/or pen testers (Maiwald and Sieglein, 2002). When executed properly, security audits enable the firm to obtain an independent view of security. They uncover security risks and potentially raise issues about employee performance (Kairab, 2005). Therefore, security audit is a very effective way to provide information on the outcomes of a firm's security organization's work. As the result, the information asymmetry between IT and users is reduced.

2.6.2.1 Process-based mechanisms and information asymmetry

The benefits of implementing process-based mechanisms include the formalization of IT-related processes, standard language of communication, and metrics of IT performance. All these facilitate the conducting of security audits.

For example, CobiT groups IT processes into four "domains" covering the entire life cycle of IT process – Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Each domain contains a number of "control objectives" that govern IT processes belonging in that domain. Each control objective, in turn, is divided into a number of activities that are termed "detailed control objectives." CobiT distills a set of common, high-level information criteria. The goals for each control objective are specified with regard to which of those criteria the control objective should fulfill, and to what extent. It is notable that out of the

seven criteria three are for information security, i.e., the CIA triad. To measure each process' performance, ITGI also devises a system of metrics that include maturity models, critical success factors (CSFs), key goal indicators (KGIs), and key performance indicators (KPIs). Maturity models allow the organization to benchmark each of its IT process against the industry, the international standards, or the organization's strategic goal for that process. The CSFs are the most important issues or actions that must be addressed successfully to be compliant with that control objective. KGIs measure whether an IT process has achieved its business requirements. While KGIs measure the "what" of goal achievement, KPIs measure the "how" side – how well the process is utilizing resources toward the achievement of the goals (ITGI, 2004; Lahti and Peterson, 2005).

Similarly, ITIL groups IT processes into a number of areas. The guidance for improving the service quality of each is laid out in its corresponding publication. ITIL's governance framework is established by the collection, or "library," of these publications (hence the "L" in ITIL). These IT areas include: Business Perspectives, Service Management, Service Delivery, Service Support, ICT Infrastructure Management, Security Management, etc. Within each, a number of subjects are addressed in more details. The publications specify the objectives, activities, inputs, and outputs for processes categorized in each of these subjects (ITSMF, 2005). ISO17799, the international standard for information security best practices, groups InfoSec activities into ten domains, each containing a number of control objectives (Peltier, 2002).

What these frameworks try to capture, organize, and govern are really the same set of IT processes and services. The differences between them are more a matter of organizing logic. In fact, ITGI's Security Baseline contains mappings between CobiT and ISO17799 control objectives. More extensive mappings between Cobit, ISO17799, and ITIL are provided in Aligning CobiT, ITIL, and ISO17799 for Business Benefits.

In summary, these process-based frameworks organize IT processes into a manageable number of control objectives. This lends well to the checklist methodology that audits usually adopt. For instance, based on the CobiT system of organizing IT processes and metrics, ITGI also creates an Audit Guidelines for IT audits. They enable the auditors to review specific IT processes that are most relevant to the audit purpose at hand. In addition, these frameworks also create a common terminology inside the firm that makes interpretation and comparison of audit results much easier. Therefore,

H1b: Process governance mechanisms reduce the information asymmetry between IT and users.

2.6.2.2 Structural mechanisms and information asymmetry

Of particular importance are the structural mechanisms regarding security audits. Proper implementation of structural mechanisms establishes an independent feedback channel and gives assurance to users regarding the quality of monitoring information (Jordan and Silcock, 2005).

Proper governance ensures that audit responsibilities are entrusted with the proper organizational unit that is impartial to the audit results. An important mission of the audit committee is to ensure the independence of the audit function, which, ideally, should report directly to the audit committee. Independence of the audit function allows auditors to be free from undue influence, monitor fairly, and serve the organization's overall goals by focusing on the risks most critical to the business (Rittinghouse and Hancock, 2003; Schweitzer, 1987; Straub, 1988).

Also, a proper audit committee has representatives from every major group in the firm. This helps to achieve adequate coverage of information security issues related to each of the groups (Rittinghouse and Hancock, 2003).

Therefore, structural governance mechanisms ensure proper composition and positioning of the audit function and audit committee. As the result, the monitoring information gathered is most likely to be complete, impartial, and suitable to the firm's business needs. With this faithful audit information, users will be better informed of IT's actions and the state of the organization's information security. Therefore,

H2b: Structural governance mechanisms reduce the information asymmetry between IT and users.

2.6.2.3 Relational mechanisms and information asymmetry

Relational mechanisms enhance communication and understanding between IT and users.

With better understanding of IT staffers' qualifications, work environment, the profession they are in, their risk stance, and their basic approach to problem solving qualifications, users are more informed when they interpret and evaluate security audit results.

Both agency theory and signaling theory (Morris, 1987) suggest that the agent may be motivated to offer information to the principal to assure the latter of desirable results from the task. Such information is beneficial to the principal even if there might be some "noise" created by the agent's intentional shaping of the communication of that information (Levinthal, 1988). A pleasant relationship motivates IT to have more interactions with business and be more willing to furnish users with information regarding IT's qualifications for, approaches to, and actions in providing InfoSec services.

For example, if IT staffers voluntarily seek and obtain industry certifications on information security, it provides users information on the staff's capabilities that would otherwise be difficult to assess. If IT initiates frequently communication regarding the firm's current information security status, new information security threats likely to affect the organization, new trends in InfoSec defense measures, etc., users will feel not as uninformed when it comes to evaluate the IT's performance. The result of IT providing information like this is that users arrive in a position that is better able to evaluate IT's technology provisioning, recommendations for information security services, and results from security audits. Therefore,

H3b: Relational governance mechanisms reduce the information asymmetry between IT and users.

2.6.3 Governance and Effectiveness of InfoSec Services

As discussed earlier, the effectiveness of InfoSec services include three aspects – quality service, asset protection, and business function support. Addressing the root causes for agency problems enhances effectiveness in these aspects.

Better understanding of "client" goals allows IT to better deliver the information, products, and services the client desires (Peak and Guynes, 2003). Governance mechanisms improve the goal congruence between IT and the internal customers. Part of the improvement comes from the rapport built between IT and business departments because one type of the governance mechanisms focuses on relationship building. When IT understands users' requirements with positive emotional predisposition, it is more willing to treat the users with better service and strives to seek out technical solutions, plan resources, and implement proper protection measures so that assets are better protected. IT is also more willing to provide support the users on their job by providing InfoSec related services to help them fulfill operational, regulatory, and legal requirements so that they can perform better on their jobs. Therefore,

H4: Enhanced goal congruence between IT and users are positively related to higher effectiveness in InfoSec services provided by IT.

On the other hand, reduction in information asymmetry makes the users much better "shopper" for services. Suboptimal service quality is more likely to result in "customer complaints" which

can lead to corrective actions taken upon IT. In extreme cases, it may lead to the outsourcing of the InfoSec function thus threatening IT's job security. Hence, IT will be more sensitive toward its service quality.

Proper monitoring activities such as security assessments help to spot security vulnerabilities and loopholes and alert the firm in a timely manner. Users thus are more informed of IT's performance and security measures' effectiveness in protecting information assets. Remedy of the problems is more likely to take place promptly and results in better protection of assets. Also, when evaluating users' job performance, the information generated from monitoring helps to identify the impact caused by inadequate InfoSec services provided by IT. This strengthens accountability and encourages IT to do their part to avoid the embarrassment of being traced down as the obstacle to users' job performance. Therefore,

H5: Reduced information asymmetry between IT and users are positively related to higher effectiveness in InfoSec services provided by IT.

2.7 Conclusion

Organizations are implementing IT governance initiatives and investing heavily in information security. Due to the nature of information security, in most organizations information security is implemented and managed primarily by the internal IT department. In essence, IT acts as an agent for internal "customers" – the various business departments. To ensure that IT provides the desired outcomes, i.e., best protection of information assets and quality services to business

departments, proper governance of the information security function is needed. Information security governance is an integrated part of IT governance and can be implemented with a variety of IT governance mechanisms. This essay delves into the rich array of governance mechanisms and presents them as a trio of process-based, structural, and relational mechanisms. It explains the efficacy of these mechanisms in guiding information security function toward more effective InfoSec services by adopting an agency theory perspective. More specifically, it suggests that suboptimal outcomes occur when the agent does not act in the best interest of the principal, i.e., when agency problems occur. The two root causes for agency problems are goal incongruence and information asymmetry between the agent and the principal. IT governance mechanisms help to reduce agency problems by addressing these two root causes. In the context of information security, they work by facilitating better understanding of user requirements for information security and providing information feedback through objective assessment of the state of security in the organization. These reduce the goal congruence and information asymmetry and lead to higher effectiveness in InfoSec services.

2.8 Chapter 2 List of Reference

1. Adams, M. B. (1994). Agency theory and the internal audit. *Managerial Auditing Journal,* 9(8), 8-12.

2. Alberts, C., & Dorofee, A. (2003). *Managing Information Security Risks: The OCTAVE Approach*. Boston, MA: Addison-Wesley.

3. Arrow, K. J. (1985). The economics of agency. In J. W. Pratt & R. J. Zeckhauser (Eds.), *Principals and Agents: The Structure of Business* (pp. 37-51). Boston, MA: Harvard Business School Press.

4. Avižienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing,* 1(1), 11-33.

5. Baiman, S. (1982). Agency research in managerial accounting: A survey. *Journal of Accounting Literature,* 1, 154-213.

6. Baiman, S. (1990). Agency research in managerial accounting: A second look. *Accounting, Organizations and Society,* 15(4), 341-371.

7. Brown, A. E., & Grant, G. G. (2005). Framing the frameworks: A review of IT governance research. *Communications of the AIS,* 15, 696-712.

8. BSA, & ISSA. (2004). *BSA-ISSA Information Security Study Online Survey of ISSA Members*: Business Software Alliance and Information Systems Security Association.

9. Clark, T. (1993). The market provision of management services, information asymmetries and service quality - Some market solutions: An empirical example. *British Journal of Management,* 4, 235-251.

10. De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal, 2004,* 1-7.

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

12. Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review,* 14(1), 57-74.

13. Galbraith, J. R. (1993). *Competing with Flexible Lateral Organizations* (2nd ed.). Reading, MA: Addison-Wesley.

14. Gentile, M., Collette, R., & August, T. (2006). *The CISO Handbook, A Practical Guide to Securing Your Company*. Boca Raton, FL: Auerbach Publications.

15. Gollmann, D. (2006). *Computer Security* (2nd ed.). West Sussex, UK: John Wiley & Sons.

16. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

17. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *2006 CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

18. Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). *NIST Special Publication 800-35: Guide to Information Technology Security Services*. Washington, D.C.: National Institute of Standards and Technology.

19. Hiles, A. N. (1994). Service level agreements: Panacea or pain? *The TQM Magazine,* 6(2), 14-16.

20. Indjejikian, R. J. (1999). Performance evaluation and compensation research: An agency perspective. *Accounting Horizons,* 13(2), 147-157.

21. ITGI. (2000). *CobiT 3rd Edition Executive Summary*. Rolling Meadows, IL: IT Governance Institute.

22. ITGI. (2003). *Board Briefing on IT Governance* (2nd ed.). Rolling Meadows, IL: ITGI.

23. ITGI. (2004). *CobiT Security Baseline*. Rolling Meadows, IL: IT Governance Institute.

24. ITGI. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2nd ed.). Rolling Meadows, IL: IT Governance Institute.

25. ITSMF. (2005). *Foundations of IT Service Management Based on ITIL*. Hogeweg, The Netherlands: Van Haren Publishing.

26. Jap, S. D. (1999). Pie-expansion efforts: Collaboration processes in buyer-supplier relationships. *Journal of Marketing Research,* 36(4), 461-475.

27. Jap, S. D., & Anderson, E. (2003). Safeguarding interorganizational performance and continuity under *ex post* opportunism. *Management Science,* 49(12), 1684-1701.

28. Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency cost and ownership structure. *Journal of Financial Economics,* 3, 305-360.

29. Jensen, M. C., & Murphy, K. (1990). Performance pay and top-management incentives. *Journal of Political Economy,* 98, 225-284.

30. Jordan, E., & Silcock, L. (2005). *Beating IT Risks*. West Sussex, UK: John Wiley & Sons.

31. Kairab, S. (2005). *A Practical Guide to Security Assessments*. Boca Raton, FL: Auerbach Publications.

32. Lahti, C. B., & Peterson, R. (2005). *Sarbanes-Oxley IT Compliance Using CobiT and Open Source Tools*. Rockland, MA: Syngress Publishing, Inc.

33. Larson, K. D. (1998). The role of service level agreements in IT service delivery. *Information Management & Computer Security*, 6(3), 128-132.

34. Levinthal, D. (1988). A survey of agency models of organizations. *Journal of Economic Behavior and Organization*, 9, 153-185.

35. Maiwald, E., & Sieglein, W. (2002). *Security Planning and Disaster Recovery*. Berkeley, CA: McGraw-Hill/Osborne.

36. Martin, V. A., Hatzakis, T., Lycett, M., & Macredie, R. (2004). Building the business/IT relationship through knowledge management. *Journal of Information Technology Cases and Applications*, 6(2), 27-47.

37. McKenna, B. (2002). Managed security services - New economy relic or wave of the future. *Computers & Security*, 21(7), 613-616.

38. Mills, P. K. (1990). On the quality of services in encounters: An agency perspective. *Journal of Business Research*, 20, 31-41.

39. Morgan, A. G., & Poulsen, A. B. (2001). Linking pay to performance - Compensation proposals in the S&P 500. *Journal of Financial Economics*, 62, 489-523.

40. Morris, R. D. (1987). Signalling, agency theory and accounting policy choice. *Accounting and Business Research*, 18(69), 47-56.

41. Neely, A., & Wilson, J. (1992). Measuring product goal congruence: An exploratory case study. *International Journal of Operations & Production Management*, 12(4), 45-52.

42. Nilakant, V., & Rao, H. (1994). Agency theory and uncertainty in organizations: An evaluation. *Organization Studies*, 15(5), 649-672.

43. Nordblom, C. (2006). Involving middle managers in strategy at Volvo Group. *Strategic Communication Management*, 10(2), 26-29.

44. Peak, D., & Guynes, C. S. (2003). Improving information quality through IT alignment planning: A case study. *Information Systems Management*, 20(4), 22-29.

45. Peltier, T. R. (2002). *Information Security: Policies, Procedures, and Standards*. Boca Raton, FL: Auerbach Publications.

46. Peterson, R. R. (2004). Crafting information technology governance. *Information Systems Management*, 21(4), 7-22.

47. Peterson, R. R., O'Callaghan, R., & Ribbers, P. M. A. (2000). Information technology governance by design. *Proceedings of the Twenty-first International Conference on Information Systems*, Brisbane, Australia, December 10-13, 2000. 435-452.

48. Pitt, L. F., Watson, R. T., & Kavan, C. B. (1995). Service quality: A measure of information systems effectiveness. *MIS Quarterly*, 19(2), 173-187.

49. Pontes, M. C. (1995). Agency theory: A framework for analyzing physician services. *Health Care Management Review*, 20(4), 57-67.

50. Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23, 638-646.

51. Rittinghouse, J. W., & Hancock, W. M. (2003). *Cybersecurity Operations Handbook*. Burlington, MA: Digital Press.

52. Sambamurthy, V., & Zmud, R. W. (2000). The organizing logic for an enterprise's IT activities in the digital era - A prognosis of practice and a call for research. *Information Systems Research*, 11(2), 105-114.

53. Schweitzer, J. A. (1987). *Computers, Business, and Security: The New Role for Security*. Stoneham, MA: Butterworth Publishers.

54. Singh, J., & Sirdeshmukh, D. (2000). Agency and trust mechanisms in consumer satisfaction and loyalty judgments. *Academy of Marketing Science Journal*, 28(1), 150-167.

55. Singleton, J. P., McLean, E. R., & Altman, E. N. (1988). Measuring information systems performance: Experience with the management by results system at Security Pacific Bank. *MIS Quarterly*, 12(2), 325-337.

56. Snedaker, S. (2006). *IT Security Project Management Handbook*. Rockland, MA: Syngress.

57. Straub, D. W. (1988). Organizational structuring of the computer security function. *Computers & Security*, 7(2), 185-195.

58. Sturm, R., Morris, W., & Jander, M. (2000). *Foundations of Service Level Management*. Indianapolis, IN: Sams.

59. Symantec. (2004). *Sarbanes-Oxley Act: A Regulatory Perspective*. Cupertino, CA: Symantec Corporation.

60. Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structure, process and relational mechanism for IT governance. In W. V. Grembergen (Ed.), *Strategies for Information Technology Governance* (pp. 1-36). Hershey, PA: Idea Group Publishing.

61. Volonino, L., Gessner, G. H., & Kermis, G. F. (2004). Sarbanes-Oxley links IT to corporation compliance. *Proceedings of the Tenth Americas Conference on Information Systems*, New York, NY. 4600-4607.

62. Von Solms, B. (2005). Information security governance - Compliance management vs operational management. *Computers & Security*, 21(4), 356-371.

63. Von Solms, S. H. (2005). Information security governance - Compliance management vs operational management. *Computers & Security*, 24, 443-447.

64. Warkentin, M., & Johnston, A. C. (2006a). IT Governance and Organizational Design for Security Management. In D. Straub, S. Goodman & R. Baskerville (Eds.), *Information Security Policies and Practices*. Armonk, NY USA: M.E. Sharpe.

65. Warkentin, M., & Johnston, A. C. (2006b). IT security governance and centralized security controls. In M. Warkentin & R. Vaughn (Eds.), *Enterprise Information Systems Assurance and System Security*. Hershey, PA: Idea Group Publishing.

66. Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA: Harvard Business School Press.

67. Whitman, M. E., & Mattord, H. J. (2005). *Principles of Information Security*. Boston, MA: Thomson Course Technology.

68. Wickramasinghe, N., & Ginzberg, M. J. (2001). Integrating knowledge workers and the organization: The role of IT. *International Journal of Health Care Quality Assurance*, 14(6), 245-253.

69. Williams, P. (2007). Executive and board roles in information security. *Network Security, 2007*, 11-14.

70. Wylder, J. (2004). *Strategic Information Security*. Boca Raton, FL: Auerbach Publications.

71. Yermack, D. (2004). Remuneration, retention, adn reputation incentives for outside directors. *Journal of Finance*, 59(5), 2281-2308.

CHAPTER 3 EFFECTS OF IT GOVERNANCE MECHANISMS ON INFORMATION SECURITY SERVICE EFFECTIVENESS: AN EMPIRICAL TEST

3.1 Introduction

To protect business information, executives and business users rely on a number of information security (InfoSec) services (Grance, Hash, Stevens, O'Neal, and Bartol, 2003). If the IT department cannot provide effective InfoSec services, the results can be costly. Recently, there are calls for better governance of the information security function to ensure that it serves the company's business needs (Posthumus and von Solms, 2004). The board of directors and executive management, therefore, should take the lead in the implementation of a proper governance framework (Posthumus and von Solms, 2004; Williams, 2007).

Information security governance is an integral part of IT governance (ITGI, 2006; Posthumus and von Solms, 2004; Von Solms, 2005). As such, it usually is implemented by taking advantage of broader, enterprise-wide IT governance mechanisms. For instance, some governance function of InfoSec can be implemented as part of the implementation of Control Objectives for Information and related Technology (CobiT) or Information Technology Infrastructure Library (ITIL). In addition to these mechanisms that are IT process oriented, a variety of other governance mechanisms are available, with a focus on organizational structure or relationships. These governance mechanisms, however, have not been sufficiently addressed in

academic research, which largely stresses the traditional centralized-decentralized-federal trichotomy of governance forms (e.g.,Warkentin and Johnston, 2006a, 2006b). Thus, this study addresses these research questions:

1. *Does implementation of various IT governance mechanisms improve the effectiveness of information security services?*
2. *Which type(s) of mechanisms are more critical for improving information security?*

To understand these questions, we use agency theory to explain their efficacy in governing information security to explain the effectiveness of three types of governance mechanisms. IT is viewed as an agent providing InfoSec services to the business departments, who are the principals. The governance mechanisms are hypothesized to reduce goal incongruence and information asymmetry between the agent and the principal. They, in turn, improve the effectiveness of InfoSec services.

The rest of the essay proceeds as follows. First, the role of IT as a provider of information security services is discussed. This is followed by a discussion of agency relationship and agency problems in the context of information security function. Next, IT governance and three types of governance mechanisms are introduced. We then present hypotheses on the relationships among (a) the governance mechanisms, (b) two root causes of agency problems, i.e., goal congruence and information asymmetry, and the (c) the effectiveness of InfoSec services. Next, we describe a survey of security managers and business managers for empirical testing of

those hypotheses. Research findings are presented, followed by a discussion of those findings and the theoretical contribution. Implications for future research also are discussed.

3.2 Information Security Services

IT is a staff function that provides services to internal "customers" – other departments throughout the organization (Pitt, Watson, and Kavan, 1995). This is particularly true when it comes to information security. The outcomes of InfoSec activities fit the characteristics of services as described by Clark (1993) – (a) *intangibility*: The outcomes of information security are usually intangible; (b) *inseparability*: InfoSec services are "sold" and "consumed" at the same time; (c) *heterogeneity*: each instance of InfoSec service is unique due to the differences in the user's specific computer environment, the context of a security problem, and the IT staffer's individuality; (d) *perishability*: InfoSec services cannot be stored; and (e) *non-transferability*: there is no transfer of ownership when InfoSec services are rendered.

InfoSec services provided by IT address InfoSec at three levels – (a) *management*: developing and maintaining an organization-wide security program, formulating security policies, designing the security architecture, etc.; (b) *operations*: handling important InfoSec operations such as contingency planning, incident response, security testing, user training, etc.; and (c) *Technical*: technical implementation of InfoSec mechanisms, such as firewall configuration and management, intrusion detection system design and monitoring, public key infrastructure (PKI) implementation, etc. (Grance et al, 2003)

In theory, these services can be offered by internal IT or external vendors (Grance et al, 2003). In practice, however, industry surveys continuously show that only a very small percentage of firms actually outsource their information security services and, even then, usually only to a limited extent (BSA and ISSA, 2004; Gordon, Loeb, Lucyshyn, and Richardson, 2005, 2006; McKenna, 2002). The information security function normally sits within an internal InfoSec function or IT department.

Whether IT provides effective InfoSec should be evaluated in three areas – business function, customers, and effective security. Any metrics of effectiveness should include efficacy of implementation, service delivery, and business impact (Grance et al, 2003).

The efficacy of implementation is reflected in how services protects the safety of information assets. Second, an important measurement of the effectiveness of IT is the quality of service it provides (Pitt et al, 1995). IT should deliver reliable services, be responsive to user service requests, be considerate with user requirements, perform services in a professional manner, etc. Third, the security assurance provided by IT should support business users in their job functions.

3.3 Agency Relationship in Information Security

As the provider of security services to the internal "customers," IT in essence acts as an agent for the principal, i.e., the business departments. Agency relationships exist because the principal

delegates the task because of lack of time or ability to do the task (Nilakant and Rao, 1994), among other reasons. Similarly, although business departments are the owner of information assets in the company, they need to delegate the provision of InfoSec services to IT because IT usually is the only organizational unit that has the expertise and skills for it.

The downside to agency relationship is the loss of principal welfare, which is commonly referred to as two agency problems – (a) *adverse selection* refers to the agent's exerting inappropriate types of effort (Nilakant and Rao, 1994). For example, a security administrator may dismiss abnormal activities on corporate network as transient peaks in traffic while the reality is that an attacker is scanning the network; and (b) *moral hazard* means that the agent exercises inadequate effort (Mills, 1990). A security administrator may dislike the mundane task of reviewing logs from firewalls, intrusion detection systems, Windows operating systems, etc. In such cases, she thus only performs a cursory daily review of the log entries and sometimes skips the review altogether.

Agency problems are the result of two fundamental causes – goal incongruence between the agent and the principal and the principal's difficulty in verifying the agent's abilities and efforts due to asymmetric information (Eisenhardt, 1989). The difficulty in verification is mostly the result of information asymmetry. Since, in many cases, the agent has the expertise the principal does not have and is directly involved in performing the task, the agent accumulates and possesses a wealth of information to which the principal cannot gain easy access.

Agency literature in fields such as accounting and finance has focused on governance as a way to control agency problems. Often the goal is to use compensation structures to align managers' (the agents') interest with the principal's (e.g., Indjejikian, 1999; Jensen and Murphy, 1990; Morgan and Poulsen, 2001; Yermack, 2004) or to create, through monitoring, an "information system" that the principal can utilize to reduce the performance-based asymmetry (Baiman, 1982, 1990). However insightful this literature in accounting and finance is, this study draws upon the IT governance literature for mechanisms to reduce goal incongruence and information asymmetry between the agent and the principal.

3.4 IT Governance Mechanisms

IT governance is an integral part of corporate governance. It is the organizational capacity to ensure that IT sustains and extends the organization's strategy (ITGI, 2003). The extant IS literature on IT governance has long centered on decision making patterns that can be centralized, decentralized, or federal. Of more practical importance and research interest, however, are the governance mechanisms such as sourcing arrangements, strategic alliances, roles, teams, processes, and informal relationships (Sambamurthy and Zmud, 2000). Although some researchers have proposed three types of IT governance mechanisms (De Haes and Van Grembergen, 2004; Peterson, 2004a; Van Grembergen, De Haes, and Guldentops, 2004), much of this has been carried out at the theoretical level. To the best of our knowledge, no empirical research in InfoSec literature has concentrated on governance mechanisms. Therefore, we

explore three categories of IT governance mechanisms in this study, one basing on process, one on structure, and one on relations:

1. *Process-based governance mechanisms* are IT management techniques that ensure that daily behaviors are consistent with IT policies and that all stakeholders are involved in the effective management and use of IT (Weill and Ross, 2004). It is the formal institution of strategic IT decision making or IT monitoring procedures. Examples include CobiT, ITIL, and ISO17799.

2. *Structural governance mechanisms* are the organizational units and roles that are instituted to properly locate decision-making responsibilities, to promote horizontal connection between IT and business functions, and ultimately, to achieve IT governance goals (Peterson, 2004a; Peterson, O'Callaghan, and Ribbers, 2000; Weill and Ross, 2004). Formal groups such as executive teams, committees, councils, task forces are an important horizontal integration structures for coordinating IT decision making across business and IT. These structures provide a holistic view that is beneficial to the governance goals. Linkages between business and IT can also be fostered with mechanisms such as joint decision councils (Weill and Ross, 2004).

3. *Relational governance mechanisms* are the organizational practices that encourage voluntary two-way communication and collaboration between business and IT (De Haes and Van Grembergen, 2004; Peterson, 2004a; Van Grembergen et al, 2004). The main

desired outcomes of such mechanisms are better mutual understanding and effective communication channels among the various stakeholders in the organization, such as corporate management, business unit management, IT management, among others (Peterson, 2004a). Relational governance mechanisms include direct (informal) contacts, lobbying, joint performance incentives and rewards, collocation of business and IT managers, cross-functional training, job rotations, continuous education, etc.

3.5 Governance Mechanisms and Agency Problem Reduction

IT governance holds the potential to improve InfoSec outcomes by tackling the two underlying causes of agency problems. Reduction of the two root causes, in turn, leads to more effective InfoSec services. Figure 1 presents our theoretical model.

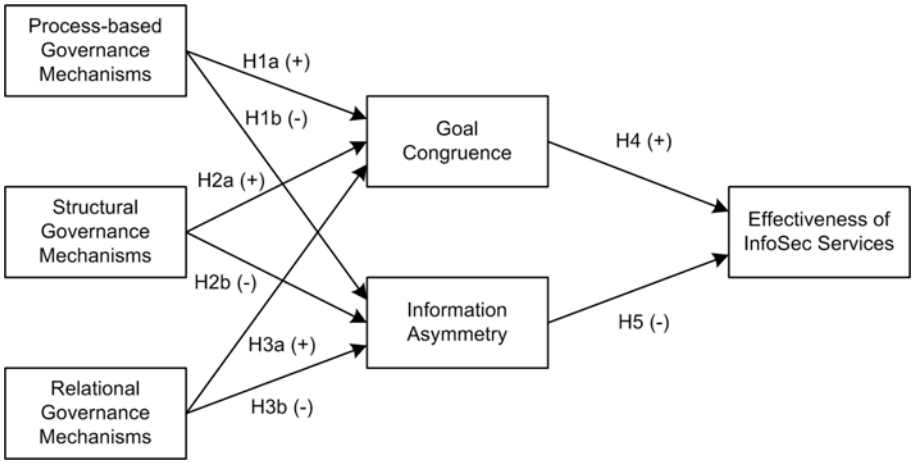


Figure 3.1 Research Model

The three types of governance mechanisms improve the effectiveness of InfoSec services by addressing the underlying causes – goal incongruence and information asymmetry. This study

addresses these relationships through a critical aspect of providing InfoSec service – gathering users' requirements for security and assessing and monitoring of the fulfillment of those requirements.

3.5.1 Goal congruence

Goal congruence has been defined as the extent to which the relative importance of key performance criteria (Neely and Wilson, 1992; Wickramasinghe and Ginzberg, 2001), including the achievability of goals (Jap, 1999; Jap and Anderson, 2003), are understood between/among parties. For InfoSec services, agreement on key performance criteria can be achieved through a well-implemented process of defining security requirements. IT should understand users' high-level business requirements, those that capture the essence of what InfoSec will achieve for the business, as well as functional requirements that describe how an InfoSec solution or a system, when properly protected, meets the business requirements. Based on understanding of these requirements, IT can then derive specific technical requirements and implement the proper security mechanisms accordingly (Gentile, Collette, and August, 2006; Snedaker, 2006).

In the process of requirement determination, collaboration and communications between IT and user departments is essential to enhancing goal congruence between the two. Governance mechanisms promote such collaboration and communications.

When implementing process-based governance mechanisms, companies have to explicate their IT processes and organize them logically. This can be seen in the CobiT model where IT processes are grouped into four broad areas and further subdivided into control objectives and detailed control objectives. ISO17799 has a similar hierarchy that focuses exclusively on security-related processes.

A benefit of implementing process-based mechanisms is that in the implementation process the company encourages IT and business departments to dialogue about IT processes and assets. As the result IT gains a better understanding of what assets to protect in addition to the business and IT contexts for such protection. IT can discuss with users the technical feasibility or difficulty of fulfilling their security requirements, given the current state of security technologies and the firm's resources. Therefore,

H1a: *Process-based governance mechanisms enhance goal congruence between IT and users.*

In addition to the process-based mechanisms, various structural mechanisms also allow IT and business objectives and priorities to be discussed openly and formally (Peterson, 2004a; Peterson et al, 2000; Weill and Ross, 2004). Structural mechanisms such as IT steering committees, IT budget committees, and IT strategy committees and similar organizational councils and committees are the venue through which IT and user departments present their cases and viewpoints regarding information security. Competing ideas and projects are debated and consensus is built. As the result, IT achieves a better understanding of user requirements for

InfoSec and is better prepared to devise security plans in accordance with such goals and priorities. Therefore,

H2a: *Structural governance mechanisms enhance goal congruence between IT and users.*

Relational governance mechanisms try to consciously catalyze the voluntary relationship building process employees experience every day. Such voluntary relationships, in fact, are an important way by which employees build network of contracts and communication channels that they can use for job performance. Relational governance mechanisms reduce the randomness and increase the chances that these voluntary contacts occur in pursuit of the firm's goals (Galbraith, 1993). As the result, a good relationship between IT and business promotes better communications and understanding between the two and encourage IT to be more interested in and sensitive to user security requirements. Therefore,

H3a: *Relational governance mechanisms enhance goal congruence between IT and users.*

3.5.2 Information Asymmetry

Information asymmetry is the second underlying cause of agency problems. Reduction of information asymmetry is achieved primarily by creating an "information system" of monitoring information (Adams, 1994; Baiman, 1990). Monitoring of InfoSec effectiveness usually is performed through security assessments and IT audits.

A security assessment is the process of determining whether the existing information security program is adequately addressing the firm's security risks and is promptly updated for changes in

business (Kairab, 2005; Snedaker, 2006). Depending on a company's specific needs, the scope of assessment can go from a simple network scanning to penetration testing. Or the assessment can be performed with more technical focus such as a penetration test or with more business focus in the form of a risk assessment. Under certain circumstances, intensive and purposive assessment in the form of a formal audit can be performed (Kairab, 2005; Maiwald and Sieglein, 2002). Security assessments inform business users and top management of what IT is doing to protect information assets and how they are performing in that respect. Governance mechanisms help to reduce the information asymmetry by implementing a process to ensure regular security assessments and assessment results that are objective and comprehensible to the principal.

Process-based mechanisms help companies to organize IT processes into a manageable number of control objectives. The benefits include formalization of IT processes, standard language of communication, and usable metrics of IT performance. These fit well with the checklist methodology that audits usually adopt. For instance, based on the CobiT system of organizing IT processes and metrics, ITGI has also created an *Audit Guidelines* for IT audits. They enable the auditors to review specific IT processes that are most relevant to the audit purpose at hand. In addition, these frameworks also create a common terminology inside the firm that makes interpretation and comparison of audit results much easier. Therefore,

H1b: *Process governance mechanisms reduce the information asymmetry between IT and users.*

Proper implementation of structural mechanisms establishes an independent feedback channel and assures users high quality feedback (monitoring) information (Jordan and Silcock, 2005).

For instance, an important mission of the audit committee is to ensure the independence of the IS audit function, which, ideally, should report directly to the audit committee. Independence of the audit function allows auditors to be free from undue influence, monitor fairly, and serve the organization's overall goals by focusing on the risks most critical to the business (Rittinghouse and Hancock, 2003; Schweitzer, 1987; Straub, 1988). Also, if the committee has representatives from every major group in the firm, adequate coverage of information security issues related to each of the groups is ensured (Rittinghouse and Hancock, 2003). As the result, the monitoring information gathered is most likely to be complete, impartial, and suitable to the firm's business needs. With this faithful audit information, users will be better informed of actions by the IT group and the state of organizational information security. Therefore,

H2b: *Structural governance mechanisms reduce the information asymmetry between IT and users.*

Relational mechanisms enhance communication and understanding between IT and users. With better understanding of IT staffers' qualifications, their work environment, their profession, their risk stance, and their basic approach to problem solving qualifications, users are better informed to interpret and evaluate security audit results. A good relationship motivates IT to have more interactions with business units and be more willing to furnish users with information regarding the qualifications of IT personnel and IT's approaches to and actions for providing InfoSec services. The result of IT providing information like this is that users arrive in a position that is better able to evaluate the technology provisioning of the IT group, its recommendations for information security services, and results of security audits. Therefore,

H3b: *Relational governance mechanisms reduce the information asymmetry between IT and users.*

3.5.3 Governance and Effectiveness of InfoSec Services

Governance mechanisms improve the goal congruence between IT and the internal customers. Better understanding of "client" goals allows IT to better deliver the information, products, and services the client desires (Peak and Guynes, 2003). When IT approaches user requirements with a positive predisposition, it is more willing to respond to the users with better services and seek out technical solutions, plan resources, and implement proper protection measures so that assets are better protected. IT is also more willing to support users on their job by providing InfoSec related services to help them fulfill operational, regulatory, and legal requirements. Therefore,

H4: *Goal congruence between IT and users are positively related to effective InfoSec services.*

With reduction in information asymmetry, suboptimal service quality is more likely to result in "customer complaints" which can lead to IT being "corrected" by management. Proper monitoring activities such as security assessments help to spot security vulnerabilities and loopholes and alert the management in a timely manner. Users thus are more informed of IT's performance and the effectiveness of security measures in protecting information assets. Remedy of the problems is more likely to take place promptly and results in better protection of assets. Also, when evaluating user job performance, the information generated from monitoring

helps to identify the impact caused by inadequate InfoSec services provided by IT. This strengthens accountability and encourages IT to do their part to avoid the embarrassment of being traced down as the obstacle to user job performance. Therefore,

H5: *Information asymmetry between IT and users are negatively related to higher effectiveness in InfoSec services.*

3.6 Methodology

To test our research model, a survey was conducted with information security managers. Since there are no existing scales for the constructs in the model, we developed various items for the constructs. Following methods suggested by Dillman (2000), Mangione (1995), and Sivo et al. (Sivo, Saunders, Chang, and Jiang, 2006), paper questionnaires containing those items were distributed and online versions created. A few sources were solicited for responses. In total 102 responses were received and used for data analysis.

3.6.1 Operationalization of Constructs

Because current research on the three governance mechanisms remains largely on the conceptual level, we had to create items to measure the implementation of the three types of governance mechanisms, specifically in the context of information security. The items for governance mechanisms were derived from academic and practitioner literature on IT governance, in particular, Lahti and Peterson (2005), ITSMF (2005), Van Grembergen (2004), and Galbraith (1993), as well as information gathered from the domain experts and conferences.

The *process-based mechanisms* were operationalized with regard to the extraction of information security requirements and security assessments. Items were designed to ask whether security requirements were effectively extracted and implemented. To avoid bias toward any particular governance framework such as CobiT, ITIL, or ISO17799, the items captured the key controls that all frameworks try to achieve, rather than using the terminology specific to a particular framework.

For *structural governance mechanisms*, items were created to ask about the formal organizational units and roles that oversee the information security function and security audits. With respect to the success of implementation, these questions ask about the various committees and roles, such as IT steering committee, information security, security audit committee, etc.

Since *relational governance mechanisms* foster better communication between IT and business departments in the company, these items were created to measure whether and how a company implements various methods to encourage the interaction between IT and business users.

Measures of goal congruence were based on the definition of this construct as the extent to which the relative importance of key performance criteria (Neely and Wilson, 1992; Wickramasinghe and Ginzberg, 2001) is understood between/among parties. Therefore, the measures for goal congruence between IT and user departments were based on information from ITSMF (2005) and Gopal, Krishnan, Mukhopadhyay, and Goldenson (2002).

Given that *information asymmetry* occurs when the agent has private information to which the principal cannot costlessly gain access items were created with this in mind for the context of this study. One source for this was Gallouj (1997), who theorizes on aspects of information asymmetry.

To measure the *effectiveness of InfoSec services*, self-report measures were used. This is largely due to (a) the intangibility nature of outcomes from InfoSec services, and (b) the sensitive nature of questionnaire on InfoSec. First, measuring the effectiveness of InfoSec services is inherently difficult due to the intangible nature of the outcomes from the services. A company usually benefits from the InfoSec services through mitigation of risks (Purser, 2004). While other organizational investments can be assessed by tangible financial returns, it is very difficult, if at all possible, to calculate expected financial returns from InfoSec investments (Newman and Scholtz, 2003).

Theoretically, the effectiveness of InfoSec services could be measured by summary results from security assessments an organization has performed. However, it is highly unlikely that respondents will be able to answer such requests. In fact, asking sensitive questions in an InfoSec-related questionnaire can prevent recipients from returning the questionnaire, as argued by Kutolic and Clark (2003).

Effectiveness of InfoSec services thus has been operationalized as three items asking the respondent to estimate top management satisfaction with InfoSec services.

3.6.2 Development of Instrument

There are no existing instruments for constructs in the research model. Thus, an instrument was created. A group of domain experts consisting of information security and IT audit practitioners in the field were asked to help in the process of instrument development and validation. As the first step of the instrument development, an initial pool of items was generated based on review of the extant literature, discussion with the domain experts, and information and input that we gathered while attending various practitioner conventions on information security and IS audit.

The candidate items in the initial pool were then put through four rounds of Q-sort modeled after Moore and Benbasat (1991). A different group of four people served as judges in each round. For the first and second rounds, the judge included a practitioner expert, two Ph.D. students in the IS field, and a Ph.D. student in a non-IS field. For the third and four rounds, they were a practitioner expert, an IS Ph.D. student, and two non-IS Ph.D. students.

In the first round, we did not provide constructs and their definitions to the judges. We asked them to sort the items that they believed should load on the same constructs together and provide their definition of the constructs. If the judge found any items that were ambiguous or problematic, they were asked to discuss them with us.

In the second round, the judges had the constructs and their definitions and sorted each item into the construct to which they believed the item belonged. Again, ambiguous and problematic items were discussed.

Based on the results from the first two rounds, we revised the items and put them through another two rounds of Q-sort. The third round was identical to the first round but conducted with a different group of judges. Similarly, the fourth round was the same as the second round except the judges. After these four rounds of Q-sort, 45 items were generated for the six constructs.

Since the security managers usually have more detailed, first-hand knowledge about what and how IT governance mechanisms are implemented in an organization, we collected answers from them. For items about goal congruence, information asymmetry, and effectiveness of InfoSec services, we also obtained, in addition to security managers' responses, answers from their supervisors or representative business users as well. Thus the security manager answers could be compared to business manager answers to evaluate objectivity. Therefore, another set of similar items for business managers were also created and Q-sorted.

The items were organized into two draft questionnaires – a security manager version and a business manager version. The business version was pre-tested with graduate students in two master-level MIS classes for format, wording, and time required to complete. We then pre-tested the security manager version at a monthly meeting of the local chapter of the Information

Systems Security Association (ISSA) with 12 security managers. The managers were also asked to bring the business version back to their company and ask their supervisor to fill them out. Four business manager versions were returned. Feedback from the pre-tests was used to revise the questionnaires both in content and format.

3.6.3 Survey Administration

The recipients of the paper questionnaire were primarily IT leaders in the 2006 *InformationWeek* 500 (IW500) organizations. Each year, the *InformationWeek* magazine publishes a list of 500 organizations that are considered savvy technology users. Since the publicly available list includes the name and job title of IT leaders in those organizations, it is a convenient sample for researchers to contact IT leaders. For example, for their study on InfoSec budgeting process, Gordon et al (2006) surveyed IW500 companies on a previous year's list. This study uses the most up-to-date list at the time of the survey administration. After excluding organizations that are not based in the U.S. and those organizations whose IT leader information or mailing address was not available, questionnaires were mailed to 425 organizations.

The paper questionnaire administration largely followed the process as laid out by Dillman (2000), Mangione (1995), and Sivo et al (2006). Four contacts were made with the recipients at various points in time: (a) a pre-notice letter notifying the recipients of the upcoming questionnaire; (b) the complete survey packet; (c) a follow-up postcard to remind the recipient;

and (d) a second follow-up letter that was accompanied by a replacement questionnaire. These contacts occurred during the period from the middle of May through late July, 2007.

The questionnaire packet included both a security manager and business manager version. The former was used to collect responses from security managers, who were defined as the person in charge of managing the InfoSec function. The latter was targeted at the security manager's supervisors, which were referred to as "business managers" and could include CIO, Executive/Senior VP, CFO, COO, CEO, etc. Since the IT leaders listed in the IW500 list all were in the "business manager" category, the cover letter asked them to fill out the business manager version and then forward the other questionnaire to the security manager in their organizations. The other materials in the packet included, for each version, the IRB-approved informed consent letter, instruction sheet, a notification postcard, and a business reply mail (BRM) return envelope. Except the return envelopes, the materials for each version were printed on a distinct color, color-matched, and pinned together.

The respondents' anonymity was strictly protected. Both versions of the questionnaire were anonymous. They had demographic questions that the respondents could optionally answer but did not ask about the identity of the respondents or the companies they worked for. Each questionnaire had a pre-stamped sequence number but it was exclusively for matching up the returned questionnaires from the security manager and business manager in the same company. No individual sequence numbers were recorded and tied to any companies. The notification

postcards allowed the respondents to inform the researchers only that they had returned the questionnaire.

In addition, several other sources of potential respondents were tapped. These sources were members of two professional organizations – Information Systems Audit and Control Association (ISACA) and Information Systems Security Association (ISSA). To survey these groups, an online version of the paper questionnaire was created. The ISACA headquarters included the survey in its Academic Advocate initiative and sent out the URL to its contact list of information security managers. Two local ISACA chapters sent out email to their members and solicited participation in the online survey. A local ISSA chapter also encouraged its members to participate. In addition, members of the advisory boards of two universities were asked to participate.

At the conclusion of the survey, altogether 102 security manager responses were collected. Out of these, 53 responses were collected online and 49 were paper-based. Fifty-three business manager responses (13 online, 40 paper-based) were collected. Between the security manager and business manager responses, 38 pairs were matched. The job titles of security managers are listed in Table 3.1 and the industries they represented are listed in Table 3.2.

Table 3.1 Job Titles of Respondents (Security Managers)

Job Title	Respondents
Chief Information Officer	6
Chief Information Security Officer	21
Chief Security Officer	5
IT Director	13
Security Director	4
Security Manager	23
Security Specialist (Security analyst, architect, engineer, trainer, etc.)	21
Prefer not to disclose	9
Total	**102**

Table 3.2 Industry of Respondents (Security Managers)

Industry	**Respondents**
Automotive	1
Banking and Financial Services	15
Biotechnology and Pharmaceuticals	2
Chemicals	1
Consulting	7
Consumer Goods	1
Distribution	1
Energy and Utilities	2
Health Care and Medical	6
Hospitality and Travel	2
Information Technology	7
Insurance	5
Logistics and Transportation	2
Manufacturing	5
Media and Entertainment	2
Metal and Natural Resources	1
Retail: General Merchandising	2
Retail: Specialty Merchandising	1
Telecommunications	3
Education	4
Public Sector	8
Prefer not to disclose	24
Total	**102**

3.7 Data Analyses

Partial Least Square (PLS) is used to analyze the data. We use PLS because PLS is more suitable for theory building and exploratory studies (Gefen, Straub, and Boudreau, 2000) and there are formative constructs in the model (Petter, Straub, and Rai, 2007). In particular, SmartPLS (Temme, Kreis, and Hildebrandt, 2006) was used.

Since the instrument was created for this study and no pre-existing scales were used, the first stage of data analysis was to validate the items in the instrument. Three of the six new constructs are reflective and the other three are formative.

3.7.1 Content Validity

Content validity is the extent to which items represent all of the ways that could be used to measure of the content of a given construct (Straub, Boudreau, and Gefen, 2004). Content validity is not easy to assess and is established with literature reviews and expert judges. It is highly recommended but not mandatory for IS studies (Straub et al, 2004). For this study, we examined content validity during the process of the four rounds of Q-sorts and via discussion with domain experts.

3.7.2 Construct Validity

Construct validity assesses whether the items designed for a construct really measure what they are supposed to measure. It is typically evaluated by convergent validity and discriminant validity.

3.7.2.1 Convergent Validity Test with PCA

When convergent validity is good, indicators for the same construct are more correlated with one another than with any other indicators for other constructs. For reflective constructs, indicators should be highly correlated and interchangeable. Purging of problematic indicators is recommended (Petter et al, 2007). Convergent validity can be established using factor analytic techniques such as PCA, confirmatory factor analysis, etc. (Straub et al, 2004). After cross-loading items are dropped, indicators should load cleanly on their respective constructs. In comparison, indicators for a formative construct measure different aspects of the construct and thus may not correlate with each other closely. Convergent validity of formative indicators, therefore, are established using conceptual methods such as Q-sorts (Petter et al, 2007).

Since constructs in various causal stage (independent variables, mediators, or dependent variables) by design are correlated, indicators of constructs in different causal stages could cross load or result in poor loadings for constructs that were otherwise valid. Thus, Straub et al (2004) recommend that factorial validity examines the constructs independent of the theoretical connections. In other words, it is best not to mix IVs and DVs in factoring.

Following this advice, we perform a PCA on the 24 items that are intended to measure the three independent variables: process-based governance mechanisms (PG), structural governance mechanisms (SG), and relational governance mechanisms (RG). Kaiser's criterion is used to extract all factors with a eigenvalue greater than 1. The solution is rotated orthogonally with Varimax rotation. Although six factors are extracted in the first run, the scree plot clearly (Figure 3.2) shows that in fact three factors are a more appropriate number to extract.

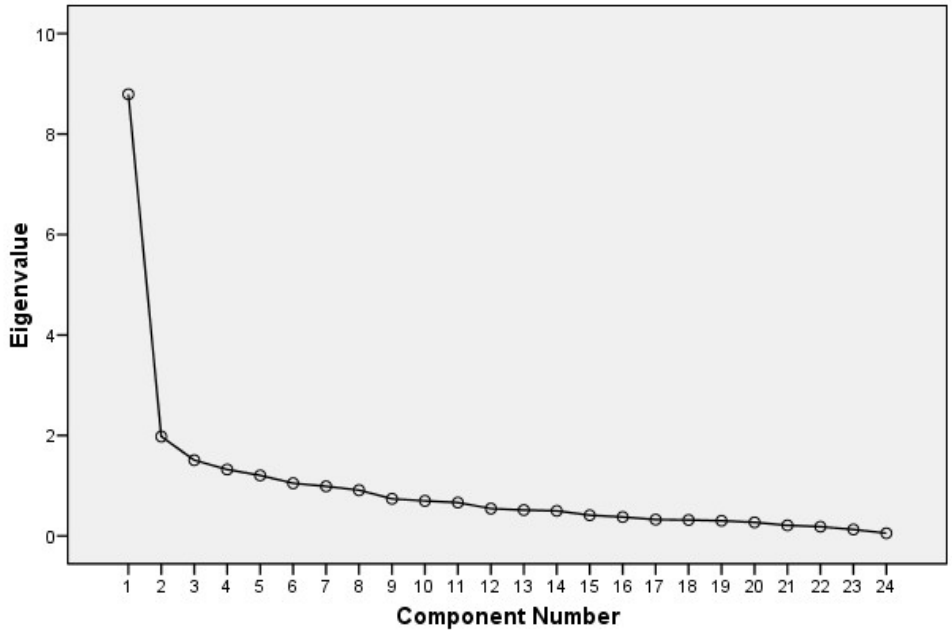


Figure 3.2 Scree Plot from First Principal Component Analysis

This is in agreement with the fact that these 24 items are designed to measure three constructs. After the items loading on multiple or unintended constructs were dropped, the final solution

retained five indicators for PG, four items for SG, and four items for RG. The loadings of the items are listed in Table 3.3.

Table 3.3 Item Loadings from Principal Component Analysis (Independent Variables)

	Factor		
	PG	SG	RG
PG1POL	.796	.076	.205
PG2STD	.834	.101	.080
PG4RKA	.642	.311	.302
PG6CHG	.658	.252	.188
PG8EAU	.707	.223	.022
SG1STR	.183	.505	.488
SG3BGT	.079	.638	.072
SG4ACA	.280	.861	.181
SG5ACB	.255	.851	.134
RG3EVT	.420	.025	.661
RG4XFT	.273	.298	.723
RG5COL	.008	.052	.797
RG6CCY	.100	.179	.859

Factors extracted with Keiser's criterion of eignevalue greater than 1.
Rotation method: Varimax.

When evaluating the loadings, for a sample size of 100, .512 is recommended (Field, 2005; Stevens, 2002). All the items retained, except SG1STR, load on their related constructs with loadings substantially higher than .512. SG1STR also loads high on RG. However, since it is an

important type of structural governance mechanisms, we retain it tentatively, pending further validation.

There are a few other statistics used to evaluate the appropriateness of the final rotated solution. Although a certain degree of multicollinearity is in fact necessary for factor analysis, excessive multicollinearity lessens the distinction between factors. The R-matrix of the final solution has a determinant of .001, signifying a sufficient but not excessive level of multicollinearity. The Kaiser-Meyer-Olkin (KMO) statistic is .808. A KMO value above .8 is considered very good and indicates a high likelihood that the factor analysis yields distinct and reliable factors. The measures of sampling adequacy (MSAs) are all above the .5 acceptable level, with many of them above .8, a level that is considered meritorious (Field, 2005; Hair, Anderson, Tatham, and Black, 1998). Table 3.4 lists the communalities and MSAs for the final solution for the independent variables.

Table 3.4 Communalities and MSA for Final Rotation (Independent Variables)

	Communalities	MSA
PG1POL	.682	.867
PG2STD	.713	.816
PG4RKA	.601	.885
PG6CHG	.531	.915
PG8EAU	.551	.862
SG1STR	.526	.887
SG3BGT	.419	.806
SG4ACA	.852	.688
SG5ACB	.808	.664
RG3EVT	.613	.824
RG4XFT	.687	.847
RG5COL	.639	.778
RG6CCY	.781	.809

The dependent variable, effectiveness of InfoSec services (ES), is a reflective construct. Another PCA is performed on the items for the endogenous variables. Again, the items demonstrate high loadings on the ES construct (See Table 3.5).

Table 3.5 Item Loadings from Principal Component Analysis (Dependent Variables)

	Component		
	GC	IA	ES
GC1WHA	.824	.066	.180
GC2WHO	.861	.062	.190
GC3PRI	.881	-.031	.211
GC4RSC	.771	.038	.299
GC5FSB	.863	.054	.275
GC6EXP	.836	.138	.069
GC7MTR	.760	-.046	.129
IA1CMP	.076	.807	.115
IA2EXP	.061	.828	.137
IA3ACT	.041	.877	.040
IA4EFT	-.002	.821	-.011
IA5QUL	.013	.843	.059
IA6RND	.034	.688	.140
ES1SRV	.403	.144	.777
ES2PTN	.259	.108	.810
ES3SUP	.282	.173	.880

For formative constructs such as goal congruence and information asymmetry (IA), high loadings for all indicators are not absolutely necessary (Petter et al, 2007). Therefore, we also retain the items for GC and IA for further validation. Thus, 29 items are retained. These items, as well as the complete wording for the items, are listed in Table 3.6. Their means and standard deviations are listed in Table 3.7.

Table 3.6 Retained Items and Complete Wording

Code	Item
Process-based Governance Mechanisms	
PG1POL	In my company, users' requirements for information security are addressed in information security policies.
PG2STD	In my company, users' requirements for information security are addressed in information security standards.
PG4RKA	In my company, risk assessment is performed before information security services are planned.
PG6CHG	In my company, proper change management procedures are followed when information security plans are updated for changes in user requirements for information security.
PG8EAU	In my company, external IS audits are performed regularly by accounting firms, contractors, etc.
Structural Governance Mechanisms	
SG1STR	In my company, the IT steering committee (or its equivalent) is effective in deciding strategic IT matters.
SG3BGT	In my company, the IT budget committee (or its equivalent) is effective in overseeing IT budget matters.
SG4ACA	In my company, the IS audit committee (or its equivalent) is effective in overseeing IS audit matters.
SG5ACB	In my company, the IS audit committee (or its equivalent) is composed of members with backgrounds in various business functions.
Relational Governance Mechanisms	
RG3EVT	My company often sponsors events where we (security organization) interact with employees in other departments.
RG4XFT	My company implements cross-functional training between us (security organization) and other departments.
RG5COL	My company physically locates our offices so that we (security organization) have maximum interaction with employees in important departments.
RG6CCY	My company Encourages us (security organization) and other departments to cc each other, when appropriate, on important decisions.

Code	Item
Goal Congruence	
GC1WHA	In my company, we (security organization) and other departments generally have consensus on What information assets to protect.
GC2WHO	In my company, we (security organization) and other departments generally have consensus on who in the security organization implements which security mechanisms.
GC3PRI	In my company, we (security organization) and other departments generally have consensus on the priorities of information security.
GC4RSC	In my company, we (security organization) and other departments generally have consensus on the allocation of resources for information security.
GC5FSB	In my company, we (security organization) and other departments generally have consensus on the feasibility of implementing information security services.
GC6EXP	In my company, we (security organization) and other departments generally have consensus on the expected results for information security.
GC7MTR	In my company, we (security organization) and other departments generally have consensus on the metrics to define the success of information security.
Information Asymmetry	
IA1CMP	In my company, we (security organization) have more information than other departments do about The precise level of our own competence in implementing information security mechanisms.
IA2EXP	In my company, we (security organization) have more information than other departments do about the precise level of our own experience in implementing information security mechanisms.
IA3ACT	In my company, we (security organization) have more information than other departments do about what we (security organization) are doing to protect information assets.
IA4EFT	In my company, we (security organization) have more information than other departments do about the amount of effort we (security organization) are exerting.
IA5QUL	In my company, we (security organization) have more information than other departments do about the quality of services we (security organization) provide to protect information assets.
IA6RND	In my company, we (security organization) have more information than other departments do about the random, external factors that may influence our effectiveness in protecting information assets.
Effectiveness of InfoSec Services	
ES1SRV	In my company, top management, in general, is satisfied with the services provided by us (security organization) to protect information assets.
ES2PTN	In my company, top management, in general, is confident that information assets are well protected.
ES3SUP	In my company, top management, in general, feels that the level of information security supports its jobs well.

Table 3.7 Descriptive Statistics

Item	Mean	Std. Deviation
PG1POL	3.88	1.163
PG2STD	3.60	1.137
PG4RKA	3.06	1.209
PG6CHG	3.43	1.231
PG8EAU	3.92	1.272
SG1STR	3.31	1.398
SG3BGT	2.90	1.592
SG4ACA	2.32	1.889
SG5ACB	2.23	1.825
RG3EVT	2.56	1.271
RG4XFT	2.61	1.204
RG5COL	2.86	1.365
RG6CCY	3.34	1.294
GC1WHA	3.51	1.174
GC2WHO	3.67	1.127
GC3PRI	3.42	1.188
GC4RSC	3.00	1.135
GC5FSB	3.16	1.132
GC6EXP	3.38	1.217
GC7MTR	2.91	1.228
IA1CMP	3.98	.832
IA2EXP	4.04	.922
IA3ACT	3.88	.915
IA4EFT	3.82	.999
IA5QUL	3.69	.931
IA6RND	3.87	.951
ES1SRV	3.75	.927
ES2PTN	3.72	.924
ES3SUP	3.62	.932

After the exploratory factor analysis, and the retaining of 16 items for PG, SG, RG, and ES, and 13 items for GC and IA, we conducted a confirmatory factor analysis using PLS to validate the convergent and discriminant validity of the items. In a PLS model, each item is designated to load on the construct that it measures. Then the measurement and structural model are estimated using the PLS algorithm. As standard in PLS analysis, bootstrap samples are then generated to estimate the significance of item loadings and path coefficients.

3.7.2.2 Convergent Validity Test with PLS

Items show convergent validity when they load with significant t-values on its construct and at least the .05 significance level is desired (Gefen and Straub, 2005). For this study, the retained items and the constructs they load on, as well as the corresponding t-values, are listed in Table 3.8. As can be deduced from the table, all these loadings are at the .001 significance level.

3.7.2.3 Discriminant Validity Test with PLS

To test the discriminant validity of the items, first we examine the item loadings on the constructs. Table 3.9 shows the loadings of each item on each of the constructs.

Table 3.8 Significance of Item Loadings

Item	Construct	Original Sample	Sample Mean	Standard Deviation	Standard Error	T Statistic
PG1POL	PG	0.7968	0.7962	0.0402	0.0402	19.8307
PG2STD	PG	0.8048	0.7921	0.0619	0.0619	13.0080
PG4RKA	PG	0.7894	0.7821	0.0532	0.0532	14.8349
PG6CHG	PG	0.7670	0.7793	0.0413	0.0413	18.5746
PG8EAU	PG	0.7144	0.7140	0.0624	0.0624	11.4572
SG1STR	SG	0.7693	0.7473	0.0566	0.0566	13.5852
SG3BGT	SG	0.5841	0.5863	0.1133	0.1133	5.1558
SG4ACA	SG	0.8939	0.8991	0.0347	0.0347	25.7700
SG5ACB	SG	0.8490	0.8550	0.0528	0.0528	16.0873
RG3EVT	RG	0.7662	0.7692	0.0616	0.0616	12.4445
RG4XFT	RG	0.8516	0.8517	0.0305	0.0305	27.9532
RG5COL	RG	0.7421	0.7411	0.0637	0.0637	11.6595
RG6CCY	RG	0.8693	0.8703	0.0215	0.0215	40.3861
GC1WHA	GC	0.8125	0.7834	0.0689	0.0689	11.7953
GC2WHO	GC	0.8478	0.8286	0.0689	0.0689	12.2964
GC3PRI	GC	0.9072	0.8785	0.0422	0.0422	21.4780
GC4RSC	GC	0.8330	0.8035	0.0659	0.0659	12.6434
GC5FSB	GC	0.9592	0.9284	0.0389	0.0389	24.6482
GC6EXP	GC	0.8088	0.8014	0.1052	0.1052	7.6880
GC7MTR	GC	0.6883	0.6829	0.0916	0.0916	7.5163
IA1CMP	IA	0.7850	0.5665	0.2634	0.2634	2.9798
IA2EXP	IA	0.7832	0.5932	0.2588	0.2588	3.0263
IA3ACT	IA	0.6715	0.4712	0.2691	0.2691	2.4958
IA4EFT	IA	0.3876	0.3528	0.2568	0.2568	1.5093
IA5QUL	IA	0.6450	0.4617	0.2672	0.2672	2.4140
IA6RND	IA	0.8268	0.5838	0.2906	0.2906	2.8454
ES1SRV	ES	0.9102	0.9123	0.0187	0.0187	48.5781
ES2PTN	ES	0.8301	0.8284	0.0640	0.0640	12.9747
ES3SUP	ES	0.9432	0.9427	0.0129	0.0129	73.0782

Table 3.9 Item Loadings

	PG	SG	RG	GC	IA	ES
PG1POL	0.7968	0.3707	0.3858	0.4262	0.1078	0.3947
PG2STD	0.8048	0.3448	0.2985	0.3365	0.1960	0.2592
PG4RKA	0.7894	0.5230	0.4665	0.4609	0.1776	0.3875
PG6CHG	0.7670	0.4522	0.3627	0.4821	0.0712	0.4698
PG8EAU	0.7144	0.3662	0.2561	0.3099	0.1119	0.2904
SG1STR	0.4272	0.7693	0.5100	0.5798	-0.0097	0.4337
SG3BGT	0.2622	0.5841	0.2184	0.2561	0.0164	0.1798
SG4ACA	0.4972	0.8939	0.4025	0.4611	0.1054	0.3700
SG5ACB	0.4572	0.8490	0.3696	0.4106	0.1256	0.3444
RG3EVT	0.4771	0.3422	0.7662	0.4514	0.2494	0.2923
RG4XFT	0.4618	0.5215	0.8516	0.6240	0.1927	0.3741
RG5COL	0.2325	0.2943	0.7421	0.4888	0.1683	0.3483
RG6CCY	0.3433	0.4504	0.8693	0.6319	0.2218	0.4125
GC1WHA	0.4286	0.4245	0.5867	0.8125	0.1845	0.4589
GC2WHO	0.4631	0.5050	0.5726	0.8478	0.0983	0.4821
GC3PRI	0.4533	0.5505	0.6372	0.9072	0.0632	0.5041
GC4RSC	0.4187	0.4908	0.5181	0.8330	0.1573	0.5250
GC5FSB	0.5058	0.5467	0.6567	0.9592	0.1521	0.5535
GC6EXP	0.4898	0.4394	0.5895	0.8088	0.1905	0.4256
GC7MTR	0.4081	0.3604	0.4724	0.6883	0.0475	0.3953
IA1CMP	0.1036	0.0116	0.1919	0.1461	0.7850	0.2400
IA2EXP	0.1285	0.1100	0.1944	0.1320	0.7832	0.2663
IA3ACT	0.1306	-0.0280	0.1258	0.0824	0.6715	0.2083
IA4EFT	0.1082	0.0719	0.0861	0.0485	0.3876	0.1313
IA5QUL	0.1218	0.0115	0.1422	0.0723	0.6450	0.1981
IA6RND	0.1845	0.1033	0.2240	0.1040	0.8268	0.2421
ES1SRV	0.4392	0.4128	0.4260	0.5613	0.3316	0.9102
ES2PTN	0.3706	0.3754	0.3056	0.4695	0.1873	0.8301
ES3SUP	0.4631	0.4149	0.4506	0.4976	0.2864	0.9432

As Gefen and Straub (2005) point out, it is common to have much higher loadings in PLS than in a PCA; a loading above .7 is considered high. As Table 3.9 shows, each indicator of PG, SG, RG, and ES loads much higher on the construct than on any other constructs. This can be verified by either examining horizontally an item's loadings across all constructs or, vertically, loadings on a construct across all items. The same can be observed in our results from the PCA (Tables 3.3 and 3.5).

Also, SG1STR's loading on SG is at least "an order of magnitude" (Gefen and Straub, 2005, p. 93) higher than its loadings on other constructs. Therefore, we decide to retain this item.

Analysis of average variance extracted (AVE) is the next step in testing discriminant validity. A construct with good discriminant validity should have an AVE whose square root is above .50 and much higher than any correlation among any pairs of constructs (Chin, 1998; Gefen and Straub, 2005). The construct AVEs are listed in Table 3.10 and their correlation coefficients are shown in Table 3.11. As can be deduced from the tables, all of the four constructs meet the criteria for discriminant validity. In other words, the correlation between each of the constructs with its measurement items is larger than its correlation with other constructs. Therefore, all the constructs demonstrate discriminant validity.

Table 3.10 Average Variance Extracted

Construct	AVE	Square Root
PG	0.6008	0.7751
SG	0.6132	0.7831
RG	0.6547	0.8091
ES	0.8024	0.8958

Table 3.11 Correlations between Constructs

	PG	SG	RG	GC	IA	ES
PG	.					
SG	0.5396	.				
RG	0.4679	0.5065	.			
GC	0.5313	0.5755	0.6867	.		
IA	0.1701	0.0739	0.2555	0.1508	.	
ES	0.4757	0.4484	0.4443	0.5718	0.3055	.

3.7.2.4 Discriminant Validity Test for Formative Constructs

To validate formative constructs, statistics such as reliability and AVE are not applicable (Chin, 1998; Liang, Saraf, Hu, and Xue, 2007). However, an item that contributes to its construct should have significant path weights, and these should be examined to evaluate the validity of those items. As can be seen in Table 3.8, for the two formative constructs, GC and IA, all but one path is insignificant (IA4EFT). The items therefore contribute significantly to form the constructs of GC and IA.

Although IA4EFT has a low *t*-value, we decided to retain it because items for formative constructs measure different aspects of a construct and particular caution should be exercised when dropping formative indicators (Petter et al, 2007). Conceptually this item makes good sense and did not raise any concern during Q-sorts. Thus we decide not to drop the item.

3.7.3 Reliability

It is difficult to assess reliability for formative constructs, especially with PLS. For the reflective constructs, reliability of the scale was verified, i.e., the correlation between any two items should be positive if they measure the same construct (Petter et al, 2007). Next, we evaluate the reliability of those items for the reflective constructs. Table 3.12 displays the Cronbach's alphas for reflective constructs and they are all above 0.8 expect for SG, which is close to 0.8.

Table 3.12 Reliability

Construct	Alpha
PG	0.8346
SG	0.7867
RG	0.8230
ES	0.8762

3.7.4 Hypothesis Testing

The relationships between the governance mechanisms, goal congruence, information asymmetry, and effectiveness of information security services are shown in Figure 3.3. In total, the R^2 of .376 indicates that the model explains a large amount of variance in the effectiveness of InfoSec services.

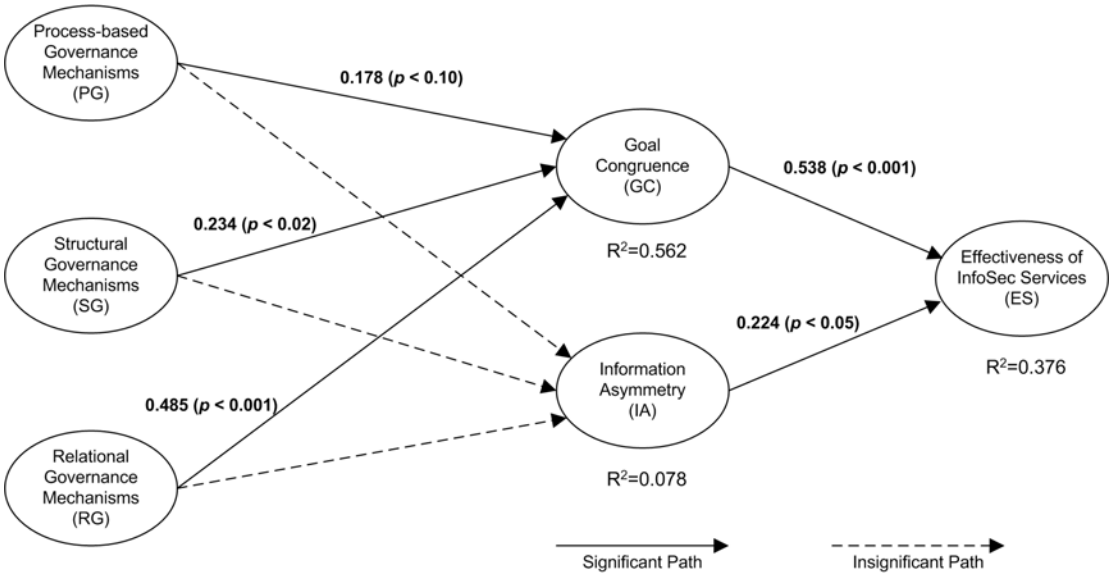


Figure 3.3 Structural Model

The path coefficients for the relationships between constructs are displayed in Figure 3.4. The significance (*t* values) for those coefficients is shown in Figure 3.5.

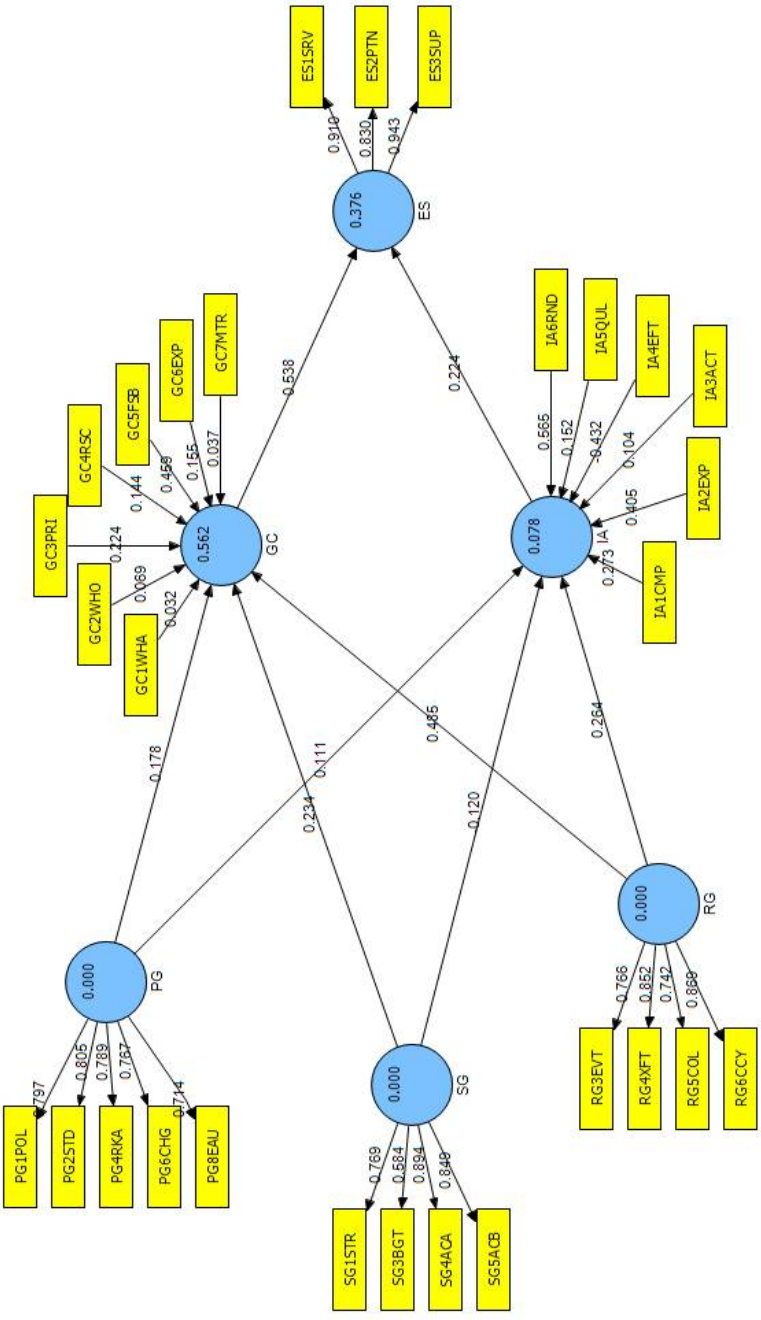


Figure 3.4 Path Coefficients (SmartPLS Output)

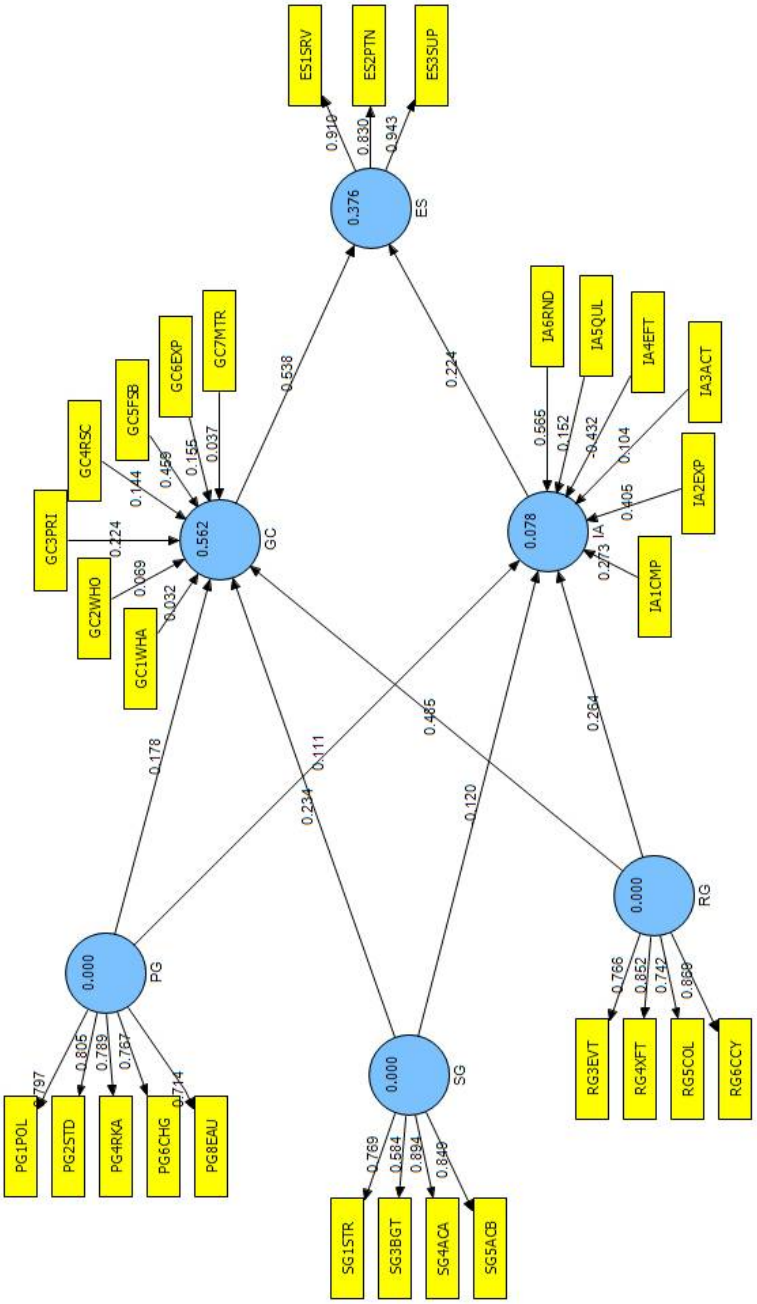


Figure 3.5 Path Significance (SmartPLS Output)

The structural model shows that all three types of governance mechanisms are positively related to goal congruence between IT and business. SG and RG are strongly related to GC at .02 and .001 level, respectively, while PG is related to GC at the .10 level. GC, in turn, is strongly related to ES at the .001 level. Therefore, H1a, H2a, H3a, and H4 are supported.

Interesting findings results surface when information asymmetry (IA) is involved. The relationships between IA and each of the three types of governance mechanisms are all insignificant. Therefore, H1b, H2b, and H3b are not supported.

Since the indicators of IA are self-report measures, a suspicion is that these may be due to the lack of objectivity of what the security managers reported. Thus, we pair up the answers to GC and IA items by the security manager and the business manager from the same organization. Since all together only 38 pairs were found, the small sample size prevent us from running another equivalent model by using the security manager answers to the governance mechanisms items and the business manager answers to the GC, IA, and ES items. However, a series of *t*-tests on the two groups' answers to GC and IA items yield some insights regarding these insignificant relationships. Table 3.13 shows the results of the *t*-tests.

Table 3.13 Security and Business Managers Answers to GC and IA Questions

Item	Security Mean	Business Mean	Sig.	Item	Security Mean	Business Mean	Sig.
GC1WHA	3.97	3.87	.712	IA1CMP	4.18	3.79	.061
GC2WHO	4.11	4.11	1.000	IA2EXP	4.24	3.82	.068
GC3PRI	3.92	3.87	.839	IA3ACT	4.13	3.68	.070
GC4RSC	3.55	3.61	.840	IA4EFT	4.13	3.50	.009
GC5FSB	3.68	3.53	.566	IA5QUL	4.08	3.34	.008
GC6EXP	3.92	3.66	.385	IA6RND	4.26	3.55	.010
GC7MTR	3.16	3.05	.740				

* Scale was 5-point Likert scale ranging from Strongly Disagree (1) to Strong Agree (5).

These tests reveal that there are obviously no differences between a security manager's and a business manager's answers to questions about GC. In other words, the security manager and business manager are very similar in their estimates of goal congruence in their organization. In contrast, when it comes to their answers to the IA questions, the significance levels of the *t*-tests are between .008 and .01. Therefore, there is a fairly high likelihood that the two manager groups differ in their estimates of information asymmetry in their organizations. More specifically, security managers tend to see a larger asymmetry than the business managers do.

Another surprising finding we observe in the structural model is the relationship between IA and ES. There is a significant positive relationship between the two (b = .224, $p < .05$). Since the IA questions are not reverse coded, a higher value means that IT has more information than business.

Therefore, a larger information asymmetry is positively related to more effective InfoSec services. The sign of relationship thus is the opposite of what H5 hypothesizes.

3.8 Discussion

This study creates and empirically tests a set of measures to gauge a company's IT governance mechanisms, goal congruence, information asymmetry, and InfoSec service effectiveness. Our data analyses first validate the psychometric properties of the instrument. Analyses of the results collected from security and business managers reveal both expected and surprising but interesting findings.

First, IT governance mechanisms that are implemented as IT process control techniques, organizational roles and structures, and relationship building do enhance the goal congruence between IT and business. In terms of process-based mechanisms, the use of security policies and standards formalizes and institutes the thought process and practical exercise needed to capture users' business and functional requirements for information security. These requirements help to guide IT in its assessment of the users' business processes, information assets, and the risks these processes and assets may entail. If proper risk assessment is performed before InfoSec services are planned and implemented, the chances are IT will be serving the users' business objectives more closely and effectively. Continuous effects can be guaranteed by proper implementation procedure such as change management and audit of results. Goal congruence also can be boosted via the use of organizational structures such as IT steering committee, IT budget

committee, IS audit committee, etc. The IT steering committee is the most tried and true venue by which IT and non-IT units voice and weigh their IT-related, including InfoSec-related concerns and priorities. The IT budget committee can put real teeth into agreed-upon IT priorities. The processes by which this committee works makes sure that those priorities are not the results of whims of either IT or business. As far as InfoSec is concerned, committees such as IS audit committee constitute a feedback channel through which IT and business can be on the same page with regard to where IT stands in protecting users' information assets and supporting their business processes. This should prompt IT to anticipate and fulfill user goals for information security.

The formal processes and organization structures can never replace the informal "lateral organizations" and informal relationships that users build at work to communicate their goals and get their job done. Relational governance mechanisms reduce the randomness in those informal structures and relationships and guide them toward congruent goals. Altogether, the process-based, structural, and relational mechanisms facilitate goal congruence between IT and business. Clear understanding of user goals in turn can help IT plan and allocate their priorities and activities so that it can better serve the users. A direct result from such efforts is that users see more effective InfoSec services, as judged by the level of protection, business support, and customer service provided.

Our research findings strongly support this chain of reasoning. We find significant positive relationships between each of the three types of mechanisms and goal congruence, and between goal congruence and InfoSec service effectiveness.

Our findings, however, do not support relationships between the governance mechanisms and information asymmetry. The asymmetry occurs because business users cannot effortlessly or costlessly gain access to IT information regarding the InfoSec services. Therefore, the asymmetry theoretically allows IT to act opportunistically and hurt users. This rather negative view of information asymmetry is rooted in agency theory. It follows that governance mechanisms allow users easier access to information on IT competence and actions and, as the result, IT will not "shirk" and put in more efforts for the betterment of the users (i.e., the principal). For instance, IS audits done by auditors and impartial audit outcomes guaranteed by a properly structured audit committee represent a great source of information to reduce asymmetry. Informal relationships theoretically also enable users to gain insight into what IT does for InfoSec.

Our analyses, however, show that information asymmetry actually is not related to the governance mechanisms. A possible explanation may be that the profession of InfoSec is such that the barrier to acquisition of even shadow knowledge of InfoSec is difficult to surmount. Contributing to the reinforcement of such a barrier may be the popular press' dramatization of hacking activities and the common, simplistic practice of equating InfoSec to cryptography. As the result, information asymmetry is not readily amenable to alleviation through governance

mechanisms. For instance, regardless of what informal relationships that the company fosters through relational governance mechanisms, a regular user may not have the motivation for more informal InfoSec education than the security manager's occasional elevator speeches. It may be much less enticing for a CEO to leaf through an IS audit report than to peruse a financial audit report, which she may feel less daunting to start with.

In fact, the lack of expertise typically is the reason for a principal to delegate a task to an agent. In the case of InfoSec, business leaders may view the information asymmetry between IT and users a legitimate existence. This possibly explains the unexpected finding that information asymmetry is positively related to InfoSec service effectiveness. Business leaders entrust IT with InfoSec tasks and may view widening information asymmetry as a sign of IT working hard on InfoSec. Indeed, to be more effective in providing security, IT tends to implement more sophisticated protection measures and build a wealth of information that is harder to comprehend by laypersons. Even if a layperson tries to obtain information on what IT is doing, advances in technologies and attack and protection measures can easily outpace the asymmetry reduction process. Therefore, it is likely that more effective protection comes at the cost of higher information asymmetry, especially when the business leaders do not view it as something negative that needs to be tamed.

3.9 Theoretical Contribution

Our study contributes to both the IT governance and agency theory literature as discussed below.

3.9.1 IT Governance

A major contribution of this study is to create an instrument to measure various aspects of IT governance. To date, much of the discussion regarding IT governance mechanisms (e.g., Peterson, 2004a, 2004b; Van Grembergen et al, 2004) has been conceptual. Weill and Ross' study (Weill and Ross, 2004) is empirical but the focus is on the organizing logic of decision rights. Their attention is primarily on the structural mechanisms. This study marks an early effort to empirically measure IT governance practices. Given the purpose of this study, and considering that IT governance is a far-reaching concept, the instrument measures those governance mechanisms that are related to InfoSec. Using survey data, the instrument was validated and shown to have satisfactory construct validity. Future studies thus can take advantage of this set of scales for empirical measurement of security governance.

An important utility of IT governance is to ensure the alignment of IT and business goals (Peak and Guynes, 2003; Weill and Ross, 2004). This study indeed supports this hypothesis by showing that IT governance mechanisms enhances the goal congruence between IT and business, at least as far as InfoSec services are concerned. While there are previous efforts like Luftman (2000) to measure the alignment between IT and business, this study makes a contribution by coming up with and testing a much more parsimonious set of measures.

3.9.2 Agency Theory

Baiman (1982) suggests that an approach to empirical validation of the agency theory is to concentrate less on deriving optimal compensation contracts because its discussion often is based on assumptions and lacks real-life counterparts. Rather, more fruitful research should concentrate more on more easily observed aspects of the firm.

Like Baiman, Nilakant and Rao (1994) suggest that there seems to be a saturation in studies on contract design. Thus, they recommend studying reduction of agency problems through organizational design, trust, and collaboration. In this regard, Nilakan and Rao stress structural and cultural mechanisms. Both are examined in this study, with relational mechanisms being equivalent to cultural mechanisms.

Thus, this study contributes to agency theory in performing a much needed test from a concrete, organizational perspective. Instead of simplistically using compensation structure as the cure-all solution to agency problems, it peeks into the richness of the variety of governance mechanisms that are at the tips of organization for solving their agency problems.

Although goal congruence and information asymmetry are the standard-issue elements in most, if not all, discourse on agency theory, they are bypassed in empirical studies. The hypothesized causal link typically goes straight from whatever causal factors in focus to some sort of performance measure. This study thus makes an important contribution by explicating this black box of causal relationship and studying the role of these two factors explicitly.

More specifically, information asymmetry is generally viewed in a negative light because it allows the agent to hide information away from the principal and be able to act opportunistically (Baiman, 1990; Pavlou, Liang, and Xue, 2007). Thus, it should be reduced (Baiman, 1990). By looking at information asymmetry specifically, this study finds at least one situation in which information asymmetry may not be all bad and possibly even is indicative of the effectiveness of the agent's actions. Another contribution is that we create a set of theory-based items to measure information asymmetry in the InfoSec context and validate it empirically.

Thus, this study contributes to the IT governance and agency theory literature both by taking a closer look at some pivotal constructs and by creating and validating parsimonious sets of scales to measure key constructs. These contributions are tabulated in Table 3.14.

Table 3.14 Theoretical Contribution

Literature	Contribution
IT Governance	Studies governance from the perspective of rich sets of mechanisms.
	Creates and validates scales for measuring governance practices in the InfoSec context. Future empirical studies of information security governance can take advantage of the instrument.
	Provides a parsimonious set of scale to assess goal alignment between business and IT in the InfoSec context.
Agency Theory	Explicates the black box of causal relationships between agency problem control measures and effectiveness.
	Validates the role of goal congruence in controlling agency problems. Brings attention to reconsidering the role of information asymmetry.
	Provides a set of scales to measure information asymmetry in the InfoSec context.

3.10 Limitations and Directions for Future Research

This study is an early effort to empirically measure and test governance practices from the perspective of governance mechanisms. Although our validation process and results suggest that the measurement scales very likely have desirable psychometric properties, it is early to call that conclusive. Also, the external validity of this study can be limited. This is for two reasons. First, the scope of this study is intentionally limited to information security and more specifically, with relation to understanding and fulfilling users' InfoSec requirements. While this makes the scope of study manageable and measurement scales usable, it is unclear whether the findings can be extended to other IT contexts. Second, given various resource limitations, we are able to collect

responses only from a relatively small set of security managers and business managers. Researchers of future studies may want to try different channels to collect data from a larger set of security managers to validate the findings in this study.

Another type of replication that is suitable for future studies is to design sets of similar measures for other IT contexts and examine the usability of those instruments in those contexts. If the instruments demonstrate good psychometric properties and practical usability, it bolsters the value of our scales. A general set of scales to measure IT governance practices across various IT contexts may even be possible. The same can be said of the items we create to measure goal congruence and information asymmetry.

It definitively will be interesting for researchers to further investigate the role of information asymmetry in agency relationships. Whereas the importance of goal congruence is fairly straightforward, the role played by information asymmetry appears to be more complex than has been postulated by theorists and researchers. It may be because the asymmetry is the reason for agency relationships to begin with. Usually, the asymmetry in specialized knowledge gives rise to the agency theory. However, at least in theory, it also causes further asymmetry in terms of knowledge about the task performance. We try to differentiate between these two types of asymmetry and term them expertise-based asymmetry and performance-based asymmetry and design our scales around the latter. We believe that the expertise-based asymmetry is what gives legitimacy to agency relationships and thus not what is at play in agency problems. What we try to capture is the performance-based asymmetry, which is the "bad" asymmetry that needs to be

reduced. However, our findings seem to suggest that even performance-based asymmetry may be viewed by the principal as legitimate. Future studies may investigate in more depth the differences in expertise-based asymmetry and performance-based asymmetry and their respective roles in agency relationships and problems. It is possible that the principal's acceptance of the asymmetry can depend on the context. For relatively simple tasks such as retail sales or customer service, the principal (the mangers) may not want to allow the agent (the cashier or customer service representative) much privilege to the service information. For more complex tasks such as building security defenses for a data center, reduction in asymmetry may not mean as much to the principal. Future research in this direction may yield interesting findings that enrich our understanding of agency theory.

3.11 Conclusion

This study addresses a timely and important issue in information security management that is receiving attention recently – the proper governance of the security function. Governance is the key to ensuring that IT provides InfoSec services in such a way that information assets are sound and safe and business strategies and objectives are well served by those services. With this study we delve into the various governance mechanisms and examine their efficacy on governance by adopting an agency theory perspective. We hypothesize that the mechanisms have their effects through improving goal congruence and reducing information asymmetry between IT and business. We conduct a survey to collect responses from security managers and business managers to test our hypotheses. The analyses of survey data partially support our hypotheses

but bring up intriguing questions about the role of information symmetry in the agency relationships in the InfoSec context. We believe it is a research direction for future studies in information security governance and agency theory. Another direction that is worth future research efforts is the measurement of IT governance practices. To conduct this study we create and validate a set of measure scales for the three categories of governance mechanisms that have been conceptually defined but untested in literature. With researchers' interest in IT and security governance on the rise, parsimonious, usable, and psychometrically sound scales of IT governance practices are indispensable for empirical studies in that area.

3.12 Chapter 3 List of References

1. Adams, M. B. (1994). Agency theory and the internal audit. *Managerial Auditing Journal,* 9(8), 8-12.

2. Baiman, S. (1982). Agency research in managerial accounting: A survey. *Journal of Accounting Literature,* 1, 154-213.

3. Baiman, S. (1990). Agency research in managerial accounting: A second look. *Accounting, Organizations and Society,* 15(4), 341-371.

4. BSA, & ISSA. (2004). *BSA-ISSA Information Security Study Online Survey of ISSA Members*: Business Software Alliance and Information Systems Security Association.

5. Chin, W. W. (1998). The partial least square approach for structural equation modeling. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research* (pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates.

6. Clark, T. (1993). The market provision of management services, information asymmetries and service quality - Some market solutions: An empirical example. *British Journal of Management,* 4, 235-251.

7. De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal, 2004,* 1-7.

8. Dillman, D. A. (2000). *Mail and Internet Surveys: The Tailored Design Method.* New York, NY: Wiley.

9. Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review,* 14(1), 57-74.

10. Field, A. (2005). *Discovering Statistics Using SPSS* (2nd ed.). Thousand Oaks, CA: Sage Publications.

11. Galbraith, J. R. (1993). *Competing with Flexible Lateral Organizations* (2nd ed.). Reading, MA: Addison-Wesley.

12. Gallouj, C. (1997). Asymmetry of information and the service relationship: Selection and evaluation of the service provider. *International Journal of Service Industry Management,* 8(1), 42-64.

13. Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the AIS,* 16, 91-109.

14. Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of AIS,* 7(7), 1-78.

15. Gentile, M., Collette, R., & August, T. (2006). *The CISO Handbook, A Practical Guide to Securing Your Company*. Boca Raton, FL: Auerbach Publications.

16. Gopal, A., Krishnan, M. S., Mukhopadhyay, T., & Goldenson, D. R. (2002). Measurement programs in software development: Determinants of success. *IEEE Transactions on Software Engineering*, 28(9), 863-875.

17. Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM,* 49(1), 121-125.

18. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

19. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *2006 CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

20. Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). *NIST Special Publication 800-35: Guide to Information Technology Security Services*. Washington, D.C.: National Institute of Standards and Technology.

21. Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis* (5th ed.). Upper Saddle River, NJ: Prentice-Hall.

22. Indjejikian, R. J. (1999). Performance evaluation and compensation research: An agency perspective. *Accounting Horizons,* 13(2), 147-157.

23. ITGI. (2003). *Board Briefing on IT Governance* (2nd ed.). Rolling Meadows, IL: ITGI.

24. ITGI. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2nd ed.). Rolling Meadows, IL: IT Governance Institute.

25. ITSMF. (2005). *Foundations of IT Service Management Based on ITIL*. Hogeweg, The Netherlands: Van Haren Publishing.

26. Jap, S. D. (1999). Pie-expansion efforts: Collaboration processes in buyer-supplier relationships. *Journal of Marketing Research,* 36(4), 461-475.

27. Jap, S. D., & Anderson, E. (2003). Safeguarding interorganizational performance and continuity under *ex post* opportunism. *Management Science,* 49(12), 1684-1701.

28. Jensen, M. C., & Murphy, K. (1990). Performance pay and top-management incentives. *Journal of Political Economy*, 98, 225-284.

29. Jordan, E., & Silcock, L. (2005). *Beating IT Risks*. West Sussex, UK: John Wiley & Sons.

30. Kairab, S. (2005). *A Practical Guide to Security Assessments*. Boca Raton, FL: Auerbach Publications.

31. Kotulic, A. G., & Clark, J. G. (2003). Why there aren't more information security research studies. *Information & Management,* 41, 597-607.

32. Lahti, C. B., & Peterson, R. (2005). *Sarbanes-Oxley IT Compliance Using CobiT and Open Source Tools*. Rockland, MA: Syngress Publishing, Inc.

33. Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly,* 31(1), 59-87.

34. Luftman, J. (2000). Assessing business-IT alignment maturity. *Communication of the AIS,* 4(14), 1-50.

35. Maiwald, E., & Sieglein, W. (2002). *Security Planning and Disaster Recovery*. Berkeley, CA: McGraw-Hill/Osborne.

36. Mangione, T. W. (1995). *Mail Surveys: Improving the Quality*. Thousand Oaks, CA: Sage Publications.

37. McKenna, B. (2002). Managed security services - New economy relic or wave of the future. *Computers & Security,* 21(7), 613-616.

38. Mills, P. K. (1990). On the quality of services in encounters: An agency perspective. *Journal of Business Research,* 20, 31-41.

39. Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research,* 2(3), 192-222.

40. Morgan, A. G., & Poulsen, A. B. (2001). Linking pay to performance - Compensation proposals in the S&P 500. *Journal of Financial Economics,* 62, 489-523.

41. Neely, A., & Wilson, J. (1992). Measuring product goal congruence: An exploratory case study. *International Journal of Operations & Production Management,* 12(4), 45-52.

42. Newman, A., & Scholtz, T. (2003). Can security investments show ROI? *Optimize, October 2003,* 25-28.

43. Nilakant, V., & Rao, H. (1994). Agency theory and uncertainty in organizations: An evaluation. *Organization Studies,* 15(5), 649-672.

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

45. Peak, D., & Guynes, C. S. (2003). Improving information quality through IT alignment planning: A case study. *Information Systems Management,* 20(4), 22-29.

46. Peterson, R. R. (2004a). Crafting information technology governance. *Information Systems Management*, 21(4), 7-22.

47. Peterson, R. R. (2004b). Integration strategies and tactics for information technology governance. In W. V. Grembergen (Ed.), *Strategies for Information Technology Governance* (pp. 37-80). Hershey, PA: Idea Group Publishing.

48. Peterson, R. R., O'Callaghan, R., & Ribbers, P. M. A. (2000). Information technology governance by design. *Proceedings of the Twenty-first International Conference on Information Systems*, Brisbane, Australia, December 10-13, 2000. 435-452.

49. Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4), 623-656.

50. Pitt, L. F., Watson, R. T., & Kavan, C. B. (1995). Service quality: A measure of information systems effectiveness. *MIS Quarterly,* 19(2), 173-187.

51. Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security,* 23, 638-646.

52. Purser, S. A. (2004). Improving the ROI of the security management process. *Computers & Security,* 23, 542-546.

53. Rittinghouse, J. W., & Hancock, W. M. (2003). *Cybersecurity Operations Handbook*. Burlington, MA: Digital Press.

54. Sambamurthy, V., & Zmud, R. W. (2000). The organizing logic for an enterprise's IT activities in the digital era - A prognosis of practice and a call for research. *Information Systems Research,* 11(2), 105-114.

55. Schweitzer, J. A. (1987). *Computers, Business, and Security: The New Role for Security*. Stoneham, MA: Butterworth Publishers.

56. Sivo, S. A., Saunders, C. S., Chang, Q., & Jiang, J. J. (2006). How low should you go? Low response rates and the validity of inference in IS questionnaire research. *Journal of Association for Information Systems,* 7(6), 351-414.

57. Snedaker, S. (2006). *IT Security Project Management Handbook*. Rockland, MA: Syngress.

58. Stevens, J. P. (2002). *Applied Multivariate Statistics for the Social Sciences* (4th ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

59. Straub, D. W. (1988). Organizational structuring of the computer security function. *Computers & Security,* 7(2), 185-195.

60. Straub, D. W., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the AIS,* 13(24), 380-427.

61. Temme, D., Kreis, H., & Hildebrandt, L. (2006). *PLS path modeling - A software review,* Humboldt University working paper.

62. Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structure, process and relational mechanism for IT governance. In W. V. Grembergen (Ed.), *Strategies for Information Technology Governance* (pp. 1-36). Hershey, PA: Idea Group Publishing.

63. Von Solms, S. H. (2005). Information security governance - Compliance management vs operational management. *Computers & Security,* 24, 443-447.

64. Warkentin, M., & Johnston, A. C. (2006a). IT Governance and Organizational Design for Security Management. In D. Straub, S. Goodman & R. Baskerville (Eds.), *Information Security Policies and Practices*. Armonk, NY USA: M.E. Sharpe.

65. Warkentin, M., & Johnston, A. C. (2006b). IT security governance and centralized security controls. In M. Warkentin & R. Vaughn (Eds.), *Enterprise Information Systems Assurance and System Security*. Hershey, PA: Idea Group Publishing.

66. Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA: Harvard Business School Press.

67. Wickramasinghe, N., & Ginzberg, M. J. (2001). Integrating knowledge workers and the organization: The role of IT. *International Journal of Health Care Quality Assurance,* 14(6), 245-253.

68. Williams, P. (2007). Executive and board roles in information security. *Network Security, 2007,* 11-14.

69. Yermack, D. (2004). Remuneration, retention, adn reputation incentives for outside directors. *Journal of Finance,* 59(5), 2281-2308.

APPENDIX A: GLOSSARY

Information security (InfoSec) The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

Confidentiality The absence of unauthorized access, disclosure, and use of information.

Integrity Information is trustworthy and reliable because it has not been altered or corrupted by unauthorized users or computer processes

Availability The authorized users' ability to have timely and reliable access to information assets

IT governance The organizational capacity to ensure that IT sustains and extends the organization's strategy. It as the responsibility of the board of directors and executive management.

Process-based governance mechanisms IT management techniques that ensure that daily behaviors are consistent with IT policies and that all stakeholders are involved in the effective management and use of IT.

Structural governance mechanisms Organizational units and roles that are instituted to properly locate decision-making responsibilities, to promote horizontal connection between IT and business functions.

Relational governance mechanisms Organizational practices that encourage voluntary two-way communication and collaboration between business and IT

Goal congruence The extent to which the relative importance of key performance criteria, including the achievability of goals, are understood between/among parties.

Information asymmetry The situation in which the agent has private information to which the principal cannot costlessly gain access.

Effectiveness of InfoSec Services The extent to which the services are delivered successfully, in terms of business impact, service delivery, and the efficacy of implementation.

Adverse selection An agency problem in which the agent exerts the inappropriate type of effort. In this situation, the principal is unable to determine the agent's qualifications and abilities and whether the agent's decisions and actions are in the principal's best interest.

Moral hazard An agency problem in which the agent exercises inadequate effort. In this situation, the principal is unable to verify the quantity and quality of the agent's efforts.

Control Objectives for Information and related Technology (CobiT) An IT governance tool created by IT Governance Institute (ITGI). CobiT is a process-based governance framework that covers the entire life cycle of IT systems.

Information Technology Infrastructure Library (ITIL) A set of publications developed and endorsed by IT Service Management Forum (ITSMF) that describe the best practices in IT processes. It has a strong focus on IT service delivery and management.

Code of Practice for Information Security Management (ISO/IEC 17799:2005) An international standard governing information security management. It provides a series of systematic recommendations and best practices for implementing and managing information security program.

APPENDIX B: IRB DOCUMENTS

University of Central Florida

Office of Research & Commercialization

March 30, 2007

Yu Wu
c/o Dr. Carol Saunders
University of Central Florida
Department of Management Information Systems
BA 325A
Orlando, FL 32816

Dear Mr. Wu:

The University of Central Florida's Institutional Review Board (IRB) received your protocol IRB #07-4307 entitled, "Effects of IT Governance on Information Security Service Quality." The IRB Chair reviewed the study on 3/30/2007 and did not have any concerns with the proposed project. The Chair has indicated that under federal regulations (Category #2, research involving the use of educational tests, survey or interview procedures, or the observation of public behavior, so long as confidentiality is maintained) this research is **exempt** from further review by our IRB, so an approval is not applicable and a renewal within one year is not required.

Please accept our best wishes for the success of your endeavors. Should you have any questions, please do not hesitate to call me at 407-823-2901.

Cordially,

Joanne Muratori

Joanne Muratori
(FWA00000351 Exp. 5/13/07, IRB00001138)

Copies: IRB File
Carol Saunders, Ph.D.

JM:jm

THE UNIVERSITY OF CENTRAL FLORIDA

INSTITUTIONAL REVIEW BOARD (IRB)

IRB Committee Approval Form

#07-4307

PRINCIPAL INVESTIGATOR(S): Yu Wu
(Supervisor – Carol Saunders, Ph.D.)

PROJECT TITLE: Effects of IT Governance on Information Security Service Quality

[X] New project submission [ ] Resubmission of lapsed project #
[ ] Continuing review of lapsed project # [ ] Continuing review of #
[ ] Study expires [ ] Initial submission was approved by expedited review
[ ] Initial submission was approved by full board review but continuing review can be expedited
[ ] Suspension of enrollment email sent to PI, entered on spreadsheet, administration notified _____

Chair
[ ] Expedited Approval

Dated: _____
Cite how qualifies for expedited review:
minimal risk and _____

[X] Exempt

Dated: 3/30/07
Cite how qualifies for exempt status:
minimal risk and #2

[ ] Expiration Date: _____

IRB Reviewers:

Signed: _____
Dr. Tracy Dietz, Chair

Signed: _____
Dr. Craig Van Slyke, Vice-Chair

Signed: _____
Dr. Sophia Dziegielewski, Vice-Chair

Complete reverse side of expedited or exempt form
[ ] Waiver of documentation of consent approved
[ ] Waiver of consent approved
[ ] Waiver of HIPAA Authorization approved

NOTES FROM IRB CHAIR (IF APPLICABLE): _____

07-4307

UCF IRB Protocol Submission Form

☑ Initial ☐ Resubmission of IRB #_____

Please type this form using the Microsoft Word document. Expand as needed. Allow a minimum of 2-3 weeks for the approval process. A letter of approval will be mailed to you once approved. Information on this form must match information on the grant application, dissertation or thesis, consent forms or letters, and flyers for recruitment. **There are no deadlines for submission of minimal risk studies as they are reviewed at least weekly.** If it is deemed by the IRB that the study involves greater than minimal risk or extenuating factors, the complete IRB packet must be submitted by the 1st business day of the month for consideration at that monthly IRB meeting. At title note if investigator is Student, Master's Candidate or Doctoral Candidate.

1. **Title of Protocol:** Effects of IT governance on information security service quality

2. **Principal Investigator:** [List the faculty supervisor as both the Principal Investigator and the faculty supervisor if student(s) or staff members are doing the research. List student(s) as co-investigator(s).]

Signature: Carol Saunders
Name: Carol Saunders
Mr./Ms./Mrs./Dr. (choose one) Dr.
Employee ID or Student PID #: C1172150
Degree: Ph.D.
Title: Professor of MIS
Department: Management Information Systems
College: Business Administration
E-Mail: csaunders@bus.ucf.edu
Telephone: (407) 823-6392
Facsimile: (407) 823-2389
Home Telephone: (407) 671-1667

Co-Investigator(s):

Signature:
Name: Yu Wu
Mr./Ms./Mrs./Dr. (choose one) Mr.
Employee ID or Student PID #: Y1050441
Degree: Master of Science
Title: Ph.D. Candidate
Department: Management Information Systems
College: Business Administration
E-Mail: awu@bus.ucf.edu
Telephone: (407) 823-1581
Facsimile: (407) 823-2389
Home Telephone: (407) 281-6950

Signature:
Name:
Mr./Ms./Mrs./Dr.(choose one)
Employee ID or Student PID #:
Degree:
Title:
Department:
College:
E-Mail:
Telephone:
Facsimile:
Home Telephone:

Signature:
Name:
Mr./Ms./Mrs./Dr. (choose one)
Employee ID or Student PID #:
Degree:
Title:
Department:
College:
E-Mail:
Telephone:
Facsimile:
Home Telephone:

Signature:
Name:
Mr./Ms./Mrs./Dr.(choose one)
Employee ID or Student PID #:
Degree:
Title:
Department:
College:
E-Mail:
Telephone:
Facsimile:
Home Telephone:

03-08-07 P03:34 IN

3. **Supervisor:** (complete if researcher is a student or staff member – Put contact information above)

Signature: Carol Saunders
Name: Carol Saunders

Informed Consent

IT Governance and Information Security Survey

Dear information security manager,

You are among hundreds of information security managers who have been selected to participate in an **anonymous** survey. Your company will receive an aggregate report of findings from this survey. Your participation and honest answers are crucial for studying how IT governance can be implemented to improve the quality of information security services.

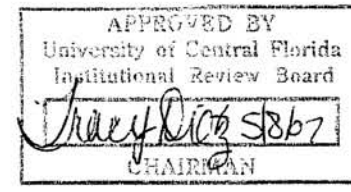
- This survey is completely voluntary. You may choose not to participate or not to answer any specific questions. You may skip any question you are not comfortable answering. There are no anticipated direct risks or benefits.
- **Do not take this survey if you are under the age of 18.**
- The survey is anonymous. You can be assured that your responses will never be matched with your company.
- Only authorized research personnel and the UCF Institutional Review Board and its staff, and other individuals, acting on behalf of UCF, may inspect the records from this research project.
- Composite data will be assessed to determine the most effective way for companies to implement IT governance mechanisms with respect to enhancing the quality of information security services.
- The results of this study may be published. However, the data obtained from you will be combined with data from others in the publication. The published results will not include your information that would personally identify you in any way.
- The following questions ask about the implementation of IT governance mechanisms in your company.
- **Please answer questions honestly.**
- If you have any questions about this survey, please contact me or my academic advisor, Dr. Carol Saunders, at:

  Yu (Andy) Wu, SecurityStudy@gmail.com, (407) 580-4198
  Carol Saunders, Ph.D. csaunders@bus.ucf.edu, (407) 823-6392
  Dept. of MIS, College of Business Administration, University of Central Florida, Orlando, FL 32816
- Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (IRB). Questions or concerns about research participants' rights may be directed to UCF Institutional Review Board Office at the University of Central Florida, Office of Research and Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246. The phone numbers are 407-823-2901 or 407-882-2276.

Thank you for taking the time and thought to complete this survey. We sincerely appreciate your participation. Your time and effort in helping us gather information is greatly appreciated and will ultimately help companies achieve a higher level of information security.

Sincerely,

Yu (Andy) Wu



Informed Consent

IT Governance and Information Security Survey

Dear manager,

You are among hundreds of information security managers who have been selected to participate in an **anonymous** survey. Your company will receive an aggregate report of findings from this survey. Your participation and honest answers are crucial for studying how IT governance can be implemented to improve the quality of information security services.

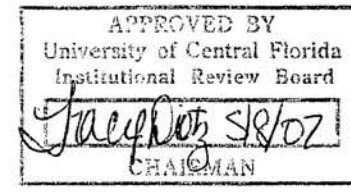
- This survey is completely voluntary. You may choose not to participate or not to answer any specific questions. You may skip any question you are not comfortable answering. There are no anticipated direct risks or benefits.
- **Do not take this survey if you are under the age of 18.**
- The survey is anonymous. You can be assured that your responses will never be matched with your company.
- Only authorized research personnel and the UCF Institutional Review Board and its staff, and other individuals, acting on behalf of UCF, may inspect the records from this research project.
- Composite data will be assessed to determine the most effective way for companies to implement IT governance mechanisms with respect to enhancing the quality of information security services.
- The results of this study may be published. However, the data obtained from you will be combined with data from others in the publication. The published results will not include your information that would personally identify you in any way.
- The following questions ask about information quality and security organization's service quality in your company.
- **Please answer questions honestly.**
- If you have any questions about this survey, please contact me or my academic advisor, Dr. Carol Saunders, at:

  Yu (Andy) Wu, SecurityStudy@gmail.com, (407) 580-4198
  Carol Saunders, Ph.D. csaunders@bus.ucf.edu, (407) 823-6392
  Dept. of MIS, College of Business Administration, University of Central Florida, Orlando, FL 32816
- Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (IRB). Questions or concerns about research participants' rights may be directed to UCF Institutional Review Board Office at the University of Central Florida, Office of Research and Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246. The phone numbers are 407-823-2901 or 407-882-2276.

Thank you for taking the time and thought to complete this survey. We sincerely appreciate your participation. Your time and effort in helping us gather information is greatly appreciated and will ultimately help companies achieve a higher level of information security.

Sincerely,

Yu (Andy) Wu



APPENDIX C: MAIL SURVEY QUESTIONNAIRES

IT Governance and Information Security Survey

Security Manager Version

Time to complete: Approximately 15 minutes

Please indicate the degree to which you **agree** with each of the following statements (1=Strongly Disagree, 3 = Neither Agree nor Disagree, 5 = Strongly Agree):

In my company, processes are in place to ensure that…

	Strongly Disagree				Strongly Agree
1. Users' requirements for information security are addressed in **information security policies**.	1	2	3	4	5
2. Users' requirements for information security are addressed in **information security standards**.	1	2	3	4	5
3. Users' requirements for information security are expressed as formal or informal **internal service level agreements** (SLAs) between us (security organization) and users.	1	2	3	4	5
4. **Risk assessment** is performed before information security services are planned.	1	2	3	4	5
5. **Information security plans** are updated in a timely manner to address changes in user requirements for information security.	1	2	3	4	5
6. Proper **change management** procedures are followed when information security plans are updated for changes in user requirements for information security.	1	2	3	4	5
7. **Internal IS audits** are performed regularly.	1	2	3	4	5
8. **External IS audits** are performed regularly by accounting firms, contractors, etc.	1	2	3	4	5
9. Regular security assessments (e.g., penetration tests) are performed by **internal testers**.	1	2	3	4	5
10. Regular security assessments (e.g., penetration tests) are performed by **external testers** such as consultants.	1	2	3	4	5

In my company…

	Strongly Disagree				Strongly Agree
11. **Liaisons or relationship managers in business units** manage the relationship with the security organization.	1	2	3	4	5
12. **A liaison or relationship manager in the security organization** manages the relationship with other departments.	1	2	3	4	5
13. **Business units often invite us** (security organization) to attend business conferences with them.	1	2	3	4	5
14. **We (security organization) often invite** employees in business units to attend information security conferences with us.	1	2	3	4	5

My company…

	Strongly Disagree				Strongly Agree
15. Often sponsors **events** where we (security organization) interact with employees in other departments.	1	2	3	4	5
16. Implements **cross-functional training** between us (security organization) and other departments.	1	2	3	4	5
17. **Physically locates our offices** so that we (security organization) have maximum interaction with employees in important departments.	1	2	3	4	5
18. Encourages us (security organization) and other departments to **cc each other**, when appropriate, on important decisions.	1	2	3	4	5

Continued on back. Please turn over.

In my company…

19. The **IT steering committee** (or its equivalent) is… ☐ Non-existent ☐ Ad Hoc Only ☐ Permanent (meets regularly)

If your answer is "ad hoc only" or "permanent", please also answer Question 19A. ⇘

	Strongly Disagree				Strongly Agree
19A. The **IT steering committee** (or its equivalent) is effective in deciding strategic IT matters.	1	2	3	4	5

If your answer is "non-existent", please proceed to Question 20. ⇩

20. The **information security committee** (or its equivalent) is… ☐ Non-existent ☐ Ad Hoc Only ☐ Permanent (meets regularly)

If your answer is "ad hoc only" or "permanent", please also answer Question 20A. ⇘

	Strongly Disagree				Strongly Agree
20A. The **information security committee** (or its equivalent) is effective in overseeing important information security matters.	1	2	3	4	5

If your answer is "non-existent", please proceed to Question 21. ⇩

21. The **IT budget committee** (or its equivalent) is… ☐ Non-existent ☐ Ad Hoc Only ☐ Permanent (meets regularly)

If your answer is "ad hoc only" or "permanent", please also answer Question 21A. ⇘

	Strongly Disagree				Strongly Agree
21A. The **IT budget committee** (or its equivalent) is effective in overseeing IT budget matters.	1	2	3	4	5

If your answer is "non-existent", please proceed to Question 22. ⇩

22. The **IS audit committee** (or its equivalent) is… ☐ Non-existent ☐ Ad Hoc Only ☐ Permanent (meets regularly)

If your answer is "ad hoc only" or "permanent", please also answer Questions 22A and 22B. ⇘

	Strongly Disagree				Strongly Agree
22A. The **IS audit committee** (or its equivalent) is effective in overseeing IS audit matters.	1	2	3	4	5

	Strongly Disagree				Strongly Agree
22B. The IS audit committee (or its equivalent) is composed of **members with backgrounds in various business functions**.	1	2	3	4	5

If your answer is "non-existent", please proceed to Question 23. ⇨

Continued on next page. ⇨

23. The **internal IS audit department** (or its equivalent) is… ☐ Non-existent ☐ Ad Hoc Only ☐ Permanent

If your answer is "ad hoc only" or "permanent", please also answer Question 23A. ↘

		Strongly Disagree				Strongly Agree
23A.	The internal IS audit department (or its equivalent) is **not influenced by other departments**.	1	2	3	4	5

If your answer is "non-existent", please proceed to Question 24. ⇩

In my company, we (security organization) and other departments generally have consensus on…

	Strongly Disagree				Strongly Agree
24. **What** information assets to protect.	1	2	3	4	5
25. **Who** in the security organization implements which security mechanisms.	1	2	3	4	5
26. The **priorities** of information security.	1	2	3	4	5
27. The **allocation of resources** for information security.	1	2	3	4	5
28. The **feasibility** of implementing information security services.	1	2	3	4	5
29. The **expected results** for information security.	1	2	3	4	5
30. The **metrics to define the success** of information security.	1	2	3	4	5

In my company, we (security organization) have more information than other departments do about each of the following:

	Strongly Disagree				Strongly Agree
31. The precise level of our own **competence** in implementing information security mechanisms.	1	2	3	4	5
32. The precise level of our own **experience** in implementing information security mechanisms.	1	2	3	4	5
33. **What we (security organization) are doing** to protect information assets.	1	2	3	4	5
34. The amount of **effort we (security organization)** are exerting.	1	2	3	4	5

In my company, we (security organization) have more information than other departments do about each of the following:

	Strongly Disagree				Strongly Agree
35. The **quality of services** we (security organization) provide to protect information assets.	1	2	3	4	5
36. The **random, external factors** that may influence our effectiveness in protecting information assets.	1	2	3	4	5

In my company …

	Strongly Disagree				Strongly Agree
37. **Top management**, in general, is satisfied with the services provided by us (security organization) to protect information assets.	1	2	3	4	5
38. **Employees**, in general, are satisfied with the services provided by us (security organization) to protect information assets.	1	2	3	4	5
39. **Top management**, in general, is confident that information assets are well protected.	1	2	3	4	5
40. **Employees**, in general, are confident that information assets are well protected.	1	2	3	4	5
41. **Top management**, in general, feels that the level of information security supports its jobs well.	1	2	3	4	5
42. **Employees**, in general, feel that the level of information security supports their jobs well.	1	2	3	4	5

Continued on back. Please turn over.

My company implements the following (please check all that apply):

Framework / Standard	How long has it been implemented (in months)	Comments
☐ CobiT		
☐ ITIL		
☐ ISO17799		
☐ ISO27001/27002		
☐ NIST		
☐ OCTAVE		
☐ Other third-party governance frameworks*		
☐ Other in-house governance frameworks*		

* Please specify in the "Comments" column.

My position:		Position of the person I report directly to:	
Company's annual revenue:	☐ Less than US$1 million ☐ US$1 – 9 million ☐ US$10 – 99 million ☐ US$100 million – 1billion ☐ Greater than US$1billion	Number of employees in company:	☐ 1 – 99 ☐ 100 – 499 ☐ 500 – 1499 ☐ 1500 – 9999 ☐ 10,000 – 49,000 ☐ More than 50,000
Industry:			

Thank You!

Next, Please do these…

- Insert this questionnaire in the supplied postage-prepaid envelope and mail it back to us.
- Write your company name on the attached postage-prepaid **notification postcard** and drop it in the mail so that we will know you have responded and will not follow up with you unnecessarily. To ensure your anonymity, please do **not** put it into the return envelope with the questionnaire.

Thank you very much for your participation in our research project! If you want to share your insights into information security issues or to make suggestions regarding this questionnaire, please comment below.

Andy Wu, Department of MIS, University of Central Florida, Orlando, FL 32816-0014 • (407) 580-4198 • SecurityStudy@gmail.com

Definitions

Security Organization: The organizational unit inside your company that implements and manages information security in your company, regardless of its name or location in the organizational chart. You have been asked to complete this questionnaire because of your role inside the security organization. If you are not involved in information security management, please kindly forward this questionnaire to someone who is in that role.

Business Units/Other Departments: All other organizational units inside your company aside from the security organization, whether they are revenue-generating units (production, sales, etc.) or support functions (accounting, legal, etc.).

IT Governance and Information Security Survey

Business Manager Version

Time to complete: Approximately 10 minutes

Please indicate the degree to which you agree with statements 1-13 and mark your rating for statements 14–38 as instructed.

In my company, the security organization and other departments generally have consensus on…

	Strongly Disagree				Strongly Agree
1. **What** information assets to protect.	1	2	3	4	5
2. **Who** in the security organization implements which security mechanisms.	1	2	3	4	5
3. The **priorities** of information security.	1	2	3	4	5
4. The **allocation of resources** for information security.	1	2	3	4	5
5. The **feasibility** of implementing information security services.	1	2	3	4	5
6. The **expected results** for information security.	1	2	3	4	5
7. The **metrics to define the success** of information security.	1	2	3	4	5

In my company, the security organization knows a lot more than I do about…

	Strongly Disagree				Strongly Agree
8. The precise level of their **competence** in implementing information security mechanisms.	1	2	3	4	5
9. The precise level of their **experience** in implementing information security mechanisms.	1	2	3	4	5
10. **What they are doing** to protect our information assets.	1	2	3	4	5
11. The amount of **effort** they are exerting.	1	2	3	4	5
12. The **quality of services** they provide to protect information assets.	1	2	3	4	5
13. The **random, external factors** that may influence their effectiveness in protecting information assets.	1	2	3	4	5

With regard to each of the following, my perception of our security organization's performance is…

(1 = Low, 3 = Average, 5 = High)

	Low				High
14. Providing services as promised.	1	2	3	4	5
15. Dependability in handling users' security problems.	1	2	3	4	5
16. Performing security service right the first time.	1	2	3	4	5
17. Providing security services at the promised time.	1	2	3	4	5
18. Maintaining reliable technology and systems.	1	2	3	4	5
19. Prompt service to users.	1	2	3	4	5
20. Willingness to help users.	1	2	3	4	5
21. Readiness to respond to users' requests for security services.	1	2	3	4	5
22. Making users feel safer in using information technologies.	1	2	3	4	5
23. Courtesy when interacting with users.	1	2	3	4	5
24. Knowledge to answer users' questions about threats and protective solutions.	1	2	3	4	5
25. Giving users individual attention.	1	2	3	4	5
26. Dealing with users in a caring fashion.	1	2	3	4	5
27. Having the users' best interest at heart.	1	2	3	4	5
28. Understanding of users' security needs.	1	2	3	4	5
29. Proper maintenance of security equipment and facilities.	1	2	3	4	5
30. Maintaining professionalism.	1	2	3	4	5
31. Providing useful support materials (documentation, training, videos, etc.).	1	2	3	4	5

Continued on back. Please turn over.

Regarding information security in my company, <u>my level of confidence</u> in each of the following is…
(1 = Low, 3 = Average, 5 = High)

	Low				High
32. Information is accessible only to those people who have a legitimate reason to access it.	1	2	3	4	5
33. Information is not altered by people with malicious intent.	1	2	3	4	5
34. Information is not altered unintentionally.	1	2	3	4	5
35. Information is available when needed.	1	2	3	4	5
36. Computer systems remain up and running without unplanned downtime.	1	2	3	4	5
37. Overall, our information assets are secure.	1	2	3	4	5
38. Overall, the level of information security supports our business functions adequately.	1	2	3	4	5

My position:		Position of the person I report directly to:	
Company's annual revenue:	☐ Less than US$1 million ☐ US$1 – 9 million ☐ US$10 – 99 million ☐ US$100 million – 1billion ☐ Greater than US$1billion	Number of employees in company:	☐ 1 – 99 ☐ 100 – 499 ☐ 500 – 1499 ☐ 1500 – 9999 ☐ 10,000 – 49,000 ☐ More than 50,000
Industry:			

Thank You!

Next, Please do these…

- Insert this questionnaire in the supplied postage-prepaid envelope and mail it back to us.
- Write your company name on the attached postage-prepaid **notification postcard** and drop it in the mail so that we will know you have responded and will not follow up with you unnecessarily. To ensure your anonymity, please do **not** put it into the return envelope with the questionnaire.

Thank you very much for your participation in our research project! If you want to share your insights into information security issues or to make suggestions regarding this questionnaire, please comment below.

Andy Wu, Department of MIS, University of Central Florida, Orlando, FL 32816-0014 • (407) 580-4198 • SecurityStudy@gmail.com

Definitions

Security Organization: The organizational unit **inside** your company that implements and manages information security, regardless of its name or location in the organizational chart.

Business Units/Other Departments: All other organizational units inside your company aside from the security organization, whether they are revenue-generating units (production, sales, etc.) or support functions (accounting, legal, etc.).

APPENDIX D: ONLINE SURVEY INTERFACE


IT Governance and Information Security Survey - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.bus.ucf.edu/awu/dissertation/survey.aspx
Go Links SnagIt
IT Governance & InfoSec
online survey
Greetings from Andy Wu at University of Central Florida! Thank you very much for participating in the survey to support my dissertation.
This survey is designed to collect and match responses from information security managers and a business managers. To help me properly record the responses, please make sure you enter the correct code or sequence number when you are asked.
Please be assured that this code or sequence number is used solely to match anonymous answers from security and business managers who work for the same company. The code/number is not related to your or your company's identity in any way.
Would you please answer a couple of questions so that I can present you the proper version of the survey?
What is your job role? *
Security Manager
Business Manager
* For this study, "business managers" include IT managers and executives not directly in charge of information security, for example, CIO, CTO, VP-IT, etc.
© 2007 Andy Wu Contact Info
Internet