

**AN EMPIRICAL ANALYSIS ON THE EFFECTIVENESS OF INFORMATION  
SECURITY POLICIES, INFORMATION TECHNOLOGY GOVERNANCE, AND  
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION SECURITY**

**CERTIFICATION**

by

Jon W. Paarlberg

WENBIN LUO, PhD, Faculty Mentor and Chair

GLENN BOTTOMLY, PhD, Committee Member

APIWAN BORN, PhD, Committee Member

Bill Dafnis, PhD, Interim Dean of Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

June 2016

ProQuest Number: 10129949

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

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



ProQuest 10129949

Published by ProQuest LLC (2016). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code  
Microform Edition © ProQuest LLC.

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

© Jon W. Paarlberg, 2016

## Abstract

Security professionals and researchers believe that information security policies are a crucial element to good information security. This study sought to explore the relationship between information security policies, Information Technology (IT) governance, International Organization for Standardization (ISO) security certification and the number and severity of breaches suffered by organizations in the US. This quantitative study used an online survey to collect responses from IT professionals about information security policies, IT governance, and ISO security certifications. It then compared those qualities to the number and severity of breaches experienced by the organization. Multivariate analysis was used to analyze the results. This study finds that there is a significantly higher number of more severe breaches suffered by organizations that have an information security policy. Organizations that follow an IT governance framework also reported a higher number of severe breaches. ISO certification did not exhibit a statistically significant relationship. Further research should be performed to discover why organizations that are attempting to follow security best practices would report higher numbers of severe breaches.

## Dedication

So many people have provided support for this work that it is difficult to sufficiently express my gratitude in this small space. First and foremost, I thank my wife and 5 children for the long hours that they had to put up with me while performing this work. Without their understanding and encouragement, none of it would be possible or worthwhile. Thank you Tammy, Charles, Mary, Elayne, Isabelle and Nicole. My mentor, Dr. Wenbin Luo was a fantastic help and provided the right advice when I needed it. My many friends were always supportive when I expressed the need to work on this study and were genuinely interested in seeing it finished, so thank you Darren Quinn, Anne Foskett, Rita Shammass, Carolyn Cook, Dolores McClead, Kathi Pacquet, Dana Harris, John Kappelhoff, Zach Kaye, Brian Lapins, Ryan Berg, Kevin Racicot, Devin Church, Brian Wheeler, Peter Bliss, Dmitri Chvetsov, Bill Cassels, and Cathi Bishop.

## Table of Contents

List of Tables	vii
List of Figures	ix
CHAPTER1. INTRODUCTION	
Introduction to the Problem	1
Background of the Study	2
Statement of the Problem	8
Purpose of the Study	9
Rationale	10
Research Questions	12
Significance of the Study	13
Definition of Terms	14
Assumptions and Limitations	15
Nature of the Study (or Theoretical/Conceptual Framework)	17
Organization of the Remainder of the Study	18
CHAPTER 2. LITERATURE REVIEW	
Introduction	20
IT Governance	20
ISO Certification	34
Sarbanes Oxley	37
Theory	38

Integrating the Information Security Policy into IT Governance	42
Information Security Policy Theory	43
Information Security Policies	44
Organizational Security Management	50
Breaches	52
Information Security Policy Effectiveness	60
Conclusion	63
<b>CHAPTER 3. METHODOLOGY</b>	
Research Design	66
Population/Sample	73
Instrument	76
Data Collection	77
Data Analysis	79
Validity and Reliability	82
Ethical Considerations	84
Summary	89
<b>CHAPTER 4. RESULTS</b>	
Population and Sample	87
Summary of Results	89
Details of Analysis and Results	95
Conclusion	122

## CHAPTER 5. DISCUSSION, IMPLICATIONS, AND RECOMMENDATIONS

Results Summary	123
Results Discussion	125
Implications	130
Limitations	132
Recommendations for Further Research	133
Conclusion	133

## APPENDICES

Appendix A: G*Power Analysis of Required Sample Size	149
Appendix B: Study Survey Instrument	150
Appendix C: Doherty and Fulford (2005) Hypotheses	172
Appendix D: Pilot Test Analysis	173



## List of Tables

Table 1. Sample Demographics	88
Table 2. Job Position Demographics	89
Table 3. Existence of an Information Security Policy MANOVA summary	91
Table 4. Frequency of Information Security Policy Update MANOVA Summary	92
Table 5. Length of Information Security Policy Adoption MANOVA Summary	93
Table 6. Adoption of IT Governance Framework MANOVA Summary	94
Table 7. ISO Security Certification MANOVA Summary	95
Table 8. Existence of an Information Security Policy Normality Tests	97
Table 9. MANOVA for Existence of a Security Policy	100
Table 10. Post-hoc Tests for Existence of a Security Policy	100
Table 11. Normality Tests for Frequency of Policy Update	103
Table 12. MANOVA for Policy Update Interval	105
Table 13. Post-Hoc Tests for Policy Update Interval	105
Table 14. Normality Test for Length of Time	108
Table 15. MANOVA for Length of Time	110
Table 16. Post-hoc Tests for Length of Time	110
Table 17. Normality Tests for Policy Length of Time	113
Table 18. MANOVA for Adoption of an IT Governance Framework	115
Table 19. Post-hoc Tests for Adoption of an IT Governance Framework	116
Table 20. Normality Test for ISO Certification	119

Table 21. MANOVA for ISO Certification	121
Table 22. Post-hoc Tests for ISO Certification	122

## List of Figures

Figure 1. Conceptual Framework	18
Figure 2. Literature Review Map	20
Figure 3. Map of variable relationships for Research Questions 1-3	72
Figure 4. Hypothesis 1 Means	96
Figure 5. Hypothesis 1 Outliers	97
Figure 6. Hypothesis 1 Q-Q Plots	98
Figure 7. Hypothesis 1 Scatter Plots	98
Figure 8. Hypothesis 2 Means	101
Figure 9. Hypothesis 2 Outliers	102
Figure 10. Hypothesis 2 Scatter Plot	104
Figure 11. Hypothesis 3 Means	106
Figure 12. Hypothesis 3 Outliers	107
Figure 13. Hypothesis 3 Scatter Plots	109
Figure 14. Hypothesis 4 Means	111
Figure 15. Hypothesis 4 Outliers	112
Figure 16. Hypothesis 4 Q-Q Plots	113
Figure 17. Hypothesis 4 Scatter Plot	114
Figure 18. Hypothesis 5 Means	117
Figure 19. Hypothesis 5 Outliers	118
Figure 20. Hypothesis 5 Q-Q Plots	119

Figure 21. Hypothesis 5 Scatter Plot	120
Figure 22. Hypothesis 1 Means	126
Figure 23. Hypothesis 2 Means	127
Figure 24. Hypothesis 3 Means	128
Figure 25. Hypothesis 4 Means	129
Figure 26. Hypothesis 5 Means	130

## CHAPTER 1. INTRODUCTION

### Introduction to the Problem

Information security policies have long been touted as being the cornerstone of information security, and are referred to as the singular, most important control for an organization (Höne & Eloff, 2002; Knapp, Franklin Morris Jr., Marshall, & Byrd, 2009). Frequently, such policies are required by legislation, such as section 164.308(a)(1)(i) of the Health Insurance and Portability and Accountability Act (“Sample Security Policies,” 2010), or for certification, as in ISO 17799 (Myler & Broadbent, 2006). Are these policies effective in the real world? Is there empirical evidence that they add benefit to the organization, and does that benefit outweigh the cost of maintaining the policy?

Many organizations have an information security policy (Hagen, Albrechtsen, & Hovden, 2008), but, even with the policy, security breaches continue to occur frequently (Richardson, 2011). If an information security policy is so important and pivotal to information security, then it can be assumed that organizations that have a policy should be less at risk than those that do not. Research shows that this assumption may not be true (Davis, Garcia, & Zhang, 2009; Doherty & Fulford, 2005). Organizations that spend time and money to institute an information security policy, or to make their policies better, may be damaged just as frequently or severely as those organizations that do not. Thus, the research problem of this project is to discover if development of an information security policy is truly beneficial to an organization: Are there measurable benefits to developing and maintaining an information security policy?

## **Background of the Study**

Businesses and organizations spend vast amounts of resources on the construction and maintenance of information security policies. Frequently, those policies are required by legislation, such as section 164.308(a)(1)(i) of the Health Insurance and Portability and Accountability Act (“Sample security policies,” 2010), or for certification, as in ISO 17799 (Myler & Broadbent, 2006). Information is recognized as a critical element in strategic business planning, operations, communication, managerial decision making, financial transactions and a host of other organizational facets (Doherty & Fulford, 2005). Consequently, information and the infrastructure that holds and controls it, should be managed, governed and protected (Drugescu & Etges, 2006; Lainhart, 2000; Peterson, 2004). Part of governing information assets is the construction of information security policies. Organizations pursue the creation and maintenance of these policies with significant expenditures of time and money. The policies extend throughout the organization and impact every employee through signed agreements and training (Hazari, Hargrave, & Clenney, 2008). However, despite the pervasive existence of extensive information security policies, information security breaches are increasing in frequency and severity (Doherty & Fulford, 2005; Peters, 2009). This study seeks to further determine and test this relationship with the purpose of discovering if there is a relationship between information security policies and information security breaches.

Doherty and Fulford (2005) based an entire, groundbreaking study on this perplexing and concerning topic. Their prior studies (Doherty & Fulford, 2003) were aimed at evaluating frameworks for information security policies and how organizations could develop them, similar to Hagen et al’s study (2008). While performing research into all the intricacies of information security policies, they decided to ask a question, which is best expressed through the title of their

pivotal study: “Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis” (Doherty & Fulford, 2005). It seemed to be an obvious question that had not been asked at that time in the available literature. Doherty and Fulford (2005) reasoned that it was a good question to ask, given the amount of resources that were being poured into developing such policies. It also challenged some of the assumptions that they had been using in the past.

Their study turned from frameworks and models of security policies into exploration of the effectiveness of information security policies (Doherty & Fulford, 2005). Because of their earlier studies, the authors were aware that all information security policies were not alike; each had its own characteristics. In order to address these characteristics, they used an exploratory model that took into account the following: whether or not the organization had an approved information security policy, the age of that policy, the frequency of its updates, and the scope and adoption of best practice. They also realized the need to evaluate the effectiveness of information security policy adoption and development because they understood that the policy does not exist in a vacuum. For this particular study they utilized a strictly empirical evaluation of the policy’s effectiveness, which is the amount of reduction of the number and severity of security breaches.

Just as security policies possess different characteristics, so do security breaches. Doherty and Fulford (2005) took into account a number of breach qualities and types as well as the number of times breaches occurred. Breaches were identified as computer viruses, hacking incidents, unauthorized access, theft, fraud, human error, natural disaster, and damage by employees. By breaking breaches down into types, the researchers hoped to find correlation to

the qualities of the information security policies. Because of their extensive work in prior studies, they fully expected to show that not only do security policies result in reduction of breach damage, but that there were parts of the security policy that could be focused on to maximize effectiveness. According to the data that they collected and the analysis conducted, they were not correct in their assumptions. None of the security policy attributes impacted the frequency or severity of any of the breach types significantly.

In order to evaluate both the security policies and the nature and number of breaches, Doherty and Fulford (2005) performed survey analysis on 2,838 mid to large sized organizations in the United Kingdom. Executives comprised the majority of the targeted employees, though the authors realized the survey responses might have been delegated to lower level employees. 219 valid responses were obtained; a response rate of 7.7%. The majority of respondents were from manufacturing and government services.

Results were evaluated utilizing quantitative statistical analysis. Survey instruments included questions that quantified what organizations had experienced, both with information security policy development and with security breaches. Most of these data were collected and assigned categorical values, including the use of a Likert scale. The researchers used statistical tests such as chi square and correlation in an attempt to compare information security policy characteristics with breach qualities. Statistical significance was determined at  $p < .05$ .

Their study showed that there was no significant relationship between the breach incidence or severity suffered by an organization whether that organization had spent the resources to obtain and develop the policy than if they had not. It was rather shocking to the researchers that an organization that did not bother with implementing a policy did not suffer a



significantly different number of breaches. Nor did the breaches show any increased severity in the absence of an information security policy. Additionally, updating the policy more frequently, or having a policy in place for a longer period of time also did not reduce breach number or severity.

Doherty and Fulford (2005) concluded that there was a need for further study to discover why this gap existed. They put forth some possible explanations such as difficulty of enforcement, difficulty of raising awareness, policy standards being too complex, and inadequate resourcing. Given the positivistic nature of the study, it was far outside its scope to address any of the possibilities, so the authors called for more research in these areas.

Research questions posed by Doherty and Fulford (2005) are still valid and of current academic interest even though security professionals understand that simply having an information security policy may not be sufficient to protect the assets of the organization. The information security policy is an essential component to the design and engineering of information security (Höne & Eloff, 2002; Knapp et al., 2009). It gives the organization a framework for structuring, guiding, evaluating, and communicating the objectives and expectations to all of its members. More than just a rubber stamp that expresses compliance or an outward proclamation, a well-constructed policy will guide decision makers as well as system users on acceptable use (Knapp et al., 2009). Past research shows that information security policies are primarily internal documents. Some even restrict viewing or sharing of the policy to those external to the organization. So, the research questions proposed by Doherty and Fulford (2005) should not really be viewed as a measure of the deterrent effect of the information security policy to would-be attackers, but should be an evaluation of the effectiveness of the

information security policy and how well it steers the information security program and establishes compliance to the acceptable use that is defined within it. Answers to Doherty and Fulford's research questions will help explore possible relationships between the qualities and characteristics of information security policies and actual, real-world, measurable results with regards to breach frequency and severity.

Additionally, the passage of time may make asking these same questions again a more valid activity and may produce valuable trending results that are applicable to information security efforts worldwide. For instance, suppose that the results of this study do not agree with the original Doherty and Fulford (2005) study. Perhaps there is now a significant relationship between how many breaches an organization suffers and whether an information security policy exists or not. A result like that could indicate that organizations are becoming better at creating an effective information security policy and putting it into real action at the levels where it matters. Conversely, results that are similar to the Doherty and Fulford (2005) study would support and add validation to their conclusions within a wider population.

Other studies in addition to Doherty and Fulford (2005) also inferred that having an information security policy as well as the age, scope, and update frequency do not significantly reduce the number or severity of security breaches in an organization (Heikkila, 2009; Kwo-Shing Hong et al., 2006; Wiant, 2005). This goes against the assumptions of many of the fundamental works and resultant frameworks designed around the information security policy (Fulford & Doherty, 2003; Higgins, 1999; Höne & Eloff, 2002). It brings into question the basis of many information security programs, and undermines the confidence of policies and procedures that are based on such a policy. If the number of breaches and the damage from such

breaches is not significantly different between companies that have an information security policy versus those that do not, then either the importance of information security policies has been overstated and they are not significant, or there are other related variables. These variables would have to be of such a magnitude to cause organizations with information security policies to fail more often in actual application than those that do not have such a policy. In other words, if the information policy is so important and effective, then there must be a failure greater than the success to bring it into relative equality with the organization that does not have such a tool. Since the prior logical conclusion, that the importance of an information security policy has been overstated, is far more reasonable than the latter, that a company successful in creating an information security policy must fail more in other areas, measuring the number and severity of breaches can logically be interpreted inductively as a measure of the overall effectiveness of the information security policy.

Information security policies are influenced by a broader organizational effort, namely IT governance. Security is one of the triune elements of IT governance as defined by the ISACA: “an implementation of controls to sustain the quality, fiduciary, and security of information assets” (“Information Technology - Information Security – Information Assurance | ISACA,” 2014). Because IT governance is the driving force behind information security policies, it makes sense to explore the implementation of governance, including governance frameworks such as COBIT or ITIL, to provide context for information security policy implementation. Exploring whether organizations that implement and maintain information security policies also implement and strive to adhere to IT governance frameworks would provide depth to the study. It would add a facet that was previously not explored, but that may show correlation.

Likewise, ISO certifications require implementation and development of information security policies, and are part of IT governance. Organizations that strive for certification should be exhibiting attempts of increased governance. This study explored whether these attempts net real-world results such as fewer or less severe breaches. Additionally, ISO certification may serve as an indicator of how well organizations are operationalizing their security policy (Saint-Germain, 2005). Significant results could help support the pursuit of certification.

Given the admitted weaknesses of prior empirical studies and the small number that have been performed (Bulgurcu, Cavusoglu, & Benbasat, 2010; Doherty, Anastasakis, & Fulford, 2009; Siponen, Pahlila, & Mahmood, 2010), conclusions about the effectiveness of the information security policy are probably too broad to point to a definitive relationship. Deviation of these data may simply make a large range of breaches fall within significance, making the actual effectiveness hidden by error of the quantitative analysis. The solution for this dilemma is to conduct more measurement, and to conduct analysis from different approaches.

### **Statement of the Problem**

Recent empirical research suggests that the presence of an information security policy does not significantly reduce the number or severity of security breaches in an organization (Doherty & Fulford, 2005; Heikkila, 2009). If true; this is in direct opposition to what had been expected by some researchers, especially those that have involved themselves in study of the information security policy, its benefits, framework, purpose and construction. While the reasoning behind having a policy is sound, it seems that the impact of having a policy is not as great as it should be, which is unfortunate and possibly frustrating to organizations that are interested in securing their information. There is a disparity between what is expected in

research and what is being experienced in practice. Time and effort spent on the information security policy may not be netting the returns on effectively helping organizations reduce costs of security breaches. Organizations will want to know the value that they are adding by spending resources on the information security policy.

A study such as this one can provide information about the apparent disparity between security policy efforts and the results netted from such efforts. While there have been similar studies in the past, this study addresses a different population, and approaches the research from a different angle. By also evaluating the overarching IT governance of these organizations, evidence may be uncovered that shows the security policy does not operate in a vacuum. In the event that security policies still show no significant relationship to reduced breaches, then prior studies would be confirmed and following research would take a different track into why the policies are ineffective.

### **Purpose of the Study**

The purpose of this survey research is to explore the effects of information security policies, IT Governance or ISO certification on the severity and frequency of information security breaches suffered by organizations. A gap currently exists in the literature because few studies have been performed that collect breach data and compare it to organizational methods of information security design and management (Doherty & Fulford, 2005; Straub, 1990). Organizational leaders have a need to understand the proven effectiveness of different security techniques and methodologies so that they can make informed decisions on business strategy (Pieters, Dimkov, & Pavlovic, 2013). Information security academics seek to further define and understand relationships between information security efforts and their results so that theory can

be more fully developed (Doherty, Anastasakis, & Fulford, 2009; Doherty & Fulford, 2005; Straub, Goodman, Baskerville, Goodman, & Ebrary, 2008). This study was designed to target this gap and to bolster previous efforts to explore relationships between organizational security efforts and the results. Results of this research contribute to knowledge about the results of practical application of information security policies in real-world organizations. This knowledge will sustain or undermine theory of information security policy design, importance, and implementation.

### **Rationale**

Studies in the topic of security policies use empirical measurement of the number and severity of breaches to evaluate the strength of such policies (Davis et al., 2009; Doherty & Fulford, 2005; Kwo-Shing Hong, Yen-Ping, Chao, & Tang, 2006; Straub, 1990). By examining the characteristics of the policy against the characteristics of security failures (breaches) or successes (lack of breaches) a study can derive a concrete evaluation of the efficiency and effectiveness of a security policy. Organizations may be spending too much time and energy on the information security policy, or put too much reliance on the policy as a form of protection. Measuring qualities of the policy such as the age of the policy and frequency of updates may help in exploring whether certain qualities of the information security policy are more important or effective than others.

Doherty and Fulford (2005) applied this type of thinking when they designed their ground-breaking study to measure the effectiveness of information security policies. They focused on the assumption that measuring the number and severity of breaches would reflect the actual strength of the information security policy, since that is what the policies are designed to

do. They also acknowledged that there are several considerations to take into account besides the fact that an organization may possess an information security policy and sought to measure some of these other attributes of the organization that may have an effect on information security.

A work that closely parallels Doherty and Fulford (2005) is a noteworthy study by Wiant (2005), where the propensity of reporting security incidents was related to the existence and utilization of an information security policy. The Wiant (2005) study used a similar approach of Doherty and Fulford (2005), where the number and severity of information security breaches for healthcare organizations was compared to the existence of an information security policy. The statistical analysis used to determine the findings was also similar, as were the findings themselves. Wiant (2005) found that there was no statistical difference in the number and severity of reported breaches between the organizations that had an active information security policy and those that did not.

Romanosky, et al. (2011) also took the approach that measuring the number of information security breaches reflects the strength of policy. They were interested in how the enacting of privacy laws affected the number of privacy breaches in the US. During a seven-year period from 2002 to 2009, they observed the number of reported breaches by analyzing panel data from the Federal Trade Commission. Even though their study did not include severity of breaches, it was for want of data. They stated in their conclusions that severity of privacy data loss should be included in federal reporting, but acknowledged that just getting the number of breaches was challenging enough. Even with this scarcity of data, they were able to show a possible 6% decrease in privacy data breaches after the enacting of privacy protection laws.

This study is based on similar assumptions and structure as those represented above. The data collected on the occurrence of security breaches can be compared to characteristics of information security policies to explore possible empirical relationships. Evidence that supports or undermines such relationships can then be used by academia for further studies or information security professionals to help make business decisions.

### **Research Questions**

RQ 1: Do organizations that have a written information security policy experience fewer security breaches or have fewer records compromised than those that do not (Doherty & Fulford, 2005)?

RQ 2: Do organizations that update their information security policy more frequently experience fewer security breaches or have fewer records compromised than those organizations that update their policies less frequently (Doherty & Fulford, 2005)?

RQ 3: Do organizations with an information security policy that has been in place for a longer period of time experience fewer security breaches or have fewer records compromised than those with a younger policy (Doherty & Fulford, 2005)?

RQ 4: Do organizations that implement an IT governance framework (such as CobiT or ITIL) experience fewer security breaches or have fewer records compromised than those organizations that do not implement an IT governance framework?

RQ 5: Do organizations that are certified in one or more ISO security certifications experience fewer security breaches or have fewer records compromised than those organizations that are not certified?



### **Significance of the Study**

The significance of this study is that it will further test and either support or undermine the results of Doherty and Fulford (2005), thus advancing the quantity of analysis of the topic, and furthering the research frontier. In general, the positivist approach encourages testing results of other research in order to help validate conclusions presented in the earlier research, or to present contradictory evidence. That does not mean that the same study should be carried out, but that the same, or similar, tests should be performed in different environments, on different populations, or with variations of methods in order to establish the generalizability of the theory and the repeatability of results.

This study will test the main conclusions of the Doherty and Fulford (2005) study in a different population, with a different data collection approach, and a slightly different analysis method in the hopes of shedding more light on their original conclusions. This study will be structured to address possible shortcomings that were identified by Doherty and Fulford (2005), such as the difficulty of acquiring a large enough number of valid responses for a sample, or the narrow population of the study. Consequently, this study will target a much larger population of all IT security professionals, regardless of their station, as long as they have knowledge of the security policy and breach knowledge. The hope is that, with a large enough sample, more precise statistical analyses can be applied, and, either significant findings will be revealed, or that the conclusions of the original study would be able to be applied with more confidence; thereby strengthening academic theory.

By including a wider range of organizations, this study attempts to capture a sample of the population that may have been missed by the original study. Part of replicating a quantitative, positivist study should be to apply it to a different sample to find if the results are

the same. In this study, it may be found that small organizations usually do not have an information security policy. Exploring data on the number of breaches for such an organization would be a new application of a proven, solid study. Including smaller organizations and organizations outside of the UK would reduce the risk of sampling error. Business managers will want to know that the information security policy is more than just a formality that must be performed to satisfy stakeholders or legislation. Information security must show a return on investment (ROI) just as any other service (Drugescu & Etges, 2006; Gordon & Loeb, 2002). Additionally, cultivating an information security culture requires that members of an organization can have faith that security efforts will reap results, otherwise compliant security behavior will flag and undermine the whole effort (Walter, 2003). The central placement of the information security policy within the information security effort of an organization demands an evaluation of its empirical effectiveness.

### **Definition of Terms**

*Information Security Policy*- “a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations. [It] encompasses established rules that address specific security issues by providing instructions to the employees as to what they should do when they interact with the information and technology resources of their organizations (Bulgurcu, Cavusoglu, & Benbasat, 2010, pp. 526–527).”

*Security Breach*- An event that adversely affects the confidentiality, integrity, or availability of an organization’s information assets (Kannan, Rees, & Sridhar, 2007). Types of breaches can be classified as, but not limited to: release of viruses, worms, or Trojans; hacking;

unauthorized access; theft; fraud; human error; natural disasters; insider damage (Doherty & Fulford, 2005).

*Compromised Record-* A discrete piece of stored data that has had one or more parts that have been compromised in a security breach. The data can be pictured as one line in a database traditional tabular structure (Garrison & Ncube, 2011). Examples include one credit card transaction record or one user account.

*IT Governance Framework-* “used as a starting point by an organization to govern information security by developing guidelines and implementing controls to address risks identified by the organizations (Da Veiga & Eloff, 2007, p. 368).” Some examples of common IT governance frameworks are CobIT, ITIL, and ISO 17799.

*ISO Certification-* Official certification from the International Organization for Standardization (ISO). An organization must prepare for and pass a certification audit performed by an independent assessor in order to be registered (Brenner, 2007).

### **Assumptions and Limitations**

The study assumes some things about how information security policies and the overall organizational governance affect the behavior and performance of individuals within the organization. It assumes that information security policies formally define acceptable use of an organization’s information systems in the hope of reducing unacceptable use (Straub Jr., 1990). The more effective that an information security policy is at defining acceptable use and disincentives for going outside acceptable use, the less people will partake in unacceptable behavior, which lowers the vulnerability of the organization and lowers the number and severity of breaches (Beccaria, 2011; Straub Jr., 1990; Wiant, 2005). The number of information security

breaches and the number of compromised records can be used as a metric for measuring effectiveness of the overall information security of an organization (Doherty & Fulford, 2005; Wiant, 2005). Organizations that have an information security policy in effect, update it frequently, and have had one for a long time are more experienced in security management (Doherty & Fulford, 2005). While members of an organization ultimately have the choice to pursue acceptable behavior, more effective information security policies will share an overall correlation with better compliance (Bulgurcu et al., 2010).

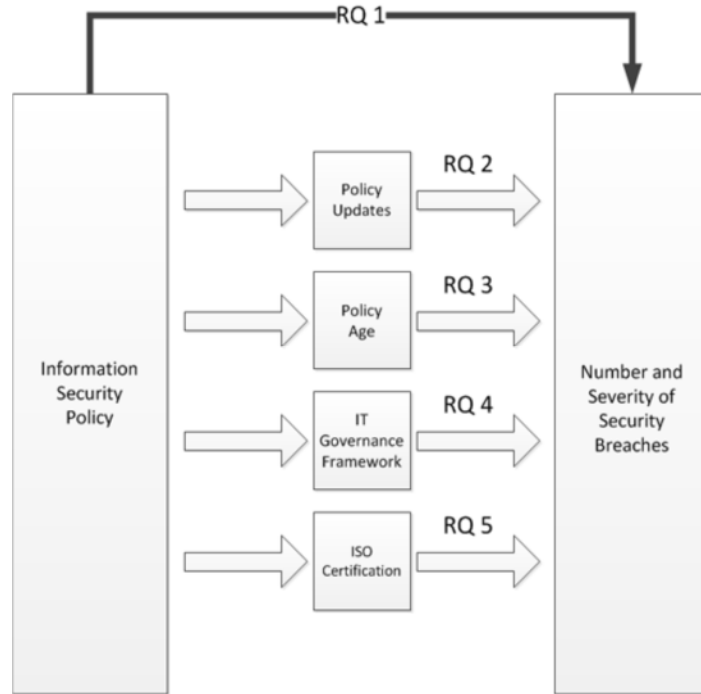
This study has an inherent limitation of not being able to directly measure enforcement. Any policy, no matter how well written or how often it is updated, can have much effect on the behavior of an individual without some form of formal or informal enforcement. Consequently, because this study measures the policy, governance, and ISO certifications versus the breaches experienced, there are dynamics going on in between that cannot be accounted for. The number of security breaches that occur and the number of records compromised because of breaches may be more closely related to execution of information security activities, such as end-user instruction, than to the information security policy (Hagen et al., 2008). An organization that has no information security policy, but has very self-disciplined employees may encounter fewer and less severe breaches than an organization with a very good policy, but no oversight or accountability.

Attempts were made to address this limitation. With a quantitative, positivist study such as this one, the number of variables is controlled and limits are set in order to accurately measure one small piece of what is going on. This study is designed to measure the piece that is involved with the information security policy, governance, and ISO certifications. Measuring

enforcement of the policies and exploring the effects on different types of enforcement is outside the scope of this project. If enforcement is measured at the same time, then the purpose of the study becomes muddled, and research questions are less direct; less clear. Enforcement of, or compliance with, information security policies involves a wide range of social, technical, and organizational factors which are not fully understood (Son, 2011). Researchers have tried to find what is effective: punishment, reward, peer pressure, firewalls, user roles. A myriad of tools and techniques have been explored to increase conformance with the information security policy (Basin, Jugé, Klaedtke, & Zălinescu, 2013; Khoury & Tawbi, 2012). But, the question that has not been empirically evaluated is “Do organizations that comply more closely with their information security policy suffer fewer breaches or have a lower number of records compromised?” This would be a worthy pursuit of another project.

### **Conceptual Framework**

Conceptually, this study attempts to continue bridging the gap between information security policies and information security breaches by conducting further exploration and validation of research that has been conducted in this area (Doherty & Fulford, 2005; Heikkila, 2009; Kwo-Shing Hong et al., 2006). Because this is a quantitative, post-positivist study, the research questions will be stated as hypotheses and tested directly against collected data with accepted statistical analysis.



*Figure 1. Conceptual Framework. The relationship of information security policies and the number and severity of security breaches is tested via the five research questions (Doherty & Fulford, 2005).*

### **Organization of the Remainder of the Study**

The study progresses through a full research cycle after this chapter. Following this section, a review of current literature is conducted which reveals the history, foundations, and trends of information security policy research along with the place of the policy within governance in general. The third chapter displays the research design of the study and provides justification for its construction. The plan for data collection and the basis for the formulation of the survey instrument are explained as well. Chapter four presents the raw findings of the completed survey without interpretation or discussion what the results may point to. The final

chapter summarizes the results, provides conclusions, and presents recommendations for further research.

## CHAPTER 2. LITERATURE REVIEW

### Introduction

This study focuses on effectiveness of information security policies, not the policy itself. Consequently, this review of the literature is organized around that topic, and explores the topics that surround it. Foundations of the information security policy, such as IT governance and deterrence theory, are explored first, to set the stage for extended discussion of the policy. Following review of information security policy literature, the ways that organizations attempt to enact the policy through organizational behavior and compliance are evaluated. A review of information security breaches conclude the review, as they are the critical litmus test of information security for the organization. The result should be a smooth journey through all facets of the effectiveness of the information security policy.

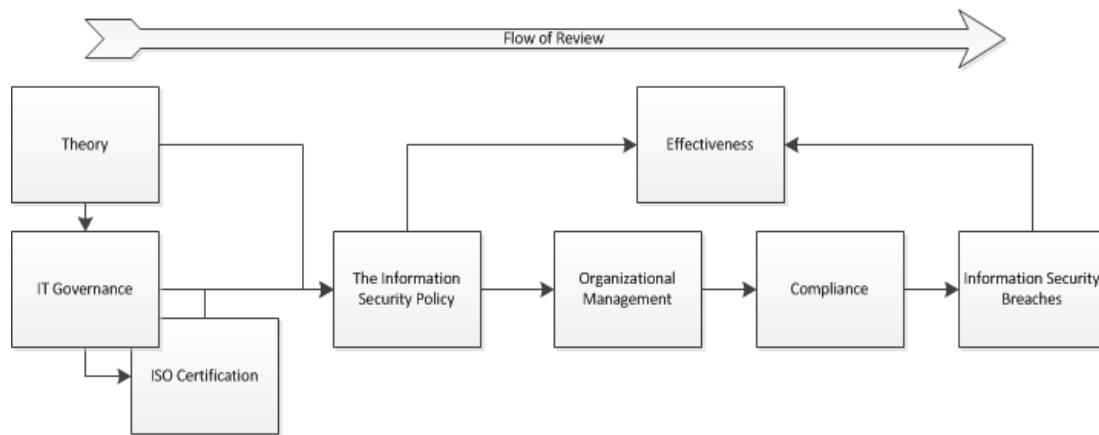


Figure 2. Literature review map

### Information Technology Governance

During the mid-1990's, organizations realized that spending unrestricted amounts of money on IT without carefully evaluating what results should be expected can be disastrous. Businesses found that investing in IT that was not aligned with their strategic goals resulted in



extra systems that did not give a tangible benefit, or worse, continued to incur costs. IT to business alignment evolved into what was referred to as IT Governance, which included frameworks and controls to help businesses keep their IT expenditures in step with their strategic plans and goals (De Haes & Van Grembergen, 2008, 2009; Simonsson, Lagerström, & Johnson, 2008).

Since that time, IT governance has come to be not only understood, but adopted by organizations that wish to keep IT investment under control. Frameworks evolved to help organizations create, organize, and set internal controls that would measure alignment and give solutions to help identify and correct misalignment. As De Haes and Van Grembergen (2008, p. 1) state, “the goal of IT governance is achieving a better alignment between the business and IT”. Similarly, Tarn et al. (2009) promote that the two objectives of IT governance are: “to ensure that IT investments create value for the business and to moderate any risks associated with information systems” (p. 133).

Part of IT governance is managing information security and the information security policy (Da Veiga & Eloff, 2007). Sometimes this subset of IT governance is referred to as information security governance, but it still falls under general IT governance in most research (Moulton & Coles, 2003). Managing security under one of the common IT governance frameworks such as COBIT or ITIL requires an information security policy especially if an international security certification such as ISO17799 or 27001 is desired (Da Veiga & Eloff, 2007). From the literature, it seems to be almost assumed that any organization willing to attempt to govern IT has to have security in mind, and that an information security policy is one

of the first requirements of an information security program (Knapp, Franklin Morris, Marshall, & Byrd, 2009).

Given the relationship of IT governance to information security and the policy, it makes sense to explore IT governance generally in order to give reasons and context for the information security policy. What follows is an examination of what IT governance means to an organization and why security is an important part of it.

### **Concept of IT Governance**

IT Governance may strike the researcher as “an ephemeral and ‘messy’ phenomenon, emerging in ever-new forms with increasing complexity” (Peterson, 2004, p. 7). An exact definition that transcends individual articles is difficult to come by, not to mention that the number of articles on IT Governance is low (Simonsson et al., 2008). Even so, Peterson (2004) provides a good starting definition that will suffice for this study: “IT governance describes the distribution of IT decision-making rights and responsibilities among different stakeholders in the enterprise, and defines the procedures and mechanisms for making and monitoring strategic IT decisions” (Peterson, 2004, p. 8). According to case studies, different organizations are at a continuum of levels of IT governance integration, and at different points of maturity (Marrone, Hoffman, & Kolbe, 2010; Tugas, 2010). Putting to use the complex network of decision-making rights and responsibilities and formalizing controls requires an organization to provide long-term commitment.

Just designing a network of communication and controls is not enough, however. The organization has to have an idea of what it wants to accomplish with the great effort of IT governance. “The goal of IT governance is not only to achieve internal efficiency in an IT organization, but also to support IT’s role as a business enabler” (Simonsson et al., 2008, p. 1).

Organizations have found that IT, just as with other investments, must be managed intelligently and aligned with the business strategy of the organization. Once the organization establishes decision-making networks, it is up to the decision makers to pursue the goal of making IT work with, and influence, business strategy. IT governance puts the strategy of the business into action, and also feeds back into strategy what IT is capable of, and any advantages that it has inherently, or that may emerge as a result of enabling strategy (Knapp et al., 2009).

In order to put strategy into action, IT governance must be properly deployed and executed, which is even more complex than defining it. Organizations that make the efforts to align business and IT through IT governance are taking on a great challenge, and they hope to obtain benefits because of it. Indeed, managers of some organizations feel that the benefits do not outweigh the costs, and either choose not to develop a formal IT governance program, or they enact a program simply to comply with legal regulations such as Sarbanes-Oxley (Braganza & Desouza, 2006). Other organizations report satisfactory success, especially the ones that put more effort and resources into development. Marrone et al. (2010) report that the more mature an organization is with COBIT, a popular IT governance framework, the more satisfied that they are with the outcome, and with the amount of business-IT alignment that they experience. Briefly visiting the evolution of IT governance will demonstrate how it works within organizations.

### **History of IT Governance**

Organizations learned the painful lessons of IT-business alignment after the dot-com boom of the 1990s. Organizations during the boom invested in IT just to be able to show shareholders that they were progressive and competitive with other businesses at the time.

Generally, it did not seem to matter much what kind of IT was being invested in, or if it had

anything to do with what the organization wanted to achieve strategically (Cross, 2004; Healy & Palepu, 2003; Sonnenfeld, 2004). IT was being invested in for IT's sake.

After the dot-com bust, many companies re-evaluated where they were committing their resources in terms of IT. Since the post dot-com boom period was characterized by more careful spending and more attention to improving traditional measures of the financial foundations of a company, organizations sought to get more results from their investments. Long-term maintenance of IT assets became more focused as companies looked past the initial cost and benefits, and considered how manageable the new resource was and how much it would contribute to strategy (Hardy, 2006).

Organizations discovered that they needed to govern IT just as they learned to practice overall governance in earlier years (Cross, 2004). Cost overruns, inefficiencies, and low or negative rates of returns on IT investment drove managers to start managing IT using tools borrowed from other types of organizational governance. Eventually, IT Governance took on its own identity in many organizations and was formally recognized as a legitimate way to strengthen the organization (Simonsson et al., 2008). IT became a core part of strategy, not just an enabler of it (Lainhart IV, 2000).

Once organizations recognized the need for IT governance, they needed a way to construct and mobilize it. General organizational governance had been in use for a while, and there were some qualities and characteristics that could be borrowed from it, but it was a far cry from being a simple, direct translation of controls and networks of communication and responsibility. Vast amounts of effort and resources from thousands of organizations began to try to formulate what IT governance should be, and what was effective. Many different

frameworks evolved, but only a few have fully developed into products that provide comprehensive guidance (Da Veiga & Eloff, 2007; Knapp et al., 2009). This is currently the point of IT governance development, and the continuing history of it starts today.

### **Qualities of IT Governance**

In order to be valuable to an organization, IT governance should produce good results. Good results, in this sense, would be to provide the best support possible to the organization and to maximize business-IT alignment (De Haes & Van Grembergen, 2008; Ruey-Shiang, Che-Pin, & Sheng-Pao, 2013). The uses, development, and investments in IT will then be more strongly related to business strategy, which reduces wasted resources and misdirected growth of the business. Maximization of business-IT alignment requires framing IT investments, protecting them, and leveraging their benefits to help feed back into strategy (Knapp et al., 2009). IT can be leveraged as a core strategy if it is governed properly. IT governance provides value delivery to the organization by managing costs and return on investment (ROI). Part of protecting value of an investment is managing the risks. Risk management is also a component of IT governance that requires transparency, honest evaluation of risks, and meaningful ways to reduce, eliminate, transfer, or accept risk (Hardy, 2006). Another part of providing value is to manage resources, which helps to provide cost savings and reduce wasted time. Performance measurement ensures that business-IT alignment is being met (Hardy, 2006).

Although the controlling of IT is important to IT governance, it should not be confused with IT management (De Haes & Van Grembergen, 2009; Ruey-Shiang et al., 2013). Governance is more concerned with helping IT meet the current and future needs of the organization and its stakeholders and customers. It is an executive function that focuses on performance and helping IT become a strong force of the organization for the future (De Haes &

Van Grembergen, 2009). It ensures that business strategy is executed within the boundaries of executive direction over a period of time; it is forward-looking. Management, on the other hand, focuses on maintaining present IT operations and making them efficient. Costs of present production of goods and services are kept low, while economy of scale, inventory turnover, and quality are kept as high as possible.

Other qualities of IT Governance are that it utilizes processes, structures, and relational mechanisms to foster business-IT alignment (De Haes & Van Grembergen, 2008). Processes relate to internal and external controls suggested by such frameworks as COBIT, or an IT balanced scorecard. Controls give management the ability to restrict, allow, measure, and scale organizational operations. Ideally, controls are set in such a way as to maximize business-IT alignment, and thus help IT governance meet its objective. Structures, on the other hand, are formal tools invoked by executive bodies, such as steering committees, to guide and measure IT. They relate to the “distribution of IT decision-making rights and responsibilities among different stakeholders in the enterprise” from the definition of IT governance provided by Peterson (2004) above. The relational mechanisms referred to by De Haes and Van Grembergen (2008) are less concrete, but just as important. They relate to the relationships between executives and managers; between governance and management. They help tie the strategy of the business in with the running of the business, and vice versa. All three components are equally and vitally important.

Information security can be considered as one of the prime qualities of IT governance. Without it, IT governance would be missing an integral part of taking care of IT investment, and organizational strategy would have an unwanted weakness. Information security may be one of

the more difficult governance elements to steer because of its lack of tangible returns (Drugescu & Etges, 2006; Gordon & Loeb, 2002). In addition, management of information security may be difficult because of the organizational challenges of getting the cooperation and compliance of employees as well as the challenging and changing nature of the threat (Tarn et al., 2009; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). In order to help conceive where information security fits into IT governance, it may help to picture it in terms of the five domains of IT governance as described by Hardy (2006): strategic alignment, value delivery, risk management, resource management, and performance measurement. Information security touches all of those domains to one extent or another (Ruey-Shiang et al., 2013).

While information security touches all of the domains, the ones that rely most on information security are risk management and resource management. Failures of security are seen as risks, and information security is closely aligned with risk management throughout the literature (Atkinson, 2005; Fariborz, Shamkant, Gunter, & Philip, 2005; Pironti, 2008). Amir Ameri (2004) created the five pillars of information security based on risk management practices of: protection, detection, reaction, documentation, and prevention. Resource management entails not only using resources as sparingly as possible, but protecting those resources as well. Information assets are some of the most valuable in the company, so they would require some of the best protection (Poore, 2005). Breaches require expenditure of time, money, and specialized personnel in order to recover, and the breach may have caused damage to the information resources of the organization. Such recovery can be very expensive and painful. The CSI Computer Crime and Security Survey (Peters, 2009) estimates that the average losses due to information security breaches to be between \$168,000 and \$345,000 annually per organization.

There are also probably intangible losses such as reputation and customer perception and satisfaction that are hard to measure. Information security is such an important part of IT governance that it is included in many of the most popular frameworks.

Many IT governance frameworks specifically list security as their core processes (Ramlaoui & Semma, 2014). In COBIT 5, security is listed in the align, plan, organize (APO) domain, and in the distribute, service, and support (DSS) domain. ITIL lists information security management in its service design processes. Additionally, CMMI and PMBOK have notable sections of their frameworks dedicated to risk management, which probably is the hierarchal parent of security in these models. Even if not specifically listed, information security is a notable component of IT governance, either by definition or by direct reference within commonly used frameworks. Sometimes in the literature, information security is so important to IT governance that it is referred to as information security governance.

### **Information Security Governance**

Similar to the way that IT Governance is concerned with ensuring that IT and business are aligned strategically, information security governance also seeks to maintain alignment in IT Security investments and development. “Information security governance can be described as the overall manner in which information security is deployed to mitigate risks” (Da Veiga & Eloff, 2007, p. 362). Another definition is offered by Moulton and Coles (2003, p. 581) “the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems”. Both definitions provide the same core idea, which is very similar to IT governance: it distributes information security decision-making rights and responsibilities among different



stakeholders, and it defines the procedures and mechanisms for making and monitoring strategic information security systems.

There are some differences between IT governance and information security governance: structure, measures and controls, and resource prioritization (Poore, 2005). One difference is that the organizational structure cascades through the chief information security officer instead of the chief information officer (CISO). Parts of the organization concerned with technical security, identity and access management (IAM), and vulnerability assessment (VA) fall under the CISO and differ from the ones that fall under the chief information officer (CIO) (Poore, 2005). The controls, measures, and metrics are also different. “Traditional metrics, such as return on investment (ROI) and budget compliance, may prove problematic” (Poore, 2005, p. 4). Consequently, security investment measures and metrics were developed based on traditional ones (Gordon & Loeb, 2002; Tichenor, 2007). One of the more common examples is Return on Security Investment (ROSI), which is based on the traditional attempt to define the value of an investment based on its expected future returns using ROI. ROSI uses an additional manipulation of the calculations in order to try to capture the deterrent effect of security and the intangible benefits realized by a lack of breaches. Resources are prioritized differently when governing information security as well. An investment that is expected to produce no monetary return may be placed above an investment that will provide one in order to achieve business goals when security is taken into consideration.

Given all the complexity of IT governance, information security, and information security governance, organizations have a difficult time knowing what to adopt and where to start if they wish to govern their IT resources and protect them (Lainhart IV, 2000). Some

organizations create their own governance systems, but others look to standards, best practices, and published frameworks.

## **Frameworks**

Given the immature, complex and vaguely defined foundations of IT Governance, it is understandable that organizations would seek out concrete guidelines that could help them form their own governance and be able to compare it to other organizations and industry standards. Because of this need, IT governance frameworks evolved in the late 1980's and became popular around 2000 (Lainhart, 2000). What follows is an overview of the concept of frameworks and a review of some of the most popular frameworks available.

IT Governance frameworks are a popular method by which organizations can evaluate their level of IT to business alignment maturity. They also provide a list of tasks and competencies to invest resources in to help increase alignment. The assumption about IT frameworks is that they have been carefully structured and tried by other organizations. Case studies and success stories are published by some of the more prevalent framework organizations, like COBIT, and promoted to industry in order to garner support for the framework. Frameworks that are popular have advantages of scale, common core elements, widespread communication, standards, and certifications. All of these things can be shared between heterogeneous organizations, making pursuit of IT governance available for a wide range of businesses regardless of size, industry, or level of IT integration.

Taking advantage these frameworks is not easy, though. The lists of competencies to develop can be daunting, and require substantial money, personnel, equipment, and time to put into action. Some organizations decide such investment is not worth the benefits (Simonsson et

al., 2008). Other organizations settle for a certain level of maturity within a framework, understanding that satisfying every requirement may not be possible, or even worthwhile.

**COBIT.** Control Objectives for Information Related Technology (COBIT) is the leading IT Governance framework used currently in the world (Hardy, 2006). COBIT started in 1996 and has gone through several versions. Published by the ISACA, COBIT 5 combines the qualities of COBIT, Val IT, and Risk IT. Part of its appeal is that it provides a comprehensive approach to the governance and management of IT, so it is not strictly an IT governance framework alone. Comprehensive in the case of COBIT is extreme: it covers the entire enterprise with one single, integrated framework (Ramlaoui & Semma, 2014). COBIT seeks to enable business-process owners by assigning them full responsibility over their business processes and giving them the tools to measure and control them.

The control model of COBIT is divided into four domains: plan and organize, acquire and implement, deliver and support, monitor and evaluate. Within those four domains live 34 processes that support their respective domain. For example, in the planning and organization group, there are processes such as: define a strategic plan, determine the technological direction, and manage quality (Hardy, 2006; Lainhart, 2000). In the delivery and support group: define service levels and ensure system security. Reviewing the controls shows a continuum that covers both IT Governance and management at a high level, with a goal of translating business objectives into real, measurable activities by the organization. By balancing and reporting on information technology's use of controls, COBIT helps IT form a complimentary relationship with business strategy, where IT can not only execute strategy, but can also influence it (Hardy, 2006; Lainhart, 2000).

In addition to controls, COBIT measures maturity. This quality can be very important to organizations so they can evaluate how they compare to other organizations, even if they are from different industries or have differing goals. The path to maturity shows the next steps that the organization can follow, and it shows how much progress has been made. This is appealing to stakeholders because it portrays the state of IT in an effective, accurate, and simple way (Hardy, 2006).

Organizations can also communicate more effectively when utilizing such a well-known framework as COBIT. They can use terminology that translates between organizations that are using the same framework. For example, an auditor could review how organizations define a strategic plan in an equal way, and against the same metric. Using the same core terminology allows aggregation of results which is especially useful for multi-business unit firms (Fonstad & Subramani, 2009).

Information security, as previously noted, is built into COBIT, but, because COBIT is very high level, some have criticized it as being weak on security (Tuttle & Vandervelde, 2007). As a result, standards such as ISO 17799 are used as security frameworks to focus on some of the higher risk processes. “Focus on the ISO/IEC 17799 standard is warranted, given that it provides the most comprehensive approach to information security management. The other best practices [COBIT] focus more on IT governance” (Saint-Germain, 2005, p. 61). While this may be seen as a shortcoming of COBIT, it also stands as evidence of the framework’s flexibility and allowance for other systems to incorporate with it. Another system that works well with COBIT is ITIL.

**ITIL.** Information Technology Infrastructure Library (ITIL) approaches IT governance from a service management perspective. “ITIL is a set of comprehensive publications providing descriptive guidance on the management of IT processes, functions, roles and responsibilities related to service delivery and service support” (Pollard & Cater-Steel, 2009, p. 165). It is more of a bottom-up approach than the hierarchal model of other frameworks such as COBIT. ITIL focuses on continual management and improvement of IT delivery. It may sound too shallow for an IT governance framework to only focus on end service delivery, but, in order to enact measurement and improvement in the end product or service, the entire organization has to be engaged (Pauli, 2008). Excellence in service can only come about when all the other governance and management structures are in place and functioning well. “Presenting a better face to users is at the heart of ITIL” (Anthes, 2005, p. 39). Since ITIL has demonstrated success improving IT service delivery for the business and the customer, it has become very popular. One benefit of being a bottom-up governance model is that it can be used with other frameworks such as COBIT (Ramlaoui & Semma, 2014).

ITIL originated in the UK in the 1980s, and enjoyed prosperity throughout Europe in the 1990s. The UK Central Computer and Telecommunications Agency (CCTA) started ITIL, and since then it has gone through a couple of versions. ITILv2 was augmented by ITILv3 in 2007 and introduced lifecycle management for IT services not just individual products or applications. ITILv3 represents the attempt to align IT service delivery with the core business strategy, which gives the framework more of an IT governance approach as opposed to mostly a management approach.

Organizations should be prepared to understand that ITIL will not save money right away, but that long-term strategy and returns from an overall improvement in process delivery will be the advantage (Pauli, 2008). Putting ITIL in place takes a lot of time and money. Service delivery will not improve very much immediately as it takes time for the efforts that are put into organizational structure to happen. Fifth Third Bank reportedly spent \$1.2M out of a \$250M budget just to implement 3 out of 10 ITIL processes (Anthes, 2005). Using ITIL on everything IT may not be the best use of resources either. Because it is a modular framework, it can be applied in stages or only in the needed areas to keep administration to a minimum. Proctor and Gamble provides an example of this when they first started using ITIL in the 90s. They started with only 2 out of the 10 available ITIL components: incident management and configuration management, in an attempt to curb outages (Anthes, 2005). They eventually adopted problem management, change management, and help desk management as they were able to become more proactive.

Similar to COBIT, ITIL is not focused only on security, which may mean that it alone is not sufficient to control security sufficiently. Companies seek to adhere to standards that will meet compliance guidelines such as HIPAA and SOX in addition to governing IT. That is where ISO security certifications come into play. They are considered frameworks in their own right, and are focused on the specific, specialized needs of information security.

### **ISO Certification**

ISO certifications are an essential part of compliance and are considered to be a measure of quality for an organization regardless of size, industry, or nationality. While they would seem to be more of a certification to a standard, researchers consider them to be IT governance and IT

security governance frameworks in their own right. Robinson (2005) and Saint-Germain (2005) claim ISO/IEC 17799:2000 as frameworks, listed alongside COBIT and ITIL. Tarn et al. (2009) also group ISO certifications in with COSO and COBIT. How can certification standards be considered governance frameworks? They do not seem to be the same type of construct. The common quality seems to be that both the IT governance frameworks and the ISO certification standards reflect best business practices and provide clear, concise lists of controls to implement. This is very attractive to organizations that are struggling to find answers to very complex and obscure problems such as solving how to invest in IT (Marrone et al., 2010; Tugan, 2010). Both types provide solutions for managing and governing IT and information security.

There are many ISO certifications. In the interest of the scope of this study, only the ISO certifications that are generally the focus of information security will be included: ISO 27001- information security management systems and ISO 27002- information security management controls. There are different versions of each that utilized different numbers in the past. The literature references different numbers throughout, and the ISO number that is referenced depends on when the article was written.

### **ISO 27001**

The aim of the ISO 27001- information security management standard, developed by BSI, is to help an organization implement security management and controls without focusing on technology. It is a set of standards that enables the creation of an information security management system (ISMS) that can steer the organization in covering all the necessary topics and establishing all the needed controls to manage risk and to be compliant (Brenner, 2007). The standard is broad enough to be able to address compliance in a broad range of requirements if fully implemented. Organizations consider that a core strength given the rapid change of laws in

the financial and healthcare sectors because the organization can be compliant even before new legislation is introduced (Fitzgerald, 2006). It is also technologically agnostic, and can be applied in an organization with any level of IT resources (Brenner, 2007; Tarn et al., 2009). The standard also provides full guidance on needed risk management items such as: risk assessment methodology, risk assessment reports, treatment plans, and other documented procedures (Brenner, 2007). Organizations that certify in this standard are assumed to have achieved a high level of formal information security management, which may be appealing to their stakeholders.

### **ISO 27002- formerly ISO 17799**

The ISO 27002 standard is the most prevalent certification in regards to information security today, and is probably the most popular in use. “The ISO/IEC 17799/BS 7799 best practice framework provides a set of best practices and controls that address the essential issues of information confidentiality, availability, and integrity existing at the heart of regulatory efforts” (Saint-Germain, 2005, p. 66). It originated as BS7799 in England and became the famous ISO 17799 later when it was instituted internationally (Theoharidou et al., 2005). ISO 27002 is a collection of security best practices and controls, with one of the most prominent being the information security policy (Saint-Germain, 2005). The standard is broad, and encompasses more than just the technical aspects of information security such as physical and personnel security (Saint-Germain, 2005; Theoharidou et al., 2005). It aims to be an all-encompassing approach to managing security based on best practices. At its core, ISO 27002 has ten domains that exhibit just how broad it is: security policy, organizational security, asset classification and control, personnel security, physical and environment security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance. Many organizations use this



particular set of controls to achieve and maintain compliance with a variety of laws, including the very impactful Sarbanes Oxley Act (Wallace, Lin, & Cefaratti, 2011).

### **Sarbanes Oxley**

“Nothing has driven the current climate of intense high-level board attention to IT governance, control and security more powerfully than the Sarbanes–Oxley Act (SOX)” (Hardy, 2006, p. 57). Even though a piece of legislature may seem a bit out of place in an academic study as a foundational element, SOX is such a widespread, impacting law for IT governance that it ends up being a strong driver of not only IT governance implementation and compliance, but also development. SOX comes up again and again in a review of IT governance and IT security governance literature, often paired with IT solutions to address the law such as COBIT and ISOs (Braganza & Desouza, 2006; Brown & Nasuti, 2005; Edelstein, 2004; Hall & Gaetano, 2006; Pabrai, 2006; Wallace et al., 2011). SOX forces American traded companies, regardless of location, to follow its rules and to enact a complete form of governance. Because some organizations did not actively pursue governance pre-SOX, they sought to quickly get a framework to help them. COSO and COBIT are the most popular frameworks for SOX compliance, and augmenting with ISO 17799 or ISO 27001 helps insure the confidentiality, integrity, and availability of their reporting data. These frameworks work as a roadmap for setting up all the controls needed to be SOX compliant.

Sarbanes Oxley was initiated on the coattails of the controversial collapse of Enron, WorldCom and other big corporations. Specifically, section 404 “requires the management of publicly traded corporations to establish internal controls over their financial reporting systems and test these controls to ensure their effectiveness” (Jory, Peng, & Ford, 2010, p. 285). Section

404 assigns direct responsibility to management for the actions of their systems. Ignorance cannot be claimed as an excuse anymore for a failure as management has to guarantee that all the needed controls are in place. The legislation has had impacts worldwide, as the location of the corporation does not matter, as long as it is traded publically in an American market.

### **Theory**

This section provides a brief review of governance and management theories that have been applied to IT and information security governance and management. Several theories fall into IT governance. The most prominent are: agency theory, institutional theory, shareholder theory, and stakeholder theory. They are not exclusive, but may work together to help explain the underlying dynamics of the relationship between owners and decision-makers of an organization.

#### **Agency Theory**

Agency Theory is a concept of conflicting interests that are inherent in the structure of an organization (Poole, 2009). The theory fits most closely in a corporation, but is still evident even in non-corporate organizations. In agency theory, shareholders that give decision-making responsibility to the executives, directors, and managers, who are referred to as agents, represent the owner, called the principal. A problem arises when the agents fail to make decisions that are in the best interest of the principal. Maximization of shareholder wealth is usually the goal of the principal, but sometimes, agents pursue things that do not maximize wealth. They may try to maximize a bonus, or perform well on a project at the expense of company resources or wealth (Braganza & Desouza, 2006; Feizizadeh, 2012).

The reason that this theory plays in with governance in general, and IT governance specifically, is that governance attempts to provide transparency and control to the principal so that the agents' decision-making aligns more completely with what the principal needs (Daily, Dalton, & Cannella, 2003). Properly constructed controls keep business strategy and IT aligned. They also protect shareholders from agent decisions that may not be in the best long-term interests of the organization. Institutional theory is closely related to agency theory, but it has a broader scope of influences to the organization.

### **Institutional Theory**

Argued by Braganza and Desouza (2006) to be a better approach to analyzing SOX compliance than agency theory, institutional theory involves the environment in which an organization exists and how that organization tries to maintain legitimacy by conforming to rules and regulations. Institutional theory includes many more actors than simply a principal and agents, as agency theory does (Jensen, Kjærgaard, & Svejvig, 2009). Instead, many internal and external stakeholders and the organization are used. The stakeholders exert pressure upon the organization, causing it to react in some way. The pressures exerted are classified as coercive, mimetic, and normative. Coercive pressures are delivered by organizations onto organizations which they depend upon; a parent-child relationship. Mimetic pressures influence organizations to be more like other competitors, while normative pressures involve motivation towards the ethics and standards of peers (Rowlands, 2009; Sherer, 2009).

Describing institutional theory in terms of IT governance may provide clarity and relativity (Braganza & Desouza, 2006). For example, an organization may adopt an IT governance framework such as COBIT to alleviate all three types of pressure. SOX compliance may be mandated not only by the SEC, but by a parent company, both of which exert coercive

pressure. Other competitors in the industry may adopt COBIT to show that internal and external controls and governance are important and to show that they wish to be compliant with SOX, thus pressuring the organization to follow suit through mimetic pressures. In addition, the social acceptability of implementing adequate controls in order to keep people from becoming victims of corporate mismanagement would exert normative pressures. All of these combined pressures would influence the organization towards adoption of COBIT.

### **Shareholder and Stakeholder Theory**

The theories above referred to stakeholders and shareholders as key players when evaluating organizations. Conceptualizing these key players in the proper frame is important to understanding agency and institutional theories. Consequently, there are also theories behind what stakeholders and shareholders are. Stakeholder theory evolved from shareholder theory, which became prominent around 2009, and reflects more of a community approach to organizational theory (Tse, 2011). Comparing agency and institutional theory, one can clearly see that agency theory has a narrow view of what group cares about the performance of an organization, shareholders, while institutional theory has a much larger scope of actors that care about the performance of an organization, stakeholders. Shareholders are simply people that own a part of the organization, usually in the form of corporate shares, while stakeholders are people or things that have tangible or intangible investments in an organization. Shareholders are treated as an external entity while stakeholders are a mix of internal and external entities (Braganza & Desouza, 2006; Moore, 1999; Tse, 2011).

Shareholder theory has several advantages, and is very mature when compared to stakeholder theory, having enjoyed at least 45 years of prominence in accounting and organizational theory (Moore, 1999; Tse, 2011). It simplifies organizational complexities into

one main goal; long-term maximization of shareholder wealth. Viewed in this light, application of this theory becomes familiar business strategy and creates fertile ground for IT governance. Aligning IT investments and practices with business strategy should maximize shareholder wealth in the long term. As stated by Feizizadeh (2012), corporate governance is an artificial mechanism to compensate for imperfect markets and imperfect competition by attempting to close the agency theory gap between the interests of the principal, maximization of wealth, and agent interests, which are usually a variety of short-term individual benefits. IT governance, in the light of shareholder theory, provides the vehicle to align the principle/agent interests. All of the internal and external controls, objectives, and maturity models boil down to helping maximize shareholder wealth.

The results of using the same logic with stakeholder theory provide similar results, but with a different semantic view. Stakeholder theory is far more integrated and widely-scoped, encompassing not only shareholders, but a variety of internal and external entities that have an interest and reliance on the organization (Braganza & Desouza, 2006; Moore, 1999; Tse, 2011). The theory suggests that managing stakeholders will make the organization stronger and more profitable financially, not just because the shareholders and managers have aligned their interests and decision-making, but because all groups that can exert pressure on an organization will benefit. IT governance becomes a mechanism with which stakeholders can interact and create overall wealth, and not just shareholder profits. Stakeholders are actively integrated into IT governance efforts and use it as a tool for gaining overall wealth.

## **Integrating the Information Security Policy into IT Governance**

So far this study has provided a review of governance in general, and IT governance specifically, to form a foundational understanding of the stage upon which the information security policy is set. At this point of the literature review, there should be an understanding that there is an expectation from the organization. Shareholders, management, auditors, customers, employees, and other stakeholders all expect the organization to take certain responsibilities in regards to governing and managing IT resources and investments. Several of those responsibilities, risk management, resource management, asset management, compliance, and a general need to protect the confidentiality, integrity, and availability of information, fall under information security. Essentially: good information security contributes to good governance, and “Simply put, good governance—enterprise and IT—is good business” (Lainhart IV, 2000, p. 33).

Given the currently presented literature, it is clear that there is a valid, strong need for good information security within an organization. The question then becomes; how does an organization ensure that their information is secure? While there are many methods, techniques, technologies, and frameworks to answer this question in part, there is one overriding concept that is ubiquitous: the information security policy (Bulgurcu et al., 2010; Fulford & Doherty, 2003; Higgins, 1999; Höne & Eloff, 2002; Knapp & Boulton, 2006; Straub et al., 2008). Without an information security policy to outline the basic expectations and concepts of information security to the organization, application of disjointed technology, techniques, and standards falls apart logically. For an organized, complete effort towards information security, an information security policy must be constructed, implemented, and formally supported by management (Höne & Eloff, 2002). The following part of the review of literature will focus on providing a

complete view of the information security policy and its related concepts, theory, and application.

### **Information Security Policy Theory**

Whereas corporate and IT governance theory is based in agency, institutional, shareholder, and stakeholder theories, the information security policy focuses on defining, guiding and enforcing actions within the organization (Fulford & Doherty, 2003; Höne & Eloff, 2002). The theory base turns from one of ownership and responsibility to one of scope, definition, and enforcement. The forefront of information security policy theory is one that has been used for many years to explain the workings of legal systems, criminology, compliance, and human behavior: deterrence theory (Beccaria, 2011; Jintae & Younghwa, 2002; Knapp et al., 2009; Siponen, Pahlila, & Mahmood, 2010; Straub et al., 2008).

### **General Deterrence Theory**

Rooted in criminology, deterrence theory attempts to explain how people make compliance decisions based on benefit maximization and minimization of cost (D'arcy & Herath, 2011). Cesare Beccaria founded it during the mid-1700s. His pivotal work entitled *On Crimes and Punishments* advocated for a break from some of the more traditional methods of deterrence such as capital punishment and torture. He promoted the ideas of punishment that fit the crime and codification of laws that would be applied equally to all, regardless of station (Carpenter, 2010). Reflective of this experience, deterrence theory posits that the higher the perception of certainty, severity, and swiftness of sanctions results in deterring more individuals from making illicit decisions.

Several researchers have applied deterrence theory and its constructs to information security, focusing on employee compliance with security policies (D'arcy & Herath, 2011; Lee, Lee, & Yoo, 2004; Siponen et al., 2010; Straub, 1990; Theoharidou et al., 2005; Wiant, 2005). Straub (1990) found that information security deterrents resulted in reduced incidence of computer abuse. D'arcy and Herath (2011) found a construct that was a bit more complex. They found that there have been disparities in information system use of deterrence, and they suggested being aware of contingency factors and methodological issues that may cloud the results. Self-control, computer self-efficacy, moral beliefs, virtual status, and employee position all could cause variations in the deterrent effect. Additionally, the disparate measurement of sanction constructs in research result in different results. Siponen et al. (2010) found that deterrence was significantly related to actual information security policy compliance, while normative beliefs, threat appraisal, self-efficacy, and visibility were related with the intention to comply. Theoharidou et al. (2005) found that ISO 17799, a popular information security standard, follows general deterrence theory. Lee et al. (2004) acknowledges general deterrence theory and uses it as a leverage point to introduce the possible usefulness of social control theory application to information security. Overall, general deterrence theory is the only visible theory that is directly related to the information security policy and compliance with the policy. Now that the underlying of the information security policy has been discussed, the review will focus on what the information security policy should be to an organization.

### **Information Security Policies**

Information security policies represent the pivotal point of transition from concepts, frameworks and abstract construction of IT governance and information security to the



engagement of empirical, practical, and concrete action. The policy is the portal where members of the organization learn what is expected of technical and human resources that are part of the information assets. The precepts, guidelines, and expectations that the organization wishes to communicate about information security to managers and employees should be contained in the information security policy. It defines acceptable use of the information assets of the organization (Da Veiga & Eloff, 2007; Höne & Eloff, 2002).

Just having a document that contains expectations would not be enough, however. The document should also incorporate governance and management elements to align information security with the business goals, and to provide guidance on how to direct and enforce compliance with the policy (Doherty & Fulford, 2006; Höne & Eloff, 2002). In order to accomplish those goals, the information security policy should be accurately aligned with the business and governance efforts of the business. It should also have reasonable actions for managers to take to ensure that the things that need to be done to achieve business goals are met. It should educate the intent of the organization and provide guidance for carrying out those activities. Otherwise, information security would have gaps and efforts pushed in various directions, possibly not in the best interests of IT governance or strategic business goals. These qualities, among others, drove Hone and Eloff (2002) to claim “Undoubtedly, the singularly most important of [information security] controls is the information security policy” (p. 402).

### **Importance**

There is little doubt in the literature that the information security policy is an important document. Several researchers have shown that the concept of a singular reference for information security behavior is valuable not only for the users of the system, but to managers and executives in steering the governance of information security within their organization

(Fulford & Doherty, 2003; Higgins, 1999; Höne & Eloff, 2002; Siponen et al., 2010; Wiant, 2005). The security policy should define what types of information require protection, how to protect it, and also have management's endorsement of the policy (Höne & Eloff, 2002; Wiant, 2005). Without this kind of formal definition, the whole effort to secure information assets could fall apart (Higgins, 1999).

In addition to the reasons given above, sometimes the law requires an information security policy, or it is required in order to meet standards. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) security rule requires several security elements to be outlined in policy such as administrative, physical, and technical safeguards. The organization must also update its policies and keep them current (U. S. Department of Health and Human Services, 2010; Wiant, 2005). Organizations wishing to comply with SOX must have an information security policy, usually compliant with ISO 17799 or ISO 27002 (Pabrai, 2006; Wallace et al., 2011). Pabrai (2006) also includes a list of other laws that may require an information security policy to be actively used: Federal Information Security Management Act (FISMA), Food and Drug Administration Title 21 CFR, along with various state government laws. In addition to meeting laws, organizations may want to be compliant with standards and frameworks such as Basel II, ISO 27002 or COBIT. All of these require an information security policy and possible some subordinate policies based upon it.

### **Structure**

Given that the information security policy is important to the organization, understanding what a good information security policy should contain is critical to fill the need for one. After all, good performance should not be expected if the policy is designed poorly (Bulgurcu et al., 2010). Managers should be able to have enough material in the policy to enforce it with their

personnel. They should also be able to reference the policy in order to make information security investment decisions that are in line with the strategy of the business. Technical workers should be able to reference the policy to ensure that systems are configured to enforce security in accordance with the policy so that holes are not left open in the infrastructure.

While researchers have provided quite a bit of guidance on the role, importance and formulation of information security policies, very little has been written to address the content of them (Doherty et al., 2009; Doherty & Fulford, 2006).

“In sharp contrast to the literature on the structure of the [information security policy], which is plentiful but lacking in empirical contributions and consensus, the academic discussion of the specific issues that should be addressed by the [information security policy] is simply very sparse” (Doherty et al., 2009, p. 450)

Even so, the basic elements and characteristics of the policy can be gleaned from the current literature.

**Elements.** Overall content of a policy should contain certain base elements in order to cover all aspects of information security for an organization. This is stated clearly by Höne & Eloff (2002) in one of the seminal documents on information security policy content. Their work provides a concise guide as to what the policy should contain, and why. They explain that the need and scope of a policy should be established so that managers and users can understand why there is a policy and to what extent it should be exercised. Objectives of information security in terms of the organization should be aligned with the strategy of the business so that the transition from governance to management is able to take place. A clear definition of information security should be provided so that members can gain a unified idea of what

information security means to the organization. They argue that the “singularly most important statement in an information security policy” (p. 403) is management’s commitment to information security, and it must be explicitly stated. The purpose and objective of the policy itself, not information security in general, should also be stated. Additionally, a section on the principles of information security should describe rules of the organization in regards to certain types and methods of security topics. For example, the general method in which a firewall is used to block network traffic to protect a server would be a principle that would probably be similar throughout the organization, and may be included in the policy. This section would change over time and need to be updated (Höne & Eloff, 2002). They also explain that roles and responsibilities of users and individuals should be expressly stated. This would include outside vendors, casual users, managers, and administrators. Violations and disciplinary action should be firmly put in place in the policy as well, otherwise, users will not have anything with which to evaluate the value of adhering to the policy (Bulgurcu et al., 2010; Höne & Eloff, 2002). For discipline to be able to be given, a clear description of expected punishment should be available and backed by management. The way in which the organization conducts monitoring and review is another important item to explain in the policy. The organization can hold people accountable only if their monitoring policies are reasonable, according to court rulings, and reasonable monitoring involves notifying users that they are being monitored (Wakefield, 2004). A user declaration and acknowledgement should be a distilled version of the policy as it applies to an individual. It should be short and clear and should outline what is expected from the user, and should be signed before employment and periodically afterwards. The policy should also cross-reference other organizational policies, guidelines, standards, and processes. Höne and Eloff

(2002) also go on to explain that a policy must also have certain characteristics in order to be received well by stakeholders.

**Characteristics.** Just as important as what is contained in the policy, the way it is presented can affect how members of the organization perceive information security (Höne & Eloff, 2002). The policy should be as short as possible and easy to read. The organizational culture should be reflected in the document but should be stated in terms that everyone in the organization can understand. Visual impact of the policy should also be considered. The policy should be reviewed periodically to ensure its relevancy and accuracy. Information security is a rapidly evolving field and policies can quickly become outdated with new technology or adversarial methods. One of the most essential characteristics of the policy is that it is practical, realistic, and implementable. It should also be easily communicated throughout the organization. A security policy that can balance these characteristics along with good content would have better chances of being absorbed and followed by members of an organization. But, what is the current state of the contents and characteristics of information security policies? How do they match up to the standards set by Höne & Eloff (2002)?

### **Empirical State of Information Security Policies**

While frameworks and guidelines abound for the role and importance of information security policies, results from studies that evaluate real policies show that there is a wide disparity of content. They exhibit a lack of coverage in essential information security issues, especially non-technical ones (Doherty et al., 2009). Wiant (2005) expresses “Corporate information security policies have historically been unfocused until an external ‘threat’, or most often a regulation confronts them” (p. 453). Unfortunately, the guidance that organizations are relying on, namely IT governance frameworks or ISO certifications, are not consistent in

declaring what an information security policy should contain (Höne & Eloff, 2002). So, it is little wonder that the true content and characteristics of information security policies may vary widely. Even with a good policy, though, it may be troublesome for an organization to instill or enforce secure behavior in its members. That is where security management plays a role.

### **Organizational Security Management**

Given that an information security policy can be viewed as a transition point between governance and management, no security policy should be effective without ways to ensure compliance (Bulgurcu et al., 2010). Part of the responsibility for the effectiveness of an information security program falls on the management of what is distributed in the policy. An organization that cannot manage its users or the technology that it has for resources cannot really expect policy in general to be effective, and should not expect effective information security no matter how well the information security policy is written. Conversely, an organization that is good at management, but has a poorly constructed policy would also see an impact on the effectiveness of information security, but it would be in the form of disparate, uncoordinated efforts that would leave huge gaps. The focus of this section of the review is to cover the research on security management, what it entails, what some of the challenges are, and what is effective.

#### **Compliance**

The most prevalent theme of security management in regards to the information security policy is compliance (Bulgurcu et al., 2010; Tarn et al., 2009). Organizations struggle with understanding how to keep users of information systems within the boundaries set by security managers. Information systems by default give a lot of freedom, and many users require access

to a number of them, sometimes with administrative abilities. Restricting that behavior technically poses problems, as users cannot perform work efficiently much of the time (Hagen, Albrechtsen, & Hovden, 2008). When a user works within a narrowly defined set of access, they continually bump up against the technical controls, which are unforgiving and hard to change. The problem compounds when the user has to take over the duties of someone else, or needs to do work outside their normal routine. Additionally, the user may use workarounds, such as writing down passwords on a sticky note and placing it on the monitor, which technical measures cannot stop (Albrechtsen, 2007). Administrative measures can be put in place, but compliance with these is ultimately up to the user. A manager may catch the user after the fact, but by then the damage may have been already done. Humans are the weakest link when it comes to information security (Cox, 2012; Hazari et al., 2008; Lineberry, 2007; Tarn et al., 2009). Therefore, the question that plagues organizations is how to proactively encourage employees to behave in a secure manner.

Researchers have attempted to explain compliance with information security policies using behavioral science methods and theory (Cavusoglu & Bulgurcu, 2010). They seek to understand why users comply or not, and seek ways in which compliance can be encouraged. Generally, users state that they intend to engage in secure work behavior, but do not properly perform secure individual actions (Albrechtsen, 2007). Security is seen as a barrier to getting work done (Hagen et al., 2008), and users usually get compensated for performing work, not for being secure. Hazari, Hargrave, and Clenney (2008) attempted explaining compliance behavior using the theory of planned behavior for users that performed work related computing activities from home. They found that attitude and confidence were related to knowledge of security and

the intent to maintain security awareness. Knowledge of security problems, issues, and current concerns can help users want to be more compliant. Albrechtsen (2007) showed an inverse relationship between the frequency and effectiveness of organizational formal controls, such as the information security policy, and security awareness training. Formal policies, while the most frequently used, were deemed to be the least effective by users, while security awareness training, the least used, was shown to be perceived as being the most effective. Perhaps information security is still at a stage where frameworks, policies, procedures, and formal controls are being focused on more than what should be the results of those efforts, such as users that are effectively trained and knowledgeable of information security risks and proper actions. Unfortunately, there are consequences when employees are not knowledgeable, trained, or compliant with secure behavior. The result: information security breaches.

### **Breaches**

For a full understanding of measuring information security empirically, security breaches must be explored (Doherty & Fulford, 2005; Wiant, 2005). Breaches are used often in the literature as a measure of the effectiveness of information security, and they provide concrete, quantifiable numbers for evaluation (Doherty & Fulford, 2005; Garrison & Ncube, 2011; Romanosky, Telang, & Acquisti, 2011). Some studies rely on metrics such as executive perception of security, which may be easier to obtain, but are harder to ground in reality (Kwo-Shing Hong et al., 2006). Breaches appear to be an attractive measure of the true success of an information security program, even though there are other measures that could be just as important, such as deterring the surveillance, penetration, theft, or destruction of information integrity, but these are very hard to measure (Tichenor, 2007).



Information security breaches are defined in different ways. There seems to be no perfect definition, but some common elements are involved. The breach should involve the loss, damage or exposure of data or information stored or on the move in an information system. Such loss or exposure can come as the result of many activities ranging from losing storage media, an attacker's intentional actions, a careless employee's inadvertent disclosure, or a natural disaster (Doherty & Fulford, 2005; Galbraith, 2013; Wikina, 2014). Almost any event or act that compromises the confidentiality, integrity, or availability of data can be considered an information security breach.

### **Types**

Breaches as defined above come in many varieties and have various causes. Researchers tend to categorize breaches similarly, by associating them with their root cause (Davis et al., 2009; Doherty & Fulford, 2005; Garrison & Ncube, 2011; Hazari et al., 2008; Wikina, 2014). A common set of causes emerged and created a taxonomy of breach types.

Viruses, worms, Trojan horses, logic bombs, and similar malicious software make up a large portion of reported incidents. These types of attacks are usually automated, sometimes autonomous, programs that can cause information security breaches (Doherty & Fulford, 2005; Hazari et al., 2008). They range from totally harmless to substantially dangerous. These malicious programs can be very hard to detect and can multiply and spread without intervention from an attacker. Users of a system can accidentally release them by normal internet browsing or opening attachments and clicking links in email. They are used in concert with sophisticated attacks sometimes, like phishing.

Hacking Incidents are defined as intentional penetration of an information system (Doherty & Fulford, 2005; Hazari et al., 2008). Hacking usually involves surveillance, targeting

specific interests, enumeration of the system, and exploitation for the purpose of stealing or damaging information resources. Attackers use tools and techniques such as password cracking, social engineering, rouge access points, DNS poisoning, address spoofing, man-in-the-middle attacks, and network sniffing in order to find gaps on the security infrastructure. Once a gap is found, the attackers exploit the vulnerability in order to gain further access into the system or to the data goal. Defense against this kind of concerted, intelligent effort is extremely difficult.

While outside attackers are fearsome to organizations, the majority of attacks may come from users of the system (Garrison & Ncube, 2011; Mahmood, Siponen, & Pahlila, 2009; Warkentin & Willison, 2009). Unauthorized access refers to abuse of an information system by users of that system that already have a level of access. The problem is exacerbated by organizations that do not de-provision users properly, or that grant large amounts of access to avoid the hassles of having users be prevented from doing work in the system. Either case allows people to be able to access things that they do not normally need for work. System administrators can be a serious problem as they have wide-ranging access to a number of systems, generally. Because of its strict privacy laws, healthcare organizations face a big challenge keeping patient data secure even with the most basic access by legitimate users (Warkentin & Willison, 2009).

Hardware, software, and data can be stolen from an organization (Doherty & Fulford, 2005; Wiant, 2005). While stealing a computer monitor may not reveal trade secrets or release privacy data, the cost to the organization to replace it can be substantial. Data theft can include credit card information, privacy data, or healthcare information, which are all large concerns currently (Cadrain, 2005; Holtfreter & Holtfreter, 2006; Netschert, 2008). Hardware may

contain information storage that holds sensitive information, or information that can be used to gain further access, like password hashes or encryption keys. Stealing equipment may also bring down critical systems, especially when dealing with network equipment. Several systems may be impacted. Physical security is an important element of preventing these kinds of breaches, but is often overlooked (Radcliff, 1998).

Information systems can be used to conduct fraudulent activities, sometimes referred to as computer-based fraud (Doherty & Fulford, 2005; Hawser, 2008). Fraud can be used in conjunction with hacking incidents as mentioned above. Users can be inappropriately misdirected to spoofed websites, which are designed to look like authentic ones, in the hopes that the user will type in their login credentials or other personal information. Malicious software can also be embedded in these web pages. Communication in email may be similarly spoofed, tricking a user into believing that the message comes from someone else. Fraud can be internal or external to an organization.

Perhaps not expected as a breach classification, employee errors are included in some research (Doherty & Fulford, 2005; Garrison & Ncube, 2011). Human error can be very costly in an information system. Downtime frequently results from human error, not technical error. In addition, human error may allow a more serious breach to occur (Liginlal, Sim, & Khansa, 2009). Carelessly clicking on a link in an email which allows an attacker to penetrate the information system is an example. A large number of organizations report that non-malicious employee behavior represents a substantial percentage of losses. 16% of respondents in the 2009 CSI Computer Crime and Security survey report that nearly all of their losses were caused by

careless employee actions (Peters, 2009). Reducing human error is a reflection on the controls of an organization, both operational and security.

Disasters, both natural and man-made, are also a cause for loss of confidentiality, integrity, and availability of information (Doherty & Fulford, 2005; Heikkila, 2009). Natural disasters include earthquakes, hurricanes, floods, tornadoes, volcanic activity, comet strikes, and a host of other gruesome possibilities. While damage from some disasters like these are unavoidable, organizations plan and deploy resources to mitigate such a risk. Backup data centers, supported by server and storage mirroring, are usually located in a separate city to keep everything in one locale from being wiped out. Similarly, human disasters like power outages, network failures, air conditioning failures, fires, and plumbing accidents can take out one or more data centers very quickly. Recovering from disasters is difficult and expensive, even more so if plans and auxiliary resources are not in place (Peters, 2009).

Employee damage refers mostly to the vandalism of information resources by members of an organization (Doherty & Fulford, 2005; Radcliff, 1998). Reasons for the damage may be related to revenge for any number of work or personal reasons. To prevent these kinds of breaches, employers sometimes use policies like automated, instant de-provisioning, or escorting IT admins out of the building as soon as they receive a termination briefing. Unfortunately, that is not enough some of the time. As explained by Radcliff (1998), a fired employee left a logic bomb that wiped out all of Omega Engineering's research, development, and production programs 10 days after he was fired. Damages were an estimated \$10 million and years of rewriting designs and programs by teams of engineers.

Breaches come from a variety of directions, but how often do such things occur?

Measuring the frequency of breaches may not be as straightforward as it seems.

### **Frequency**

Discovering the frequency of breaches is problematic for organizations, but the problem is still widespread. Most organizations do not find out about a breach until months after it has occurred, if at all (Swartz, 2008). Many have suffered breaches of some kind whether aware of them or not. Unfortunately, the research does not show firm numbers on how many breaches are experienced by an organization on average.

While breaches may provide a set of concrete numbers, their usefulness in a study must be carefully evaluated. The method with which quantitative data about breaches is collected is not consistent between studies or reports (Doherty et al., 2009; Garrison & Ncube, 2011; Kannan et al., 2007). Counting the number of breaches suffered by an organization seems straightforward, but can be difficult, especially in widespread, long-term attacks. Many breaches may not even be discovered. Evaluating the true vulnerability of a system relies on that system's ability to discover breaches. For example, an organization may report no breaches, even though it has been compromised several times, simply because attackers left stolen records on the original server undisturbed. They would have to be able to track data transfers and also spend the resources to have audits performed. Frequency of breaches alone does not accurately reflect the amount of damage done either, as the severity of a breach is critical to measure as well.

### **Severity**

Severity of a breach is difficult to define and hard to measure. While we know that breaches cause some amount of loss, quantifying that loss is inconsistent and questionable at best in the research. Kannan (2007) states "Losses due to breaches of information security are

difficult to assess because the methodology and processes used to measure them are inherently unrealistic” (p.69). Some research and reports use a severity scale, which is an estimate based on the perceived severity. Doherty and Fulford (2005) and Heikkila (2009) both utilized a 5-point Likert scale ranging from “Fairly Insignificant” to “Highly significant”. Wiant (2005) only states severity as “seriousness” in regards to reporting health information breaches. Other studies use a dollar amount, which includes a currency layer of complexity, clouding the real effects (Peters, 2009). Garrison and Ncube (2011) utilized the number of records breached as a measure of security. This seems straightforward, but records are also abstract. For example, is a record just one credit card transaction, or the credit card information itself, which may have been involved in thousands of transaction records? What a record is has to be defined in this instance to understand what is being measured. While severity gives an idea of the magnitude of a breach, the effects can vary widely and may not have much reflection on the frequency or severity of the breach.

### **Effects**

The full range of effects from a breach can be complex. Monetary loss is probably the most obvious loss, and, as mentioned earlier, is a common way to state the severity of a breach’s effect (Davis et al., 2009; Doherty & Fulford, 2005; Garrison & Ncube, 2011). In addition to monetary loss, organizations can suffer reputation damage, loss of customers, market share, and company value. Web traffic may drop, and frequency of purchases may go down. Breaches may have to be reported to regulatory agencies, as is the case with the HIPAA laws, and these cause embarrassment and turmoil. When privacy data is lost, customers may have to be personally notified of the mistake, a complex and painful procedure for all involved. There may be state and federal punishments as well, usually in the form of fines, and the organization will

be more closely watched afterwards. These rippling effects can add up to long-lasting and expensive consequences.

Surprisingly though, breaches may not have long term impacts on an organization. Research supports that ill effects such as lower stock price may be minimal and short-lived (Kannan et al., 2007). Davis, Garcia and Zhang (2009) reported no difference in web traffic for online businesses following a cyber-security incident. So while breaches occur frequently, and there may be an initial loss, the loss of customer base, market share, and revenue may not be very severe, or as severe as expected. Still, reporting such breaches to the government, media, or affected customers is not a pleasant thing to consider for an organization.

## **Reporting**

The responsibility to report breaches varies widely between industries and locales. Privacy data loss seems to be the most prevalent reporting concern in regards to federal and state laws (U. S. Department of Health and Human Services, 2010). However, state laws vary widely in their reporting requirements, and the federal government only requires reporting on certain types of breaches (Dimitropoulos & Rizk, 2009). Additionally, there is the question of how many breaches are reported even when the organization knows that a breach has occurred. Roberts (2005) indicates that in 2005, only 20% of organizations reported to law enforcement and only 12% to legal counsel. Statistics on reporting to regulatory agencies that may punish the organization possibly could be assumed to be even lower. There are also loopholes to reporting. For instance, HIPAA requires reporting the loss of any protected health information (PHI), with some serious penalties, especially if over 500 records. But, if the data were encrypted to a certain standard, then the breach does not have to be reported (U. S. Department of Health and Human Services, 2010). This gives organizations another “out” from reporting, as they can

claim that lost or stolen PHI was in an encrypted format. Reporting seems to be just as inconsistent and undefined as many of the other elements of information security.

### **Information Security Policy Effectiveness**

This review of the literature would not be complete without an exploration of similar studies that have attempted to evaluate the effectiveness of information security policies. Each study mentioned has had an original methodological approach, and the results from each study cast different angles of light on how effective information security policies may be.

#### **Doherty and Fullford (2005)**

The seminal study for this work, Doherty and Fulford's research (2005), is a groundbreaking study that sought to determine if what was believed about the information security policy had any bearing in the real world on reducing information security breaches. Their study was initiated after they had performed extensive research into information security policies, what they should contain, and how they should be the leading element of information security in an organization. At the time of their study, information security policies were being touted as the most important elements of information security (Higgins, 1999; Höne & Eloff, 2002). Higgins (1999) states "the security policy is to the security environment like the law is to a legal system" and "a policy is the start of security management" (p. 2). Höne & Eloff (2002) claim "There are various controls and measures that can be – and indeed need to be – implemented within an organization to ensure the effective working of information security...undoubtedly, the single most important of these controls is the information security policy" (p. 402).



Doherty and Fulford (2005) noted that although the information security policy seemed so important, and while there was plenty of guidance on how it should be formulated, that breach incidents seemed to be increasing. “The role and importance of information security policies and the incidence and severity of security breaches are both topics that have attracted significant attention in the literature, but there is little evidence that these topics have been explicitly linked” (Doherty & Fulford, 2005, p. 22). They sought to explore that link in an objective and empirical way.

In order to explore the link, they conducted research via a survey in the UK inquiring about the existence and qualities of information security policies and about breaches suffered and performed statistical analysis to determine if there were any relationships between the two. The survey went out to senior IT executives, and inquired as to whether the organization had an information security policy, how long it had been in effect, and how often it was updated. They asked the number, severity, and type of breaches suffered in the past 2 years. Analysis was performed on the data, and they concluded that there was no significant link between the existence or other qualities of the information security policy and the incidence or severity of any of the breach types. In their words: “it came as something of a surprise in the present study to find almost no statistically significant relationships between the adoption of information security policies and the incidence or severity of security breaches” (Doherty & Fulford, 2005, p. 34).

Their study represented the first empirical study into the effectiveness of information security policies. They recommended further exploration between the information security policy and breaches to try to understand the phenomenon. They noted that their survey had

limitations, and that further studies should verify what they found. Studies should be conducted to find ways to make the policy more effective.

### **Wiant (2005)**

Wiant (2005) conducted a study to evaluate the benefits of having an information security policy in a healthcare environment. The recent adoption of the HIPAA rule drove interest in the study. He sought to discover relationships between the policy and the number and seriousness of computer abuse incidents. He sent 2,500 survey instruments out to CIOs, CISOs, and MIS directors in US hospitals, and, with only a 5.6% completed response rate, ended up with 140 valid responses. 62% reported that they had computer abuse incidents, and 44% reported the seriousness of the computer incidents.

Wiant only tested 2 hypotheses that hospitals with an information security policy are more likely to report incidents of computer abuse, and that they are aware of the abuse more frequently than hospitals that do not have a policy. Neither hypothesis was supported by the analysis.

The similarities between this study and Doherty and Fulford (2005) are interesting because they were both performed at the same time and in different countries, yet they had similar constructs. Both addressed the frequency and severity of computer abuse or information security breaches. While the Doherty and Fulford (2005) study was far more detailed, it is interesting that both ended up with very similar results.

### **Heikkila (2009)**

The Heikkila (2009) study is a dissertation based on the Doherty and Fulford (2005) study, except that its target population was US law firms. The qualities of the information security policy, such as the existence of a policy, its age, and frequency of updates were

measured and compared to breach frequency and severity. The methodology and hypotheses were almost identical to the Doherty and Fulford (2005) study. The main difference was in the sample.

The survey instrument was delivered to members of the ILTA, and Heikkila received 88 responses with a 7.83% response rate. Because of the low number of responses, Heikkila had to resort to less strict, non-parametric statistical analysis. Nevertheless, the results were the same. No significant relationships existed between the existence, longevity, or frequency of updates of the information security policy and the number or severity of security breaches experienced by US law firms.

### **Conclusion**

This literature review painted a comprehensive picture of the major elements involved with the effectiveness of information security policies. The foundations of the information security policy were explored, namely: IT governance, governance frameworks, ISO certifications, legislation and regulatory requirements, and theory. The policy itself was discussed in detail as to the content and qualities that an information policy should have. Organizational challenges, such as getting employees to comply with the policy, were reviewed. Security breaches were explored in detail, along with the difficulties of identifying and measuring them. Altogether, the above review established the firm position of the security policy in regards to the organization, and to the threats that it defends against. Chapters 3, 4, and 5 of this study will present the method of research, results, and discussion of the results.

### CHAPTER 3. RESEARCH METHOD

Organizations that take the time and resources to implement an information security policy and to keep it current may not be any less danger of damaging security breaches (Doherty & Fulford, 2005; Wiant, 2005). There appears to be no significant link between the two at this point in the research. Knowledge of this problem may influence organizations to either refuse to bother with an information security policy, and possibly other parts of security governance, or to treat it as a trivial document, with no real meaning. They may implement one solely used as an audit appeasement tool, and may not take advantage of using it as a real instrument of influencing and steering information security.

This would be unfortunate given the possible benefits available from a properly constructed and implemented policy (Doherty & Fulford, 2006; Hazari et al., 2008; Höne & Eloff, 2002). Not only are information security policies used to guide investments and provide strategic direction to management, they also should be used in day-to-day activities. End users should have access to the policy and be required to read the applicable parts in an easy to understand format (Höne & Eloff, 2002). Including security awareness training guidance in the policy and utilizing it to implement a solid training program should help reduce risky security behavior by users and ultimately lower breach risk (Albrechtsen, 2007; Hazari et al., 2008; Higgins, 1999). Managers could take advantage of the guidance and executive support in the policy to influence and enforce secure behavior. In addition, administrators that configure networks, databases, servers, and other information systems can use the policy as guidance for integrating security into their operations (Ma, Schmidt, & Pearson, 2009). Unfortunately, most

organizations may not be using information security policies to their full potential, and may be suffering from the same mistakes as those that do not make the effort.

Consequently, there is a gap in understanding how information security works empirically. Theoretically, the information security policy should be able to form some kind of organizational protection, but according to Doherty and Fulford (2005), there seems to be no evidence for it. They reached this conclusion by measuring organizations that had an information security policy and those that did not, and then compared the number and severity of security breaches suffered by those organizations to the characteristics of the policy. They also measured other factors such as the age of the policy and the frequency of its updates. They found that there was no significant difference in the number or severity of breaches, regardless of the existence of a policy, or of the quality of its maintenance. Nevertheless, that was ten years ago, and the sample was only located in the UK. In addition, the sample focused on large organizations and on executives exclusively. Things may have changed over time, or may be different in another location. Smaller organizations may have different experiences implementing an information security policy, and may have less incentive to adopt a formal governance framework. There is value in replicating a quantitative study in order to take another measurement that may support or undermine previous works (Galinac Grbac et al., 2013). This study seeks to further the works of Doherty and Fulford (2005) by not only replicating their study in a different population and locale, but by adding elements such as IT governance and ISO certification to evaluate the effectiveness of those elements as well as information security policies.

## Research Design

The study utilizes a post-positivist, quantitative, non-experimental approach to test hypotheses formed from the research questions. The essence of the research problem implies that information security policies have been put forward as truly effective means of reducing security threats, but empirical evidence suggests otherwise (Doherty & Fulford, 2005; Heikkila, 2009). In order to avoid collecting data that are favorable toward information security policies, not because they are effective but because they are popular, an objective stance must be taken and empirical data collected. By utilizing the positivist approach, the study seeks to explore objective data in order to verify current studies. If further support is found that information security policies are not effective, then this study could springboard further research into why information policies are not effective, and what can be done to either make them more effective or what cost savings could be achieved by spending fewer resources on creating and maintaining them.

Exploratory survey analysis has been deemed as the best method for testing the hypotheses generated from the research questions in this study. Positivist methods allow and encourage follow-on research to test different aspects of the topic with similar, or the same research design (Swanson & Holton, 2005). Doherty and Fulford (2005) stated “follow-up studies should be conducted employing different methods and targeting different populations” (p.36). While this study would use similar methods, it would target a different population. Verification of the Doherty and Fulford (2005) study in a population other than the UK would add a global element to their findings and further validation of their theory.

As an added facet, measuring the adoption of IT governance frameworks and the pursuit of ISO certifications will provide depth to the study and further contextual understanding of the

results. Possible relationships may be uncovered as results could show correlation between IT governance adoption and ISO certification with the number and severity of security breaches. The absence of correlation would be useful as well, and could steer further research towards discovering why these important organizational pursuits are not netting significant empirical results.

Questions regarding the characteristics of both the information security policies developed by organizations as well as the number of breaches suffered and the total number of records compromised over a two-year period will be included in the survey instrument. Security policy questions relating to the adoption of the policy, the age of the policy, the frequency of policy updates, adoption of governance frameworks and ISO security certification will be measured. Breach questions will relate to the number of breaches, the number of records compromised, and types of breaches, and severity of breaches. Responses will be quantified using ratio, categorical, and ordinal scales.

Statistical analysis will focus on using MANOVA to explore relationships between organizational implementation of information security policies and the number of security breaches and the number of records compromised (Doherty & Fulford, 2005). Significance will be evaluated at the  $p < .05$  level. Hypotheses will be rejected or fail to be rejected based on the results of tests and whether or not the results are deemed to show significance

Quantitative studies, based in post-positivism, provide an inherent objectivity (DeLuca, Gallivan, & Kock, 2008). Characteristics such as strict numerical analysis and drawing conclusions that can only be supported directly by evidence encourage divorce from prevailing thought, popular assumption, and emergent theoretical frameworks. Since information security

policy research and information security in general, are relatively new fields, the majority of current studies are more inductive than deductive. Much of the current literature consists of theoretical frameworks, logical models, and remarks based on the experience and observations of researchers or practitioners (Autry & Bobbitt, 2008; Cannoy, Palvia, & Schilhavy, 2006; Fadlalla & Wickramasinghe, 2004).

Balancing the research in this field demands more concrete analysis and this study seeks to add to the objective, empirical composition of research.

The interactions of security breaches and information security policies would be almost impossible to accurately reconstruct in the laboratory. The organizational nature and necessary multivariate interactions make this study decidedly non-experimental (Doherty & Fulford, 2005; Siponen & Vance, 2010; Wiant, 2005). Random assignment will not be used, and there is no control group. Instead, a target group will be selected from a larger population of information security professionals and their observations will be measured using a quantitative instrument.

### **Research Questions with Hypotheses**

**RQ 1:** Do organizations that have a written information security policy experience fewer security breaches or have fewer records compromised than those that do not (Doherty & Fulford, 2005)?

**H1<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have a documented information security policy and those that do not.

**H1<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have a documented information security policy and those that do not.



**RQ 2:** Do organizations that update their information security policy more frequently experience fewer security breaches or have fewer records compromised than those organizations that update their policies less frequently (Doherty & Fulford, 2005)?

**H2<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that update their information security policy more frequently than other companies.

**H2<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that update their information security policy more frequently than other companies.

**RQ 3:** Do organizations with an information security policy that has been in place for a longer period of time experience fewer security breaches or have fewer records compromised than those with a younger policy (Doherty & Fulford, 2005)?

**H3<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have had their information security policies in place for a longer period of time than other companies.

**H3<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have had their information security policies in place for a longer period of time than other companies.

**RQ 4:** Do organizations that implement an IT governance framework (such as CobiT or ITIL) experience fewer security breaches or have fewer records compromised than those organizations that do not implement an IT governance framework?

**H4<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented an IT governance framework and those that have not.

**H4<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented an IT governance framework and those that have not.

**RQ 5:** Do organizations that are certified in one or more ISO security certifications experience fewer security breaches or have fewer records compromised than those organizations that are not certified?

**H5<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented one or more ISO certifications and those that have not.

**H5<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented one or more ISO certifications and those that have not.

## **Constructs**

Constructs of a study form the foundation of the data, and thus drive the analysis and conclusions. What follows is a concise statement of the fundamental constructs and how study variables are derived from them.

**Construct 1- information security policy.** Three characteristics of an organization's information security policy will be measured: existence, age, frequency of update. Existence will be a dichotomous nominal variable, either the organization has a formal security policy or it

does not. Age of the policy will be categorical, representing 5 increasing ranges. Frequency of update will be defined by categorical ranges of how often the policy is updated.

**Construct 2- IT governance.** One characteristic of IT governance will be evaluated: whether the organization follows an IT framework or not. The variable will be a dichotomous nominal type.

**Construct 3- ISO security certification.** ISO Security Certification will be similarly evaluated by measuring if the organization possesses an ISO security certification or not. The variable will be a dichotomous nominal type.

**Construct 4- security breaches.** Security breaches will be measured in two ways: the number of breaches, and the number of records compromised. The number of breaches represents the total number of breaches suffered by the organization, regardless of severity. The number of breaches will be categorized into ranges of incidents of equal value so that the measurement can be considered as a ratio measurement. Number of records compromised will represent the total number of records that have been lost, stolen, corrupted, deleted, or exposed due to breaches. Both measurements will cover the last 2 years. These two measurements will reflect the frequency of breach activity as well as the cumulative damage suffered, which can be related to breach severity in other studies.

### **Relationships**

This study utilizes multivariate analysis, and has a challenge of two dependent variables to evaluate: number of breaches and severity of breaches. The overall variable relationships for this project can be diagrammed in the following manner:

Dependent Variables:

- Number of Breaches- DV1

- Number of Records Compromised- DV2

Independent Variables:

- Existence of an Information Security Policy
- Age of the policy
- Frequency of policy updates
- Adoption of an IT governance framework
- Certification in an Information Security ISO

The variables can be mapped comprehensively as follows (Salkind, Neil J., 2010):

$$Y = X\beta + \epsilon$$

Where:

Y = a vector of dependent variables: Breach Frequency and Records Compromised

X = a matrix of independent variables: Policy Existence, Age, Update, IT Governance Adoption, ISO certification

$\beta$  = a vector of weighted regression coefficients

$\epsilon$  = a vector of error terms

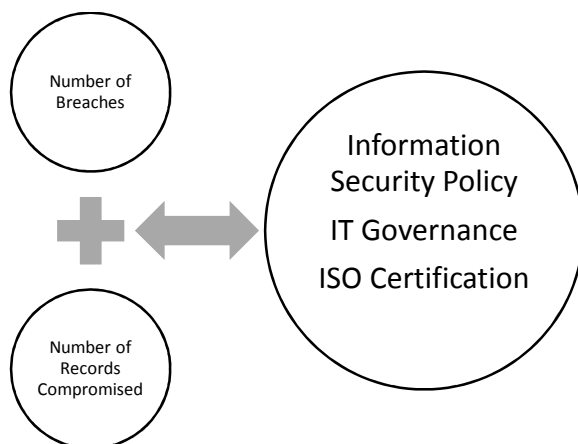


Figure 3. Map of variable relationships for Research Questions 1-3

### **Population/Sample**

United States based organizations that have IT resources formed the population of this study. Representatives of these organizations would be individuals that have knowledge of information security breaches and of organizational security policies. These individuals have a wide range of titles from Chief Executive Officer (CEO) to analyst. Organizational size of the population ranged from sole-proprietorships to multi-national corporations. A sample of organizations was selected based on respondent willingness to submit to the study.

Organizations represented by respondents to a SurveyMonkey Audience targeted survey comprised the sample of this study. Targeted audience titles include, but are not limited to Chief Information Officer (CIO), Chief Information Security Officer (CISO), Director of Management Information Systems, Security Administrator, Network Administrator, Database Administrator, Technical Manager, technicians, or programmers that have working knowledge of the Information Security Policy and breach activity.

This approach engaged a wider range of IT representatives than previous, similar studies. Doherty and Fulford (2005) and Wiant (2005) targeted only senior IT staff such as Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Director of Management Information Systems, with mixed results. Wiant (2005) admits that even though their study targeted executive officers and directors “In reality, the respondents hold various positions in the hospitals with at least some of their duties being related to management information systems” (p. 455). Considering that the sample of these two studies did not impose restriction on the size of the organization, they may have skewed the returns towards larger organizations, as few small companies would have positions in those categories. For example, a small organization may only utilize one or two people for network, database, and workstation

support, with no CIO. In order to include even the smallest organizations such as sole-proprietorships, the scope of the population had to be increased. Studies related to this topic suffer from low rates of return for survey instruments, and broadening the sample population would probably increase the number of valid returns (Doherty & Fulford, 2005; Hagen et al., 2008; Wiant, 2005).

In the interest of providing more substantial and generalizable results, this study was applied to a wider range of organizations. As noted by Doherty and Fulford (2005), “the selection of a very narrow sampling frame reduces the generalizability of the results;... these limitations do highlight the need for follow-up studies to be conducted employing different methods and targeting different populations” (p. 36). This study targeted respondents across the United States of America, although some valid responses from outside the US were possible.

### **Sample Size**

Calculated sample size was based on the number of valid returns desired, and was tailored to provide enough responses to perform more powerful parametric analysis. MANOVA is the predicted test for this study. Minimum sample size calculations were necessary in order to determine if the target sample and expected return rate would be sufficient to achieve the goal of using parametric, multi-variate analysis. The estimated sample size requirements for each type of test were calculated using G\*Power 3 based on the criteria of the Doherty and Fulford (2005) study (Faul, Erdfelder, Lang, & Buchner, 2007). MANOVA with the requirements of effect size medium ( $f=.25$ ) and confidence above 95% would require an approximate sample size of 172. SurveyMonkey Audience was requested to provide as close to 300 valid results as possible, in order to provide a robust, solid sample and to guarantee the ability to use MANOVA and other parametric tests as valid analyses.

300 SurveyMonkey Audience responses were purchased, and correspondence with SurveyMonkey representatives about expected survey return rates led them to request responses from approximately 5,000 IT professionals in order to meet the target. SurveyMonkey Audience methods dictate that they request responses until they achieve the target number of valid responses. Other studies have reported valid return rates of 5.6%, 7.7%, and 7.83% (Doherty & Fulford, 2005; Heikkila, 2009; Wiant, 2005). The mean of these return rates is 7.2%. If the return rate is similar for this study, then the expected return of valid surveys for 5,000 requests would be approximately 350 (280-391), which is consistent with studies of this nature that use chi-square and ANOVA tests for statistical analysis (Doherty & Fulford, 2005; Wiant, 2005). In addition, this number would reasonably fall above the G\*Power reported requirement for MANOVA of 172. If the number of returned valid responses should fall below 120, then non-parametric statistical tests may be used (Heikkila, 2009), although this would weaken the generalizability of the results.

### **Sampling Rationale**

The research questions involve knowledge of the information security policy, breach frequency and severity, IT governance, and ISO Security certifications. Members of the target sample will belong to IT organizations and, although not guaranteed, will have a high probability of meeting the inclusion criteria for the survey. In addition to targeting IT professionals using SurveyMonkey Audience, a pre-screening response was placed at the beginning of the survey that asked if the respondent had knowledge of the information security policy and of breaches suffered by their organization. This was done to ensure that, no matter the respondent's title, they would be able to understand if they had the requisite knowledge to respond to the survey instrument.

## Instrument

This study utilized a survey instrument based on the original Doherty and Fulford (2005) survey (Appendix B). Just as in the original instrument, respondents were asked their position, size of the company, and if the company was multi-national. They were also asked to report on the number of different types of breaches that had occurred in the last 2 years, and the approximate number of records compromised by breach type. Questions about the information security policy characteristics were also asked, such as if the organization had a policy, how long they had used it, and how often it was updated. Respondents were also asked how the policy was disseminated and what issues were covered by the policy. Questions about factors for successful security implementation and how successful their organization implemented the factors were also asked, and responses were measured with a 5-point Likert scale.

Some questions and sections were added to this survey in order to address IT governance and ISO certifications. The additional sections followed the question structure of the original survey and sought to uphold the approach taken by the original. For example, question 6 of the Doherty and Fulford (2005) study asks, “Does your organization have a documented information security policy?” while the new question about IT governance used in this study is, “Does your organization actively use one or more IT governance frameworks?” (Appendix C). IT governance was measured by a generic maturity model put forth by Hawkins (2003): non-existent, initial, repeatable, defined, managed, or optimized. ISO certifications were measured only if the organization was certified in certain certifications. Questions about breach types remained the same, but questions about the severity of breaches changed from a 5-point Likert scale of “fairly insignificant” to “highly significant” into a logarithmic selection of number of



records compromised. Demographic questions were added to discover what kind of IT governance frameworks may be used and what ISO certifications were held.

### **Data Collection**

The survey instrument was created using SurveyMonkey's tools, and was distributed to potential respondents according to their proprietary methods. SurveyMonkey Audience recruits people to complete surveys every month and provides incentives to encourage participation. They limit the number of surveys that members can take per week, use non-cash incentives to improve the quality of responses, and benchmark the population to ensure that they are representative of the American population ("Millions of respondents on our online panel | SurveyMonkey Audience," n.d.).

Participants in the study were greeted by several pages of information about the study so that they would be fully aware of what the study entailed when asked for consent. The initial page was used to screen out participants that did not have knowledge of both the security policy and the number of security breaches experienced in the last 2 years. Participants were informed that the survey was anonymous, both for the participant and their organization. There were no questions involved that would be able to identify either. However, the respondents were also reminded to respect the policies of their organization and were asked to opt out of the study if reporting on breaches was not allowed.

SurveyMonkey Audience provided rapid response collection. Data were collected from 19-25 November, 2015. 435 responses total were collected.

### **Field Test**

A field test was performed using the survey instrument described above with special attention given to the two new questions involving IT governance and ISO certification. Five panel members were obtained by corresponding with information security professionals, 3 from the researcher's academic research committee and 2 peers. Post-review interviews were conducted, and feedback from the field-testing was integrated into the survey instrument.

### **Pilot Test**

A pilot test was conducted with the assistance of the Information Systems Security Association (ISSA). The researcher conducted a presentation at the local ISSA chapter and solicited survey responses by providing a link to the SurveyMonkey site for the pilot study. Delivery was performed in the same manner as the final survey. Comment fields were made available for respondents to give feedback.

Data from the pilot testing was analyzed to determine suitability for the final survey. 16 responses were received for the pilot. Cronbach's alpha tests were run in order to establish their internal consistency. The series of questions relating to breach frequency and severity showed a high level of internal consistency, as determined by a Cronbach's alpha of .929 (Appendix E). Responses seemed complete and appropriate.

Some of the instrument had to be adjusted based on responses and comments made by respondents. Some of the comment fields and questions were set to be considered required on the web user interface. This made the survey difficult to complete, and adjustments were made prior to deploying the instrument for the final collection. Some of the instructions were clarified,

and an additional screening question was added to the beginning of the survey to indicate knowledge of the information security policy and breach activity.

### **Data Analysis**

Previous studies in the area of empirically comparing information security breaches against organizational elements such as the information security policy and its qualities have used univariate analysis (Davis et al., 2009; Doherty & Fulford, 2005; Heikkila, 2009; Wiant, 2005). In an effort to expand the quality of analysis, this study strives to explore the multivariate relationships by using multivariate analysis. Finch (2005) explains why this may be a good, new direction to pursue: “MANOVA offers several advantages over standard analysis of variance (ANOVA), including the ability to measure multiple facets of a problem, improved power (in some cases), and a reduced type I error rate compared to multiple univariate ANOVAs” (p. 27). A possibility exists that the frequency of breaches and the severity of breaches may have underlying correlation, which would be very important to take into consideration and may significantly affect results.

What follows is an explanation of how the data analysis was performed. How variables were coded, outliers were handled, how missing data was treated, and any transformations performed will be demonstrated. Testing of MANOVA assumptions and the execution of statistical testing will then be discussed.

### **Coding**

Data were coded in such a way as to set up the structure of the data to be favorable for a multi-variate analysis. Dependent variables in MANOVA should be continuous, while independent variables should be categorical or nominal (Salkind, Neil J., 2010).

The variables for frequency and severity of data breaches were collected as continuous variables. Frequency was coded as a series of equal intervals that made estimation simple and straightforward for the respondent, as in the Doherty and Fulford (2005) study: 0, 1-5, 6-10, >10. Severity of breaches was coded differently, however. 10 intervals of a logarithmic scale were set in order to capture the vast range of number of compromised records: 0, 1-10, 11-100, 101-1000, 1001-10,000, 10,001-100,000, 100,001-1M, 1M-10M, 10M-100M, >100M. Both of these variables were stored as the interval number that reflected the range selected.

Independent variables were coded as nominal or ordinal variables. The existence of an information security policy, ISO certification, and IT governance framework were all binary, yes or no type questions that fall into the nominal variable type. How long a policy had been in use, and the update frequency were both coded as ordinal variables.

### **Data Preparation**

Data were transformed to minimize impact of skewness, outliers or missing values by using the Data Preparation module of IBM SPSS 23. Box-Cox transformation reduced skew to a final mean of 0, and final standard deviation to 1. If the value of outliers were more than 3 standard deviations above or below the mean, they were trimmed to the cutoff value of 3 standard deviations. Missing values were not replaced as there were no missing values in the continuous variables, and the missing values in the nominal variables could not be assigned yes or no without impacting the study.

Hypothesis testing required aggregation of the dependent variables in order to make it straightforward. The survey instrument collected breach frequency and severity for each type of incident: computer virus, hacking incident, unauthorized access, theft, fraud, human error, natural disaster, and employee damage. Without aggregation, each hypothesis would have to be

tested 8 times, one for each type, resulting in 40 detailed evaluations that would obfuscate the findings. By summing the data in all types, a valid total number of breaches and the total severity of breaches was obtained. This technique was verified by running MANOVA on each type separately and comparing the results.

### **Tests**

Statistical analysis for this study utilized one-way MANOVA to test for significance at a 95% significance level, or  $p < .05$ . The multi-variate nature of the study's dependent variables, breach frequency and severity, drove the decision to use MANOVA, which is a powerful and robust statistical analysis method to be used when there may be multiple, underlying relationships that may not be apparent when the variables are isolated (Finch, 2005; Gupta, 2009). Calculations were performed using IBM SPSS Statistics Premium Grad Pack 23.0.

MANOVA has several assumptions that must be tested (Finch, 2005; Lund & Lund, 2013; Salkind, Neil J., 2010):

- Univariate outliers- Use of boxplot analysis determined if outliers were present. Transformation during variable preparation should have removed univariate outliers that are over 3 standard deviations above mean by limiting them to the value of 3 standard deviations.
- Multicollinearity- Dependent variables in MANOVA should have a certain amount of correlation in order to be effective. This study utilized Pearson correlation to evaluate multicollinearity, significant at  $p < .01$ .
- Linearity- Unique to MANOVA, the dependent variables must exhibit linearity. Scatterplot analysis will be used on the dependent variable pairs to look for an elliptical pattern (Lund & Lund, 2013; Salkind, Neil J., 2010)

- Multivariate Normality- Best evaluated by conducting univariate analysis for normality on the dependent variables. Histograms, scatter plots, normality plots and Q-Q plots were used as well as the Shapiro Wilk and Kolmogorov-Smirnov tests for normality.
- Multivariate outliers- Even if univariate outliers are handled, multivariate outliers may be discovered because of the interaction between dependent and independent variables. Analysis will utilize Mahalanobis distance to evaluate multivariate outliers at  $p < .001$  using a critical value of 13.82, since 2 dependent variables are being tested.
- Homogeneity of variance-covariance matrices- George Box's M statistic was used to evaluate whether variances and covariances are similar enough to meet the assumption at the  $p < .001$  level of significance.
- Independence and Randomness- Based on the structure of this study, independence and randomness requirements should be met (Salkind, Neil J., 2010).

MANOVA results will be evaluated at the  $p < .05$  level of significance. When MANOVA showed significant results, post-hoc tests utilized one-way ANOVA on each dependent variable to verify which dependent variable was contributing to the statistically significant MANOVA (Lund & Lund, 2013).

The following chapter presents the results of statistical tests and analyses after the validity, reliability, and ethical considerations of the study are explained.

### **Validity and Reliability**

Doherty and Fulford (2005), in their foundational study on the effectiveness of information security policies, provide a very direct and relevant statement in terms of the importance of valid and reliable data: "When undertaking survey-based research, there is always

the danger that the results will be undermined or even invalidated through the introduction of bias. Therefore, it is important that active measures be taken to reduce the likelihood of bias having any such negative effects” (p.29). In their study, content validity was established by initially linking the variables to research literature and then testing them with pre and pilot tests, as was performed in this study. Non-response sample bias was a stated concern, and Doherty and Fulford (2005) addressed this potential problem by performing an independent samples t-test of early versus late responses to see if there was a significant difference between the response profiles. This study utilized the same method and compared the first 100 responses to the survey instrument, including the pilot test, and performed a t-test comparison against the last 100 survey responses. As in the original study, this study detected no significant differences in response profiles of all variables measured at the .05 level, which implies that there are no noticeable impacts from non-response bias.

Additionally, this study evaluated constructs by using Cronbach’s alpha test for reliability. The constructs for breach frequency and severity are represented by multiple questions as to the type of breach, so it was important to assess how reliably these questions and their scales assess the underlying data qualities. Cronbach’s alpha measured at .951, which is considered as a very high indicator of reliability (Duhachek & Iacobucci, 2004).

Based on the techniques used in the original study, this study appears to meet at least the same standards as the original instrument. The additional questions that were added to this study passed the same rigor as the original questions with similar results.

## **Ethical Considerations**

This study presents some important points within the spectrum of ethical considerations. Because this study is not experimental, and does not entail physically invasive procedures, many of the more severe ethical considerations are not in play. However, as with all research, there are things that must be considered, even with performing voluntary survey research on the Internet.

The Belmont Report (Assistant Secretary of Health, 1979), provides comprehensive guidance over three main ethical principles, respect for persons, beneficence, and justice. The structure of this study ensures that all three principles are addressed.

As a voluntary study, people that do not wish to participate do not have to, thereby meeting the intent of respect for persons. There will be no coercion, nor will people with diminished autonomy be tricked into participating. A fully detailed and plainly worded consent form presented at the beginning of the study ensures that an informed decision can be made as to whether or not the subject wishes to participate. Additionally, the associations involved in the study have policies in place to disallow any expectations of participation from their membership and they emphasize that it is a voluntary study.

This study seeks to protect all participants that voluntarily partake in the study. Physical harm is not a large concern for web-based surveys, but, in the case of this type of study where details of information security lapses are collected, potential of organizational harm or harm to reputation definitely exists (Doherty & Fulford, 2005). Safeguards to data and the process of execution of data handling must be performed in a way to absolutely minimize the chances of inappropriate viewing of data. Steps will be taken to inform the participants and their respective organizations as to the safeguards and security of the study.



Participants were treated equally in the study, whether they finished the survey or not. All who voluntarily submitted were be given the reward of having full access to the final product, which is a complete, published copy of the dissertation as far as University policy allows. Additionally, no participant suffered more of a burden than another. The main concern in regards to the principle of fair burdening for this study is that exposure of data would show some participants or their organizations will have to expose more security concerns or data breaches than others, resulting in more risk for that participant. Measures were taken to lower this risk for all participants, such as anonymizing survey responses.

### **Summary**

This chapter provided a detailed description of the structure of the research design and approach of the study. Research questions, constructs, and their relationships established the framework. Information on the population, sample, and sampling rationale relayed how the proper respondents were selected. Discussion on the survey instrument and data collection explained how content was collected and introduced within the parameters of the framework. Analysis method described how the collected data was processed and also the establishment and verification of the validity and reliability of the data and its analysis. Finally, even though it may be the most important part of the chapter, a full explanation of ethical considerations was presented. Disclosure of results follows in Chapter 4, and Chapter 5 presents a discussion of the results.

## CHAPTER 4. RESULTS

This study explores the possible relationships between information security policies, IT governance, and ISO security certification with the number of information security breaches and the severity of breaches suffered by organizations. Past studies have shown no significant relationship between information security policies and breach frequency or severity (Davis et al., 2009; Doherty & Fulford, 2005; Heikkila, 2009; Wiant, 2005). However, this study addresses a different population and employs multivariate analysis as opposed to the univariate analysis used in previous studies.

The following research questions were designed for exploring these organizational relationships:

**RQ 1:** Do organizations that have a written information security policy experience fewer security breaches or have fewer records compromised than those that do not (Doherty & Fulford, 2005)?

**RQ 2:** Do organizations that update their information security policy more frequently experience fewer security breaches or have fewer records compromised than those organizations that update their policies less frequently (Doherty & Fulford, 2005)?

**RQ 3:** Do organizations with an information security policy that has been in place for a longer period of time experience fewer security breaches or have fewer records compromised than those with a younger policy (Doherty & Fulford, 2005)?

**RQ 4:** Do organizations that implement an IT governance framework (such as CobiT or ITIL) experience fewer security breaches or have fewer records compromised than those organizations that do not implement an IT governance framework?

**RQ 5:** Do organizations that are certified in one or more ISO security certifications experience fewer security breaches or have fewer records compromised than those organizations that are not certified?

Data collection utilized a survey composed of questions based on the original instrument used by Doherty and Fulford (2005), which collected data about breaches and information security policies. The survey instrument in this study included additional questions to collect data about IT governance and ISO security certification as well.

### **Population and Sample**

Data collection targeted a sample of the IT professional population in the US. Professional titles of the population include: CEO/President, CTO, CIO, CISO, IS Director, IS Manager, IS Administrator, IS Analyst, IT Director, IT Manager, IT Analyst, Programmer, Database Administrator, Server Systems Analyst, End Client Systems.

That population was sampled by soliciting participation in the study through SurveyMonkey Audience, which is a commercial survey distribution and collection company. Respondents were qualified by responding to a question that asked if they had knowledge of both their organization's information security policy and information security breaches that their organization had suffered in the past 2 years. Responses were limited and collection was ended by SurveyMonkey when approximately 300 valid responses were achieved.

Complete responses numbered 435 total, with 63 (14.5%) indicating that they did not have knowledge of the security policy or breaches. A further 7 (1.9%) declined to participate. 56 (12.9%) other responses were incomplete, bringing the total number of valid responses to 309.

The survey instrument also collected demographics on the respondent's organization. 98.7% of respondents reported that their organization was headquartered in the US, and 65% reported that their organization was multi-national. Respondents reported the following for the size of their organizations:

Table 1

*Sample Demographics*

**Approximately how many people are employed in your organization?**

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Less than 500	51	16.5	16.5	16.5
500-1,000	65	21.0	21.0	37.5
1,001-1,500	31	10.0	10.0	47.6
1,501-2,000	23	7.4	7.4	55.0
2,001-3,000	24	7.8	7.8	62.8
3,001-5,000	49	15.9	15.9	78.6
5,001-10,000	37	12.0	12.0	90.6
over 10,000	29	9.4	9.4	100.0
Total	309	100.0	100.0	

Likewise, the position that was reported as the respondent's title:

Table 2

*Job Position Demographics*

**Pick the position that most closely relates to your title:**

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Other (please specify)	7	2.3	2.3	2.3
Chief Executive Officer/President	53	17.2	17.2	19.4
Chief Information Officer	39	12.6	12.6	32.0
Chief Technical Officer	17	5.5	5.5	37.5
Information Security (IS) Director	26	8.4	8.4	46.0
Information Security (IS) Manager	17	5.5	5.5	51.5
Information Security (IS) Administrator	10	3.2	3.2	54.7
Information Security (IS) Analyst	5	1.6	1.6	56.3
Information Technology (IT) Director	49	15.9	15.9	72.2
Information Technology (IT) Manager	66	21.4	21.4	93.5
Information Technology (IT) Analyst	9	2.9	2.9	96.4
Programmer	6	1.9	1.9	98.4
Database Administrator (DBA)	2	.6	.6	99.0
End Client Systems	3	1.0	1.0	100.0
Total	309	100.0	100.0	

This chapter continues with results reporting for the testing of hypotheses. The first section reports on all hypotheses in summary fashion, while the section following it involves a much more detailed format.

**Summary of Results**

This study utilized one-way MANOVA as the primary test used to evaluate hypotheses. Use of MANOVA assessed the relationships between information security breach frequency and severity together and how they relate to the information security policy, IT governance

framework adoption, and ISO security certification. All MANOVA tests were performed to a 95% confidence interval and a 0.05 significance level. The tool chosen for statistical analysis was IBM SPSS Statistics Premium Grad Pack 23.0.

### **Hypothesis 1- Existence of an Information Security Policy**

**H1<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have a documented information security policy and those that do not.

**H1<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have a documented information security policy and those that do not.

Several MANOVA tests compared each category of breach type measured: computer virus, hacking incident, unauthorized access, theft, fraud, human error, natural disaster, and employee damage to the existence of an information security policies. The results are reflected below (Table 3):

Table 3

*Existence of an Information Security Policy MANOVA Summary*

Type of Breach	Incidence and Severity of Breaches- MANOVA						
	Wilk's Lambda	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Significant at p < .005
Computer Virus	0.976	3.716	2	306	0.025	0.024	X
Hacking Incident	0.977	3.531	2	306	0.030	0.023	X
Unauthorized Access	0.973	4.166	2	306	0.016	0.027	X
Theft of Resources	0.982	2.757	2	306	0.065	0.018	
Computer-based Fraud	0.963	5.870	2	304	0.003	0.037	X
Human Error	0.958	6.681	2	306	0.001	0.042	X
Natural Disaster	0.982	2.801	2	302	0.062	0.018	
Damage by Employees	0.987	1.971	2	305	0.141	0.013	
Aggregate	0.967	5.250	2	306	0.006	0.033	X

The null hypothesis must be rejected. The alternate hypothesis is not rejected.

**Hypothesis 2- Frequency of Information Security Policy Updates**

**H<sub>20</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that update their information security policy more frequently than other companies.

**H<sub>2A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that update their information security policy more frequently than other companies.

The following results display MANOVA tests for each breach category as compared to the frequency and severity of information security breaches. The aggregate results determined whether the null hypothesis would be rejected or not.

Table 4

*Frequency of Information Security Policy Update MANOVA Summary*

Type of Breach	Incidence and Severity of Breaches- MANOVA						
	Wilk's Lambda	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Significant at p < .005
Computer Virus	0.946	2.099	8	602	0.034	0.027	X
Hacking Incident	0.970	1.142	8	602	0.333	0.015	
Unauthorized Access	0.967	1.266	8	602	0.259	0.017	
Theft of Resources	0.959	1.603	8	602	0.121	0.021	
Computer-based Fraud	0.948	2.050	8	602	0.039	0.027	X
Human Error	0.958	1.637	8	602	0.111	0.021	
Natural Disaster	0.951	1.934	8	602	0.053	0.025	
Damage by Employees	0.941	2.322	8	602	0.019	0.03	X
Aggregate	0.945	2.156	8	602	0.029	0.028	X

The null hypothesis must be rejected. The null hypothesis is not rejected.

### **Hypothesis 3- Information Security Policy Length of Time Adopted**

**H3<sub>0</sub>**: There is no significant difference in the number of security breaches and the number of compromised records between companies that have had their information security policies in place for a longer period of time than other companies.

**H3<sub>A</sub>**: There is a significant difference in the number of security breaches and the number of compromised records between companies that have had their information security policies in place for a longer period of time than other companies.

Some companies have had a security policy longer than others. The tests below reflect the comparison of the time that a policy has been in place with the frequency and severity of breaches.



Table 5

*Length of Information Security Policy Adoption MANOVA Summary*

Type of Breach	Incidence and Severity of Breaches- MANOVA						
	Wilk's Lambda	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Significant at $p < .005$
Computer Virus	0.883	1.720	22	588	0.022	0.060	X
Hacking Incident	0.896	1.503	22	588	0.066	0.053	
Unauthorized Access	0.818	2.825	22	588	0.000	0.096	X
Theft of Resources	0.837	2.479	22	588	0.000	0.085	X
Computer-based Fraud	0.845	2.341	22	588	0.001	0.081	X
Human Error	0.845	2.346	22	588	0.001	0.081	X
Natural Disaster	0.866	2.002	22	588	0.004	0.070	X
Damage by Employees	0.892	1.579	22	588	0.045	0.056	X
Aggregate	0.813	2.910	22	588	0.000	0.098	X

The null hypothesis must be rejected. The alternate hypothesis is not rejected.

#### **Hypothesis 4- IT Governance Framework**

**H4<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented an IT governance framework and those that have not.

**H4<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented an IT governance framework and those that have not.

Some organizations have instituted an IT governance framework. These tests compared the frequency and severity of breaches between companies that had an IT governance framework versus those that did not.

Table 6

*Adoption of IT Governance Framework MANOVA Summary*

Type of Breach	Incidence and Severity of Breaches- MANOVA						
	Wilk's Lambda	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Significant at p < .005
Computer Virus	0.918	13.628	2	304	0.000	0.082	X
Hacking Incident	0.880	20.699	2	304	0.000	0.120	X
Unauthorized Access	0.892	18.411	2	304	0.000	0.108	X
Theft of Resources	0.905	15.941	2	304	0.000	0.095	X
Computer-based Fraud	0.860	24.760	2	304	0.000	0.140	X
Human Error	0.919	13.370	2	304	0.000	0.081	X
Natural Disaster	0.866	23.451	2	304	0.000	0.134	X
Damage by Employees	0.887	19.459	2	304	0.000	0.113	X
Aggregate	0.844	28.049	2	304	0.000	0.156	X

The null hypothesis must be rejected. The alternate hypothesis is not rejected.

**Hypothesis 5- ISO Certification**

**H5<sub>0</sub>**: There is no significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented one or more ISO certifications and those that have not.

**H5<sub>A</sub>**: There is a significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented one or more ISO certifications and those that have not.

Organizations can seek certification in security standards defined by ISO. They are widely recognized as measuring the amount which an organization complies with industry best practices. The following tests reflect a comparison between the number and severity of breaches suffered by organizations that were certified in a security ISO and those that were not.

Table 7

*ISO Security Certification MANOVA Summary*

Type of Breach	Incidence and Severity of Breaches- MANOVA						
	Wilk's Lambda	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Significant at p < .005
Computer Virus	0.989	1.663	2	304	0.191	0.011	
Hacking Incident	0.989	1.767	2	304	0.173	0.011	
Unauthorized Access	0.994	0.974	2	304	0.379	0.006	
Theft of Resources	0.988	1.922	2	304	0.148	0.012	
Computer-based Fraud	0.992	1.237	2	304	0.292	0.008	
Human Error	0.985	2.282	2	304	0.104	0.015	
Natural Disaster	0.993	1.062	2	304	0.347	0.007	
Damage by Employees	0.994	0.965	2	304	0.382	0.006	
Aggregate	0.991	1.343	2	304	0.262	0.009	

The null hypothesis is not rejected.

### Details of Analysis and Results

#### Hypothesis 1 Detail

**H1<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have a documented information security policy and those that do not.

**H1<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have a documented information security policy and those that do not.

**Mean Comparison.** Comparison of means shows that the number and severity of breaches are both reported as being higher for organizations that have an information security policy than those that do not.

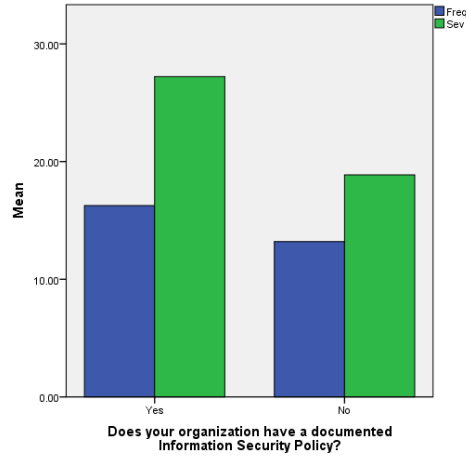


Figure 4. Comparison of mean breach frequency and severity for organizations that have an information security policy and those that do not.

**Univariate outliers and missing data.** Before transformation, there were 12 outliers in the data, as assessed by inspection of a boxplot for values greater than 1.5 box-lengths from the edge of the box. After transformation limiting outliers to 3 standard deviations above mean, 4 outliers were present but accepted.

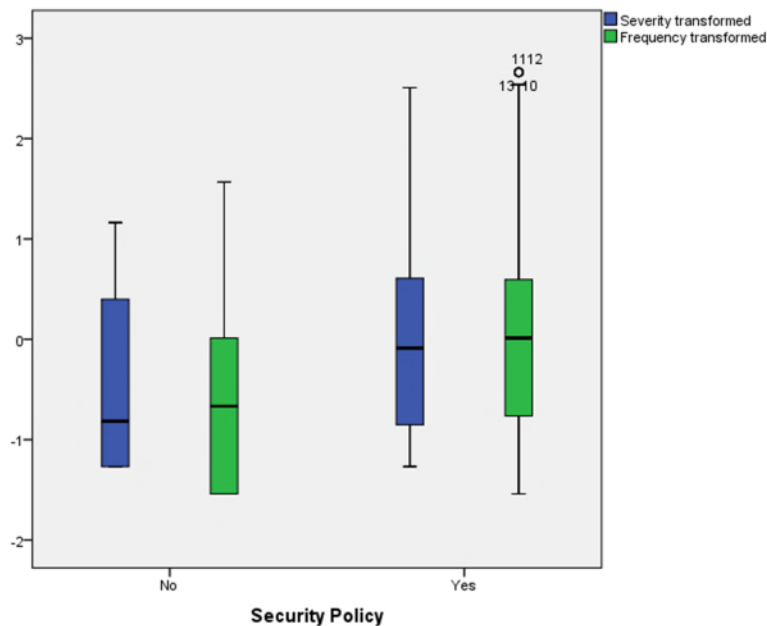


Figure 5. Univariate outliers after transformation for breach severity and frequency and for the existence of a security policy.

**Assumption testing.**

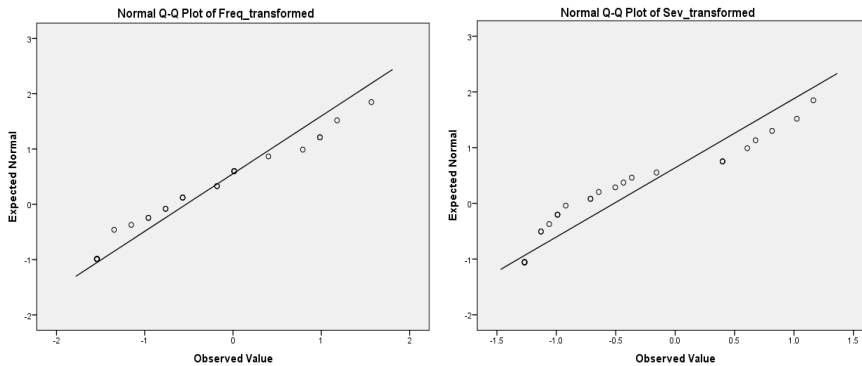
**Normality.** Breach frequency and severity were not normally distributed for the existence of an information security policy, as assessed by Shapiro-Wilk’s test ( $p < .05$ ). Q-Q plots show that the data may be approaching a normal distribution, but the assumption is still violated.

Table 8

*Existence of an Information Security Policy Normality Tests*

Tests of Normality							
INSPY_transformed		Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Sev_transformed	.00	.194	30	.006	.839	30	.000
	1.00	.094	279	.000	.939	279	.000
Freq_transformed	.00	.154	30	.068	.891	30	.005
	1.00	.084	279	.000	.968	279	.000

a. Lilliefors Significance Correction



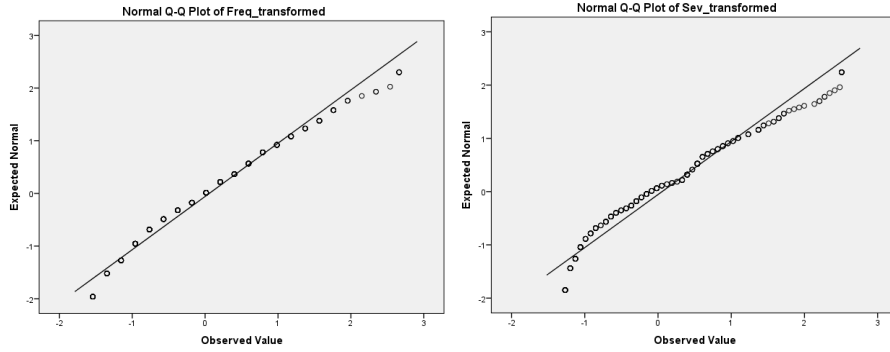


Figure 6. Q-Q plots for breach frequency and severity versus no information security policy (top row) or an information security policy in place (bottom row)

**Multicollinearity.** There was no multicollinearity, as assessed by Pearson’s correlation ( $r=.777$ ,  $p=.000$ )

**Linearity.** There was a linear relationship between breach frequency and severity for existence and non-existence of an information security policy, as assessed by scatterplot.

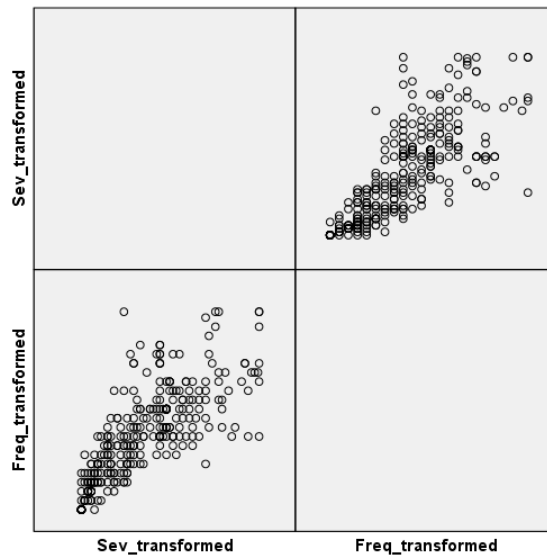


Figure 7. Scatterplot showing linearity of dependent variables breach frequency and breach severity.

**Multivariate outliers.** There were 2 multivariate outliers in the data, as assessed by Mahalanobis distance ( $p > .001$ ). These 2 cases were removed from further MANOVA testing.

**Homogeneity of variance-covariance matrices.** There was homogeneity of variance-covariances matrices, as assessed by Box's test of equality of covariance matrices ( $p = .080$ ).

**Homogeneity of variances.** There was homogeneity of variances for both dependent variables, as assessed by Levene's test of equality of error variances ( $p > .05$ ).

**Results.** There was a statistically significant difference between the existence of an information security policy and the number and severity of breaches,  $F(2,304) = 5.115$ ,  $p < .007$ ; Wilks'  $\Lambda = .967$ ; partial  $\eta^2 = .033$ . Post-hoc tests using a Bonferroni adjusted  $\alpha$  level of .025 revealed that there was a statistically significant difference in breach frequency and the existence of an information security policy,  $F(1,305) = 9.060$ ,  $p < .002$ ; partial  $\eta^2 = .030$ . There was a statistically significant difference in breach severity and the existence of an information security policy,  $F(1,305) = 8.531$ ,  $p < .003$ ; partial  $\eta^2 = .028$ . Null hypothesis 1 was rejected.

Table 9

*MANOVA for existence of a security policy*

Multivariate Tests <sup>a</sup>							
Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.023	3.545 <sup>b</sup>	2.000	304.000	.030	.023
	Wilks' Lambda	.977	3.545 <sup>b</sup>	2.000	304.000	.030	.023
	Hotelling's Trace	.023	3.545 <sup>b</sup>	2.000	304.000	.030	.023
	Roy's Largest Root	.023	3.545 <sup>b</sup>	2.000	304.000	.030	.023
INSPY_transformed	Pillai's Trace	.033	5.115 <sup>b</sup>	2.000	304.000	.007	.033
	Wilks' Lambda	.967	5.115 <sup>b</sup>	2.000	304.000	.007	.033
	Hotelling's Trace	.034	5.115 <sup>b</sup>	2.000	304.000	.007	.033
	Roy's Largest Root	.034	5.115 <sup>b</sup>	2.000	304.000	.007	.033

a. Design: Intercept + INSPY\_transformed

b. Exact statistic

Table 10

*Post-hoc tests for existence of a security policy*

Tests of Between-Subjects Effects							
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Sev_transformed	8.531 <sup>a</sup>	1	8.531	8.879	.003	.028
	Freq_transformed	9.060 <sup>b</sup>	1	9.060	9.469	.002	.030
Intercept	Sev_transformed	5.869	1	5.869	6.108	.014	.020
	Freq_transformed	6.312	1	6.312	6.597	.011	.021
INSPY_transformed	Sev_transformed	8.531	1	8.531	8.879	.003	.028
	Freq_transformed	9.060	1	9.060	9.469	.002	.030
Error	Sev_transformed	293.032	305	.961			
	Freq_transformed	291.834	305	.957			
Total	Sev_transformed	301.578	307				
	Freq_transformed	300.918	307				
Corrected Total	Sev_transformed	301.563	306				
	Freq_transformed	300.895	306				

a. R Squared = .028 (Adjusted R Squared = .025)

b. R Squared = .030 (Adjusted R Squared = .027)

## Hypothesis 2 Detail

**H<sub>20</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that update their information security policy more frequently than other companies.



**H2A:** There is a significant difference in the number of security breaches and the number of compromised records between companies that update their information security policy more frequently than other companies.

**Mean Comparison.**

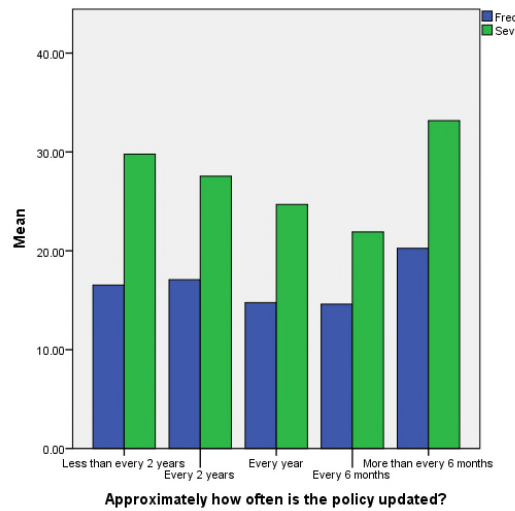


Figure 8. Comparison of breach frequency and severity of means versus how often the security policy is updated.

**Univariate outliers and missing data.** Before transformation, there were 5 outliers in the data, as assessed by inspection of a boxplot for values greater than 1.5 box-lengths from the edge of the box. After transformation limiting outliers to 3 standard deviations above mean, 2 outliers were present but accepted.

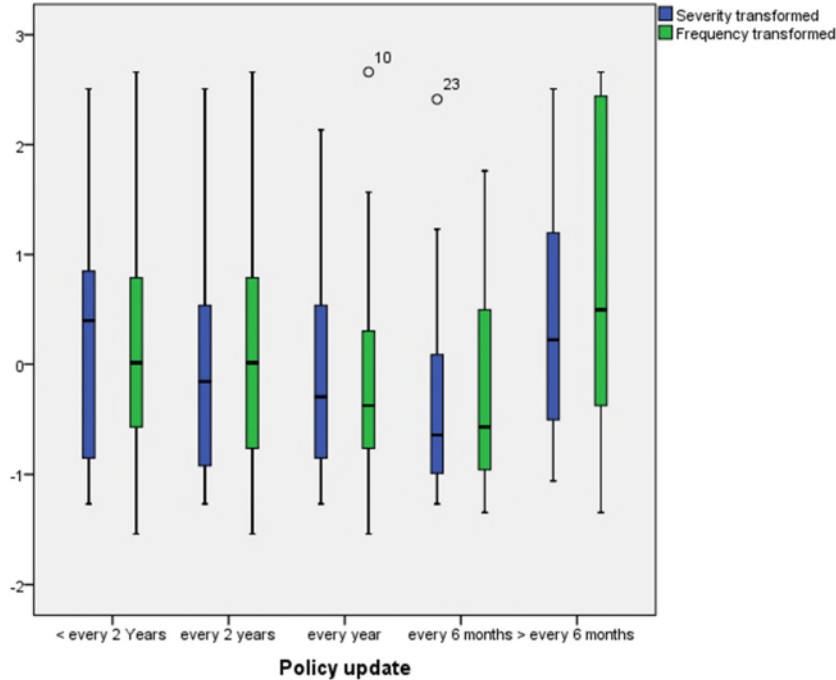


Figure 9. Univariate outliers after transformation for breach severity and frequency and existence of a security policy.

**Assumption testing.**

**Normality.** Breach frequency and severity were not normally distributed for the frequency of information security policy updates, as assessed by Shapiro-Wilk’s test ( $p < .05$ ). For organizations that updated their policy more frequently than every 6 months, the data were normally distributed, but the data as a whole were not assumed to be normally distributed. Q-Q plots show that the data may be approaching a normal distribution, but the assumption is still violated.

Table 11

*Normality tests for Frequency of Policy Update*

		Tests of Normality					
		Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
INSPYUpdate_transformed		Statistic	df	Sig.	Statistic	df	Sig.
Sev_transformed	1.00	.111	79	.018	.930	79	.000
	2.00	.119	123	.000	.941	123	.000
	3.00	.118	72	.014	.931	72	.001
	4.00	.166	23	.100	.861	23	.004
	5.00	.160	12	.200*	.918	12	.266
Freq_transformed	1.00	.080	79	.200*	.975	79	.127
	2.00	.088	123	.020	.968	123	.005
	3.00	.126	72	.007	.959	72	.019
	4.00	.195	23	.023	.901	23	.026
	5.00	.189	12	.200*	.887	12	.108

\*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

**Multicollinearity.** There was no multicollinearity, as assessed by Pearson’s correlation (r=.777, p=.000)

**Linearity.** There was a linear relationship between breach frequency and severity for existence and non-existence of an information security policy, as assessed by scatterplot.

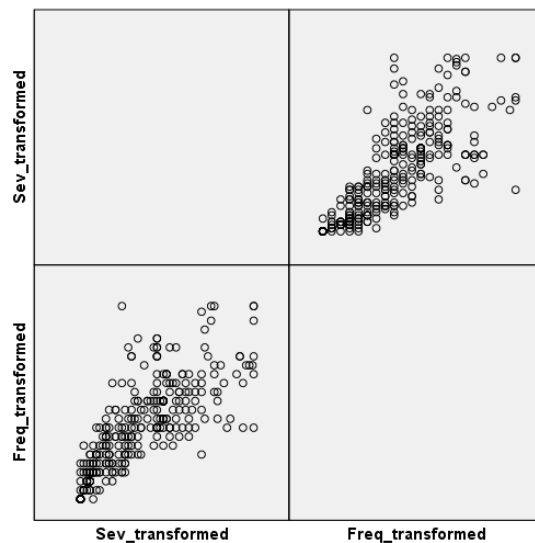


Figure 10. Scatterplot showing linearity of dependent variables breach frequency and breach severity.

**Multivariate outliers.** There were 2 multivariate outliers in the data, as assessed by Mahalanobis distance ( $p > .001$ ). These 2 cases were removed from further MANOVA testing

**Homogeneity of variance-covariance matrices.** There was homogeneity of variance-covariances matrices, as assessed by Box's test of equality of covariance matrices ( $p = .305$ ).

**Homogeneity of variances.** There was homogeneity of variances for breach severity, as assessed by Levene's test of equality of error variances ( $p > .05$ ). Breach frequency did not pass Levene's test with  $p = .022$ .

**Results.** There was a statistically significant difference between the update interval of an information security policy and the number and severity of breaches,  $F(8,604) = 2.156$ ,  $p < .029$ ; Wilks'  $\Lambda = .945$ ; partial  $\eta^2 = .028$ . Post-hoc tests using a Bonferroni adjusted  $\alpha$  level of .025 revealed that there was a statistically significant difference in breach frequency and the update frequency of an information security policy,  $F(4,302) = 10.299$ ,  $p < .002$ ; partial  $\eta^2 = .032$ . There was not a statistically significant difference in breach severity and the update frequency of an information security policy,  $F(4,302) = 8.909$ ,  $p < .059$ ; partial  $\eta^2 = .030$ . Null hypothesis 2 was rejected.

Table 12

*MANOVA for Policy Update Interval*

Multivariate Tests <sup>a</sup>							
Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.001	.198 <sup>b</sup>	2.000	301.000	.821	.001
	Wilks' Lambda	.999	.198 <sup>b</sup>	2.000	301.000	.821	.001
	Hotelling's Trace	.001	.198 <sup>b</sup>	2.000	301.000	.821	.001
	Roy's Largest Root	.001	.198 <sup>b</sup>	2.000	301.000	.821	.001
INSPYUpdate_transformed	Pillai's Trace	.056	2.162	8.000	604.000	.029	.028
	Wilks' Lambda	.945	2.156 <sup>b</sup>	8.000	602.000	.029	.028
	Hotelling's Trace	.057	2.151	8.000	600.000	.030	.028
	Roy's Largest Root	.035	2.676 <sup>c</sup>	4.000	302.000	.032	.034

a. Design: Intercept + INSPYUpdate\_transformed

b. Exact statistic

c. The statistic is an upper bound on F that yields a lower bound on the significance level.

Table 13

*Post-hoc Tests for Policy Update Interval*

Tests of Between-Subjects Effects							
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Sev_transformed	8.909 <sup>a</sup>	4	2.227	2.298	.059	.030
	Freq_transformed	10.299 <sup>b</sup>	4	2.575	2.676	.032	.034
Intercept	Sev_transformed	.298	1	.298	.308	.579	.001
	Freq_transformed	.372	1	.372	.387	.534	.001
INSPYUpdate_transformed	Sev_transformed	8.909	4	2.227	2.298	.059	.030
	Freq_transformed	10.299	4	2.575	2.676	.032	.034
Error	Sev_transformed	292.654	302	.969			
	Freq_transformed	290.596	302	.962			
Total	Sev_transformed	301.578	307				
	Freq_transformed	300.918	307				
Corrected Total	Sev_transformed	301.563	306				
	Freq_transformed	300.895	306				

a. R Squared = .030 (Adjusted R Squared = .017)

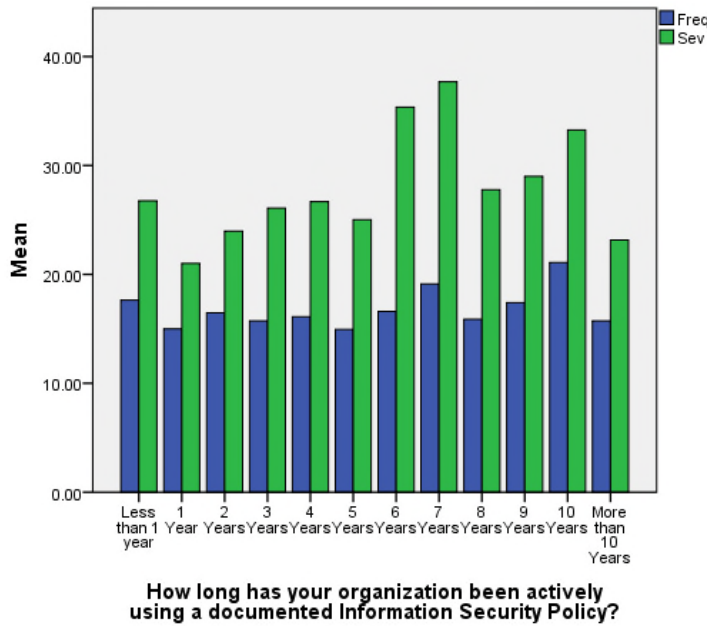
b. R Squared = .034 (Adjusted R Squared = .021)

**Hypothesis 3 Detail**

**H<sub>30</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have had their information security policies in place for a longer period of time than other companies.

**H3A:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have had their information security policies in place for a longer period of time than other companies.

**Mean Comparison.**



*Figure 11.* Comparison of breach frequency and severity means for policy length of time.

**Univariate outliers and missing data.** Before transformation, there were 9 outliers in the data, as assessed by inspection of a boxplot for values greater than 1.5 box-lengths from the edge of the box. After transformation limiting outliers to 3 standard deviations above mean, 8 outliers were present but accepted.

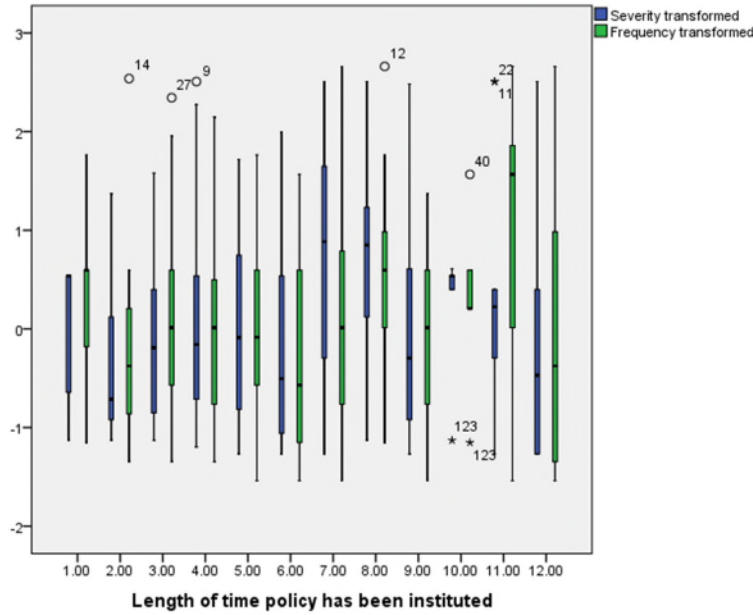


Figure 12. Univariate outliers after transformation for breach severity and frequency and length of time that an organization has had a security policy.

### Assumption testing.

**Normality.** Breach frequency and severity were not normally distributed for the length of time that an organization has maintained an information security policy, as assessed by Shapiro-Wilk's test ( $p < .05$ ). For some values of length of time, data were normally distributed, for others they were not. Frequency was more normally distributed than severity. Q-Q plots show that the data may be approaching a normal distribution, but the decision is that the assumption is still violated.

Table 14

*Normality Tests for Length of Time*

Tests of Normality							
	INSPYLength_transformed	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Sev_transformed	1.00	.375	8	.001	.699	8	.002
	2.00	.296	12	.005	.818	12	.015
	3.00	.141	28	.163	.931	28	.066
	4.00	.095	51	.200 <sup>*</sup>	.935	51	.008
	5.00	.135	28	.200 <sup>*</sup>	.923	28	.042
	6.00	.146	81	.000	.895	81	.000
	7.00	.113	25	.200 <sup>*</sup>	.948	25	.222
	8.00	.146	16	.200 <sup>*</sup>	.957	16	.604
	9.00	.162	17	.200 <sup>*</sup>	.895	17	.057
	10.00	.411	5	.006	.641	5	.002
	11.00	.308	12	.002	.850	12	.037
	12.00	.175	26	.039	.861	26	.002
Freq_transformed	1.00	.361	8	.003	.812	8	.039
	2.00	.175	12	.200 <sup>*</sup>	.843	12	.030
	3.00	.116	28	.200 <sup>*</sup>	.957	28	.303
	4.00	.115	51	.088	.955	51	.050
	5.00	.102	28	.200 <sup>*</sup>	.967	28	.513
	6.00	.114	81	.011	.933	81	.000
	7.00	.104	25	.200 <sup>*</sup>	.963	25	.483
	8.00	.151	16	.200 <sup>*</sup>	.963	16	.717
	9.00	.160	17	.200 <sup>*</sup>	.957	17	.576
	10.00	.268	5	.200 <sup>*</sup>	.947	5	.713
	11.00	.269	12	.017	.903	12	.175
	12.00	.149	26	.144	.891	26	.010

\*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

**Multicollinearity.** There was no multicollinearity, as assessed by Pearson's correlation (r=.777, p=.000)

**Linearity.** There was a linear relationship between breach frequency and severity for existence and non-existence of an information security policy, as assessed by scatterplot.



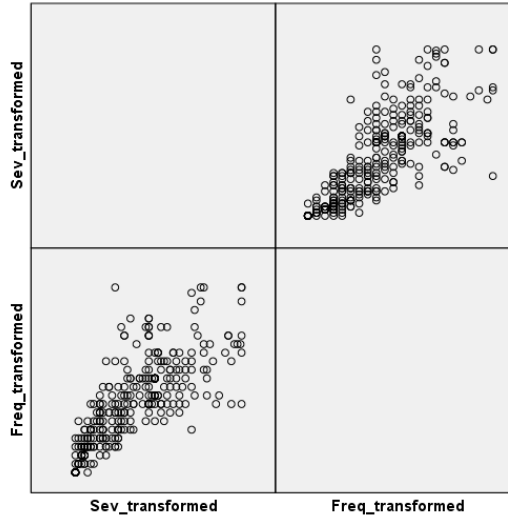


Figure 13. Scatterplot showing linearity of dependent variables breach frequency and breach severity.

**Multivariate outliers.** There were 2 multivariate outliers in the data, as assessed by Mahalanobis distance ( $p > .001$ ). These 2 cases were removed from further MANOVA testing.

**Homogeneity of variance-covariance matrices.** There was homogeneity of variance-covariances matrices, as assessed by Box's test of equality of covariance matrices ( $p = .126$ ).

**Homogeneity of variances.** There was homogeneity of variances for both dependent variables, as assessed by Levene's test of equality of error variances ( $p > .05$ ).

**Results.** There was a statistically significant difference between the length of time that an information security policy has been in use by an organization and the number and severity of breaches,  $F(22,588) = 2.910$ ,  $p < .000$ ; Wilks'  $\Lambda = .813$ ; partial  $\eta^2 = .098$ . Post-hoc tests using a Bonferroni adjusted  $\alpha$  level of .025 revealed that there was a statistically significant difference in breach frequency and the existence of an information security policy,  $F(11,295) = 2.760$ ,  $p < .002$ ; partial  $\eta^2 = .093$ . There was a statistically significant difference in breach severity and the

existence of an information security policy,  $F(11,295) = 2.399$ ,  $p < .004$ ; partial  $\eta^2 = .088$ . Null hypothesis 3 was rejected.

Table 15

*MANOVA for Length of Time*

Multivariate Tests <sup>a</sup>							
Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.015	2.232 <sup>b</sup>	2.000	294.000	.109	.015
	Wilks' Lambda	.985	2.232 <sup>b</sup>	2.000	294.000	.109	.015
	Hotelling's Trace	.015	2.232 <sup>b</sup>	2.000	294.000	.109	.015
	Roy's Largest Root	.015	2.232 <sup>b</sup>	2.000	294.000	.109	.015
INSPYLength_transformed	Pillai's Trace	.196	2.917	22.000	590.000	.000	.098
	Wilks' Lambda	.813	2.910 <sup>b</sup>	22.000	588.000	.000	.098
	Hotelling's Trace	.218	2.902	22.000	586.000	.000	.098
	Roy's Largest Root	.122	3.277 <sup>c</sup>	11.000	295.000	.000	.109

a. Design: Intercept + INSPYLength\_transformed

b. Exact statistic

c. The statistic is an upper bound on F that yields a lower bound on the significance level.

Table 16

*Post-hoc Tests for Length of Time*

Tests of Between-Subjects Effects							
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Sev_transformed	26.388 <sup>a</sup>	11	2.399	2.572	.004	.088
	Freq_transformed	28.080 <sup>b</sup>	11	2.553	2.760	.002	.093
Intercept	Sev_transformed	1.219	1	1.219	1.307	.254	.004
	Freq_transformed	3.632	1	3.632	3.928	.048	.013
INSPYLength_transformed	Sev_transformed	26.388	11	2.399	2.572	.004	.088
	Freq_transformed	28.080	11	2.553	2.760	.002	.093
Error	Sev_transformed	275.175	295	.933			
	Freq_transformed	272.814	295	.925			
Total	Sev_transformed	301.578	307				
	Freq_transformed	300.918	307				
Corrected Total	Sev_transformed	301.563	306				
	Freq_transformed	300.895	306				

a. R Squared = .088 (Adjusted R Squared = .053)

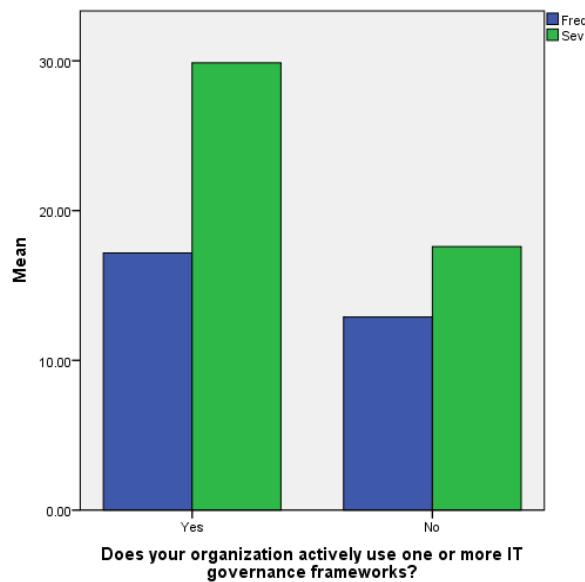
b. R Squared = .093 (Adjusted R Squared = .060)

## Hypothesis 4 Detail

**H4<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented an IT governance framework and those that have not.

**H4<sub>A</sub>:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented an IT governance framework and those that have not.

### Mean Comparison.



*Figure 14.* Comparison of breach frequency and severity means versus an organization's adoption of an IT governance framework.

**Univariate outliers and missing data.** Before transformation, there were 11 outliers in the data, as assessed by inspection of a boxplot for values greater than 1.5 box-lengths from the edge of the box. After transformation limiting outliers to 3 standard deviations above mean, 5 outliers were present but accepted.

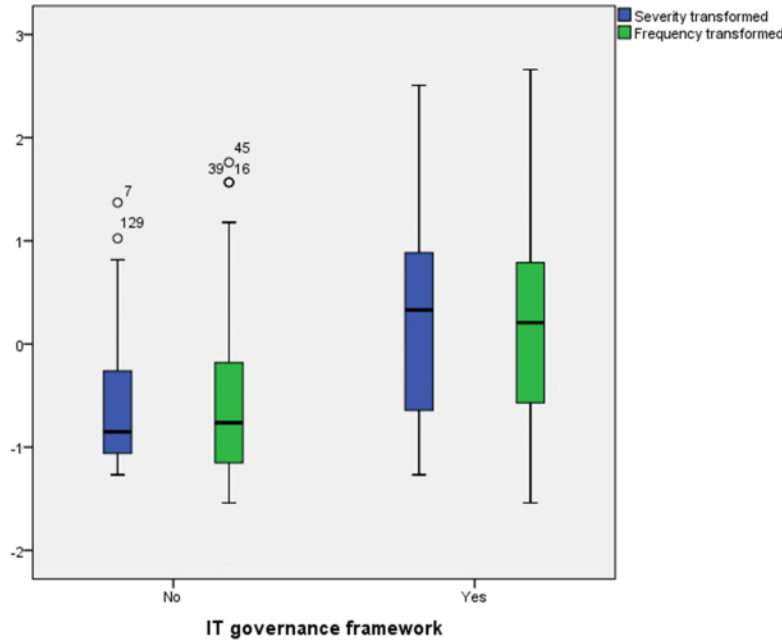


Figure 15. Univariate outliers after transformation for breach severity and frequency and existence of an IT governance framework.

**Assumption testing.**

**Normality.** Breach frequency and severity were not normally distributed for the length of time that an organization has maintained an information security policy, as assessed by Shapiro-Wilk’s test ( $p < .05$ ). For some values of length of time, data were normally distributed, for others they were not. Frequency was more normally distributed than severity. Q-Q plots show that the data may be approaching a normal distribution, but the decision is that the assumption is still violated.

Table 17

*Normality Tests for Policy Length of Time*

		Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
Gov_transformed		Statistic	df	Sig.	Statistic	df	Sig.
Sev_transformed	.00	.168	87	.000	.877	87	.000
	1.00	.071	222	.009	.959	222	.000
Freq_transformed	.00	.168	87	.000	.897	87	.000
	1.00	.070	222	.011	.980	222	.003

a. Lilliefors Significance Correction

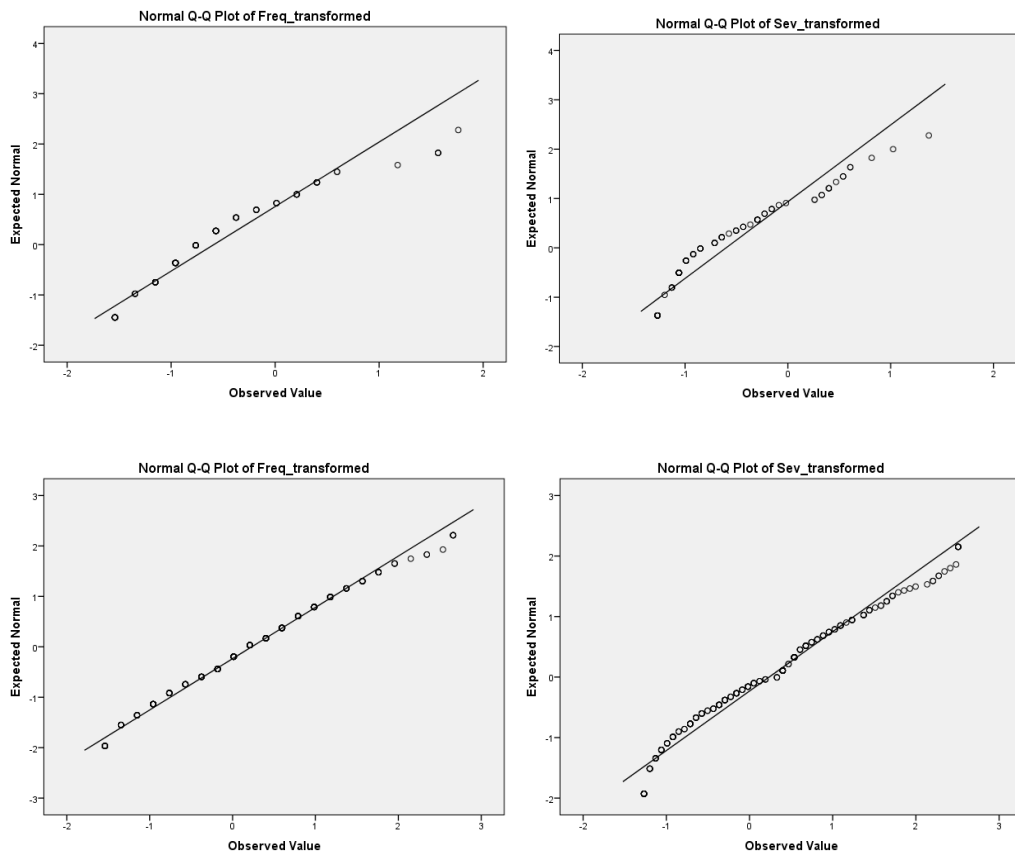


Figure 16. Q-Q plots for breach frequency and severity versus no IT governance framework (top row) or with an IT governance framework in place (bottom row).

**Multicollinearity.** There was no multicollinearity, as assessed by Pearson’s correlation ( $r=.777, p=.000$ )

**Linearity.** There was a linear relationship between breach frequency and severity for existence and non-existence of an information security policy, as assessed by scatterplot.

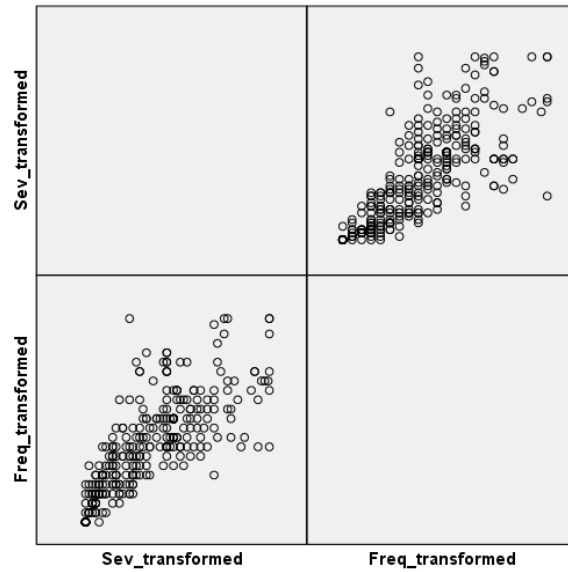


Figure 17. Scatterplot showing linearity of dependent variables breach frequency and breach severity.

**Multivariate outliers.** There were 2 multivariate outliers in the data, as assessed by Mahalanobis distance ( $p > .001$ ). These 2 cases were removed from further MANOVA testing.

**Homogeneity of variance-covariance matrices.** On the original transformed data, there was not homogeneity of variance-covariances matrices, as assessed by Box's test of equality of covariance matrices ( $p = .000$ ). Breach frequency and severity were transformed using  $\log_{10}$ , and the data achieved homogeneity of variance-covariance matrices, as assessed by Box's test of equality of covariance matrices ( $p = .415$ )

**Homogeneity of variances.** For the original transformed variables, there was not homogeneity of variances for both dependent variables, as assessed by Levene's test of equality of error variances ( $p < .05$ ). Breach frequency and severity were transformed using  $\log_{10}$  and the

data achieved homogeneity of variances as assessed by Levene's test of equality of error variances ( $p > .05$ )

**Results.** There was a statistically significant difference between the adoption of an IT governance framework and the number and severity of breaches,  $F(2,304) = 28.049$ ,  $p < .000$ ; Wilks'  $\Lambda = .844$ ; partial  $\eta^2 = .156$ . Post-hoc tests using a Bonferroni adjusted  $\alpha$  level of .025 revealed that there was a statistically significant difference in breach frequency and the existence of an information security policy,  $F(1,305) = 43.365$ ,  $p < .000$ ; partial  $\eta^2 = .143$ . There was a statistically significant difference in breach severity and the existence of an information security policy,  $F(1,305) = 44.564$ ,  $p < .000$ ; partial  $\eta^2 = .146$ . Null hypothesis 3 was rejected.

Table 18

*MANOVA for Adoption of an IT Governance Framework*

Multivariate Tests<sup>a</sup>

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.036	5.667 <sup>b</sup>	2.000	304.000	.004	.036
	Wilks' Lambda	.964	5.667 <sup>b</sup>	2.000	304.000	.004	.036
	Hotelling's Trace	.037	5.667 <sup>b</sup>	2.000	304.000	.004	.036
	Roy's Largest Root	.037	5.667 <sup>b</sup>	2.000	304.000	.004	.036
Gov_transformed	Pillai's Trace	.156	28.049 <sup>b</sup>	2.000	304.000	.000	.156
	Wilks' Lambda	.844	28.049 <sup>b</sup>	2.000	304.000	.000	.156
	Hotelling's Trace	.185	28.049 <sup>b</sup>	2.000	304.000	.000	.156
	Roy's Largest Root	.185	28.049 <sup>b</sup>	2.000	304.000	.000	.156

a. Design: Intercept + Gov\_transformed

b. Exact statistic

Table 19

*Post-hoc tests for Adoption of an IT Governance Framework*

**Tests of Between-Subjects Effects**

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	FreqLog10_transformed	43.365 <sup>a</sup>	1	43.365	50.959	.000	.143
	SevLog10_transformed	44.564 <sup>b</sup>	1	44.564	52.327	.000	.146
Intercept	FreqLog10_transformed	8.863	1	8.863	10.415	.001	.033
	SevLog10_transformed	8.911	1	8.911	10.463	.001	.033
Gov_transformed	FreqLog10_transformed	43.365	1	43.365	50.959	.000	.143
	SevLog10_transformed	44.564	1	44.564	52.327	.000	.146
Error	FreqLog10_transformed	259.551	305	.851			
	SevLog10_transformed	259.753	305	.852			
Total	FreqLog10_transformed	302.935	307				
	SevLog10_transformed	304.328	307				
Corrected Total	FreqLog10_transformed	302.916	306				
	SevLog10_transformed	304.317	306				

a. R Squared = .143 (Adjusted R Squared = .140)

b. R Squared = .146 (Adjusted R Squared = .144)

**Hypothesis 5 Detail**

**H5<sub>0</sub>**: There is no significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented one or more ISO certifications and those that have not.

**H5<sub>A</sub>**: There is a significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented one or more ISO certifications and those that have not.



### Mean Comparison.

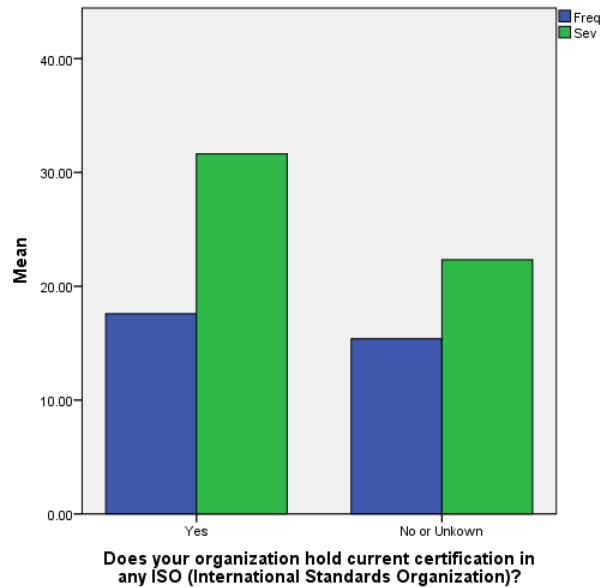


Figure 18. Comparison of breach frequency and severity means for organizations that have in an ISO security certification.

**Univariate outliers and missing data.** Before transformation, there were 6 outliers in the data, as assessed by inspection of a boxplot for values greater than 1.5 box-lengths from the edge of the box. After transformation limiting outliers to 3 standard deviations above mean, 4 outliers were present but accepted.

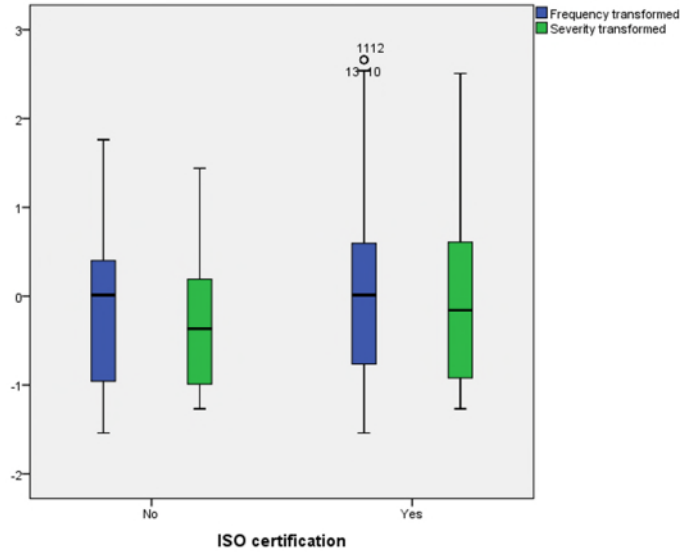


Figure 19. Univariate outliers after transformation for breach severity and frequency and ISO certification.

**Assumption testing.**

**Normality.** Breach frequency and severity were not normally distributed for the adoption of an ISO security certification, as assessed by Shapiro-Wilk’s test ( $p < .05$ ). One variable combination, no ISO certification compared to breach frequency showed normal distribution. Q-Q plots show that the data may be approaching a normal distribution, but the decision is that the assumption is still violated.

Table 20

*Normality Test for ISO Certification*

Tests of Normality						
ISO_transformed	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Freq_transformed .00	.106	41	.200*	.960	41	.153
1.00	.095	266	.000	.966	266	.000
Sev_transformed .00	.109	41	.200*	.922	41	.008
1.00	.105	266	.000	.935	266	.000

\*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

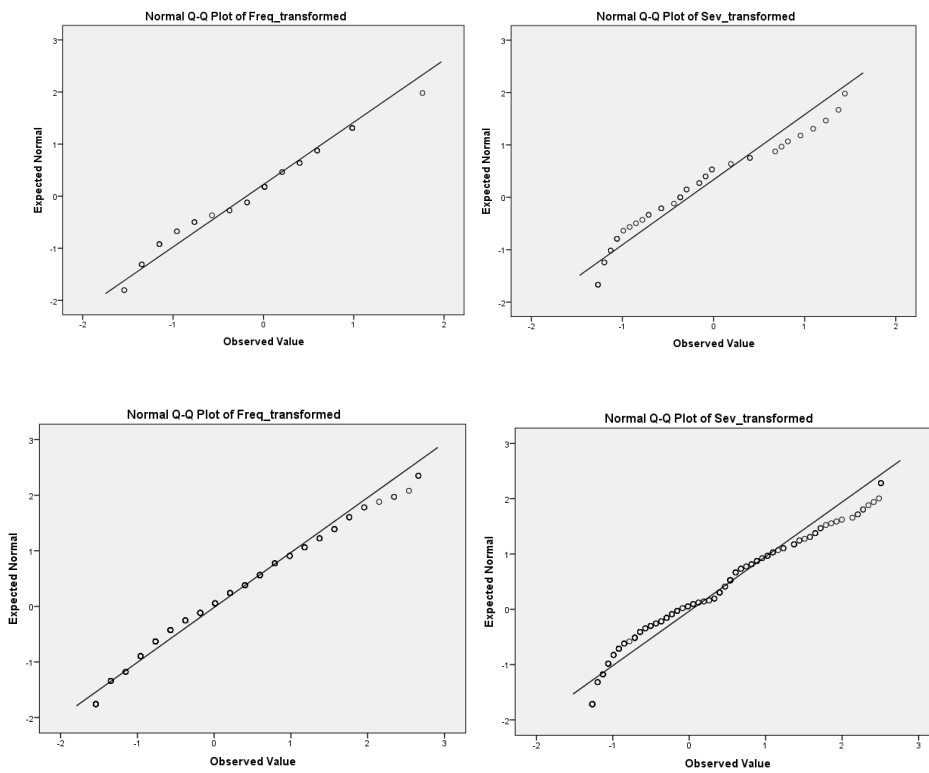


Figure 20. Q-Q plots for breach frequency and severity versus no ISO security certification (top row) or with an ISO security certification (bottom row).

**Multicollinearity.** There was no multicollinearity, as assessed by Pearson’s correlation ( $r=.777$ ,  $p=.000$ )

**Linearity.** There was a linear relationship between breach frequency and severity for existence and non-existence of an information security policy, as assessed by scatterplot.

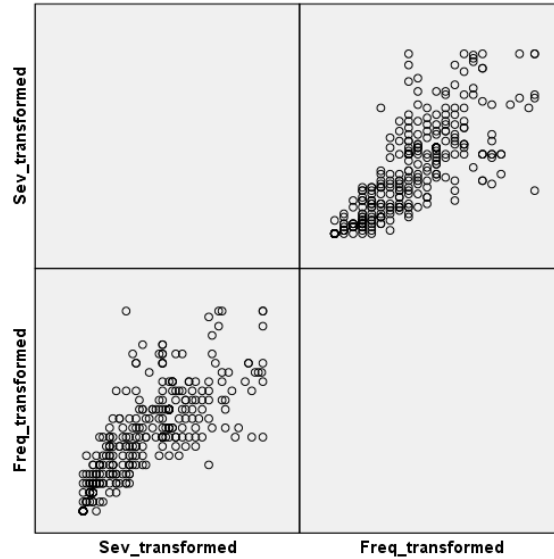


Figure 21. Scatterplot showing linearity of dependent variables breach frequency and breach severity.

**Multivariate outliers.** There were 2 multivariate outliers in the data, as assessed by Mahalanobis distance ( $p > .001$ ). These 2 cases were removed from further MANOVA testing.

**Homogeneity of variance-covariance matrices.** There was homogeneity of variance-covariances matrices, as assessed by Box's test of equality of covariance matrices ( $p = .314$ ) pre-transformation. The dependent variables had to be transformed by  $\log_{10}$  in order to achieve homogeneity of variances (below), and they exhibited homogeneity of variance-covariances matrices, as assessed by Box's test of equality of covariance matrices ( $p = .545$ ) post translation.

**Homogeneity of variances.** There was homogeneity of variances for breach frequency, as assessed by Levene's test of equality of error variances ( $p > .05$ ), but breach severity did not pass the test.  $\log_{10}$  transformation was applied to breach frequency and severity, and both

exhibited homogeneity of variances as assessed by Levene's test of equality of error variances ( $p > .05$ ) post transformation.

**Results.** There was no statistically significant difference between ISO security certification by an organization and the number and severity of breaches,  $F(2,304) = 1.343$ ,  $p < .262$ ; Wilks'  $\Lambda = .991$ ; partial  $\eta^2 = .009$ . Post-hoc tests were not performed. Null hypothesis 3 was not rejected.

Table 21

*MANOVA for ISO Certification*

**Multivariate Tests<sup>a</sup>**

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.005	.779 <sup>b</sup>	2.000	304.000	.460	.005
	Wilks' Lambda	.995	.779 <sup>b</sup>	2.000	304.000	.460	.005
	Hotelling's Trace	.005	.779 <sup>b</sup>	2.000	304.000	.460	.005
	Roy's Largest Root	.005	.779 <sup>b</sup>	2.000	304.000	.460	.005
ISO_transformed	Pillai's Trace	.009	1.343 <sup>b</sup>	2.000	304.000	.262	.009
	Wilks' Lambda	.991	1.343 <sup>b</sup>	2.000	304.000	.262	.009
	Hotelling's Trace	.009	1.343 <sup>b</sup>	2.000	304.000	.262	.009
	Roy's Largest Root	.009	1.343 <sup>b</sup>	2.000	304.000	.262	.009

a. Design: Intercept + ISO\_transformed

b. Exact statistic

Table 22

*Post-hoc tests for ISO Certification*

Tests of Between-Subjects Effects							
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Sev_transformed	26.388 <sup>a</sup>	11	2.399	2.572	.004	.088
	Freq_transformed	28.080 <sup>b</sup>	11	2.553	2.760	.002	.093
Intercept	Sev_transformed	1.219	1	1.219	1.307	.254	.004
	Freq_transformed	3.632	1	3.632	3.928	.048	.013
INSPYLength_transformed	Sev_transformed	26.388	11	2.399	2.572	.004	.088
	Freq_transformed	28.080	11	2.553	2.760	.002	.093
Error	Sev_transformed	275.175	295	.933			
	Freq_transformed	272.814	295	.925			
Total	Sev_transformed	301.578	307				
	Freq_transformed	300.918	307				
Corrected Total	Sev_transformed	301.563	306				
	Freq_transformed	300.895	306				

a. R Squared = .088 (Adjusted R Squared = .053)

b. R Squared = .093 (Adjusted R Squared = .060)

### Conclusion

Chapter 4 presented findings from the analysis of this study's hypotheses. The chapter included sample details, summary results, and detailed results. The analysis focused on using MANOVA and included details on data transformation, assumption testing, the core MANOVA tests, and post-hoc tests. The analysis rejected the null hypotheses of all hypotheses except the one that measured ISO security certification. The following chapter will take these results and use them in extensive discussion of the possible meaning and ramifications of the study.

## CHAPTER 5. DISCUSSION

This study strove to further explore the relationships between organizational information security characteristics such as the information security policy, IT governance, and ISO security certification versus the frequency and severity of information security breaches suffered by the organization. More concisely, the study evaluated the effectiveness of security policies, IT governance, and ISO certification. Researchers have been exploring this topic since at least 2005, and similar studies have found no significant relationships between information security policies and security breaches (Davis et al., 2009; Doherty & Fulford, 2005; Wiant, 2005). Organizations spend a considerable amount of time and money on security policies, and they affect every person in the organization. Frameworks and advice on how to build a policy and what it should contain abound in the literature (Doherty & Fulford, 2006; Höne & Eloff, 2002) but the questions remain if the information security policy is being correctly built and applied, and if it matters. Similarly, knowing if IT governance and ISO security certifications play an important part in bettering overall information security will help organizations decide whether or not to invest in the considerable effort to institute them. This chapter provides discussion on the findings of this study, and supplies context of how the results play a part in the body of research for information security.

### Results Summary

#### Restatement of the problem

Research shows no significant reduction in the number or severity of information security breaches based on the presence of an information security policy, or the maintenance of such a

policy (Davis et al., 2009; Doherty & Fulford, 2005; Heikkila, 2009; Wiant, 2005). This disparity confuses researchers and practitioners alike, and may cause organizational leadership to question whether they should invest in creating and maintaining a security policy. Even if the decision is made to have a security policy, the question of how important it is to the organization remains. Is the document solely used to appease auditors, partners, and customers, or does it have real value? Up until now, there has been no affirmative answer.

Likewise, IT governance and ISO security certifications are used to advertise the information security of an organization. These efforts entail even more effort than the security policy, and are supposedly an effective means of reducing security risk (Brenner, 2007; Hardy, 2006). Research performed for this study uncovered no prior analysis on the effectiveness of either IT governance or ISO certifications in regards to breaches.

### **Study Significance**

This study attempted to replicate the efforts of Doherty and Fulford (2005). In their groundbreaking study, they sought to discover if information security policies were effective. Since they had performed substantial analysis on the construction and use of security policies, they wanted to test the assumption that pouring efforts into policy development would net results. Their study collected data from executives in the UK and used univariate analysis to determine whether there was a significant difference between those organizations that had a policy and those that did not. Characteristics of the policy that were possible indicators of maintenance efforts, like updating the policy frequently, were analyzed as well. They found no significant relationships, and consequently could not claim that there was evidence for reducing breach frequency or severity with a security policy.



An objective of positivistic, quantitative studies is to replicate studies in order to validate their results, and this study attempted to perform similar testing on a similar population. The method differed, and hoped to capture a different sample of IT professionals, namely some of the non-executive professionals of smaller companies. Sample data showed that the size of company captured was very similar to the Doherty and Fulford study, though. Employee titles were not available from the original study to verify that the percentages of non-executives were any different. This study pursued multi-variate analysis in the hopes of capturing some of the relationships that previous, univariate studies did not uncover. While the multi-variate results were different, so were the univariate, post-hoc tests, which indicated that the results significantly differed from the Doherty and Fulford (2005) study in comparison. Research questions were very similar, as were hypotheses, but different results occurred. Because of the structure of this study and the similarity of the sample, approach, method, research questions, and hypotheses, this study resulted in successful replication of the original study, but showed significantly different results.

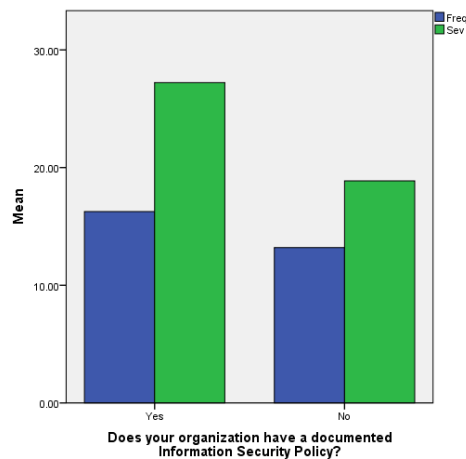
### **Results Discussion**

Analysis showed that there are some significant relationships between organizational acceptance and maintenance of the information security policy and the number and severity of breaches reported. Likewise, IT governance also showed a significant relationship to breaches. The only research area that did not show a significant relationship was ISO security certification. Research questions and the accepted hypotheses are restated below with short discussion on each.

**RQ 1:** Do organizations that have a written information security policy experience fewer security breaches or have fewer records compromised than those that do not (Doherty & Fulford, 2005)?

**H1A:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have a documented information security policy and those that do not.

Organizations that have an information security policy report higher frequency and more severe breaches than those that do not. Contrasting with Doherty and Fulford (2005), this study shows that the security policy may be even less effective than the original study, which could find no significant relationship.

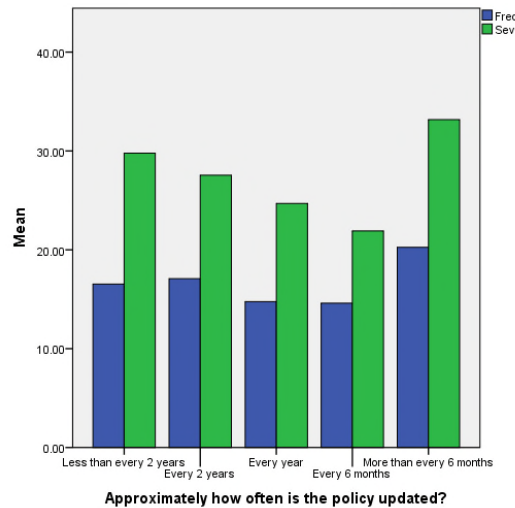


*Figure 22.* Comparison of mean breach frequency and severity for organizations that have an information security policy and those that do not.

**RQ 2:** Do organizations that update their information security policy more frequently experience fewer security breaches or have fewer records compromised than those organizations that update their policies less frequently (Doherty & Fulford, 2005)?

**H2A:** There is a significant difference in the number of security breaches and the number of compromised records between companies that update their information security policy more frequently than other companies.

Results for this analysis show that an increased frequency of policy update may reduce the number and severity of breaches, except if the updates occur more frequently than every 6 months.



*Figure 23.* Comparison of breach frequency and severity of means versus how often the security policy is updated.

**RQ 3:** Do organizations with an information security policy that has been in place for a longer period of time experience fewer security breaches or have fewer records compromised than those with a younger policy (Doherty & Fulford, 2005)?

**H3A:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have had their information security policies in place for a longer period of time than other companies.

While there is a significant difference in breaches suffered based on the length of time a policy has been instituted, the trend is difficult to ascertain. Visual inspection of the frequency graph below shows a lower number of breaches in the 1-5 year range with higher number of breaches in the 6-10 year range. Severity seems to follow similarly.

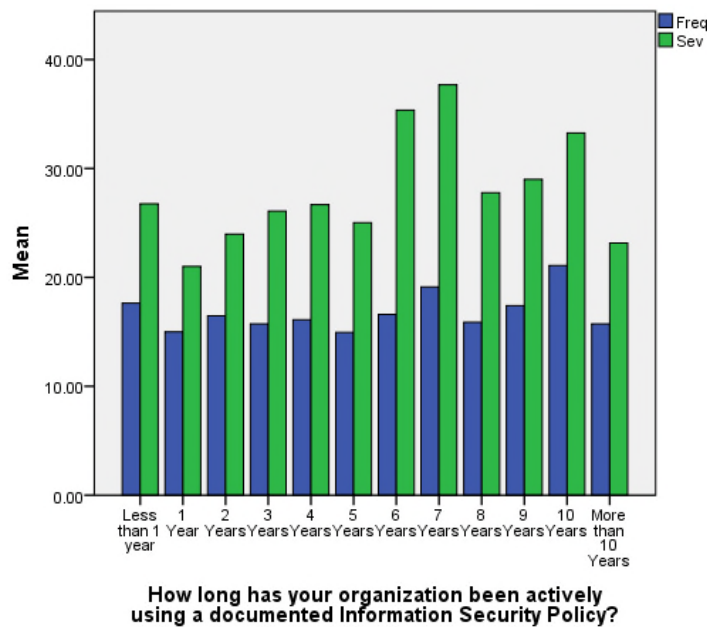


Figure 24. Comparison of breach frequency and severity means for policy length of time.

**RQ 4:** Do organizations that implement an IT governance framework (such as CobiT or ITIL) experience fewer security breaches or have fewer records compromised than those organizations that do not implement an IT governance framework?

**H4A:** There is a significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented an IT governance framework and those that have not.

IT governance framework adoption shows a very similar result as information security policy adoption. Organizations with an adopted IT governance framework suffer more frequent and more severe breaches.

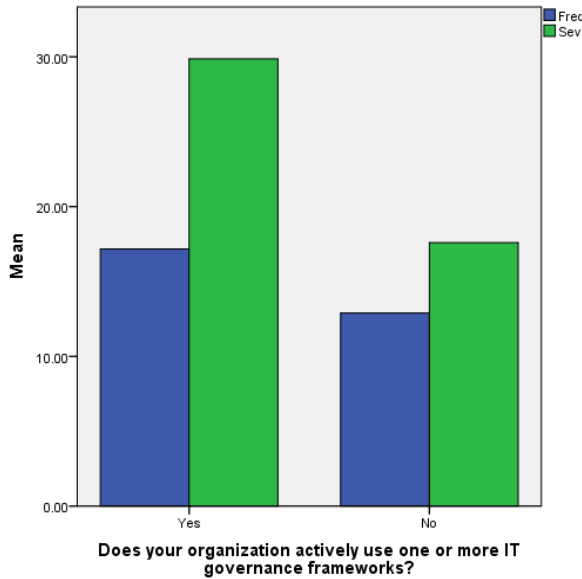


Figure 25. Comparison of breach frequency and severity means versus an organization's adoption of an IT governance framework.

**RQ 5:** Do organizations that are certified in one or more ISO security certifications experience fewer security breaches or have fewer records compromised than those organizations that are not certified?

**H5<sub>0</sub>:** There is no significant difference in the number of security breaches and the number of compromised records between companies that have formally implemented one or more ISO certifications and those that have not.

While the graph below shows a similar trend to policy adoption and IT governance, the results were not significant and no relationship could be determined.

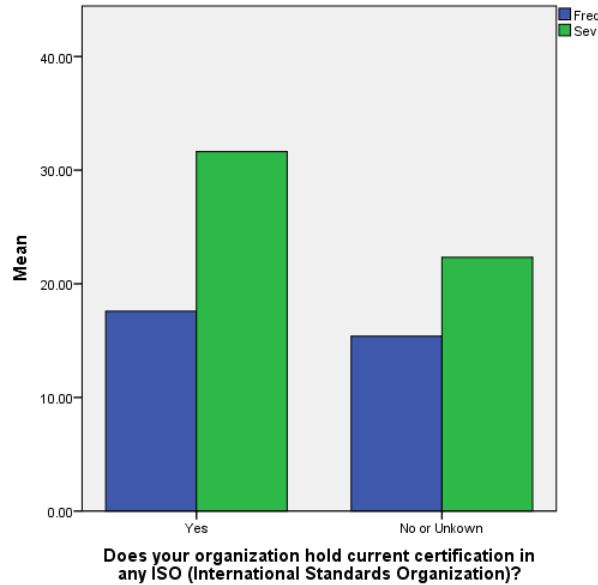


Figure 26. Comparison of breach frequency and severity means for organizations that have in an ISO security certification.

### Implications

These results contribute to the body of research by giving further depth to the previous studies that attempted to measure the effectiveness of information security policies (Davis et al., 2009; Doherty & Fulford, 2005; Heikkila, 2009; Wiant, 2005). Instead of researchers being left with an absence of affirmative evidence that security policies may or may not be effective, this study provides evidence that organizations with a policy may suffer more frequent and more severe breaches. These results run contrary to the expected results that taking the time and energy to draft, implement, and update a security policy should make an organization safer. If it was a “surprise in the present study to find almost no statistically significant relationships between the adoption of information security policies and the incidence or severity of security breaches” (p. 34) for Doherty and Fulford (2005), then the results from this study are even more surprising.

In addition, IT governance may start to fall under the same scrutiny as the information security policy. As mentioned earlier in this study, the policy is part of IT governance; the fulcrum between strategic direction and management. IT governance also does not seem to decrease breach frequency and severity, and that can imply that it may not be effective in other ways that are also assumed, such as with resource efficiency. By showing similar results between the two, this study provides alignment between the security policy and IT governance, inferring that similar organizational forces may be causing these surprising results. Improving overall IT governance effectiveness may, in turn, improve information security policy effectiveness.

Results of this study can be explained in terms of the various theories discussed in Chapter 2. According to agency theory, the wishes of shareholders and stakeholders are not in alignment. The counter-intuitive results show that organizations do not support the shareholder and stakeholder needs for securing information assets. Their business strategy may not place enough emphasis on information security to the satisfaction of the owners. Management of information security also fails shareholders and stakeholders in regards to accurately observing, measuring, and responding to breaches. In regards to institutional theory, organizations appear to be responding to coercive and mimetic pressures that are in opposition to normative pressures. Organizations may institute information security policies based on coercion because they are mandated by law or parent organizations and as a response to mimetic pressures from other organizations that are expending information security resources in a similar way and not because they effectively reduce breaches. These pressures seem to be overpowering the normative pressures to provide information security in an effective manner, which is the ethical standard of

best practice. Deterrence theory shows that compliance with the policies is not maximizing benefit in terms of cost. In other words, the benefit of complying with policies is not perceived as being worth the effort both for users and attackers.

### **Limitations**

One of the most prominent limitations of this study is the inability to measure the breach awareness of organizations. One possible explanation of the results is that organizations that spend resources to develop information security are simply more aware of information security breach frequency and severity. As an example, if an organization does not have a policy in place that mandates monitoring network intrusion, then network intrusion may never be noticed. Breach awareness of organizations would require further research to be able to assess with any accuracy.

This study also could not directly measure the effectiveness of management. Some organizations may perform very well even without formal guidance, while others may fail even with extensive documentation. While the policy indicates a certain level of engagement by management, this study did not directly measure what happened between the policy and the breach.

This study did not measure quality of the organizational constructs that were measured. Information security policies vary in quality as noted in the follow up studies by Doherty and Fulford (2009; 2011). IT governance has maturity levels that define how well the organization's IT is governed. Higher quality policies and more mature governance may show positive results in reducing breaches.



### **Recommendations for Further Research**

This study provides a springboard for investigation into several avenues of the topic. Foremost, research into breach awareness would help understanding of the surprising results obtained in this study. As mentioned above, measuring the effectiveness of quality policies and IT governance as compared to breaches may show that the manner in which policies are constructed and the maturity level of governance may show results. Studies that explore ways to make the content of the policy more relevant and effective within organizational management and thereby driving user compliance could net benefits that would help in a practice. Measuring if end user compliance reduces breaches would help understand the level of benefit of security management. This study revealed no significant relationship in breach activity related to ISO certification, research focused in that area may find more substantial conclusions. The surprising nature of this study's results produce fertile ground for further exploration.

### **Conclusion**

This study provided a well-balanced and direct progression of prior research into the effectiveness of information security policies and the protection against breaches that they provide organizations. This study accomplished its goal of finding out more about organizational efforts to combat security breaches, but what was uncovered deepens the mystery. Finding that organizations with an information security policy may be more vulnerable is discomfoting in many ways. Efforts are being made to reduce breaches, but the efforts may be having a contrary effect. Doherty and Fulford (2005) were surprised, and perhaps disappointed, that they were not able to show that information security policies are effective. This study takes those results even further in a direction opposite that which would be desirable to security professionals. The results of this study do not give executives and managers reassurance that the

frameworks and guidance previously given will net real benefits in terms of a more secure organization.

This study reveals that there are dynamics in play that may be more serious than previously understood. The results show an opposite or inverse relationship between efforts to comply with established frameworks and best practices. Understanding those dynamics may be critical in improving the information security of organizations that practice business today.

## References

- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276–289.
- Ameri, A. (2004). The five pillars of information security. *Risk Management, 51*(7), 48.
- Anthes, G. H. (2005). ITIL catches on. *Computerworld, 39*(44), 39.
- Atkinson, W. (2005). Integrating risk management & security. *Risk Management, 52*(10), 32.
- Autry, C. W., & Bobbitt, L. M. (2008). Supply chain security orientation: conceptual development and a proposed framework. *International Journal of Logistics Management, 19*(1), 42.
- Basin, D., Jugé, V., Klaedtke, F., & Zălinescu, E. (2013). Enforceable security policies revisited. *ACM Transactions on Information and System Security (TISSEC), 16*(1), 1–26.  
<http://doi.org/10.1145/2487222.2487225>
- Beccaria, C. (2011). *On crimes and punishments*. Transaction Publishers.
- Braganza, A., & Desouza, K. C. (2006). Implementing section 404 of the sarbanes oxley act: Recommendations for information systems organizations. *Communications of the Association for Information Systems, 18*, 22.
- Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk Management, 54*(1), 24.
- Brown, W., & Nasuti, F. (2005). Sarbanes--Oxley and enterprise security: IT governance -- what it takes to get the job done. *Information Systems Security, 14*(5), 15–28.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–A7. <http://doi.org/Article>

- Cadrain, D. (2005). Liability for employee identity theft is growing. *HRMagazine*, 50(6), 35.
- Cannoy, S., Palvia, P. C., & Schilhavy, R. (2006). A Research Framework for Information Systems Security. *Journal of Information Privacy & Security*, 2(2), 3.
- Carpenter, A. N. (2010). Beccaria, Cesare: Classical school. In F. Cullen & P. Wilcox, *Encyclopedia of Criminological Theory*. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc. Retrieved from <http://sk.sagepub.com/reference/criminologicaltheory/n19.xml>
- Cavusoglu, H., & Bulgurcu, B. (2010). Information security policy compliance. *Management Information Systems*, 34(3), 523–548.
- Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5), 1849. <http://doi.org/10.1016/j.chb.2012.05.003>
- Cross, S. (2004). Corporate governance, information technology and the electronic company in the United Kingdom. *Information & Communications Technology Law*, 13(2), 117–128. <http://doi.org/10.1080/1360083042000210541>
- Daily, C. M., Dalton, D. R., & Cannella, A. A. (2003). Corporate governance: Decades of dialogue and data. *Academy of Management Review*, 28(3), 371–382. <http://doi.org/Article>
- D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the is security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643–658. <http://doi.org/http://dx.doi.org.library.capella.edu/10.1057/ejis.2011.23>

- Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, 24(4), 361–372. <http://doi.org/Article>
- Davis, G., Garcia, A., & Zhang, W. (2009). Empirical analysis of the effects of cyber security incidents. *Risk Analysis*, 29(9), 1304–1316. <http://doi.org/10.1111/j.1539-6924.2009.01245.x>
- De Haes, S., & Van Grembergen, W. (2008). Analysing the relationship between IT governance and business/IT alignment maturity. In *Hawaii International Conference on System Sciences* (Vol. 0, p. 428). Los Alamitos, CA, USA: IEEE Computer Society. <http://doi.org/http://doi.ieeecomputersociety.org/10.1109/HICSS.2008.66>
- De Haes, S., & Van Grembergen, W. (2009). Exploring the relationship between IT governance practices and business/IT alignment through extreme case analysis in Belgian mid-to-large size financial enterprises. *Journal of Enterprise Information Management*, 22(5), 615–637.
- DeLuca, D., Gallivan, M. J., & Kock, N. (2008). Furthering Information Systems Action Research: A Post-Positivist Synthesis of Four Dialectics. *Journal of the Association for Information Systems*, 9(2), 48–71.
- Dimitropoulos, L., & Rizk, S. (2009). A state-based approach to privacy and security for interoperable health information exchange. *Health Affairs*, 28(2), 428–34.
- Doherty, N., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29(6), 449–457. <http://doi.org/10.1016/j.ijinfomgt.2009.05.003>

- Doherty, N., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management*, 31(3), 201–209.  
<http://doi.org/10.1016/j.ijinfomgt.2010.06.001>
- Doherty, N., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal*, 18, 21.
- Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1), 55–63.  
<http://doi.org/10.1016/j.cose.2005.09.009>
- Drugescu, C., & Etges, R. (2006). Maximizing the return on investment on information security programs: Program governance and metrics. *Information Systems Security*, 15(6), 30–40.  
<http://doi.org/10.1080/10658980601051482>
- Duhachek, A., & Iacobucci, D. (2004). Alpha's standard error (ASE): An inaccurate and precise confidence interval estimate. *Journal of Applied Psychology*, 89(5), 792–808.
- Edelstein, S. M. (2004). Sarbanes-Oxley compliance for nonaccelerated filers. *The CPA Journal*, 74(12), 52.
- Fadlalla, A., & Wickramasinghe, N. (2004). An integrative framework for HIPAA-compliant I\*IQ healthcare information system. *International Journal of Health Care Quality Assurance*, 17(2/3), 65.

Fariborz, F., Shamkant, B. N., Gunter, P. S., & Philip, H. E. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, 6(2-3), 203.

Feizizadeh, A. (2012). Corporate governance: Frameworks. *Indian Journal of Science and Technology*, 5(9), 3353.

Finch, H. (2005). Comparison of the performance of nonparametric and parametric MANOVA test statistics when assumptions are violated. *Methodology: European Journal of Research Methods for the Behavioral and Social Sciences*, 1(1), 27–38.

<http://doi.org/10.1027/1614-1881.1.1.27>

Fitzgerald, M. The art of compliance. (June 2006). Retrieved from

<http://www.allbusiness.com/company-activities-management/management-corporate-culture/13448323-1.html>

Fonstad, N. O., & Subramani, M. (2009). Building enterprise alignment: A case study. *MIS Quarterly Executive*, 8(1), 31–41. <http://doi.org/Case Study>

Fulford, H., & Doherty, N. (2003). The application of information security policies in large UK-based organizations: An exploratory investigation. *Information Management & Computer Security*, 11(2/3), 106.

Galbraith, M. L. (2013). Identity crisis: Seeking a unified approach to plaintiff standing for data security breaches of sensitive personal information. *American University Law Review*, 62(5), 1365.

Galinac Grbac, T., Runeson, P., Huljenić, D., Datavetenskap, Lunds tekniska högskola, L., Lunds universitet, ... Faculty of Engineering. (2013). A second replicated quantitative

- analysis of fault distributions in complex software systems. *IEEE Transactions on Software Engineering*, 39(4), 462–476. <http://doi.org/10.1109/TSE.2012.46>
- Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216–230.
- Gordon, L. A., & Loeb, M. P. (2002). Return on information security investments: Myths vs. realities. *Strategic Finance*, 84(5), 26.
- Gupta, M. (2009). *Social and human elements of information security : emerging trends and countermeasures*. Hershey PA: Information Science Reference.
- Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377.
- Hall, L. A., & Gaetanos, C. (2006). Treatment of Section 404 compliance costs. *The CPA Journal*, 76(3), 58.
- Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, 11(1), 55–61. <http://doi.org/10.1016/j.istr.2005.12.004>
- Hawkins, K. W., Alhajjaj, S., & Kelley, S. S. (2003). Using Cobit to Secure Information Assets. *The Journal of Government Financial Management*, 52(2), 22.
- Hawser, A. (2008). Fighting fraudsters from within. *Global Finance*, 22(4), 70.
- Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security*, 4, 3.



- Healy, P. M., & Palepu, K. G. (2003). The fall of Enron. *The Journal of Economic Perspectives*, 17(2), 3–26.
- Heikkila, F. (2009). *An analysis of the impact of information security policies on computer security breach incidents in law firms* (Dissertation). Nova Southeastern University.
- Higgins, H. N. (1999). Corporate system security: Towards an integrated management approach. *Information Management & Computer Security*, 7(5), 217.
- Holtfreter, R. E., & Holtfreter, K. (2006). Gauging the effectiveness of US identity theft legislation. *Journal of Financial Crime*, 13(1), 56.
- Höne, K., & Eloff, J. H. P. (2002). Information security policy -- what do international information security standards say? *Computers & Security*, 21(5), 402–409.  
[http://doi.org/10.1016/S0167-4048\(02\)00504-7](http://doi.org/10.1016/S0167-4048(02)00504-7)
- Jensen, T. B., Kjærgaard, A., & Svejvig, P. (2009). Using institutional theory with sensemaking theory: a case study of information system implementation in healthcare. *Journal of Information Technology*, 24(4), 343–353.
- Jintae, L., & Younghwa, L. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 10(2/3), 57.
- Jory, S. R., Peng, J., & Ford, C. O. (2010). The wealth effects of investing in information technology: The case of Sarbanes-Oxley section 404 compliance: *Review of Accounting and Finance*, 9(3), 285–305. <http://doi.org/10.1108/14757701011068075>
- Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, 12(1), 69–91.

- Khoury, R., & Tawbi, N. (2012). Corrective enforcement: A new paradigm of security policy enforcement by monitors. *ACM Transactions on Information and System Security (TISSEC)*, 15(2), 1–27. <http://doi.org/10.1145/2240276.2240281>
- Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management*, 23(2), 76–87.  
<http://doi.org/Article>
- Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7), 493–508.  
<http://doi.org/10.1016/j.cose.2009.07.001>
- Kwo-Shing Hong, Yen-Ping, C., Chao, L. R., & Tang, J.-H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, 14(2), 104–115.
- Lainhart IV, J. W. (2000). Why IT governance is a top management issue. *Journal of Corporate Accounting & Finance (Wiley)*, 11(5), 33–40. <http://doi.org/Article>
- Lainhart, J. W. (2000). COBIT: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems*, 14(1), 21.
- Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707–718. <http://doi.org/10.1016/j.im.2003.08.008>

- Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3-4), 215–228.
- Lineberry, S. (2007). The human element: The weakest link in information security. *Journal of Accountancy*, 204(5), 44.
- Lund, A., & Lund, M. (2013). One-way MANOVA in SPSS. Lund Research Ltd. Retrieved from <https://statistics.laerd.com/premium/owm/one-way-manova-in-spss.php>
- Mahmood, M., Siponen, M., & Pahlila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, 52(12), 145–147.
- Ma, Q., Schmidt, M., & Pearson, J. (2009). An integrated framework for information security management. *Review of Business*, 30(1), 58.
- Marrone, M., Hoffman, L., & Kolbe, L. (2010). IT executives' perception of CobiT: Satisfaction, business-IT alignment and benefits. Presented at the Sixteenth Americas Conference on Information Systems, Lima, Peru.
- Millions of respondents on our online panel | SurveyMonkey Audience. (n.d.). Retrieved February 27, 2016, from <https://www.surveymonkey.com/mp/audience/our-survey-respondents/>
- Moore, G. (1999). Tinged shareholder theory: Or what's so special about stakeholders? *Business Ethics, A European Review*, 8(2), 117. <http://doi.org/10.1111/1467-8608.00136>
- Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, 22(7), 580–584. [http://doi.org/10.1016/S0167-4048\(03\)00705-3](http://doi.org/10.1016/S0167-4048(03)00705-3)

- Myler, E., & Broadbent, G. (2006). ISO 17799: Standard for security. *Information Management Journal*, 40(6), 43–52. <http://doi.org/Article>
- Netschert, B. (2008). *Information security readiness and compliance in the healthcare industry* (Dissertation). Stevens Institute of Technology.
- Pabrai, U. A. (2006). Rules & regulations: The impact of compliance on IT. *Certification Magazine*, 8(3), 38–40. <http://doi.org/Article>
- Pauli, D. (2008). Think ITIL will reduce cost? You're wrong. *NetworkWorld Asia*, 4(5), 8–8.
- Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, 21(4), 7–22. <http://doi.org/Article>
- Peters, S. (2009). *14th annual CSI computer crime and security survey: Executive summary*.
- Pieters, W., Dimkov, T., & Pavlovic, D. (2013). Security Policy Alignment: A Formal Approach. *IEEE Systems Journal*, 7(2), 275–287. <http://doi.org/10.1109/JSYST.2012.2221933>
- Pironti, J. (2008). Key elements of an information risk management program: Transforming information security into information risk management. *Information Systems Control Journal*, 2, 42.
- Poole, M. S. (2009). Response to Jones and Karsten, “Giddens’s structuration theory and information systems researched.” *MIS Quarterly*, 33(3), 583–587. <http://doi.org/Article>
- Poore, R. S. (2005). Information security governance. *EDPACS*, 33(5), 1–8.
- Radcliff, D. (1998). Physical security: The danger within. *InfoWorld*, 20(16), 95.
- Ramlaoui, S., & Semma, A. (2014). Comparative study comparative of COBIT with other it governance frameworks. *International Journal of Computer Science Issues (IJCSI)*, 11(6), 95.

- Roberts, G. K. (2005). *Security Breaches, Privacy Intrusions, and Reporting of Computer Crimes*. Retrieved from <http://proquest.umi.com.library.capella.edu/pqdweb?did=999547341&Fmt=7&clientId=62763&RQT=309&VName=PQD>
- Robinson, N. (2005). IT excellence starts with governance. *The Journal of Investment Compliance*, 6(3), 45.
- Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis & Management*, 30(2), 256–286.
- Rowlands, B. (2009). A social actor understanding of the institutional structures at play in information systems development. *Information Technology & People*, 22(1), 51.
- Ruey-Shiang, S., Che-Pin, C., & Sheng-Pao, S. (2013). Correlation and impact between IT management and IT governance. *Information Technology Journal*, 12(18), 4569–4575.
- Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, 39(4), 60.
- Salkind, Neil J. (2010). *Encyclopedia of research design*. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc. Retrieved from <http://knowledge.sagepub.com/view/researchdesign/SAGE.xml>
- Sample security policies. (2010). Retrieved February 5, 2011, from <http://www.nchica.org/hipaaresources/Security/rule.htm>
- Sherer, S. A. (2009). Information Systems and Healthcare XXXIII: An Institutional Theory Perspective on Physician Adoption of Electronic Health Records. *Communications of the Association for Information Systems*, 26, 25.

- Simonsson, M., Lagerström, R., & Johnson, P. (2008). A Bayesian network for IT governance performance prediction. In *Proceedings of the 10th international conference on Electronic commerce - ICEC '08* (p. 1). Innsbruck, Austria.  
<http://doi.org/10.1145/1409540.1409542>
- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2), 64–71.  
<http://doi.org/10.1109/MC.2010.35>
- Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487–A12.
- Son, J.-Y. (2011). Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow Is Security Policies. *Information & Management*, 48(7), 296–302.  
<http://doi.org/10.1016/j.im.2011.07.002>
- Sonnenfeld, J. (2004). Good governance and the misleading myths of bad metrics. *Academy of Management Executive*, 18(1), 108–113. <http://doi.org/Article>
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276.
- Straub, D. W., Goodman, S., Baskerville, R., Goodman, S. E., & Ebrary. (2008). *Information security: Policy, processes and practices* (Vol. 11.). Armonk: M.E. Sharpe.
- Swanson, R., & Holton, E. (2005). *Research in organizations: Foundations and methods of inquiry* (1st ed.).
- Swartz, N. (2008). Record data breaches in 2007. *Information Management Journal*, 42(2), 16.

- Tarn, J. M., Raymond, H., Razi, M., & Han, B. T. (2009). Exploring information security compliance in corporate IT governance. *Human Systems Management*, 28(3), 131.
- Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24(6), 472–484. <http://doi.org/10.1016/j.cose.2005.05.002>
- Tichenor, C. (2007). A model to quantify the return on investment of information assurance. *DISAM Journal of International Security Assistance Management*, 29(3), 125.
- Tse, T. (2011). Shareholder and stakeholder theory: After the financial crisis. *Qualitative Research in Financial Markets*, 3(1), 51–63. <http://doi.org/10.1108/17554171111124612>
- Tugas, F. C. (2010). Assessing the level of information technology (IT) processes performance and capability maturity in the Philippine food, beverage, and tobacco (FBT) industry using the COBIT framework. *Academy of Information & Management Sciences Journal*, 13(1), 45–68. <http://doi.org/Article>
- Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems*, 8(4), 240–263. <http://doi.org/10.1016/j.accinf.2007.09.001>
- U. S. Department of Health and Human Services. (2010). Summary of the HIPAA privacy rule. Retrieved November 6, 2011, from <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>
- Wakefield, R. (2004). Computer monitoring and surveillance. *The CPA Journal*, 74(7), 52.
- Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information security and Sarbanes-Oxley compliance: An exploratory study. *Journal of Information Systems*, 25(1), 185.

- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101–105.  
<http://doi.org/10.1057/ejis.2009.12>
- Wiant, T. L. (2005). Information security policy's impact on reporting security incidents. *Computers & Security*, 24(6), 448–459. <http://doi.org/10.1016/j.cose.2005.03.008>
- Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management / AHIMA, American Health Information Management Association*, 11(Journal Article), 1h.



## APPENDIX A. G\*POWER 3.1 OUTPUT FOR POWER ANALYSIS OF REQUIRED SAMPLE SIZE

MANOVA power analysis for required sample size given medium effect size and above 95% confidence.

[3] -- Sunday, December 07, 2014 -- 15:51:46

F tests – MANOVA: Global effects

**Options:** Pillai V, O'Brien–Shieh Algorithm

**Analysis:** A priori: Compute required sample size

**Input:** Effect size  $f^2(V)$  = 0.0625

$\alpha$  err prob = 0.05

Power ( $1-\beta$  err prob) = 0.95

Number of groups = 4

Response variables = 2

**Output:** Noncentrality parameter  $\lambda$  = 21.5000000

Critical F = 2.1255907

Numerator df = 6.0000000

Denominator df = 336


Total sample size = 172

Actual power = 0.9525011

Pillai V= 0.1176471

## APPENDIX B. STUDY SURVEY INSTRUMENT

From Do information security policies reduce the incidence of security breaches: An exploratory analysis, by Doherty, N., & Fulford, 2005, *Information Resources Management Journal*, 18, 21. Copyright 2005 by Doherty, N. Adapted with permission.

  
**CAPELLA UNIVERSITY**

**Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot**

Hi, and thanks for your interest! The answers collected in this study will be used in a doctoral dissertation to analyze possible relationships between information security policies and information security breaches. We have one screening question to ask before we get started that involves your knowledge of information security breaches that may or may not have occurred at your organization.

Answers to all questions in the survey will be kept confidential, and you will not be asked to name the organization that you are involved with. There is no known way to connect your responses with your identity or your organization. Still, if you feel uncomfortable answering questions about information security breaches for your organization, or if you are not allowed to answer, please select "no".

Answering "yes" to the question will take you into the survey, while answering "no" will result in disqualification from the study.

If you have any questions about the study, or if you would like a copy of the study when it is released, please email me at the following address: [jonpaarlberg@gmail.com](mailto:jonpaarlberg@gmail.com)

1. Do you have knowledge of the approximate number of information security breaches that have occurred at your organization, if any, and do you know approximately how many records, if any were compromised during the last 2 years?  
(If you know that your organization hasn't had any breaches, that is OK and you can answer "yes")

1



CAPELLA UNIVERSITY

**Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot**

**INFORMED CONSENT FORM**

Study Title: An Empirical Analysis on the Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification: a Global Study  
Researcher: Jon Paarberg  
Email Address and Telephone Number: jonpaarberg@gmail.com 775.209.5062  
Research Supervisor: Dr. Wenbin Luo  
Email Address: Wenbin.Luo@capella.edu

You are invited to be part of a research study. The researcher is a doctoral learner at Capella University in the School of Business and Technology. The information in this form is provided to help you decide if you want to participate. The form describes what you will do during the study and the risks and benefits of the study.

If you have any questions or do not understand something in this form, you should ask the researcher. Do not participate in the study unless the researcher has answered your questions and you decide that you want to be part of this study.

**WHAT IS THIS STUDY ABOUT?**

The researcher wants to find out what people think about Information Security Policies, IT Governance, ISO Certification, and Information Security Breaches in their organization.

**HOW MANY PEOPLE WILL BE IN THIS STUDY?**

About 500 participants will be in this study.

**WHY AM I BEING ASKED TO BE IN THE STUDY?**

You are invited to be in the study because you are:

- A person that may have knowledge of information security policies in your organization
- A person that may have knowledge of information security breaches in your organization

All participants will be above 18 years old.

If you do not meet the description above, you are not able to be in the study.

**WHO IS PAYING FOR THIS STUDY?**

The researcher is not receiving funds to conduct this study.

**WILL IT COST ANYTHING TO BE IN THIS STUDY?**

You do not have to pay to be in the study.

2

**HOW LONG WILL I BE IN THE STUDY?**

If you decide to be in this study, your participation will last approximately 10-13 minutes.

**WHAT WILL HAPPEN DURING THIS STUDY?**

If you decide to be in this study and if you sign this form, you will do the following things:

Give information about an organization that you are involved with, such as:

Demographics- number of employees, nationality, industry

Information security policy characteristics- existence of a policy, age, frequency of updates.

IT governance frameworks- frameworks that may be used by your organization and their maturity level

ISO certifications- certifications that may be held by your organization

Information security breaches- number of breaches and number of records compromised in the past 2 years

Optionally, you may supply your email address for further communication. This is not required.

**HOW WILL BEING IN THIS STUDY HELP ME?**

Being in this study may not help you directly or immediately, but a copy of the complete study will be available to you if you participate. Information from this study might help researchers help others in the future.

**ARE THERE RISKS TO ME IF I AM IN THIS STUDY?**

No study is completely risk-free. However, we don't anticipate that you will be harmed or distressed during this study. You may discontinue participation in the study at any time if you become uncomfortable. You should be aware, however, that there is a small possibility that responses could be viewed by unauthorized parties (e.g. computer hackers because your responses are being entered and stored on a web server)

**WILL I GET PAID?**

You may receive SurveyMonkey Audience rewards according to SurveyMonkey's policies.

#### **DO I HAVE TO BE IN THIS STUDY?**

Your participation in this study is voluntary. You can decide not to be in the study and you can change your mind about being in the study at any time. There will be no penalty to you. If you want to stop being in the study, simply exit the survey.

#### **WHO WILL USE AND SHARE INFORMATION ABOUT MY BEING IN THIS STUDY?**

Any information you provide in this study that could identify you such as your name, age, or other personal information will be kept confidential. Name, age, and other personal information will not be collected unless it is voluntarily given by you in the survey. Even if given, they will be kept secure and confidential by the researcher. In any written reports or publications, no one will be able to identify you.

The researcher will keep the information you provide in either the encrypted and password protected SurveyMonkey servers or in an encrypted file on a password protected computer. If you have questions about the security of SurveyMonkey please click the link to their security statement that contains full information on how they store their data:

<https://www.surveymonkey.com/mp/policy/security/>

Only the researcher, researcher's supervisor, and dissertation committee will have access to the study data. Additionally, Capella University's IRB, the Research Compliance Committee (RCC), or its designees may review your research records.

Even if you leave the study early, the researcher may still be able to use your data. Any completed questions may be valid for analysis even though all questions were not answered.

#### **LIMITS OF PRIVACY (CONFIDENTIALITY)**

Generally speaking, the researcher can assure you that he will keep everything you tell him or do for the study private. Yet there are times where the researcher cannot keep things private (confidential). The researcher cannot keep things private (confidential) when:

The researcher finds out that a child or vulnerable adult has been abused  
The researcher finds out that that a person plans to hurt him or herself, such as commit suicide,  
The researcher finds out that a person plans to hurt someone else,

There are laws that require many professionals to take action if they think a person might harm themselves or another, or if a child or adult is being abused. In addition, there are guidelines that researchers must follow to make sure all people are treated with respect and kept safe. In most states, there is a government agency that must be told if someone is being abused or plans to hurt themselves or another person. Please ask any questions you may have about this issue before agreeing to be in the study. It is important that you do not feel betrayed if it turns out that the researcher cannot keep some things private.

#### **WHO CAN I TALK TO ABOUT THIS STUDY?**

You can ask questions about the study at any time. You can call the researcher at any time if you have any concerns or complaints. You should call the researcher at the phone number listed on page 1 of this form if you have questions about the study procedures, study costs (if any), study payment (if any), or if you get hurt or sick during the study.

Capella University's Institutional Review Board (IRB) has been established to protect the rights and welfare of human research participants. Please contact us at 1-888-227-3552, extension 6313, for any of the following reasons:

You have questions about your rights as a research participant.  
You wish to discuss problems or concerns.  
You have suggestions to improve the participant experience.  
You do not feel comfortable talking with the researcher.

4

## 2. DO YOU WANT TO BE IN THIS STUDY?

By clicking the link below you agree to the following statement:

I have read this form, and I have been able to ask questions about this study. I voluntarily agree to be in this study. I agree to allow the use and sharing of my study-related records as described above.

I have not given up any of my legal rights as a research participant. I will print a copy of this consent information for my records.

**CLICK 'I AGREE' TO CONTINUE TO THE SUVEY OR 'I DISAGREE' TO EXIT**

- I AGREE  
 I DISAGREE

5



CAPELLA UNIVERSITY

Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

3. In what country is your organization headquartered?

4. Is your organization multi-national?

- Yes  
 No

5. Which of the following best describes the principal industry of your organization?

6. Approximately how many people are employed in your organization?

- Less than 500  
 500-1,000  
 1,001-1,500  
 1,501-2,000  
 2,001-3,000  
 3,001-5,000  
 5,001-10,000  
 over 10,000

6

7. Pick the position that most closely relates to your title:

- |   |  |
|---|--|
| <input type="radio"/> Chief Executive Officer/President       | <input type="radio"/> Information Technology (IT) Director |
| <input type="radio"/> Chief Information Officer               | <input type="radio"/> Information Technology (IT) Manager  |
| <input type="radio"/> Chief Technical Officer                 | <input type="radio"/> Information Technology (IT) Analyst  |
| <input type="radio"/> Information Security (IS) Director      | <input type="radio"/> Programmer                           |
| <input type="radio"/> Information Security (IS) Manager       | <input type="radio"/> Database Administrator (DBA)         |
| <input type="radio"/> Information Security (IS) Administrator | <input type="radio"/> Server Systems Analyst               |
| <input type="radio"/> Information Security (IS) Analyst       | <input type="radio"/> End Client Systems                   |
| <input type="radio"/> Other (please specify)                  |  |

8. Please indicate any security certifications that you hold:

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Computer Associates Certified eTrust Specialist (CACES) | <input type="checkbox"/> Certification and Accreditation Professional                           | <input type="checkbox"/> Certified Counterespionage & Information Security Manager         |
| <input type="checkbox"/> Computer Security Incident Handler (CSIH)               | <input type="checkbox"/> ISSEP®: Information Systems Security Engineering Professional          | <input type="checkbox"/> Certified Electronic Evidence Collection Specialist Certification |
| <input type="checkbox"/> Cisco Certified Security Professional (CCSP)            | <input type="checkbox"/> ISSAP®: Information Systems Security Architecture Professional         | <input type="checkbox"/> Certified Forensic Computer Examiner Certification                |
| <input type="checkbox"/> Cisco Advanced Security Field Specialist                | <input type="checkbox"/> ISSMP®: Information Systems Security Management Professional           | <input type="checkbox"/> Certified Cyber-Crime Expert (C3E)                                |
| <input type="checkbox"/> Cisco Firewall Specialist                               | <input type="checkbox"/> ISO 27001:2005- Lead Auditor Course                                    | <input type="checkbox"/> Basic Internet Investigation                                      |
| <input type="checkbox"/> Cisco IPS Specialist                                    | <input type="checkbox"/> Microsoft Certified Systems Engineer: Security (MCSE: Security)        | <input type="checkbox"/> Intermediate Internet Investigation                               |
| <input type="checkbox"/> Cisco Security Sales Specialist                         | <input type="checkbox"/> Ethical Hacker   | <input type="checkbox"/> Advanced Internet Investigation                                   |
| <input type="checkbox"/> Cisco Security Solutions and Design Specialist          | <input type="checkbox"/> Computer Hacking Forensic Investigator                                 | <input type="checkbox"/> CyberSecurity Forensic Analyst (CSFA)                             |
| <input type="checkbox"/> Cisco VPN Specialist                                    | <input type="checkbox"/> Licensed Penetration Tester  | <input type="checkbox"/> CyberSecurity Institute Certified Instructor (CSICI)              |
| <input type="checkbox"/> Cisco VPN/Security Sales Specialist                     | <input type="checkbox"/> Certified Network Defence Architect                                    | <input type="checkbox"/> Field Certified™ Security Specialist (FCSS™)                      |
| <input type="checkbox"/> CIW Security Analyst                                    | <input type="checkbox"/> Network Security Administrator   | <input type="checkbox"/> Security Certified Network Professional (SCNP)                    |
| <input type="checkbox"/> CIW Security Professional                               | <input type="checkbox"/> Certified Security Analyst   | <input type="checkbox"/> Security Certified Network Architect (SCNA)                       |
| <input type="checkbox"/> CompTIA Security+                                       | <input type="checkbox"/> Certified Secure Programmer and Certified Secure Application Developer | <input type="checkbox"/> SCNP — Security Certified Network Professional                    |
| <input type="checkbox"/> GIAC, various   | <input type="checkbox"/> Security 5   | <input type="checkbox"/> SCNA — Security Certified Network Architect                       |
| <input type="checkbox"/> GIAC Security Essentials Certification (GSEC)           | <input type="checkbox"/> Associate Business Continuity Professional                             |  |
| <input type="checkbox"/> GIAC Certified Firewall Analyst (GCFW)                  |   |  |

7



- |  |   |   |
|--|---|---|
| <input type="checkbox"/> GIAC Certified Intrusion Analyst (GCIA)                     | <input type="checkbox"/> Certified Functional Continuity Professional                 | <input type="checkbox"/> The CWSP® (Certified Wireless Security Professional) certification |
| <input type="checkbox"/> GIAC Certified Incident Handler (GCIH)                      | <input type="checkbox"/> Certified Business Continuity Professional                   | <input type="checkbox"/> SPS – Symantec Product Specialist                                  |
| <input type="checkbox"/> GIAC Certified Windows Security Administrator (GCWN)        | <input type="checkbox"/> Master Business Continuity Professional                      | <input type="checkbox"/> STA – Symantec Technology Architect                                |
| <input type="checkbox"/> GIAC Certified UNIX Security Administrator (GCUX)           | <input type="checkbox"/> Certified Computer Examiner                                  | <input type="checkbox"/> SCSE – Symantec Certified Security Engineer                        |
| <input type="checkbox"/> GIAC Information Security Officer (GISO)                    | <input type="checkbox"/> PCIP (Professional in Critical Infrastructure Protection)    | <input type="checkbox"/> SCSP – Symantec Certified Security Practitioner                    |
| <input type="checkbox"/> GIAC Systems and Network Auditor (GSNA)                     | <input type="checkbox"/> Security University Software Security Engineer Certification | <input type="checkbox"/> RSA Certified Security Professional                                |
| <input type="checkbox"/> GIAC Security Leadership Certificate (GSLC)                 | <input type="checkbox"/> Certified Fraud Examiner                                     | <input type="checkbox"/> RSA SecurID Certified Administrator (RSA SecurID CA)               |
| <input type="checkbox"/> GIAC IT Security Audit Essentials (GSAE)                    | <input type="checkbox"/> Certified Security Compliance Specialist                     | <input type="checkbox"/> RSA Certified Instructor (RSA/CI)                                  |
| <input type="checkbox"/> GIAC Gold Standard Certificate (GGSC-0100)                  | <input type="checkbox"/> Network Security Certified Professional                      | <input type="checkbox"/> RSA Certified Systems Engineer (RSA/CSE)                           |
| <input type="checkbox"/> Certified Information System Auditor (CISA)                 | <input type="checkbox"/> Enterprise and Web Security Certified Professional           | <input type="checkbox"/> TICSA Professional Certification                                   |
| <input type="checkbox"/> Certified Information Security Manager (CISM)               | <input type="checkbox"/> Certified Computer Crime Investigator [Advanced]             | <input type="checkbox"/> MCSE: Security on Microsoft Windows Server 2003                    |
| <input type="checkbox"/> Certified Information Systems Security Professional (CISSP) | <input type="checkbox"/> Certified Computer Crime Investigator [Basic]                | <input type="checkbox"/> MCSA: Security on Microsoft Windows Server 2003                    |
| <input type="checkbox"/> Systems Security Certified Practitioner (SSCP)              | <input type="checkbox"/> Certified Computer Forensic Technician [Basic]               | <input type="checkbox"/> ITIL Foundation Level Certification                                |
|  | <input type="checkbox"/> Certified Computer Forensic Technician [Advanced]            | <input type="checkbox"/> ITIL Practitioner Level Certification                              |
|  |   | <input type="checkbox"/> ITIL Management Level Certification                                |

8



Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

9. Please record in the table below the approximate number of IT security breaches that your organization has experienced in the past 2 years, and indicate the total number of records that were compromised in the past 2 years as a result of those breaches. If you are unwilling or not permitted to answer any questions in this section, then you may skip them.

Breach: A security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, changed or used by an individual unauthorized to do so.

Record: A combination of fields or items from a database that, when put together, represent one set of information. For example, a patient record or customer record comprised of elements from address, appointment, and billing tables. Another example would be one transaction for payment.

	Approximate number of occurrences in the last 2 years	Approximate number of records compromised in the last 2 years
Computer Virus- Umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware	<input type="text"/>	<input type="text"/>
Hacking Incident (External)- Someone from outside the organization intentionally circumvented security measures to commit a breach	<input type="text"/>	<input type="text"/>

	Approximate number of occurrences in the last 2 years	Approximate number of records compromised in the last 2 years
Unauthorized access to or use of data (internal)- Someone from within the organization, employee, intern, volunteer, used their permitted access to copy, transmit, view, steal, change or use data in an appropriate way	<input type="text"/>	<input type="text"/>
Theft of hardware / software- Equipment, storage media, applications, scripts or code were copied or removed to be used for reasons other than intended by the organization	<input type="text"/>	<input type="text"/>
Computer-based fraud- Any act using computers, the Internet, Internet devices, and Internet services to defraud people, companies, or government agencies of money, revenue, or Internet access	<input type="text"/>	<input type="text"/>
Human Error- Loss or exposure of information assets because of a human making a mistake by executing a command, code, or hardware adjustment	<input type="text"/>	<input type="text"/>
Natural disaster- Damage, loss, or exposure not caused by humans, but by natural events such as weather, seismic activity, and fire.	<input type="text"/>	<input type="text"/>

10

	Approximate number of occurrences in the last 2 years	Approximate number of records compromised in the last 2 years
Damage by disgruntled employee- A current or past member of the organization intentionally caused damage to an information system by erasing records, damaging hardware, corrupting data, or released sensitive information	<input type="text"/>	<input type="text"/>

11



CAPELLA UNIVERSITY

Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

10. Does your organization have a documented Information Security Policy?

Yes

No

12



Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

11. How long has your organization been actively using a documented Information Security Policy?

12. Approximately how often is the policy updated?

- Less than every 2 years
- Every 2 years
- Every year
- Every 6 months
- More than every 6 months

13. How is the policy disseminated to employees?

- Company Intranet
- Staff Handbook
- Other (please specify)

14. Using the dropdown menus below, please indicate the security issues covered in your Information Security Policy and/or through separate procedures or standards. If you do not explicitly cover an issue through your policy or a separate stand-alone standard, please leave blank.

Documents covering the issue

Disclosure of information	<input type="text"/>
System access control	<input type="text"/>
Internet access	<input type="text"/>
Viruses, worms & trojans	<input type="text"/>
Software development	<input type="text"/>
Contingency planning	<input type="text"/>
Encryption	<input type="text"/>
Mobile computing	<input type="text"/>
Personal usage of IS	<input type="text"/>
Physical security	<input type="text"/>
Violations and breaches	<input type="text"/>

14

15. How important do you believe the following factors to be for the successful implementation of information security in your organization?

	Not Important	Somewhat Important	Important	Mostly Important	Very Important
Ensuring security policy reflects business objectives	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
An approach to implementing security that is consistent with the organizational culture	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Visible commitment from management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A good understanding of security requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Effective marketing of security to all employees	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Distribution of guidance on information security policy to all employees	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Providing appropriate employee training and education	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Comprehensive measurement system for evaluating performance in security management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provision of feedback system for suggesting policy improvements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

15



16. How successful do you believe your organization has been in adopting each of these factors?

	Not Successful	Slightly Successful	Successful	Mostly Successful	Very Successful
Ensuring security policy reflects business objectives	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
An approach to implementing security that is consistent with the organizational culture	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Visible commitment from management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A good understanding of security requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Effective marketing of security to all employees	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Distribution of guidance on information security policy to all employees	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Providing appropriate employee training and education	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Comprehensive measurement system for evaluating performance in security management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provision of feedback system for suggesting policy improvements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

17. Please use this space if you wish to make any comments with respect to the formulation, application, or effectiveness of the information security policy



CAPELLA UNIVERSITY

Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

18. Does your organization actively use one or more IT governance frameworks?

Yes

No

17



Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

19. Please indicate the IT Governance Maturity Level of the IT governance frameworks used by your organization, if known. If your organization does not use a particular framework, then please select Non-Existent or Unknown.

	Non-Existent or Unknown	Initial/AdHoc	Repeatable but Intuitive	Defined Process	Managed and Measurable	Optimized
Calder Moir Framework	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
TickITplus™	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ISO27001	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ISO20000	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IT Service CMM - IT Service Capability Maturity Model	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Six Sigma	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IT Balanced Scorecard	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ISO38500 - International Standard for the Corporate Governance of IT	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
COBIT®	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
M_o_R® – Management of Risk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
BISL® – Business Information Services Library®	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ITIL® – The IT Infrastructure Library®	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Business Process Framework (eTOM)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ASL® – Application Services Library®	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Non-Existent or Unknown	Initial/AdHoc	Repeatable but Intuitive	Defined Process	Managed and Measurable	Optimized
MSP® – Managing Successful Programmes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PRINCE2® – Projects in Controlled Environments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PMBOK® – Project Management Body of Knowledge®	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
OPM3® – Organisational Project Management Maturity Model	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Others- please specify frameworks and maturity levels. Multiple lines may be used.



CAPELLA UNIVERSITY

Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

20. Does your organization hold current certification in any ISO (International Standards Organization)?

- Yes
- No or Unknown

20



Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

21. Please indicate which ISO certification or certifications your organization holds:

- |   |  |
|---|--|
| <input type="checkbox"/> ISO 27001 Information security management systems              | <input type="checkbox"/> ISO 27799 Information security management in health using ISO/IEC 27002     |
| <input type="checkbox"/> ISO 27002 Code of practice for information security controls   | <input type="checkbox"/> ISO/TR 13669 Financial services- Information security                       |
| <input type="checkbox"/> ISO 27014 Governance of information security                   | <input type="checkbox"/> ISO 21827 Systems security engineering- Capability Maturity Model (SSE-CMM) |
| <input type="checkbox"/> ISO 17799 Code of practice for information security management | <input type="checkbox"/> ISO 20000 IT service management   |
| <input type="checkbox"/> ISO 13335 Information technology - Security techniques         | <input type="checkbox"/> ISO 9001 Quality management   |
| <input type="checkbox"/> Others (please specify)  |  |



CAPELLA UNIVERSITY

Effectiveness of Information Security Policies, IT Governance, and ISO Security Certification- Pilot

**Thank you for participating in this study. Your input directly impacts the accuracy and outcome of this study. I personally appreciate the time and effort that you have put into your responses. If you wish to receive a copy of the study when it is released, please ensure that you entered your email back on page 1 of this survey.**

Please feel free to contact me at any time regarding the status of this study or results. Criticism is also welcomed as are general questions about information security. My areas of scholarly focus include: Multi-agent Adaptive Security, Virtualization Security, and Organizational Information Security Management. I have experience in Law Enforcement, Special Nuclear Material Security, and Electronic Medical Record Security.

jonpaarlberg@gmail.com

22

## **APPENDIX C. ORIGINAL HYPOTHESES FROM THE DOHERTY AND FULFORD (2005) STUDY**

H1: Those organizations that have a documented [Information Security Policy] InSPy are likely to have fewer security breaches in terms of both frequency and severity than those organizations that do not.

H2: Those organizations that have had InSPy in place for many years are likely to have fewer security breaches in terms of both frequency and severity than those organizations that have not.

H3: Those organizations that update their InSPy frequently are likely to have fewer security breaches in terms of both frequency and severity than those organizations that do not.

H4: Those organizations that have a policy with a broad scope are likely to have fewer security breaches in terms of both frequency and severity than those organizations that do not.

H5: Those organizations that have adopted a wide variety of best practice factors are likely to have fewer security breaches in terms of both frequency and severity than those organizations that have not.



## APPENDIX D. PILOT TEST ANALYSIS

Cronbach's Alpha for analysis of frequency and severity of breaches:

### Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.929	.910	16

Distribution of responses:

### Does your organization have a documented Information Security Policy?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	8	50.0	50.0	50.0
	No	8	50.0	50.0	100.0
Total		16	100.0	100.0	

### How long has your organization been actively using a documented Information Security Policy?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3 Years	1	6.3	14.3	14.3
	4 Years	1	6.3	14.3	28.6
	5 Years	1	6.3	14.3	42.9
	8 Years	1	6.3	14.3	57.1
	More than 10 Years	3	18.8	42.9	100.0
Total		7	43.8	100.0	
Missing	System	9	56.3		
Total		16	100.0		

**Approximately how often is the policy updated?**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Every 2 years	1	6.3	16.7	16.7
	Every year	4	25.0	66.7	83.3
	More than every 6 months	1	6.3	16.7	100.0
	Total	6	37.5	100.0	
Missing	System	10	62.5		
Total		16	100.0		

**Does your organization actively use one or more IT governance frameworks?**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	5	31.3	71.4	71.4
	No	2	12.5	28.6	100.0
	Total	7	43.8	100.0	
Missing	System	9	56.3		
Total		16	100.0		

**Does your organization hold current certification in any ISO (International Standards Organization)?**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	1	6.3	20.0	20.0
	No or Unkown	4	25.0	80.0	100.0
	Total	5	31.3	100.0	
Missing	System	11	68.8		
Total		16	100.0		