

A Study of the Effect of Information Security Policies on Information
Security Breaches in Higher Education Institutions

by

Stanie Adolphus Waddell

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

UMI Number: 3604516

All rights reserved

INFORMATION TO ALL USERS

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

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



UMI 3604516

Published by ProQuest LLC (2013). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against unauthorized copying under Title 17, United States Code



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

We hereby certify that this dissertation, submitted by Stanie Waddell, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Ling Wang, Ph.D.
Chairperson of Dissertation Committee

Date

Marlyn K. Littman, Ph.D.
Dissertation Committee Member

Date

Peixiang Liu, Ph.D.
Dissertation Committee Member

Date

Approved:

Eric S. Ackerman, Ph.D.
Dean, Graduate School of Computer and Information Sciences

Date

Graduate School of Computer and Information Sciences
Nova Southeastern University

2013

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

A Study of the Effect of Information Security Policies on Information Security Breaches in Higher Education Institutions

by
Stan Waddell
October 2013

Many articles within the literature point to the information security policy as one of the most important elements of an effective information security program. Even though this belief is continually referred to in many information security scholarly articles, very few research studies have been performed to corroborate this sentiment. Doherty and Fulford undertook two studies in 2003 and in 2005 respectively that sought to catalogue the impact of the information security policy on breaches at businesses in the United Kingdom. The pair went on to call for additional studies in differing industry segments.

This dissertation built upon Doherty and Fulford (2005). It sought to add to the body of knowledge by determining the statistical significance of the information security policy on breaches within Higher education. This research was able to corroborate the findings from Doherty and Fulford's original research. There were no observed statistically significant relationships between information security policies and the frequency and severity of information security breaches. This study also made novel contributions to the body of knowledge that included the analysis of the statistical relationships between information security awareness programs and information security breaches.

This effort also analyzed the statistical relationships between information security policy enforcement and breaches. The results of the analysis indicated no statistically significant relationships. Additionally, this research observed that while information security policies are heavily utilized by colleges and universities, security awareness training is not heavily employed by institutions of higher education. This research noted that many institutions reported not having consistent enforcement of information security policies.

The data observed during this research implies there is room for additional coverage of formal information security awareness programs and potentially a call to attempt alternative training methods to achieve a reduction of the occurrences and impact of security breaches. There is room for greater adoption of consistent enforcement of policy at higher education organizations. The results of this dissertation suggest that the existence of policy, training, and enforcement activities in and of themselves are not enough to sufficiently curtail breaches. Additional studies should be performed to better understand how breaches can be reduced.

Acknowledgements

Without my committee and advisor this dissertation would not have been possible. Dr. Ling Wang has proven to be a wonderful dissertation chair, advisor, and mentor over the course of my dissertation journey. She took me on as a student even though she already had a huge workload and still was always there when I had questions or doubts. Dr. Marlyn Littman and Dr. Peixiang Liu were great committee members. They were always prompt and insightful with their feedback.

I would like to thank my mother Delilah Waddell. She has always been an inspiration. She has urged me further and further and higher and higher throughout all phases of my life. I am and will always be indebted to her. I am still “being a man and taking a stand.” She and my dear departed father Jessie Waddell have shaped me into the man I am today; a person capable of completing such an undertaking.

I would like to thank my loving wife Rose Waddell. Always the first person I thought of when a new milestone was met and the person I drew strength from during each challenge or perceived trouble. She and our children Victor, Alex, Stephen and Whitney all stood by me over these many years. They were very understanding when dad had to miss this event or be late for that one because duty called. I would also thank my extended family and friends who gave me encouragement throughout the program. I also thank Kirk Kirksey, my former CIO, who always said “I had it in me” and refused to let me lose focus. Now when he asks “are you a Dr. yet?” I can proudly say yes!!!!

Table of Contents

Abstract ii

List of Tables vii

List of Figures x

Chapters

1. Introduction 1

Background 1

Problem Statement and Goal 3

 Problem Statement 3

 Dissertation Goal 5

Research Questions 7

Relevance and Significance 8

Barriers and Issues 13

Assumptions, Limitations, and Delimitations 14

Definition of Terms 15

Summary 18

2. Literature Review 20

Introduction 20

Importance of Information Security in Academia 20

Importance of security policy in Academia 25

Information Security Awareness 31

Information Security Policy Enforcement 33

Breaches of Information Security in Higher Education 35

Privacy and Security Laws and Requirements affecting Higher Education 38

 Family Education Rights and Privacy Act (FERPA) 39

 Health Insurance Portability and Accountability Act (HIPAA) 41

 The Gramm-Leach-Bliley Act 44

 Payment Card Industry Data Security Standard (PCI DSS) 46

 The Fair and Accurate Credit Transitions Act (FACTA) and Red Flags Rule 48

Summary of What Is Known and What Is Unknown from Prior Research 51

The Contribution of this Study to the Body of Knowledge 54

3. Methodology 55

Overview 55

Research Methods Employed 55

Survey Instrument Development 58

Data Collection Process 67

 Sampling and Participants 67

 Survey Distribution 68

Data Collection	70
Data Analysis	71
Resource Requirements	79
4. Results	81
Introduction	81
Findings	82
Institution Demographic Data	82
Descriptive Data	86
Research Questions Answered	86
Exploratory Questions	100
Summary of Results	105
5. Conclusions, Implications, Recommendations, and Summary	109
Conclusions	109
Research Questions	110
Discussion of Results	114
Strengths	117
Limitations	118
Implications	121
Recommendations	122
Summary	124
Appendices	
A. IRB Approval	132
B. Survey Instrument	133
C. Permission to Use Carnegie Classification Data	142
D. Permission to Reprint Tables from Doherty and Fulford (2005)	143
E. Findings tables from Doherty and Fulford (2005)	144
F. Initial Survey Solicitation Notice	147
G. Expanded Exploratory Questions Tables	148
Reference List	169

List of Tables

Tables

Table 1. Breach Percentages from Hasan and Yurcik (2006)	37
Table 2. PCI DSS Security Controls	47
Table 3. Survey Review Panel Members	62
Table 4. Suggestions and Critique from Survey Panel Experts	63
Table 5. Variables and Analysis Methods	78
Table 6. Carnegie Enrollment Distribution Statistics	83
Table 7. Carnegie Classification Distribution Statistics	83
Table 8. Carnegie Size and Setting Distribution Statistics	84
Table 9. Carnegie Funding Source Distribution Statistics	85
Table 10. Carnegie Region Distribution Statistics	85
Table 11. Higher Education Institutions Frequency and Severity of Breaches	86
Table 12. Relationship Between the Age of Information Security Policy and the Incidence of Security Breaches by Total Breach Count	87
Table 13. Relationship Between the Age of Information Security Policy and the Severity of Security Breaches by Total Breach Count	87
Table 14. Results of Levene's Test for Equality of Variances	88
Table 15. Relationship Between the Frequency of Information Security Policy Updates and the Incidence of Security Breaches by Total Breach Count	89
Table 16. Relationship Between the Frequency of Information Security Policy Updates and the Severity of Security Breaches by Total Breach Count	89
Table 17. Relationship Between the Range of Issues Covered by the Information Security Policy and the Incidence of Security Breaches by Total Breach Count	90
Table 18. Relationship Between the Range of Issues Covered by the Information Security Policy and the Severity of Security Breaches by Total Breach Count	90

Table 19. Relationship Between the Successful Adoption of Success Factors and the Incidence of Security Breaches by Total Breach Count	91
Table 20. Relationship Between the Successful Adoption of Success Factors and the Severity of Security Breaches by Total Breach Count	92
Table 21. Relationship Between the Existence of an Information Security Awareness Program and the Incidence of Breaches by Total Breach Count	93
Table 22. Relationship Between the Existence of an Information Security Awareness Program and the Severity of Breaches by Total Breach Count	93
Table 23. Relationship Between the Information Security Awareness Program Scope of Coverage and the Incidence of Breaches by Total Breach Count	94
Table 24. Relationship Between the Information Security Awareness Program Scope of Coverage and the Severity of Breaches by Total Breach Count	95
Table 25. Relationship Between the Existence of Documented Consequences for Policy Violations and the Incidence of Breaches by Total Breach Count	97
Table 26. Relationship Between the Existence of Documented Consequences for Policy Violations and the Severity of Breaches by Total Breach Count	97
Table 27. Relationship Between the Scope of Consistent Enforcement of Information Security Policy and the Incidence of Breaches by Total Breach Count	98
Table 28. Relationship Between the Scope of Consistent Enforcement of Information Security Policy and the Severity of Breaches by Total Breach Count	98
Table 29. Responses to the Question “Does an Information Security Awareness Program Exist?”	101
Table 30. Responses for the Question “How often is Awareness Training Required?”	102
Table 31. Responses to the Question “How is Information Security Awareness Training Delivered?”	102
Table 32. Responses for the Question “Do Documented Consequences Exist for Failure to Comply with Policy?”	103
Table 33. Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution’s Policies Were Consistently Enforced	103
Table 34. Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution Made Users Aware of Enforcement Activities	104

Table 35. Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Compliance Activities are Visible to Users	104
Table 36. Descriptive Statistics for Incidence and Severity	120
Table 37. Skewness and Kurtosis for Incidence and Severity	120

List of Figures

Figures

Figure 1. Confidentiality, Integrity, Availability (CIA) Triad	22
Figure 2. ISO/IEC 27002:2005 Guidance Regarding the Contents of a Security Policy	28
Figure 3. ISO/IEC 27002:2005 Suggested Security Policy Provisions	29
Figure 4. Survey Instrument Map	60
Figure 5. Expanded Concept Map (Nine Hypotheses)	77

Chapter 1

Introduction

Background

Information is an important commodity in any business. The same holds true for institutions of higher education. Higher education institutions use computer systems and computing to great effect for their academic, research, and administrative activities (Rezgui & Marks, 2008). Universities and colleges of all types share this dependence on information. Institutions of higher education rely on information for the same types of strategic and tactical decision making as corporations. However, higher education institutions also rely on information for teaching, learning, and research.

Securing information is a major concern for higher education institutions. Unauthorized access to systems and the loss of confidentiality or data accuracy can damage a higher education institution's reputation. Even though security is viewed as an important concern, it sometimes conflicts with the principals of open access in the education setting (Rezgui & Marks, 2008).

Academic openness is considered a major driving force for information resources in the academic setting. Academic freedom also contributes to the development of open network architectures typically associated with higher education campuses. Freedom to pursue knowledge and to openly express and exchange ideas is a basic tenet in higher education. These strongly held beliefs lend themselves to the development of open systems well suited for information exchange, but not well suited for information

security. Experts in computer security routinely express concerns about the insecurity of higher education institutions (Rezgui & Marks, 2008).

Many college networks are designed to deliver fast, efficient, and user friendly network services with minimum administrative burdens. As such, colleges and universities are targets for cyber-attacks. Attackers perceive that universities and colleges have lax security. In some cases, large numbers of systems associated with students and research operations are not managed by Information Technology (IT) staff and are left vulnerable to attack (Jones & Stallings, 2010).

Higher education relies heavily on IT departments to manage information security. IT departments are typically required to fund information security out of existing budgets and to staff the security functions. The security goals for the various colleges and universities must then be accomplished while at the same time providing open access and ease of use to the campus and sometimes the world at large (Jones & Stallings, 2010). Education organizations often find a need to balance the desires for convenience and openness with the reductions of risk associated with information security.

The information security policy illustrates and communicates the commitment of senior leadership to information security. Information security policies also allow the readers of the policy to understand their place in the overall information security strategy for the organization (Höne & Eloff, 2002a). Universities and businesses alike rely on these sacrosanct documents as a tent pole in information security efforts and for the success of an organization in general (Knapp, Franklin Morris Jr, Marshall, & Byrd, 2009).

Problem Statement and Goal

Problem Statement

Information is as important in higher education as it is in other industry segments. Higher education institutions make great use of computer systems to store data for teaching, learning, and research purposes (Rezgui & Marks, 2008). IT systems have become an important part of the academic process. Computer systems and their associated data are involved in the education process on many levels. Higher education computing systems can have significant amounts of processing capabilities and provide support for faculty and students, as well as, administrative and management functions (Rezgui & Marks). These systems are targets and are at risk for breaches and compromises (Jones & Stallings, 2010).

Doherty, Anastasakis, and Fulford (2009) noted that breaches affect 90% of US businesses each year. Additionally, security breaches have been on the rise in the UK as well. When all security incidents were accounted for, 74% of UK businesses reported breaches in 2004 versus only 44% in the year 2000 (Doherty, Anastasakis, & Fulford, 2009). Like other industry segments, higher education is affected by breaches (Siegel, 2008).

One study, Hasan and Yurcik (2006), highlights higher education as having the highest frequency for occurrences of disclosed storage security breaches. The study posits that higher education institutions account for a full 35% of the occurrences of breaches it analyzed for a period ranging from 2005 to 2006. The study attributed the high breach occurrence rate to the possibility of loose security and more reporting of breaches than

other industry segments (Hasan & Yurcik, 2006). Another article from 2012 stated that education institutions accounted for 21% of all breaches documented by the [privacyrights.org](http://www.privacyrights.org) website. The article went on to state that the education industry accounted for more breaches than any other segment in the reporting period (Ayyagari & Tyks, 2012).

An effective information security program has been suggested as a key way to reduce the risks of breaches occurring. Of the elements of information security programs, the information security policy, is seen as one of the keys to a successful program, but there is little empirical data to support this claim (Doherty et al., 2009). Along with a sound policy, information security awareness is touted as an important part of effective information security (Ayyagari & Tyks, 2012; Beutement & Sasse, 2009; Höne & Eloff, 2002b; Knapp et al., 2009; Lebek, Uffen, Breitner, Neumann, & Hohler, 2013). Additionally, policy enforcement is viewed as key to the success of any information security program (Hosack, Twitchell, & Sagers, 2009; Knapp, Marshall, Rainer, & Ford, 2006; McKenna, 2010; Siponen, 2010).

The problem this dissertation attempted to address was the lack of empirical data available that details the effectiveness of information security policies, information security awareness, and information security policy enforcement on the severity and frequency of information security breaches. People and researchers are impacted by the dearth of research surrounding the effectiveness of these management security controls in at least two ways. First, there is limited empirical data that supports the effectiveness of information security policies in general. This lack of data is commented on in many current security publications (Doherty & Fulford, 2005; Fulford & Doherty, 2003;

Karyda, Kiountouzis, & Kokolakis, 2005; Knapp et al., 2009; Warkentin & Willison, 2009). Second, the lack of evidence available that suggests the effect of these management security controls on the security posture of organizations can lead to incorrect assumptions regarding policy effectiveness. Assumptions, such as, that various aspects of an organization's information security policy affect the frequency and severity of breaches. The aspects include: the existence, age, review frequency, update period ,use of best practices, and the scope of issues addressed in policy (Doherty & Fulford, 2005). Organizations may implement security policy and security controls based on these assumptions. Security controls implemented due to faulty assumptions might not reduce the severity or frequency of breaches (Baker & Wallace, 2007; Doherty & Fulford, 2005). Higher education is a viable study segment since it accounts for a large percentage of breaches across all industry segments (Hasan & Yurcik, 2006).

Dissertation Goal

A 2006 study of breaches points to higher education as accounting for 35% of the breaches it analyzed. The 35% of breach occurrences was the highest of any industry segment analyzed in the 2006 breach study (Hasan & Yurcik, 2006). The education industry segment accounted for 21% of all breaches catalogued between 2005 and 2011 by the website privacyrights.org (Ayyagari & Tyks, 2012). This dissertation examined the problem of whether or not information security policies have an impact on the frequency and severity of information security breaches within the higher education setting. Doherty and Fulford (2005) studied this same issue in UK companies but did not focus on any one industry segment.

Many entries in the literature surrounding information security tout the information security policy as one of the most, if not the most important way to ensure an effective information security program and to reduce breaches (Doherty et al., 2009; Doherty & Fulford, 2005; Doherty & Fulford, 2006; Fulford & Doherty, 2003; Höne & Eloff, 2002a, 2002b). Even though much of the literature points to the security policy as very important, few studies offer any empirical data to support the assertion (Doherty et al., 2009; Doherty & Fulford, 2005; Fulford & Doherty, 2003; Warkentin & Willison, 2009).

The principle goal of this dissertation was to document the effect of information security policies on the frequency and severity of information security breaches in institutions of higher education. It is important to note that although higher education has a higher occurrence of breaches at 35% of all breaches reported (Hasan & Yurcik, 2006), the segment accounts for a lower percentage of records affected by total breaches. Hasan and Yurcik (2006) attributed only 3% of all records breached to higher education. The lower numbers of affected records may translate into lower breach severity for higher education institutions. Records were categorized as instances of data containing sensitive personal information. Personal information included social security numbers (SSN), credit card numbers (CCN), tax records, financial account information, medical records, and other forms not classified by Hasan and Yurcik.

This dissertation studied the impact of information security policies on breaches put forward by Doherty and Fulford (2005), as well as, added new study goals. These new goals sought to highlight the impact of security awareness programs on the frequency and severity of security breaches. Additionally, this dissertation attempted to discern if the

consistent enforcement of information security policies has an impact on the frequency and severity of security breaches.

Research Questions

This dissertation sought to validate the research questions first used by Doherty and Fulford (2005). These questions were not previously directed at higher education concerns. These questions are as follows:

1. Are higher education institutions that have formal information security policies likely to have less security breach incidents in terms of severity and frequency than those without (Doherty & Fulford, 2005, p. 25)?
2. Does the age of the information security policy result in a reduction of security breaches in terms of severity and frequency (Doherty & Fulford, 2005, p. 25)?
3. Does the update frequency of the information security policy result in a reduction of security breaches in terms of severity and frequency (Doherty & Fulford, 2005, p. 26)?
4. Does having a broad scope of issue coverage in the information security policy result in a reduction of security breaches in terms of severity and frequency (Doherty & Fulford, 2005, p. 26)?
5. Does the adoption of best practice factors in the information security policy result in a reduction of security breaches in terms of severity and frequency (Doherty & Fulford, 2005, p. 26)?

In addition to the original study questions researched by Doherty and Fulford (2005), this dissertation additionally explored the following four questions in an attempt to expand upon the original work. The combined nine questions were expanded to form the survey instrument. Questions six through nine are depicted below this paragraph.

6. Does a formal awareness program result in a reduction of security breaches in terms of severity and frequency? Security awareness is believed to be an important facet of an effective information security program and is cited as such in entries in the literature (Rezgui & Marks, 2008; Wiles, 2008; Wright, 2008). As is the case with other assertions regarding information security, there is little in the form of empirical evidence that supports the claims.
7. Does an organization that has a wider mandatory scope of coverage for its information security awareness program have fewer and/or less severe security breaches? Per ISO/IEC 27002:2005, all employees including, where appropriate, third party affiliates should be appropriately trained.
8. Does the existence of documented consequences for policy violations result in a reduction of security breaches in terms of severity and frequency? Many works in the literature highlight the importance of the consistent enforcement of information security policies (Baker & Wallace, 2007; Hoonakker, Carayon, Deb, Desoki, & Veeramani, 2008; Hosack et al., 2009; Knapp et al., 2009; Knapp et al., 2006; McKenna, 2010; Siponen, 2010). The studies do not offer empirical evidence that supports the assertion.
9. Do organizations with greater levels of consistent enforcement of policy experience fewer and/or less severe security breaches? If the previously referenced studies' assertions that consistent enforcement of polices hold, it stands to reason that greater levels of enforcement (i.e. more segments of the campus community) would result in a greater reduction of security breaches in terms of severity and frequency.

Relevance and Significance

Doherty and Fulford (2005) attempted to describe the relationship between the information security policy and the frequency of information security breaches and the severity associated with the breaches. The study focused on the perceived importance of the information security policy. Doherty and Fulford (2005) discussed the supposition that the information security policy reduced the occurrence and severity of information security breaches. The study tested the supposition through a number of hypotheses.

Ultimately, the study determined that no significant statistical correlation existed between the information security policy and the frequency or severity of security breaches.

Given the perceived importance of the information security policy, Doherty and Fulford (2005) attempted to examine a variety of topics concerning the creation and implementation of the policies. Doherty and Fulford theorized that a number of policy aspects could influence security breaches. There were five primary aspects studied. Does an information security policy exist for the organization in question? If an information security policy exists, how long has it been in place? How often is the information security policy updated? Does the information security policy have sufficient scope? Has the organization based its security approach on a set of established best practices?

Using a mailing list of IT leaders at organizations based in the United Kingdom, the researchers sent out a total of 2,838 questionnaires via postal mail. Each of the surveyed organizations were considered large firms (firms having at least 250 employees). The study received 219 valid responses or a 7.7% response rate. The survey targeted firms from a broad spectrum of industries. Respondents included firms from healthcare, public services, manufacturing, as well as, wholesale and retail. Those researchers considered the response rate to be disappointing. Lack of organizational buy-in to the study was believed to have caused the disappointing response rate.

Doherty and Fulford (2005) concluded with a call for additional research on the effectiveness of the information security policy in reducing the frequency and severity of security breaches on organizations. The paper characterized the need for follow-up studies in this vein as urgent. The authors stated that this type of research should be of interest to the information management research discipline and that additional research is

needed to further research the association between the information security policy and information security breaches. Other studies call for additional research regarding the effectiveness of the information security policy on improving the security of an organization. Goel and Chengular-Smith (2010) discussed the need for more empirical research on the effectiveness of various forms of security policies. Bulgurcu, Cavusoglu, and Benbasat (2010) recommended additional research into the effectiveness of the information security policy in improving security by affecting changes in employee behaviors. Another study, Knapp, Morris Jr, Marshall, and Byrd (2009), offered the need to conduct additional studies on the importance of the information security policy.

Information has been described as the life-blood of any business (Doherty et al., 2009). Without access to accurate business data organizations would simply fail (Peppard, 2007). The day-to-day operations of many businesses rely heavily on their information systems (Knapp et al., 2009). The information is viewed, manipulated, transmitted, and stored, all in support of the business processes. As such, entities, both public and private alike, create information systems infrastructures to support the business goals and provide access to data (Chang & Lin, 2007). Higher education institutions are no different in this respect. They have business information, as well as, the personal information of students, faculty, staff, patients, research subjects, and others that must be protected from compromise (Rezgui & Marks, 2008).

Information security is an inherently centralized function. The old adage holds true for security: it is only as strong as its weakest link. In the context of institutions of higher learning, the college or university as a whole is responsible for all aspects of security.

The entity itself is liable for all breaches of security even those committed by individual departments (Hanson, 2008). All of these aspects of information handling present a tangible risk for compromise (Doherty, Anastasakis, & Fulford, 2010). As such, it is important to present an effective information security approach coordinated by strong policy to reduce the risk of compromise to organizational operations.

Gordon et al (2011) categorized breaches into four categories. The four categories aligned to the aspects of the information security triad of confidentiality, availability, and integrity. The researchers listed the categories as 1.) All forms of breaches, 2.) breaches of confidentiality, 3.) breaches of availability, and 4.) breaches of integrity of data (Gable, 1994). Breaches occur when systems are compromised and data is accessed in an unauthorized manner. A 2011 study, by the Ponemon Institute, reported that 90% of respondents detected information security breaches in the year prior (Ponemon Institute, 2011).

Modern computer systems provide the capability to store vast sums of business data. In some cases, this data is customer identifiable data that is deemed protected by law. Yet, as computer capabilities have increased, so have the vulnerabilities associated with the systems. Attackers use these vulnerabilities to compromise computer systems and the data they store (Papadaki & Furnell, 2010). Information security breaches can occur in several forms. Breaches can include malware infections, electronic fraud, insider abuse, physical theft, unauthorized access to sensitive data, including personally identifiable information among other types, and denial of service attacks. It is important to note that not all information security breaches lead to the exposure of sensitive information or to identity theft (Baker & Wallace, 2007; Campbell, Gordon, Loeb, & Zhou, 2003).

A breach of sensitive information is a compromise of an organization's security that leads to the unauthorized disclosure of personally identifiable information of an individual or a group of individuals. The disclosure of information may or may not lead to identity theft. Identity theft can be described as the use of personally identifiable information to obtain money, goods, or services to which the obtaining party would otherwise not be entitled (Roberds & Schreft, 2009). Large IT systems and data repositories place the data of thousands of individuals in a single location. These systems give rise to fears that thieves may compromise the security of the systems and sell the data contained within on any number of illicit data marketplaces available on the Internet (Anderson, Durbin, & Salinger, 2008).

Laws and regulations increasingly require that entities notify affected patrons of security breaches (Schwartz & Janger, 2007). California was the first state to lead the way by creating legislation that required corporate entities to notify their customers when a breach of personally identifiable data was discovered. The state created California Senate Bill 1386 in 2003. Spurred on by a number of high profile security lapses that resulted in large numbers of individuals placed at potential risk to identity theft, other states soon followed suit and enacted similar requirements (Schwartz & Janger).

Information security policies are widely touted as key portions of an effective information security program. They are viewed as being able to set clear direction to employees for their responsibilities and expectations in terms of information security. The documents establish the boundaries for acceptable use and for appropriateness of actions when corporate information resources are concerned (Höne & Eloff, 2002b). The information security policy also clearly demonstrates senior leadership's commitment to

information security for the environment and communicates roles and responsibilities across the board for execution of the information security strategy. The goal of an information security policy is to briefly describe the specific objectives of the information security approach on which the agency has decided. This allows the readers of the policy to understand where they fit in the information security approach for the agency (Höne & Eloff, 2002a).

Information security policies are but one of the controls from the group of management security controls. Information Security awareness programs are another form of controls, but they are classified under the operational controls category. Information security polices and awareness training, along with policy enforcement processes, also from the operational controls category, form the core of the information security program elements this dissertation studied. Information regarding all three elements was requested from survey respondents and then analyzed to generate the dissertation findings.

Barriers and Issues

Studying security issues with surveys has proven difficult in the past. Even other types of surveys unrelated to information security can be mistakenly perceived as spam or phishing (Roster, Rogers, Hozier, Baker, & Albaum, 2007). One study, after attempting unsuccessfully to conduct a major security research undertaking, concluded that information security research is one of the most intrusive types of research that can be conducted on an organization. The researchers cited a general mistrust of any external

agent attempting to gain access to data on the practices of the community of information security professionals (Kotulic & Clark, 2004).

The above study conducted by Kotulic and Clark (2004) detailed a number of stated reasons for non-response to a security survey. The reasons ranged from requests not complying with policy to management team being too busy to respond to surveys. Doherty and Fulford (2005) experienced disappointing response rates for their study on the effectiveness of information security policies. The researchers stated that future researchers would need to be creative when attempting to perform additional research in information security (Doherty & Fulford).

In prior studies such as Doherty and Fulford (2005) and Kotulic and Clark (2004), firms have been reticent to release information on their security programs or on corporate incidents. This may have been due to perceptions that incidents made public can affect the corporate image or damage a corporation's reputation. The reluctance to release the survey data by potential respondents could lead to response bias.

Assumptions, Limitations, and Delimitations

As discussed previously, researchers can experience reduced response rates when conducting security based research. At least one study Kotulic and Clark (2004) recommended having a well-known sponsor organization to enhance response rates. This dissertation assumed the researcher would be successful in gaining organizational sponsorship to distribute the survey instrument. However, such sponsorship proved infeasible, instead per the predetermined backup plan, this researcher distributed the survey instrument via a purchased industry contact list. The dissertation also assumed

sufficient responses would be received to constitute valid research. The research effort successfully received enough responses to conduct analysis for all hypotheses except H1. The survey received enough responses, but the responses were dominated by organizations that indicated having existing information security policies.

Per Doherty and Fulford (2005), the use of a survey format restricts the expanse of topics that can be researched. The selection of narrow sampling frame reduces the generalizability of the results and can lead to possible single informant bias. Where generalizability is reduced, so too is the reliability of the research measurement. This was a risk to the dissertation effort.

This survey sought to limit potential respondents to persons with an information technology or information security role at higher education institutions. This was accomplished by purchasing a contact list of primary IT contacts at higher education institutions and limited the sample pool to those institutions combined with a list of professional contacts available to the dissertation researcher. This limitation allowed for a manageable survey population and allowed the conduct of original research that is distinct from the research performed by Doherty and Fulford (2005). In this respect, only responses from higher education institutions were desirable or sought.

Definition of Terms

- 1. Availability** –A characteristic of data that deals with users reliable access to data in order to perform their functions within the organization (Sato & Kumamoto, 2009).

2. **Breach** – A compromise of the confidentiality, integrity, or availability of sensitive information. The American Recovery and Reinvestment Act of 2009 (ARRA), defines a breach as the “unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI)” (Johns, 2010, p. 854). A breach occurs when an unauthorized party gains access to personal data that has been collected by an organization (Roberds & Schreft, 2009).
3. **Confidentiality** – a characteristic of data that deals with ensuring the information is protected from unauthorized or inadvertent disclosure (Satoh & Kumamoto, 2009).
4. **Information Security Policy** – The information security policy is a document that serves to provide guidance to the organization’s workforce. The policy demonstrates management’s commitment to information security (Höne & Eloff, 2002a).
5. **Integrity** – Integrity deals with protection information from unauthorized or inadvertent alteration or destruction (Satoh & Kumamoto, 2009).
6. **Management Security Controls** – Management security controls are non-technical in nature and center more on policy, procedure, and personnel management. Management controls are typically enforced via the implementation of operational procedures. Examples of management security controls include the organization’s information security policy, ongoing risk management activities, requirements for periodic system audits, etc. (Guttman & Roback, 1995; NIST, 2010b).

- 7. Operational Security Controls** – Operational security controls are non-technical in nature. Operational controls are typically detailed processes and procedures designed to reduce risk. Examples of Operational security controls include awareness processes, media access and destruction processes, sensitive data handling processes, offsite storage procedures, processes designed to enforce policy, etc. Operational security controls can be implemented through a mixture of management controls, technology controls and physical countermeasures (Guttman & Roback, 1995; NIST, 2010b).
- 8. Record** – A single instance of personally identifiable information regarding an individual (Dodge, 2009; Shaw, 2010).
- 9. Risk** – Risk is a function of the probability of a threat agent taking advantage of a vulnerability causing an adverse impact to an organization (NIST, 2010b).
- 10. Safeguard** – Safeguards and controls are terms that are used interchangeably to describe measures that are used to reduce risk. Safeguards typically fall within the management, operational, or technical control types (NIST, 2010b).
- 11. Sensitive information** – Sensitive information includes any information where the compromise of the information’s confidentiality, integrity, or availability would have an adverse effect on either the hosting institution, or an individual or a group of individuals. Some examples of sensitive information include PHI, Personally Identifiable Information (PII), customer data, and corporate information not for public review (NIH CIT, 2012).
- 12. Technical Security Controls** – Technical security controls are controls that are of a technical nature. These controls are incorporated into an organizations

computing environment. Technical controls typically involve a mixture of software, hardware, and firmware based security implementations. Examples of technical controls are firewalls, encryption, antivirus software, etc. (Guttman & Roback, 1995; NIST, 2010b).

13. Threat – A threat is the potential for a threat-agent to successfully take advantage of vulnerability. The threat activity can be either accidental or intentional (NIST, 2010b).

14. User – A user can be defined as a person with authorized access to the computing resources of an organization. Users make avail of this access to accomplish their roles within the organization (Albrechtsen, 2007).

15. Vulnerability – Vulnerabilities are weaknesses or the absence of security controls that are exploitable by threat agents. Examples of vulnerabilities include un-patched computers, unlocked doors, and unencrypted mobile devices (Satoh & Kumamoto, 2009).

Summary

Many scholarly articles within the literature point to the information security policy as one of the most important information security controls. This being stated, few research works have resulted in empirical data to support this claim. Doherty and Fulford undertook studies in both 2003 and again in 2005 that studied the impact of the information security policy on breaches at businesses within the United Kingdom. Doherty and Fulford (2005) called for additional studies to continue to study the phenomena. This study sought to add to the body of knowledge by determining the

statistical significance between the security policy and breaches within academia. The study also built upon existing research efforts by researching the effect of information security awareness and policy enforcement on breaches within the higher education setting.

Chapter 2

Literature Review

Introduction

This dissertation focused on the impact the security policy has on security breaches at higher education institutions. It is therefore important to review relevant literature regarding the importance of information security within academia. It is also important to delve into the importance of the security policy as supported by the literature. Along with a review of the relevant literature regarding information security policies, the literature review section of the dissertation focuses on relevant privacy security and breach notification laws and their consequences. Since this research also explores the importance of information security awareness and policy enforcement, the review on the literature will also cover these topics. The literature review covers literature on breaches at higher education institutions. The review will culminate with a discussion of prior research that indicates the research has been regarded as a novel and worthy topic in the past, while also exploring various gaps in prior research that leave unanswered questions for this research effort to explore.

Importance of Information Security in Academia

Colleges and universities rely on computerized databases to store student information. The added convenience of electronic records is a great incentive for moving to a computerized system (Kiel & Knoblauch, 2010). However, these systems must be protected from exposure. Failure to effectively protect sensitive data can lead to public

embarrassment for the affected higher education institution coupled with various costs associated with responding to a breach. An exposure could subject the affected entity to investigations, costs for handling breaches, fines, or other penalties (Hanson, 2008).

Higher education institutions face substantial security and privacy issues. In many instances, universities and colleges require the same types of data to conduct business as corporate America, while at the same time having fewer security and privacy resources as compared to businesses. Academic freedom challenges, along with outsourcing and decentralization present many challenges to security (Culnan & Carlin, 2009). These issues are having a profound impact on all computing environments as entities scramble to become compliant with the invasive and far-reaching policies coming from Washington D.C. and state capitals alike (Burdon, 2010). Yet even with these pressures, colleges and universities continue to be the target of penetration attempts due to the computers resources and their openness (Rezgui & Marks, 2008).

The compromise of business information could present itself as a failure of the primary three characteristics of business information. The three characteristics are described as confidentiality, integrity, and availability (CIA). Each characteristic is important and must be preserved. This combination of characteristics is frequently referred to as the information security CIA triad (Kolkowska, Hedström, & Karlsson, 2009).

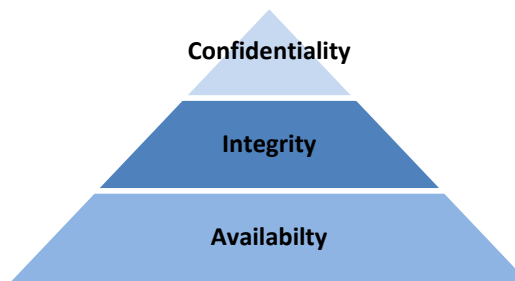


Figure 1. Confidentiality, Integrity, Availability (CIA) Triad

Confidentiality is the preservation of business information from unauthorized disclosure. The disclosure can be either accidental or malevolent. Protecting the confidentiality of information entails maintaining its secrecy (Satoh & Kumamoto, 2009). Appropriate risk reduction measures should be deployed to ensure that only authorized agents access the information assets (Satoh & Kumamoto, 2009).

Integrity involves the preservation of information accuracy and completeness. Information has integrity when it is whole, complete, and uncorrupted. Incomplete or corrupted information results in flawed business directives that impair corporate operations. Information-integrity needs to be protected while information is stored, transmitted or processed (Whitman & Mattord, 2011).

Availability of information deals with the assertion that information resources are available when needed by authorized people, processes or systems. If information assets are not available when needed, normal operations cannot continue. Access to accurate information at the correct time can lead to prudent business decisions that can lead to an advantage over competitors (Satoh & Kumamoto, 2009).

For each of the characteristics of information, there exist various quantifications of risk. Risk has several meanings. Blakely, McDermott and Greer (2001) provides a strong

foundation for understanding risk in terms of information systems. These meanings are dependent on the industry segments that define it. In regards to businesses, risk equates to the probability that an incident will occur that reduces the value associated with a business. Such an incident is referred to as an adverse event (Blakley, McDermott, & Geer, 2001). Even though many definitions for risk exist, it remains a complex issue.

Risk, as a concept, originated during the 1600s. A subset of mathematics that dealt with gambling spawned the abstract. Risk defined the relationship that existed between the probability and magnitude of gains and losses associated with games of chance. Over the course of history, risk has been associated with several industries. In the seventeen hundreds, insurance companies that focused on sea based trade used risk to calculate the potential losses and rewards associated with trade expeditions. The eighteen hundreds found risk used in the economic studies. However, by this time risk had taken on the negative connotation that is still associated with it today. Risk was primarily used to describe the potential losses associated with certain ventures. By the nineteen hundreds, scientists used risk to refer to hazards encountered during technical pursuits (Blakley et al., 2001).

In terms of information technology, risk has been defined by several sources. The National Institute of Standards and Technology's (NIST) Handbook 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, a Security Life Cycle Approach refers to risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" (NIST, 2010a, p. 1). NIST SP 800-30, Risk Management Guide for Information

Technology Systems, referred to risk as “the net negative impact of the exercise of a vulnerability” (NIST, p. 1). Risk management is a critical element in the efforts to ensure continued success of a business. Risk management provides an appropriate method of evaluating the effectiveness of security through asset inventory and the cataloging of threats and vulnerabilities for risk assessment, evaluation, and mitigation (Ekelhart, Fenz, & Neubauer, 2009).

Vulnerabilities are weaknesses in a system. These weaknesses carry a potential for exploitation which if compromised might result in devastating effects. One of the largest issues today in information security is the detection and remediation of vulnerabilities (Kraemer, Carayon, & Clem, 2009). An example of vulnerability is an un-patched web server with known security flaws. The security flaws themselves can be considered vulnerabilities, as well. A myriad of network borne attacks are realizable via the compromise of system weaknesses and vulnerabilities. In fact an un-patched computer connected to the Internet has a time to compromise of only between 3 to 70 minutes (Papadaki & Furnell, 2010).

A threat is a possible harm or adverse impact to a system. Illustrations of threats are classified as network outages, facility destruction, and storage drive failure. Threats can occur at any time and can have varying degrees of impact. Also, they can be the result of environmental, accidental or malicious acts perpetrated by humans, and or a combination of both (NIST, 2010a). For instance, the hurricane possibly destroys the front door and alarm system and then looters sack the interior of the facility destroying the network storage device in the process. This statement proves the adage that no practical grouping

of safeguards can completely eliminate the presence of threats or risk (Blakley et al., 2001).

All of these references eventually resolve to the base concept that risk is the chance that something bad will happen. In order to prevent the bad thing from occurring, risk must be managed. That premise gives birth to risk management. Risk management is the design, monitoring, and manipulation processes created to manage the risk identified during an entity's risk analysis phase. The end-result of a risk management program is to control risk via appropriate administrative, technical, and physical security controls (Ekelhart et al., 2009). In this respect, a comprehensive information security approach is management of risk via a complete process that includes risk analysis and risk management (Ekelhart et al.).

Importance of security policy in Academia

Colleges and universities face the same types of privacy and security challenges as other types of businesses. Higher education institutions conduct ecommerce activities such as web based book sales, sporting event ticket sales, electronic donations, online student registration, human resources administration, and many others. They store massive amounts of sensitive personal information. All of the information is at risk to security breach. In many cases, whereas businesses store information with predefined retention periods, higher education institutions are required to keep some forms of sensitive information indefinitely. Couple this with the fact that many higher education computing environments are distributed and decentralized, and a situation exists where

the guidance represented in the organization's information security policy becomes very important (Culnan & Carlin, 2009).

Many articles within the literature point to the information security policy as one of the most important pieces of an effective information security management approach (Doherty et al., 2009; Doherty & Fulford, 2005; Doherty & Fulford, 2006; Fulford & Doherty, 2003; Höne & Eloff, 2002a, 2002b; von Solms, van der Haar, von Solms, & Caelli, 1994; von Solms & von Solms, 2004). The basis for the problem studied by this research revolved around the attempt to gain an understanding for how information security breaches are affected by information security policies, awareness programs, and the enforcement of policy in higher education.

Generally, written policies are created to handle the dissemination of information. Examples of entities requiring information policies are governmental agencies, businesses, and education institutions among others. In the context of security, policies are designed to assure the confidentiality, integrity, and availability of information. The necessity of security can be mandated by legislation. However, operational concerns can also necessitate the implementation of security policies. In general, policies are a set of rules or management practices that define how an institution is to operate. These policies offer guidance to those in position to make choices for the entity, as well as providing guidelines and standards for employees to follow when carrying out their task (Gritzalis, 1997). Policies are part of the subset of security controls defined as management security controls (Guttman & Roback, 1995).

Information security policies are described as intersecting stipulations that govern the information security enforcement of an organization. The stipulations cover aspects of

operations that can include technological, legal, economic, political, and social concerns (Goel & Chengalur-Smith, 2010). A policy should be grounded and firmly tied to the needs of the organization and conform to appropriate regulations and laws (ISO/IEC, 2005). An organization's policy should be custom developed for the needs of the organization. Many security organizations such as SANS and EDUCAUSE provide security policy templates, but these should only be considered a starting point for policy development (Goel & Chengalur-Smith, 2010).

One objective of an information security policy is to demonstrate the support of an organization's leadership for information security (Goel & Chengalur-Smith, 2010). It is the responsibility for an organization's management to "set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization (ISO/IEC, 2005, p. 7)." According to ISO/IEC (2005), an information security policy should be approved by organizational leadership. The approved policy should then be released and distributed to all organization work force members and relevant affiliates. An organization should communicate the security policy in ways that are accessible and readily digested by the intended audience (ISO/IEC).

Information security is more than applying technical and physical controls to attempt to protect information within an organization. Technical and physical controls are important, but an organization must also endeavor to account for the vulnerabilities imparted by the human workforce. A well trained and security aware workforce can be a strong asset in the protection of organizational data. One of the primary goals of the information security policy is to guide the workforce towards acceptable decisions and

actions in regards to the organization's information. Since the security policy contains the expectations for the workforce, it is the starting point for its education. All information security training materials should be grounded in policy (Thomson, von Solms, & Louw, 2006).

Even though the information security policy is considered vital to an organization's information security strategy, these documents are not always simple to construct (Höne & Eloff, 2002a). Policy documents can be complex. They can cover many issues and topics. While example documents exist it is important that an organization's information security policy be custom tailored to meet the specific requirements of the entity. Policy development can often be attributed to some organizational calamity. A better approach is to develop policy as a part of an overall strategy with organization risk at the forefront of the development effort. A higher education institution's overall security approach should be standards based and the elements of the policy should encompass the various facets of the standard being referenced (Custer, 2010).

ISO/IEC 27002:2005 Suggested Policy Scope and Contents
Definition of information security
Statement of managerial support
Information Security controls framework (including objectives and risk management)
An explanation of the policies, principles, standard, and requirements <ul style="list-style-type: none"> • Compliance requirements (legal and contractual) • Security awareness training • Business continuity • Consequences of failure to adhere to policy
Security responsibilities and incident reporting
Relevant references

Figure 2. ISO/IEC 27002:2005 Guidance Regarding the Contents of a Security Policy

ISO/IEC 27002:2005 has a controls section dedicated to the contents of an information security policy. The guidance given within ISO/IEC 27002:2005 suggests that an information security policy should contain a definition of information security, the overall security objectives, and the role of security in information exchange. Figure 2 depicts the scope and content of an organization's information security policy as suggested by ISO/IEC 27002:2005. Doherty and Fulford, 2009 conducted a study of higher education institution information security policy contents. They found that the most commonly covered policy issues included many of the ISO/IEC 27002:2005 suggested provisions depicted in Figure 3 and many more topics.

ISO/IEC 27002:2005 Suggested Policy Provisions
<ul style="list-style-type: none"> • Violations and breaches • User access management • Responsibilities • Enforcement • Contingency planning • Physical security • Awareness and Training • Disclosure of information • Compliance with legislation • Viruses, worms, etc. • Encryption • Information Classification • BS (1)7799 reference • Mobile computing • Software development • Personal usage of information • Internet access

Figure 3. ISO/IEC 27002:2005 Suggested Security Policy Provisions

Information Security policies are often lamented as too long, too strict, and adverse to free decision making for employees. Security professionals tend to advise that the policies

be succinct, concise and easy to digest by the intended audience (McKenna, 2010).

Policies should be high level documents that are technology and solution agnostic and not dependent on current security implementations. If policies are focusing on the strategy and direction for security they will require minimal changes as various security threats rise and fall (Goel & Chengalur-Smith, 2010). Information Security policy should be short and to the point in order to entice users to read them. Goel & Smith, 2010 advised focusing on three metrics when developing information security policies: breadth, clarity, and brevity. However, the researchers do not warrant these aspects as the only elements important to the effectiveness of an information security policy.

An organization's information security policy pertains to the protection of confidentiality, integrity, and availability of electronic information stored on its systems and transmitted over its networks. Information security policies are important instruments as they convey management's support for security. The policies also inform workforce members of the penalties and consequences associated with failure to abide by policy stipulations. An information security policy, as with any other policy, provides parameters of behavior that limits the discretion of workforce members. The absence of a security policy can be construed as a lack of management commitment to information security. A perceived lack of managerial commitment can cast information security as a secondary concern not to be given priority (Knapp et al., 2009). Since the policies provide the foundation for securing information, all other information security activities should be based on them. The policies are the link between strategy and execution and are possibly the strongest means of forcing compliance within the workforce (Vroom & von Solms, 2004).

Information Security Awareness

Information security awareness lies within the group of controls defined as operational controls (Guttman & Roback, 1995). According to NIST publication 800-16 Information technology security training requirements, federal agencies cannot protect the confidentiality, integrity, and availability of information without adequately training the workforce on their roles and responsibilities. The guide goes on to say all employees need basic instruction on security fundamentals and practices. The guide recommends creating varying levels of instruction based on the role of the employee within the organization (van Niekerk & von Solms, 2008).

Employees must be made aware of their information security roles and responsibilities. A basic means to communicate these responsibilities is an information security awareness training program (Knapp et al., 2009). In regards to information security, training and awareness is used to indoctrinate workforce members to the approaches the company has outlined. This allows the employees to prepare to receive the fundamentals of the security program via formal training mechanisms (Knapp et al., 2009). A significant number of breaches can be attributed to employees failing to comply with information security policies. An effective information security policy depends on an entity's employees (Beautement & Sasse, 2009). Therefore, it is of paramount importance that security concepts be thoroughly and appropriately communicated to all areas of the organization (Höne & Eloff, 2002b). This removes the specter of ignorance as an excuse to not follow information security requirements and allows for consistent enforcement of policy.

Even though information security awareness is perceived as important, it may not be given its proper level of priority at many entities. A study conducted by Ernst & Young in 2010 highlights a need for increased importance in regards to security awareness. The survey discovered that less than 38% of responding entities would be increasing awareness activities over the 2011 year. The study goes on to report that 34% of surveyed businesses contain no processes at all for educating staff on information security responsibilities associated with social networking. Only 47% of surveyed businesses required employees to review and agree with stated security policies. The study did find encouraging data, as it noted that only 15% of survey entities had no awareness program (Ernst & Young, 2010). Many college and university IT security managers devote more time to technical controls such as firewalls and encryption than they devote to less technical issues such as awareness training and outreach for staff and students (Rezgui & Marks, 2008).

In order to achieve better security outcomes, education institutions need to require exposure to their policies. Early articles such as Denning (1999) have argued that information security training and education programs are integral to defending computer security. Allowing computer users on campus find their own way in regards to security concerns is not as effective as mandatory awareness training. The importance of fostering information security at an organization dictates the existence of information security awareness training.

An organization should construct its information security awareness program to instruct users on policy expectations as well as the disciplinary actions and consequences for failure to adhere to policy standards (Rezgui & Marks, 2008). Technical

implementations are certainly one aspect of an information security program, but the ever evolving state of threats and vulnerabilities provide many avenues to failure for technology based defenses. Additionally, the human element can increase the possibility of security failures even when the strongest, most stringent defenses are in place. Since human or end user based security failures are both accidental and alternatively malicious in nature, a security program must address education and enforcement (Rhee, Kim, & Ryu, 2009).

ISO/IEC 27002:2005 considers information security awareness training as a common practice for information security programs. ISO/IEC 27002:2005 recommends periodic training updates on information security policies and procedures. The standard states that *“All employees of the organization and, where relevant, contractors and third party users receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant to their job function (ISO/IEC, 2005, p. 26).”* It is important to note that the period associated with regular updates is not defined and is therefore customizable for the specific needs of an organization (ISO/IEC, 2005).

Information Security Policy Enforcement

Enforcement of the policies is viewed as a key indicator of program success. Policy enforcement is classified within the group of controls defined as operational controls (Guttman & Roback, 1995). Cavusoglu, Mishra, and Raghunathan, (2004) stated that many organizations perceive their employees as the weakest link in the organization’s effort to provide a secure environment for data. An organization’s employee’s failure to abide by its information security policies provides a key threat to its security (Siponen,

2010). An important element of the information security policy is a section describing enforcement and associated disciplinary actions (Knapp et al., 2006). However, having a documented policy does not imply that policy enforcement exist (Doherty & Fulford, 2005). A policy that is not enforced loses credibility with the workforce. In fact, if the policy will not be enforced perhaps it is not needed (McKenna, 2010).

While security policies are widely acknowledged as one of the best deterrents to security incidents, the policies cannot be considered effective if they are not followed by the computer users (Hosack et al., 2009). Employees make cost-to-benefit decisions when deciding on whether or not to comply with a policy. When the decision is not to comply, employees sometimes justify their decision by the effect compliance would have on their personal or organization productivity. In these cases, employees consider the need to comply against the effort required to comply. If the effort to comply with policy is perceived as not commensurate with the perceived decreases in productivity, employees may choose not to comply (Beautement & Sasse, 2009).

Sanctions influence a workforce's compliance with their organization's information security policy through deterrence. Siponen, Pahnla, and Mahomound (2010) asserted that criminology theory has focused on the concept of deterrence for more than 30 years. The concept of deterrence offers that celerity, certainty, and severity of sanctions along with the social stigmas can be a factor in an individual's decision to commit a crime or not. Severity pertains to the level of harshness associated with some punishment. Certainty pertains to the individual's perception of the likelihood an act will be detected and therefore punished. Finally, celerity deals with the rapidity in which the punishment

is carried out. The social stigma deals with the disfavor the individual may be subjected to as recourse of his or her actions (Siponen, 2010).

Policy enforcement should be a continuous activity. When policy is violated corrective action should occur (Knapp et al., 2009). When corrective action is initiated, workforce members should be made aware (McKenna). Policy should deter bad actions with the specter of consequences and at the same time it should reward good behaviors with incentives (Knapp et al.). Beutement and Sasse (2009) suggests that policy enforcement must be consistent. Sanctions are only effective when they are consistently applied whenever the policy is not followed (Beutement & Sasse, 2009).

For a policy to successfully reduce breaches, it must be practical, concise and enforceable (Höne & Eloff, 2002a).

Breaches of Information Security in Higher Education

One study, Hasan and Yurcik (2006), highlights higher education as having the highest frequency for occurrences of disclosed storage security breaches. Hasan and Yurcik aggregated a listing of breaches from data captured by two breach disclosure sites, privacyrights.org and attrition.org. Data retained by privacyrights.org includes information such as:

- a. The date the breach was reported
- b. A description of the breach
- c. The location and business name of the organization responsible for the breach including in several cases the businesses third party agents that possessed the data at the time of the breach

d. If known, the number of records affected by the data breach

Organizations like privacyrights.org primarily obtain breach reports from the Open Security Foundation. The information is readily available via email list-serve (Campana, 2008). The data set amassed accounted for a reporting period from January 1, 2005 through June 5, 2006.

Hasan and Yurcik (2006) classified breaches according to three tiers. The first tier was comprised of higher education. Medical institutions, state government entities, and banking institutions comprised the second tier. The third and final tier included federal government, data brokers, and profit/nonprofit organizations. The study posits that higher education institutions account for a full 35% of the breaches it analyzed. The study attributed the high occurrence rate to a possibility of loose security and more reporting of breaches than other industry segments. Hasan and Yurcik also makes note that although higher education has a higher occurrence of breaches, the segment accounts for a lower percentage of records affected by total breaches. In fact, the study attributed only 3% of all records breached to higher education (Hasan & Yurcik, 2006).

Table 1. Breach Percentages from Hasan and Yurcik (2006) depicts the findings from Hasan and Yurcik.

An analysis of breaches from January 2005 through October 2008, that was performed in 2008, yielded similar results. The 2008 analysis found that the education sector including higher education accounted for 31% of all breaches recorded by privacyrights.org. Of these education related breaches, higher education accounted for

79% of exposed records. K-12 school accounted for 15% of the reported education related breaches. Entities classified as others accounted for the remaining 6% of education related breaches (Campana, 2008). A review of security breaches catalogued by privacyrights.org between 2005-2011 indicated education settings accounted for 21% of all breaches and nearly eight million records (Ayyagari & Tyks, 2012).

Table 1. Breach Percentages from Hasan and Yurcik (2006)

Breach Percentages from Hasan and Yurcik (2006)		
Category	% of Breaches	% of Records Exposed
Higher Education	35.16	2.72
Federal	4.57	29.59
State	10.05	1.89
Organizations	0.46	0.47
Nonprofits	1.37	1.42
Data Brokers	3.20	0.49
Business	25.11	35.49
Banking	9.59	11.63
Medical Institutions	10.50	16.28

Data from one survey indicates that US consumers lost approximately \$49.3 billion dollars to identity thieves in 2006 (Roberds & Schreft, 2009). The \$49.3 billion dollars did not account for individual time and efforts to resolve the crimes. Over a nearly three year period, the University of Texas at Austin's Business School suffered two significant breaches. Almost 200,000 records were compromised in the breaches. In March of 2005 a University of California (UC) Berkeley laptop was stolen with 98,000 records onboard including SSNs (Rezgui & Marks, 2008). UC Berkeley was again impacted in 2009 when hackers breached a campus server that contained greater than 160,000 individual records. For the year of 2009, many higher education institutions experienced breaches. For that

year 86 breaches affecting 102 institutions were reported to various breach data aggregation sites. In all greater than 1.04 million records were compromised (Dodge, 2009).

Garrison & Ncube (2011) proffered that the high number of breaches from the education section might be due to the number of individuals that have access to identifiable information. The researchers theorize that in a typical business setting access to customer data is limited to a small group of employees. The research cites converse examples where business employees have limited opportunity to cause breaches where education employees have greater access to data and more opportunities to cause breaches. Additionally, many employees in education have simultaneous access to personally identifiable information for long periods of time. Decisions regarding the storage and protection of personally identifiable information are largely left to the education professionals at education institutions. The same is likely not true of regimented corporate environments (Garrison & Ncube, 2011).

Privacy and Security Laws and Requirements affecting Higher Education

There are many laws that have some implications for data security and more are in development. A review of every law, statute, or industry standard that affects information security is beyond the scope of this study. The review of relevant provisions focuses on several laws and one set of contractual obligations, but not all security laws and regulations are discussed. The review highlights some federal and state laws and one set of commercial provisions required by the payment card industry.

Family Education Rights and Privacy Act (FERPA)

Family Education Rights and Privacy Act (FERPA) is a sweeping piece of legislation covering the rights of parents and students regarding education information maintained by schools (Kiel & Knoblauch, 2010). Congress enacted the act, otherwise known as the Buckley Amendment, in 1974. The act guarantees that parents have access to the education records of their underage, less than 18 years of age, children. At the same time, the act limits access for other parties to those with legitimate purposes for viewing the records. FERPA prohibits institutions from releasing personally identifiable academic information without prior consent. This information covers grades and financial aid information. The laws apply to both electronic and paper copy records. FERPA applies to any education institution that receives federal funding. This excludes religion based private secondary and elementary schools as they receive no federal funding (Barboza, Epps, Byington, & Keene, 2010).

FERPA provides no direct legal remedy for persons who are the victims of FERPA violations. However FERPA does have provisions for schools that fail to protect information covered under this policy to lose federal funding (Barboza et al., 2010). While there is no precedent for liability for the unintentional exposure of student information due to unauthorized access, schools must be aware of the possibility of legal liability. This liability might exist in cases where a school failed to protect academic records. Parents and adult students have a right to file complaints if a regulated school does not follow the provisions of FERPA. Since its inception, FERPA has not resulted in any significant monetary sanctions against any institution. The act has been amended 28 times since its inception (Barboza et al., 2010).

Within the context of FERPA, education records can include numerous forms of information about a student and the student's academic progress. Education records can come in the form of place of birth, date of birth, home address, emergency contact information, assignment scores, test grades, disciplinary records, history of attendance, course history, previous education history, and personally identifiable information such as the student's social security number. Items not considered education records include law enforcement records captured and managed by the campus law enforcement agency. Additionally, personal notes created by educators or other staff members are not considered education records. Notes are classified as personal so long as they are not shared or made available to other workforce members (Barboza et al., 2010).

FERPA requires schools that receive federal funding to comply with several provisions. The schools are required to create and maintain formal policies that address student records. They must make parents aware of their rights under the provisions of FERPA. They must provide parent access to their children's education records upon request. Parents must be allowed to contest record accuracy. The schools must prohibit the disclosure of personally identifiable information unless prior consent is granted. Schools are not required to gain consent when sharing information with authorized agents such as school staff engaged in the education of the student, internal counsel, correctional facilities, providers of special education services, or activities related to child-find provisions of the Individuals with Disabilities Education Act of 2004. Once a student matriculates into a college or university, control of the education record transfers to the student. This being said, higher education institutions may still release information

regarding the education records to a student's parent in many situations (Barboza et al., 2010).

Health Insurance Portability and Accountability Act (HIPAA)

In addition to FERPA, institutions with healthcare components are tackling the Health Insurance Portability and Accountability Act (HIPAA) legislation. The United States Congress enacted HIPAA in 1996. The act was primarily designed to enhance the effectiveness and efficiency of the US health care system by promoting standards for electronic healthcare transaction sets. However, the act also contained requirements for the protection of patient records referred to as protected health information (PHI). Additionally, patients were granted the rights to review, obtain copies of, and to refute inaccuracies with their medical records (Barboza et al., 2010).

HIPAA defines a covered entity as any institution that performs any of 11 specific types of healthcare related transactions. Many higher education institutions fall into the covered entity classification because they have medical centers or other healthcare related activities (Kiel & Knoblauch, 2010). However, student health records are typically exempted from the provisions of HIPAA as they are already covered by FERPA when the records are created or maintained as part of a school's operations (Barboza et al., 2010).

HIPAA describes medical information as *“any information whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health clearing house; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past,*

present, or future payment for the provision of health care to an individual.” HIPAA contains provisions that govern both privacy and security of PHI (Adler, 2006).

The HIPAA Privacy Rule requires institutions to protect individual’s health records. Federal legislators drafted the privacy provisions with an April 14, 2003 compliance date. Since that date, covered entities have been required to adhere to the provisions of the privacy rule (Barboza et al., 2010). HIPAA compliance adoption has not been an entirely smooth implementation. Many covered entities have struggled to interpret the operational implementation of the security and privacy provisions (Williams, 2008). The HIPAA Privacy Rule primarily deals with the use and distribution of sensitive health care information or protected health information (PHI). The Privacy Rule dictates the conditions under which PHI can be released and also what parties can have access to it. Any workforce members within the higher education arena that interacts with personal health information must be aware of various HIPAA, FERPA, and state laws (Kiel & Knoblauch, 2010).

The HIPAA Security Rule established three categories of controls for the security of electronic health data. The categories are physical, administrative, and technical controls (Kiel & Knoblauch, 2010). Administrative controls are documented policies and procedures for managing security. Physical controls are controls that use physical measures such as lockable offices, and filing cabinets to limit access to PHI. Fire suppression systems and fire resistant materials are examples of physical controls that are used to reduce the likelihood that PHI might be destroyed. Technical controls deal with the implementation of technology to limit access to PHI. Technical controls include

implements like firewalls, encryption, and anti-virus software, among others (Johns, 2010).

The Security Rule has been in effect for nearly 11 years now. New guidance in the form of Health Information Technology for Economic and Clinical Health (HITECH) Act updates the rule and requires the government to investigate all situations that indicate negligence. Where negligence is substantiated the Secretary of Health and Human Services is required to impose civil penalties (Wieland, 2010). Congress created this legislation as part of the American Recovery and Reinvestment Act (ARRA) of 2009. HITECH further strengthened the security and privacy measures outlined in HIPAA. HITECH provided a clarification for breach notification situations. The provisions specify “unsecured PHI” as PHI that has not been rendered indecipherable or unusable by parties without proper authorization to access the information. Encryption is cited as one way to render PHI not unsecured. Breach notification is only required when the situation affects unsecured PHI (Johns, 2010). Under HITECH, the breach notification requirements were expanded to include business associates of covered entities as well as the covered entities themselves (Sotto, Treacy, & McLellan, 2010).

Under the HITECH Act, all covered entities must notify individuals when their unsecured PHI is affected by a security breach. The breached organization must also inform Health and Human Services (HHS) if the breach involves more than 500 individuals. In cases where the breach population exceeds 500 individuals, the local media must also be notified. Businesses located in states with no breach notification requirements or with requirements less stringent than HITECH, must follow HITECH provisions. HITECH does not supersede or lower requirements where the prescribed

state breach requirements are stronger than those specified by HITECH. HITECH extends enforcement power to state attorneys general for their state of residence. A state attorney general may bring suit on behalf of the citizenry of their home state against businesses that impinge upon the rights extended by HIPAA (Regan, 2009).

HITECH also established clear punitive measures for the failure to comply with federal regulations regarding health information security. The penalties associated with HITECH represent a substantial increase over the original HIPAA penalties. A penalty for a violation is \$10,000 when willful negligence is discovered. The penalties for violations are cumulative up to an annual cap of \$250,000 for the same types of incidents. If the violations are not corrected within 30 days, the penalty increases to \$50,000 per violation, with an annual cap of \$1,500,000 (Wieland, 2010).

The Gramm-Leach-Bliley Act

The US Congress passed the Gramm-Leach –Bliley Act (GLBA) in 1999. The GLBA is also known as the Gramm-Leach-Bliley Financial Services Modernization Act (Fritsche, 2009). Like HIPAA and FERPA, the GLBA has focuses other than information security (Shaw, 2010). The GLBA was primarily created to update the laws focused on the mergers and acquisitions of securities, insurance, and banking organizations. To foster its main goals, the act also places stipulations on how non-public personal information can be used by collecting companies. The act targets entities within the financial services industry.

The security provisions of the Gramm-Leach-Bliley Act require financial institutions to create, implement, and maintain security measures that are capable of protecting

customer data (Schwartz & Janger, 2007). In 2003 the Federal Trade Commission (FTC) stated that higher education institutions are subject to the GLBA. Under the GLBA, colleges and universities are considered financial institutions (Fritsche, 2009). The security controls that are implemented must be “adequate” according to the act. Adequate in this case being synonymous with reasonable (Romanosky & Acquisti, 2009). The GLBA also requires affected organizations to create a process that is designed to respond to breaches of customer data (Shaw, 2010).

The GLBA is important because it requires an established process driven approach to the regulation of information security within the financial industry. The provisions of the act increase the security of consumer data by establishing a duty of the financial organization to have a proactive information security program. Financial agencies must also have a process that is capable of investigating potential customer breaches to determine if a breach has occurred. Where a potential breach is discovered, the affected organization must investigate and determine if a reasonable possibility of misuse of identifiable customer information exists. If there is a reasonable chance for the misuse of customer data, the company must notify the affected individuals. In situations requiring notification, the notification must be made, as soon as possible, using a mode that is likely to be received by the customer. Some acceptable methods of notification include telephone, email, or physical mail. Additionally, a telephone number must be established to received customer calls for assistance (Shaw, 2010).

Payment Card Industry Data Security Standard (PCI DSS)

The legal authority of the states is not the only way privacy and security controls can be required. In some situations, security and privacy can be required by contractual provisions (Morse & Raval, 2008). VISA, MasterCard, Discover, American Express, and Japan Credit Bureau (JCB) issued a set of security requirements that detail how credit card data must be secured. Payment Card Industry Data Security Standard (PCI DSS) regulates merchants. Merchants are the businesses that are authorized to receive credit cards for payment. PCI DSS classifies merchants into four distinct categories. Each level of merchant has different compliance levels. The classifications are designed to balance the cost-to-benefit issues associated with compliance (Morse & Raval, 2008).

The most recent version of PCI DSS, version 1.2, contains twelve requirements for compliance. The twelve standards together are collectively known as PCI DSS. The credit card issuers require PCI DSS for any businesses that store, process, or transmit cardholder data (Shaw, 2010). Universities and colleges are also required to follow PCI DSS when they accept credit card payments for fees, goods, or services. The standards are a requirement for any entity that wishes to accept credit card payments (Romanosky & Acquisti, 2009).

Table 2. PCI DSS Security Controls

PCI DSS 12 Security Controls	
High Level Requirement	Brief Description
Build and maintain a secure network.	1. Install and maintain a firewall configuration to protect cardholder data.
Protect cardholder data.	2. Do not use vendor-supplied defaults for system passwords and other security parameters.
	3. Protect stored cardholder data.
Maintain a vulnerability management program.	4. Encrypt transmission of cardholder data across open, public networks.
	5. Use and regularly update anti-virus software.
Implement strong access control measures.	6. Develop and maintain secure systems and applications.
	7. Restrict access to cardholder data by business need to know.
	8. Assign a unique ID to each person with computer access.
Regularly monitor and test networks.	9. Restrict physical access to cardholder data.
	10. Track and monitor all access to network resources and cardholder data.
	11. Regularly test security systems and processes.
Maintain an information security policy.	12. Maintain a policy that addresses information security.

Implementation of the 12 security controls does not equate to a guarantee of security. However, the implementation of the controls can lead to a reduced likelihood of a breach of credit card data (Shaw, 2010). The 12 controls are depicted in Table 2. Merchants can be held liable for costs when they are involved in a breach. Such costs can include fees for the reissuance of credit cards. The merchants are likely to be held accountable when they have failed to meet the minimum security controls according to PCI DSS (Romanosky & Acquisti, 2009).

The Fair and Accurate Credit Transitions Act (FACTA) and Red Flags Rule

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act (FACTA). FACTA calls for creditors and other financial institutions to implement identity theft programs. The term creditor is loosely defined and potentially extends to such businesses as physicians' offices, mortgage brokers, utilities providers, and others. The term creditor for the purposes of FACTA includes any organization that regularly defers payment for goods or services rendered (Baker & Schneck-Teplinsky, 2010). Colleges and universities are subjected to Red Flags Rules since they engage in financial activities that are similar to those performed by for profit entities (Meers & Meade, 2008).

When colleges and universities engage in activities similar to those outlined below, according to Red Flags Rules, they are considered creditors (Meers & Meade, 2008):

- Participation in the Federal Family Education Loan Program as a school lender,
- Participation in the Perkins federal student loan program,
- Offering organizational loans to faculty, students or staff, or
- Offering any plans for deferred payment of tuition.

In order to be compliant with the Red Flags rules, red flags programs must identify relevant red flags. Red flags are patterns, activities, and processes that indicate possible identity theft. Programs must integrate processes to identify those red flags and respond appropriately when they are detected to reduce the likelihood of identity theft occurrences. Finally, organizations must update their red flags programs periodically to address new risks pertaining to identity theft (Baker & Schneck-Teplinsky, 2010).

Higher education institutions must also comply with breach notification bills for the states in which they are located. There are now 46 states that have some form of information security breach notification law. States are increasingly enacting new laws that require companies to protect the private data of the citizenry (Schwartz & Janger, 2007). The legislation is basically forked into two types of regulations: privacy protection laws and breach notification laws (Burdon, 2010). These laws require companies to notify individuals when their practices lead to a unauthorized disclosure of personally identifiable information (Sotto et al., 2010). The notification requirements vary depending on the laws being reviewed. The requirements differ most in regards to what forms of breaches warrant notification. The states also vary on what types and forms of information are protected under the statutes (Hilley, 2007).

At a high level, there are observable similarities between breach notification laws and privacy laws. Both infer data protection requirements. Also, both types of laws seek to enhance security of information through better security practices. However, breach notification laws tend to regulate a larger spectrum of entities and industry segments as opposed to privacy legislation which tend to focus on a specific business sector (Burdon, 2010).

California was the first state to enact a data breach notification law. California lawmakers unanimously passed the bill in response to a breach of 260,000 state employees and law makers. The Stephen P. Teale Data Center was the organization responsible for the breach. The California bill, S.B, 1386 went into effect in 2003. S.B. 1386 required organizations to notify affected citizens of California when their personally identifiable information was subject to unauthorized access. The organization was also

required to indicate that they were responsible for the breach. In the wake of S.B. 1386, numerous other states developed similar legislation (Schwartz & Janger, 2007).

As of December 21, 2011, 46 states, Puerto Rico, the US Virgin Islands, and Washington D.C. all have laws that require security breach notification. Only Alabama, Kentucky, New Mexico, and South Dakota are currently without breach notification laws (Greenberg, 2011). Hilley (2010) argues that the myriad of notification laws lead to disjointed approaches and calls for a national standard. Most state laws have emulated the standards incorporated into California S.B. 1386. Yet, others have produced statutes with alternate triggers for notification, methods of notification, reporting requirements, and conditions for notification exemptions. Data breach notification laws have highlighted any number of flawed security practices that have exposed vast numbers of individuals to risk of identity theft. They continue to indicate that general corporate information security practices are inadequate (Burdon, 2010).

One common theme that resides within many state breach notification laws is the concept of encryption based safe harbors. The encryption safe harbors can be uniformly described as exemption based. There are two forms of exemption. The two forms are non-explicit exemptions and explicit exemptions. The first form, like California's law, does not attempt to define the implementation of encryption. California makes the recommendation that organizations use the Advance Encryption Standard (AES) algorithm. This being said, the language of the law makes it clear the recommendation is not binding. The second form, explicit exemptions like those of Ohio and North Carolina, make an attempt to define the encryption standard. A majority of the states with explicit exemptions follow two threads for encryption (Shaw, 2010). The data must use a

recursive process that renders the data unintelligible and not useful. The process must also yield a low likelihood for assigning any meaning to the data (Burdon, Reid, & Low, 2010).

With the advent of the Health Information Technology for Economic and Clinical Health Act, breach notification requirements were added to the HIPAA regulations (Sotto et al., 2010). HITECH provision also follows an explicit exemption paradigm. HITECH applies to any HIPAA covered entity regardless of state of incorporation or business nexus. In light of all of the privacy and breach requirements, both federal and state, facing higher education institutions, the effectiveness of information security policies is of paramount importance. Understanding and quantifying that effectiveness is also very important (Doherty & Fulford, 2005).

Summary of What Is Known and What Is Unknown from Prior Research

Research studies have been conducted that have offered perspectives for policy development. Karyda, Kiontounzis, and Kokolakis (2005) proposed a framework rooted in the theory of contextualism in terms of two disparate organizations. Höne and Eloff (2002) explored what makes an effective policy. Studies have been dedicated to understanding the basics of effective acceptable use policies (Arnesen & Weis; Doherty et al., 2010). Another study developed a security policy process based on the responses of certified information security professionals (Knapp et al., 2009). Yet another study reviewed policy development in terms of international standards and best practices (Höne & Eloff, 2002a). These studies and many others contend that the information security policy is a key piece to ensuring the success of an information security program. So,

while these studies and others are united in their supposition of the importance of the information security policy, only a few studies attempt to quantify this importance (Doherty et al., 2009).

The literature implies that there is little empirical data available regarding the impact of information security policies on the frequency of occurrence and the severity of the impact of information security breaches (Doherty et al., 2009; Doherty & Fulford, 2005; Fulford & Doherty, 2003; Goel & Chengalur-Smith, 2010; Heikkila, 2009; Hong, Chi, Chao, & Tang, 2006; Kotulic & Clark, 2004). As was previously discussed, Doherty and Fulford (2005) studied the effect of information security policy on breaches in businesses within the United Kingdom. The researchers found no significant statistical relationship between the information security policy and the frequency and severity of information security breaches. Doherty and Fulford (2005) specifically called for additional studies comparative to the study they performed. They highlighted the need for studies that would attempt to quantify the relationship between information security policies and the frequency and/or the severity of information security breaches. Doherty and Fulford (2005) went on to comment that there was a need for future research that targeted different populations and respondents.

Heikkila (2009) built on the work by Doherty and Fulford (2005). Heikkila studied the impact of the information security policy on breaches in law firms. Heikkila expanded on the survey instrument used by Doherty and Fulford by adding questions that dealt with the implementation of security controls at the surveyed organizations. Heikkila also expanded on the original work by utilizing a sponsor organization for the distribution of the survey instrument. Heikkila solicited the assistance of the International Legal

Technology Association (ILTA) with the distribution of the survey instrument in order to combat the low response rates associated with information security survey based research. The resultant response rate of 7.83% was just slightly higher than the 7.7% response rate of Doherty and Fulford. Like Doherty and Fulford, Heikkila did not find any statistical significance between the existence of the information security policy and the frequency and severity of information security breaches. It is interesting to note that Heikkila did however find a weak statistical relationship between the scope of issues addressed by the information security policy and the frequency and severity of reported information security breaches.

A review of the literature indicates that security is important and so is policy. Due to the importance of data, information security and, therefore, the information security policy are seen as fundamental to the success of a business (Knapp et al., 2009). Employees within an organization take direction in regards to the importance of various tasks and responsibilities from senior leadership. As such, support for the policy by executive level or senior leadership is seen as essential. Management's endorsement of the security policy and the security program in general is viewed as critical for effective policy development, enforcement, and maintenance (Knapp et al., 2009). This belief is made evident by the involvement of various federal and state governments that has created legislation like HIPAA and FERPA to mandate the protection of personally identifiable information (Culnan & Carlin, 2009).

With legislation leading to cause for action by victims of security breaches, fines from state level and federal agencies, and even suites brought by state attorneys general, reducing information security breaches may have never been more important to public

and private institutions including institutions of higher education. Additionally, recent pressures from both federal and state governments, in the form of security provisions and breach notification requirements, have made it necessary for higher education institutions to revise their security approaches (Schwartz & Janger, 2007). The studies performed by Doherty and Fulford (2005) and Heikkila (2009) do not address the segment of higher education as a separate entity. Perhaps now more than ever, the empirical data is needed to understand how best to implement these information security approaches.

The Contribution of this Study to the Body of Knowledge

This dissertation sought to fill a need in the literature that has heretofore been addressed by only a small number of studies. The dissertation served to reproduce, validate, and expand upon the efforts of Doherty and Fulford (2005). The study broadened the body of knowledge by conducting original research on the impact of information security policies on the incidence of breaches within the domain of higher education. Just as Doherty and Fulford demonstrated the results from UK businesses, this study yielded results from US colleges and universities. This dissertation added to the available data on the effective of awareness programs, and policy enforcement on breaches. Also, the final results added to the empirical information available regarding information security research as whole, while also providing data on the statistical significance between information security policies, enforcement, and awareness and breaches.

Chapter 3

Methodology

Overview

This chapter describes the methodology that was used to answer the research questions asked by this dissertation. The purpose of the study was to further review the impact of the information security policy on the frequency and severity of information security breaches. The study focused on the phenomena within the domain of higher education. This dissertation continues to build upon the research of prior studies. Many surveys have been used to capture information on various aspects of information security (Da Veiga & Eloff, 2010; Gaunt, 1998; Hong et al., 2006; Knapp et al., 2006; Kotulic & Clark, 2004; Kvavik, Voloudakis, Caruso, & Pirani, 2003; Rezgui & Marks, 2008). Yet, only a small number of studies have concentrated on the effectiveness of information security policies in reducing risks associated with breaches (Doherty & Fulford, 2005; Heikkila, 2009).

Research Methods Employed

This research effort was a cross sectional survey based study. The study relied on the solicitation of survey data and the analysis of said data to catalogue the impact of information security policies on information security breaches in higher education institutions. The research emulated and expanded upon the approach taken by Doherty and Fulford (2005). Doherty and Fulford conducted a survey on large organizations based

in the United Kingdom. The survey respondents were the Information Technology directors for these firms.

This survey instrument was designed to answer the nine questions posited by the overall research study. This research effort adopted the validated questions from Doherty and Fulford and then compared the results of that prior study to the results generated in this dissertation. The questions were modified in order for them to be applicable to higher education environments. This dissertation also expanded the original work by adding survey questions designed to extract information regarding the impact of security awareness programs and policy enforcement on information security breaches. The general hypothesis of this study was that the results generated in this research effort should yield a similar outcome to the 2005 UK based study.

Doherty and Fulford (2005) had five hypotheses. The first hypothesis predicted that organizations that had information security policies would have fewer and/or less severe security breaches. The second hypothesis predicted that organizations that had more mature security policies would have fewer and/or less severe security breaches. Hypothesis three predicted that organizations that had frequent information security policy updates would have fewer and/or less severe security breaches for an organization. Hypothesis four predicted that organizations that had information security policies of broad scope would have fewer and/or less severe security breaches. Hypothesis five covered the prediction that organizations that had policies based on a wide variety of best practices would have fewer and/or less severe security breaches.

The study performed by this researcher added four additional hypotheses to the hypotheses from Doherty and Fulford (2005). The four new hypotheses combined with

the previous five from Doherty and Fulford (2005) to yield a total of nine hypotheses. Hypothesis six predicted that organizations with an information security awareness program would experience fewer security breaches or that the breaches that did occur would be less severe than organizations without security awareness programs. Hypothesis seven predicted that organization that have wider mandatory coverage of information security awareness programs would have fewer and/or less severe security breaches. Hypothesis eight predicted that organizations with documented consequences for policy violations would have fewer and/or less severe security breaches. Hypothesis nine predicted that organizations with greater levels of enforcement consistency would experience fewer and/or less severe security breaches.

This study developed over the following methodology. The methodology was based on techniques conducted by Doherty and Fulford (2005):

- A survey questionnaire was developed based on the nine proposed research questions. Doherty and Fulford (2005) formed the questionnaire basis for the first five research questions. Four additional questions were crafted from the literature
- The survey received IRB approval, as exempt, on October 26, 2012
- The questionnaire was reviewed and vetted by a panel subject matter experts and academics (Doherty & Fulford, 2005).
- Contact information for 1,468 distinct institutions of higher education was obtained
- The questionnaire was distributed on February 4th, 2013
- The questionnaire was closed on May 4th, 2013

- Obtained results were subjected to statistical analysis using correlation analysis and t-tests to determine if any statistically significant association exists between any of the independent variables of the study and the frequency and/or severity of information security breaches at the respondent institutions (Doherty & Fulford, 2005).
- Results and conclusions were interpreted and recorded in this report for submission.

Unlike Doherty and Fulford (2005), which studied the responses of a wide spectrum of industry segments, this study collected survey-based data from professionals within the higher education industry. Doherty and Fulford relied on statements from the literature, including Hone and Eloff (2002b), which describes the information security policy as a managerial implement. Based on that concept, Doherty and Fulford found it appropriate to compile its pool of respondents from IT management at the targeted firms. Similarly, this study targeted senior IT officials with policy enforcement responsibilities within higher education institutions. The targeted officials were senior IT executives and senior IT security professionals at the survey objective institutions.

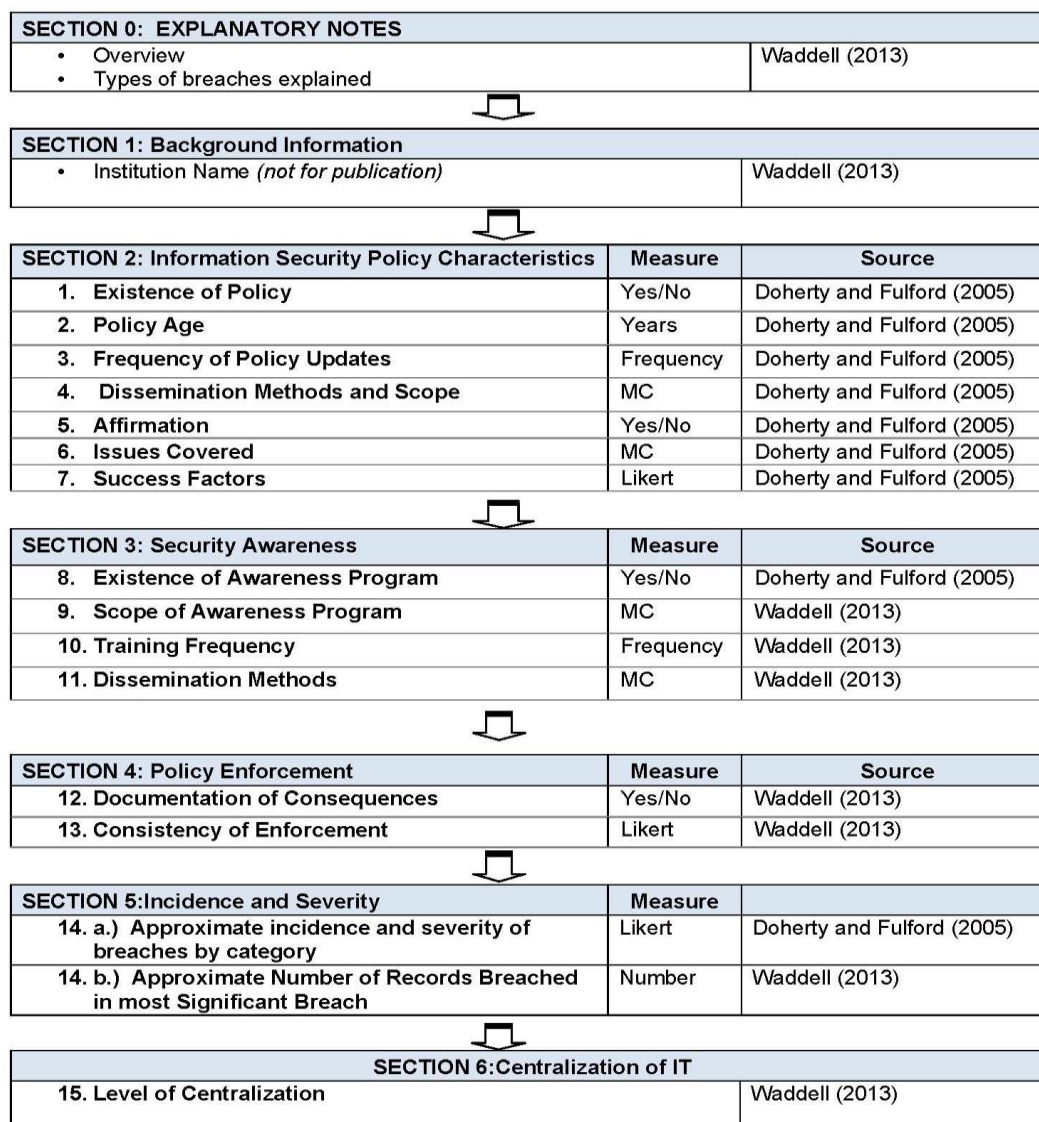
Survey Instrument Development

The two dependent variables for this study were the incidence of breaches and the severity of breaches. Respondents were asked to indicate the frequency in which security breaches occurred at their associated agencies. The respondents were also asked to rate the perceived severity of the most severe breaches in each of the eight breach categories that affected their agencies. Additional data was collected via the survey instrument that

allowed the researcher to gauge the statistical significance between the dependent variables and other aspects of the information security policy, information security awareness, and policy enforcement such as:

- Existence of policy
- Age of policy
- Time between policy review and update periods
- Scope of policy coverage
- Adoption of best practices
- Existence of an information security awareness process
- Coverage of information security awareness process across campus populations
- Existence of a documented consequences for policy violations
- Consistency of policy enforcement across campus populations

The reporting timeframe for the survey was a period of two years. Figure 4 depicts the survey instrument in a survey map format.



Note: MC denotes multiple choice

Figure 4. Survey Instrument Map

The survey instrument used by this dissertation was modeled after the survey instrument used by Doherty and Fulford (2005). This researcher developed the survey instrument in the web based survey platform hosted and operated by Qualtrics (www.qualtrics.com). Qualtrics is located in Provo, Utah. Qualtrics states that it has SAS 70 Certification and meets federally regulated privacy standards. Qualtrics describes

itself as a secure online survey hosting company. The company boasts such customers as PepsiCo, CITRIX, the Weather Channel, Six Flags, over 1,300 colleges and universities, and others. Over the course of 2012, Qualtrics reportedly distributed more than one billion surveys ("Qualtrics Crushes 2012 With Record Client Growth and More Than A Billion Surveys Served," 2013).

The Doherty and Fulford (2005) questions were tested and validated by the original researchers using a pre-experiment test pool followed by a refinement process and then executed as part of a final survey process. In addition, Doherty and Fulford (2005) conducted Cronbach's Alpha internal reliability testing to verify the validity of the derived summated scale for quantifying the adoption of information security best practices. The findings of the testing indicated a statistically significant alpha value of 0.87. According to Carmines and Zeller (1979), in general, alpha values should not be below 0.8. The reliability value for Doherty and Fulford's summated scale is higher than 0.8 signaling good internal consistency (Carmines & Zeller, 1979).

To add to the research questions offered by Doherty and Fulford (2005), additional questions were developed from the literature. Additional research questions that focused on user awareness training and consistent enforcement of information security policies were validated by a pre-experiment evaluation of a test pool of an IT professional and three academics. Pretesting focused on clarity, content, and validity (Doherty & Fulford, 2005). After the additional questions are tested appropriately, they were revised to enhance validity and reliability and to reduce any survey bias (Hong et al., 2006). The feedback from the evaluation and validation was used to refine the survey questions before they were utilized for the final survey (Knapp et al., 2006).

Table 3. Survey Review Panel Members

Panel Member	Role	Home Institution
Ramon Padilla, MBA	Deputy CIO and Associate Vice Chancellor/Information Security Officer	University of North Carolina at Chapel Hill
Steffani Burd, Ph.D	Security Researcher	Independent Consultant
Fabian Monroe, Ph.D	Associate Professor	University of North Carolina at Chapel Hill
Eric Reiter, Ph.D	Associate Professor	University of North Carolina at Chapel Hill

The research conducted by this researcher sought the assistance of an information technology professional and academics to refine the proposed survey instrument. An Information Technology (IT) professional from the researcher's peer group at The University of North Carolina institution was asked to review the initial instrument for validity, and the potential to be completed by other IT professionals. Additionally, two members of the University Of North Carolina Chapel Hill Department Of Computer Science were consulted for similar concerns. A security researcher was also asked to provide feedback on the survey instrument. Table 3 represents the members of the review panel. The review panel suggested changes to the survey that were then used to refine the instrument. The suggestions and critique are presented in Table 4.

Table 4. Suggestions and Critique from Survey Panel Experts

Survey Element	Suggestion of Critique	Action Taken
Question A1. Please enter the institution that you are providing information about. This information is only being used to ensure that there are no duplicate institutions represented in the cumulative results of the study. No institution names will be attributed to any survey responses when the results of the study are finalized.	Add another box as question A2 in case someone cannot find there institution. They will then have an option to type it in versus quitting	Added A2.
Question A2. Please type in your institution name	Added question A2.	
Question B1 -4. Demographic questions, Size classification, etc...	Delete this type of question rely on industry data to shorten your survey	Deleted these questions
Question B5-6 Name; Email address	Why are you asking for personal data?	Data not needed deleting
Question 2. How would you classify the level of centralization of IT resources at your university (On a scale of 1-10 with 5 being equally distributed between central IT and departmental IT)?	This question is more descriptive either delete or move to end of survey. This will give you a better chance at getting important questions answered	Question moved to the end to become question 15.
Question 4. Does your organization have a documented information (IT, Cyber) security policy?	Move from four to number one this is your primary question	Moved from question 4. to question 1.
2. In years, how long has your organization actively used a document information security policy (If not sure please leave blank)?	Enforce response as number to avoid variable confusion	added question enforcement (input now requires an integer)

3. Approximately how often is the policy updated?	Add a not sure to this question some - CIOs may not know the answer	Added not sure as a question option(will be treated as missing response in analysis phase)
	Ensure only single select option is available for this question currently multiple options can be selected	Corrected question Logic
4. How is the policy disseminated to faculty, staff, and students (Please check all that apply)?	seems like "I don't know" should be an option	added not sure as a question option (will be treated as a missing response in analysis phase)
5. Are faculty, staff, and students, required to affirm that they have read, understand, and agree to abide by the policy?		
6. Using the table below, please indicate the security issues covered in your IT security policy below. If the issues are only covered by policy please choose "Policy Document Only." If there is no policy covering the issue, but standards or procedures exist, please choose "Stand-alone Procedure or Standard Only." If you supplement your policies with procedures or standards please choose "Policy Document and Supplementary Procedure or Standard." If you do not explicitly cover an issue through your policy or a separate standalone standard, please choose "Not documented." If you are not sure please choose "Not Sure."	I don't think I follow what you mean by "Stand-alone procedure or standard only". Is anything that an employee is supposed to do that is not listed in the policy document then a "stand-alone procedure"?	No action taken this is a question from Doherty and Fulford (2005);

7. Using the table below, please indicate the importance of each of the following factors and the extent to which your organization is successful in adopting them.		No modifications made this is a question from Doherty and Fulford;
8. Does your institution have a formal and documented security awareness program (i.e. implemented with policies and procedures)?	You should add a unknown option	Added a not sure option
9. Security awareness training is mandatory for which of the following (check all that apply)?	You should add a unknown option	Added a not sure option
10. If training is mandatory how often is it required?		
11. When Information security awareness training is presented, how is it delivered? (Please check all that apply)	You might want to provide an example here	Added multiple choice selections
12. Does your organization have documented consequences for failure to comply with its information security policy?	Add a not sure to this question; some CIOs may not know the answer	Added a not sure option
13. Please use the following Likert scale to indicate the strength to which you agree or disagree with each of the following two statements:		No modifications made; this is a question from Doherty and Fulford;

<p>14. Please record in the table below the approximate number of IT security breaches that your organization has experienced in the past two years, and indicate the severity of the worst breach of each type, using the scale provided. For clarification please see the definitions of each type of breach location in the table below. For the purposes of this study breaches can affect confidentiality, integrity, and/or availability of data. Breaches should only be counted when they result in the notification of affected individuals under a breach notification or privacy and security law. Examples of such laws include: HIPAA, GLBA, the various state identity theft protection and breach notification laws, and others.</p>	<p>This is a complex question move to near end</p> <p>Maybe you should add the breach definition table to this page of the survey- users may not remember the categories when they get here and will not wish to go back</p>	<p>Moved from question 9. to question 14.</p> <p>Added breach definition table to this page on the online survey</p> <p>No modifications made this is a question from Doherty and Fulford;</p>
<p>15. How would you classify the level of centralization of IT resources at your university (On a scale of 0-10 with 5 being equally distributed between central IT and departmental IT)?</p>	<p>This question does not fit with the other questions – should be revised or deleted – at the very least it should be at the end of the survey</p>	<p>Moved from question two to end of survey</p>
<p>Breach Description table</p>	<p>The "types of breach" are a bit confusing in that they arguably overlap quite a bit. If that's ok with you, then you might want to comfort the reader by acknowledging this fact, e.g., "Various forms of breaches are listed below; This information would be helpful near the question about breaches</p>	<p>Refined the descriptions; Duplicated the table near the question on breached</p>

16. Please use the grid overleaf to indicate the strength to which you agree / disagree with each of the following three statements regarding end users:	This question does not fit the overall theme of your questionnaire and does not fit to your research questions - you may wish to revise it	Question deleted as not relevant to the research
Overall	Lastly, I think it would be helpful to place at the beginning of the survey how long it is and about how much time it will take and to specify that they can save in the middle	Added progress bar

Data Collection Process

Sampling and Participants

The study targeted senior IT and information security professionals at the various colleges and universities. The researcher was granted IRB approval to survey the institutions via the human subject contact list on October 26, 2013. This researcher was able to obtain contact information for 1,468 distinct institutions. The contact list was compiled from two sources. The first source was a list of 1,459 institutions that was supplied for fee from the Higher Education Directory. This research focused on Colleges and Universities that have accredited degree granting programs granting at a minimum four year degrees. In order to properly classify the responding organizations, this researcher used the Carnegie classifications hosted by the Carnegie Foundation.

The Higher Education Directory contact list included contact information for the primary IT contact at IT organizations at the target institutions. The listed contacts had titles ranging from Chief Information Officer to Director of IT or Information Systems

(IS). The second source was professional contacts known to the researcher. These contacts were primarily Chief Information Security Officers, Information Security Officers, and Information Security Managers. An additional nine institutions were added in this fashion.

Doherty and Fulford (2005) distributed a total of 2,838 surveys to firms in the UK. A total of 219 surveys were returned. This yielded a response rate of 7.7%. The researchers were disappointed by the response rate but did not consider the response rate surprising. The researchers believed the sample was acceptable for conducting the research. Information security surveys are plagued with low response rates (Kotulic & Clark, 2004). Heikkila (2009), a similar study based on Doherty and Fulford that focused on law firms, achieved a response rate of 7.83%. Low response rates also impacted this researcher's study. This survey achieved a response rate of 7.22%. A total of 106 completed and qualified surveys were received from the sample population.

Survey Distribution

Israel (2011) states that a researcher should have a prior relationship with a survey recipient when sending email invitations to complete a survey. Introductory alerts from an authority figure can increase response rates (Dillman, 2009). This researcher originally planned to utilize EDUCAUSE ECAR for the distribution of the survey invitations, but this relationship was not available. In the absence of assistance from an industry trade organizational sponsor, this researcher formulated a survey distribution plan that could be wholly executed by the researcher using resources available to the researcher as an individual.

The researcher designed the survey instrument in Qualtrics. The instrument was validated via panel review. The survey instrument was distributed to a sample population of 1,468 distinct higher education institutions. The survey was first distributed on Monday February 4th, 2013. On the fourth, a set of emails were sent to the 1,468 target institutions via the Qualtrics survey distribution interface. Potential respondents also received several reminder notices. The survey was subsequently closed on Saturday May 4th, 2013.

The survey instrument was delivered in a web based format to capitalize on cost efficiencies and data management capabilities of online surveys (Roster et al., 2007). Online surveys have numerous built in advantages which include tools for simple creation of surveys, numerous options for hosting, electronic distribution tools, data management tools, as well as, features that make for a better experience for both subjects and researchers (Monroe & Adams, 2012). Online survey participation is believed to be simple when participants have access to the Internet and are frequent users of computers (Israel, 2011). The target contact group of IT executives and Information Security professionals, at colleges and universities, could reasonably be assumed to be frequent computer users with high speed access to the Internet. Israel (2011) also found that when an email address was available response rates between clients responding to a postal invitation and those responding to an email invitation were largely indistinguishable.

The cost of an online survey with electronic survey notification is less expensive than other paper based alternatives (Israel, 2011; Monroe & Adams, 2012; Roster et al., 2007). The cost of the survey hosting which included electronic invitation distribution was \$500.00. The cost for first class postage alone for 1,468 recipients would have been

roughly \$675 at 46 cents per stamp. This cost does not include paper stocks, envelopes, printing or return postage. So, one could argue the electronic notification for an online survey was indeed more cost efficient than a postal notification with a hybrid paper and online survey instrument method.

Monroe and Adams, 2012 advocated repeated and personalized contact with potential survey respondent in order to increase response rates. This research used the contact list referred to earlier in this section to generate personalized electronic survey invitations. In a fashion similar to Monroe and Adams, this researcher personalized the message to each individual by name. The first names of the potential respondents were used (for example “Dear Stan”). The first invitations were sent on February 4th, 2013 and five sequent reminders were sent on:

- February 12th, 2013,
- February 26th, 2013,
- March 18th, 2013,
- April 9th, 2013,
- And April 29th, 2013

Data Collection

During the survey period, 253 total surveys were initiated. Of the surveys that were started, 113 were completed. This researcher disqualified seven completed surveys prior to commencement of analysis. Three of the surveys received from U.S. institutions were disqualified as they were not part of the survey population. Two completed surveys were received from institutions that were not within the U.S. or U.S. territories and were also

disqualified. Another disqualified survey had no Carnegie classification and appeared to be a part of another institution. This researcher believed this response would not represent the overall home institution. One survey arrived after the survey close date and was not added to the data analysis set. This researcher compiled a total of 106 valid surveys for analysis. This accounted for a responses rate of 7.22%.

The results of the survey were collected in the Qualtrics survey hosting solution. Only the researcher had access to the stored results. The results were protected by Qualtrics, which describes their offering as a secure hosting service that meets regulatory requirements for the hosting of sensitive data. The data was only accessible via a username and password combination. Data was exportable to various data formats including SPSS, Excel, and comma delimited text file. Only the researcher had access to any site identifying data in order to maintain the confidentiality of the data.

Data Analysis

The Qualtrics hosting solution allowed for the downloading of data for analysis in various formats. Dr. Rachel MacNair, a statistical consultant, was retained for assistance with the statistical computations. This researcher downloaded the data in excel format for delivery to the statistical consultant. The statistical consultant was only given access to the raw data that did not contain any email recipient data or any institution names. The statistical consultant subjected the data to statistical engines of Statistical Package for the Social Sciences (SPSS) 21.0 and delivered the output of the computations to this researcher for analysis.

In order to understand the relationship between information security breaches and information security policies, Doherty and Fulford (2005) collected data and subjected the data to statistical testing via various methods including one way Analysis of Variance (ANOVA) and others. This researcher used statistical correlation and t-tests to determine if statistically significant relationships exist between the various aspects of information security policies, awareness, and policy enforcement and the frequency and severity of information security breaches at the studied organizations. The aspects of information security policy, awareness, and policy enforcement formed the independent variables of this dissertation. The dependent variables were the continuous variables in the form of the frequency of breach occurrences and the perceived severity of breaches, (Doherty & Fulford, 2005). Table 5 depicts the variables and their associated statistical testing methods.

The independent variables of this research were tested for statistical significance with regards to the breaches at the responding organizations. Each of the independent variables was analyzed in conjunction with the frequency and severity of the responding organization's information security breaches to determine if a statically significant relationship exists. Doherty and Fulford (2005) denoted the incidence of breaches, dependent variable one, with a four point ordinal scale (0; 1-5; 6-10; > 10). Incidence of breaches was a continuous variable. The researchers measured the severity of the worst breaches experienced by category. This formed a continuous dependent variable that was measured via a five point Likert scale ranging from "fairly insignificant to highly significant."

The original research by Doherty and Fulford (2005) used an ordinal variable in the survey question asking about the frequency of breaches. As explained above, the variable was a four point ordinal variable. The survey question gave ranges for eight different categories of breaches. The counts of which were summed to yield a composite value for statistical analysis.

Doherty and Fulford did not actually ask for responses that yield precise numbers for the incidence of breaches. The researchers did not ask for the actual number of incidents. They asked for ranges. Also, since the responses were ranges, means or standard deviations for the number of incidents cannot be derived. Without means an ANOVA is not advisable, but the variable, as a ratio scale, did allow for a measure of more incidents versus less incidents. Also rather than executing eight different tests like Doherty and Fulford (2005), one for each category of breach types, this dissertation utilized one test for the sum of breach incidences for each hypothesis. In essence, a total score is derived by adding the incidences from each of the eight categories. This produced a continuous variable in the form of the total score. Therefore, the score for incidence of breaches, allowed for the use of correlations for comparison purposes.

Respondents were also asked to rate the perceived severity of the worst breaches that affected their agencies. The survey instrument presented the respondents with five severity categories using a five point Likert scale. The categories ranged from fairly insignificant, which was represented by a score of one, to highly significant, which was represented by a score of five. The breach severities were calculated into a total score, a continuous number, by summing the number of breach severities experienced by each

responding institution. The higher the score, the greater the severity experienced by the responding organization.

The original research by Doherty and Fulford (2005) conducted numerous statistical tests and comparisons for each of their hypotheses. This dissertation conducted the statistical tests and analyses in two fashions for the first five hypotheses. The first method involved testing for significance between the independent variables and a sum of breach frequencies across all categories. Also, testing was performed for significance between the independent variables and a sum of the breach severities across all categories. Each of the independent variables is described below:

- **Existence of the information security policy:** This was a two category independent variable. Either the organization has an information security policy or it did not. This variable was not testable due the fact only eight respondents indicated have no information security policy for their organization.
- **Age of the information security policy:** This was a continuous variable that indicates how long the information security policy had been in existence.
- **Time between policy review and update periods:** A five category independent variable that indicated how frequently the policy was reviewed and/or updated.
- **Scope of policy coverage:** A metric variable that described how broadly the scope of the information security policy covered security related issues. The Survey respondents were presented with a list of 12 distinct topics and were asked to indicate which items were covered within their organization's information security policy (Doherty & Fulford, 2005).

- **Adoption of best practice:** A continuous variable presented as a summated scale. According to Doherty and Fulford (2005) there were 10 factors covered by ISO 17799 with the potential to impact the success of an information security policy. Survey respondents were asked to indicate how well they perceived their organization had implemented each of the factors.
- **Existence of an information security awareness process:** Doherty and Fulford (2005) found that 99% of its respondents reported active dissemination of their organization's security policies. The ubiquity of dissemination in the respondents did not allow for testing a hypothesis based on dissemination of policies. This study instead focused on the existence of security awareness programs and the level of coverage of the awareness programs within the survey organizations. This variable was a categorical variable. The possible answers were either yes the awareness program exists or no it does not.
- **Scope of coverage of the information security awareness process:** This variable was a continuous variable indicated the level of coverage across the respondent organization. Respondents were asked to indicate what populations at their home institutions were served by the information security awareness process. The respondents were asked to indicate which segments of the campus community were covered by awareness training. The resultant responses were converted into a scope of coverage score; with one point given for each of the covered segments.

- **Existence of documented consequences for policy violations:** This variable indicated the existence of documented consequences and sanctions for policy violations at the respondent organization.
- **Consistency of the policy enforcement process:** This variable was a continuous variable that indicated the consistency of application of the enforcement process. Respondents were asked to indicate what segments at their home institutions were covered by consistently applied policy enforcement activities and sanctions. The respondents were asked to indicate which segments of the campus community were covered by consistent policy enforcement. The resultant responses were converted into a scope of enforcement score; with one point given for each of the covered segments.

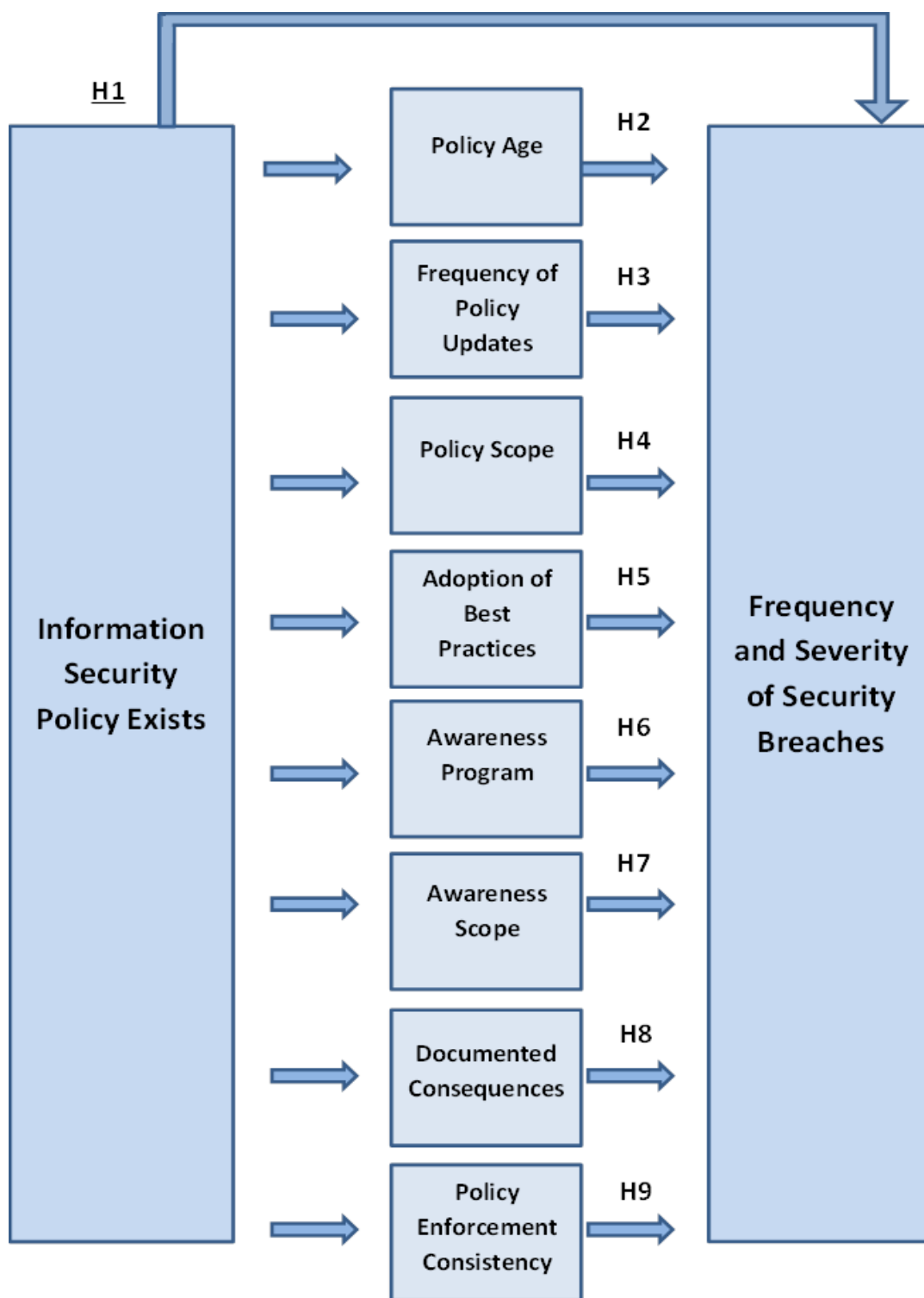


Figure 5. Expanded Concept Map (Nine Hypotheses)

Table 5. Variables and Analysis Methods

Hypothesis	Independent Variable	Variable type	Variable Measure	Breach Frequency (continuous 4 point scale)	Breach Severity (Continuous; 5 point Likert scale)
Existence of the information security policy	Policy Exists	Categorical	Yes or No	Not Conducted	Not Conducted
Age of the information security policy	Age of Policy	Continuous	Age in years 4 point ordinal scale	correlation	Correlation
Time between policy review and update periods	Frequency of Updates	Categorical	Five-item categorical	t-test	t-test
Scope of policy coverage	Broadness of Scope (range, total number, of issues covered)	Continuous	0-12 range	correlation	Correlation
Adoption of best practice	Use of Best Practices (10 Success Factors)	Continuous	Summated Scale	correlation	correlation
Existence of an awareness process	Security Awareness Exists	Categorical	Yes or No	t-test	t-test
Scope of coverage of awareness process	Scope of coverage (faculty, staff, student)	Continuous	Summated Scale	correlation	Correlation
Existence of documented consequences for policy violations	Documented Consequences Exist	Categorical	Yes or No	t-test	t-test
Consistency of enforcement	Score for consistency	Continuous	Summated Scale	correlation	Correlation

The researcher subjected the data to statistical analysis that focused on the use of information security policies, awareness programs, and consistent policy enforcement

within higher education and the associated effects on the frequency of occurrence and severity of information security breaches. The survey data was subjected to statistical analysis in order to examine the relationship between information security policies and the frequency and severity of information security breaches (Doherty & Fulford). As with Doherty and Fulford (2005), this researcher used methods such as correlation and t-tests to vet the existence of statistical significance between the independent and dependent variables. Where dependent variables were continuous values, correlation was used to measure the strength of the variables' linear association (Wuensch, 2001). Where the independent variables were categorical, t-tests were used to examine the variable's relationship.

Resource Requirements

An online hosting service, Qualtrics, was used to host the survey. Qualtrics also served as the vehicle for the delivery of the electronic survey invitations. The survey tool provided secure data access to place potential respondents at ease as to the security of the data. As no sponsor organization was available to provide contact information or bona fides for the survey, the researcher compiled a list of higher education organizations and associated contact information. The researcher obtained contact information from the Higher Education Directory and professional contacts from the higher education information security arena. This approach was less than optimal but yielded testable data.

The researcher's professional institution, the University of North Carolina at Chapel Hill Odum Institute offers free statistical consulting. In the past, they have worked with a wide variety of clients with wide ranging research needs. The Statistics and Operations

Research Department has aided individuals from students needing help with the statistical analysis for dissertation research to full time faculty. Graduate students working on PhD projects are welcome, but are advised to first obtain the approval of their advisers. The Odum institute assisted the researcher in understanding various aspects of the statistical analysis.

The researcher contracted with Dr. Rachel MacNair of MacNair Statistics for statistical analysis services. Dr. MacNair used SPSS version 21.0 to calculate the statistical values for the results section of this report. Dr. MacNair provided those results to this researcher for interpretation and documentation. Dr. MacNair was not provided with any identifiable data for statistical calculation.

Chapter 4

Results

Introduction

Chapter 4 includes an objective description and analysis of the findings and results of this dissertation. This study was created based on original research conducted by Doherty and Fulford (2005). Doherty and Fulford (2005) studied the significance between information security policies and the frequency and severity of information security breaches at businesses in the U.K. The original inspiration for this author's research, Doherty and Fulford (2005) had five hypotheses. Doherty and Fulford distributed its original survey as a paper based instrument.

This dissertation added additional questions to the Doherty and Fulford (2005) paper research instrument in order to expand upon the original research. The five hypotheses from Doherty and Fulford (2005) are augmented by four additional hypotheses. In all, this dissertation has nine hypotheses based on nine research questions. A survey was developed and presented to the target population via a web based survey instrument. There were a total of 15 questions in the survey instrument. The survey was open for a period of approximately three months. The following sections of this chapter present the results from the analysis of the responses provided by the survey respondents.

Findings

Institution Demographic Data

It is advisable to have a shorter survey completion time and fewer questions to encourage participation (Dillman, Smyth, & Christian, 2009). As a great deal of demographic data is available for institutions of higher education, this research did not ask questions regarding the demographics of the responding institutions. Instead this research relied on information provided by the Carnegie Foundation for the demographic data. This allowed for a streamlined questionnaire. Data such as enrollment, funding source, region, Carnegie Classification, and Size and Setting are presented below. This data serves to describe the characteristics for pool of respondents in absence of publishing the names of the institutions.

According to the Carnegie Foundation website, “*the Carnegie Classification has been the leading framework for recognizing and describing institutional diversity in US higher education for the past four decades*” (Carnegie Foundation). The Carnegie Foundation provides six classifications by which an organization can be categorized. This research utilizes two of the six classifications, Size and Setting and Carnegie Classification.

Table six depicts the size of responding institutions by enrollment size. The largest category of respondents was in the 10,000 through 19,999 enrolled students group at 25.47%. The second largest was institutions with from 3,000 through 9,999 enrolled students with 22.64%. All categories were well represented as no group accounted for less than 10% of the total respondent pool.

Table 6. Carnegie Enrollment Distribution Statistics

Enrollment	Frequency	Percentage
Less than 1000	12	11.32
1000-2999	15	14.15
3000-9999	24	22.64
10000-19999	27	25.47
20000-29999	14	13.21
Greater than 30000	14	13.21

Table seven depicts the Carnegie Classifications for the responding institutions. The largest group of responding organizations was Doctoral/Research Universities. The two classifications for these types of organizations, both intensive and extensive, accounted for nearly 40% of all respondents. Master's Colleges accounted for roughly 30% of respondents. The remainder of the respondents was distributed amongst the remaining categories.

Table 7. Carnegie Classification Distribution Statistics

Carnegie Classification	Frequency	Percentage
Associate's Colleges (4yr granting)	1	0.94
Baccalaureate Colleges—General	9	8.49
Baccalaureate Colleges—Liberal Arts	6	5.66
Baccalaureate/Associate's Colleges	6	5.66
Doctoral/Research Universities—Extensive	29	27.36
Doctoral/Research Universities—Intensive	12	11.32
Master's Colleges and Universities I	30	28.30
Master's Colleges and Universities II	1	0.94
Specialized Institutions—Medical schools and medical centers	2	1.89
Specialized Institutions—Other separate health profession schools	2	1.89
Specialized Institutions—Schools of art, music, and design	1	0.94
Specialized Institutions—Schools of business and management	2	1.89
Specialized Institutions—Schools of engineering and technology	1	0.94
Specialized Institutions—Teachers colleges	1	0.94
Specialized Institutions—Seminaries and faith-related institutions	3	2.83

Table eight illustrates the breakdown of respondents by Carnegie Size and Setting. This classification describes institutions' size and residential quality. Because residential quality applies to the housing status for an undergraduate student body, institutions with exclusively graduate/professional institutions are excluded from this classification. Large four year institutions that are primarily residential and large four year institutions that are non-residential both account for 21% of the respondent pool. Together they comprise 42% of the total respondent pool.

Table 8. Carnegie Size and Setting Distribution Statistics

2010 Size & Setting(sizeset2010)	Frequency	Percentage
ExGP: Exclusively graduate/professional	3	2.83
L2: Large two-year*Bachelors granting	1	0.94
L4/HR: Large four-year, highly residential	6	5.66
L4/NR: Large four-year, primarily nonresidential	21	19.81
L4/R: Large four-year, primarily residential	21	19.81
M4/HR: Medium four-year, highly residential	10	9.43
M4/NR: Medium four-year, primarily nonresidential	5	4.72
M4/R: Medium four-year, primarily residential	10	9.43
S4/HR: Small four-year, highly residential	9	8.49
S4/NR: Small four-year, primarily nonresidential	2	1.89
S4/R: Small four-year, primarily residential	4	3.77
Special focus institution	9	8.49
VL2: Very large two-year*Bachelors granting	1	0.94
VS4/HR: Very small four-year, highly residential	3	2.83
VS4/NR: Very small four-year, primarily nonresidential	1	0.94

Table 9 presents the respondent pool makeup sorted by funding source. The three categories in funding source included public, private not-for-profit, and private for profit.

The largest group of respondents (57.55%) was public institutions. Private not-for-profit accounted for the second largest pool with 40.57% of responses. Finally, private for-profit (1.89%) only accounted for a small portion of the respondents.

Table 9. Carnegie Funding Source Distribution Statistics

Funding Source	Frequency	Percentage
Public	61	57.55
Private not-for-profit	43	40.57
Private for-profit	2	1.89

Table 10 depicts the makeup of the respondent pool by region as listed by the Carnegie Foundation. There were nine regions represented in the pool of respondents. The largest group (29.25%) was located in the Southeast region. This group was nearly greater than twice as large as the next largest group (15.09%), located in the Great Lakes region. There were also two institutions from the Outlying areas that responded.

Table 10. Carnegie Region Distribution Statistics

Region	Frequency	Percentage
Far West AK CA HI NV OR WA	11	10.38
Great Lakes IL IN MI OH WI	16	15.09
Mid East DE DC MD NJ NY PA	9	8.49
New England CT ME MA NH RI VT	7	6.60
Outlying areas AS FM GU MH MP PR PW VI	2	1.89
Plains IA KS MN MO NE ND SD	13	12.26
Rocky Mountains CO ID MT UT WY	4	3.77
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	31	29.25
Southwest AZ NM OK TX	13	12.26

Descriptive Data

Table 11 depicts the descriptive results of this dissertation for the frequency and severity of breaches. Responses indicated as not sure are not depicted and are treated as missing responses. Responses of “not sure” are not used in the calculation of the mean value.

Table 11. Higher Education Institutions Frequency and Severity of Breaches

Type of Breach	Frequency of Breaches				Severity of Breaches					
	<i>Approximate Number of Breaches in Last Two Years</i>				<i>Fairly Insignificant</i>	<i>Highly Significant</i>			<i>Mean Value</i>	
	0	1-5	6-10	>10	1	2	3	4	5	
Computer Malware	17	24	11	48	34	25	16	6	2	2.00
Hacking Incident	50	42	2	7	9	21	7	8	6	2.63
Unauthorized access	40	39	7	10	19	21	9	8	2	2.20
Theft of hardware/ software	36	44	10	10	13	30	10	4	6	2.37
Computer-based fraud	71	23	2	1	9	10	6	2	2	2.24
Human Error	19	54	6	15	30	23	17	7	7	2.26
Force Majeure	79	18	0	0	6	5	8	4	0	2.43
Damage by employees	83	15	1	0	1	10	2	2	1	2.50

Research Questions Answered

The first research question depicted as item A below represents the question of “Does an information security policy have an effect on the frequency and severity of information security breaches?” Hypothesis one was derived from the first research question. Hypothesis one predicted that organizations that had information security policies would have fewer and/or less severe security breaches. This hypothesis was not tested due to insufficient responses that indicated not having a formal information security policy. However, all other hypotheses were testable.

The second research question was the question “Does the age of the information security policy have an effect on the frequency and severity of information security breaches?” Hypothesis two is derived from the second research question. Hypothesis two predicted that organizations that had more mature security policies would have fewer and/or less severe security breaches. For example, as the age of the policy increased, the frequency and severity of breaches would decrease.

Table 12. Relationship Between the Age of Information Security Policy and the Incidence of Security Breaches by Total Breach Count

Correlation		Response Period 2 Years
Incidence	Pearson Correlation	.074
	Sig. (2-tailed)	.537

Table 13. Relationship Between the Age of Information Security Policy and the Severity of Security Breaches by Total Breach Count

Correlation		Response Period 2 Years
Severity	Pearson Correlation	.052
	Sig. (2-tailed)	.662

Survey respondents were asked to state in years, how long their organization has actively used a documented information security policy. This study relied on two correlation tests as the analysis methods. The dissertation used one correlation test for the relationship between the age of policies and the incidence of breaches. The results of this test are represented by Table 12. A second correlation test was utilized to analyze

the relationship between the severity of the worst breaches reported by each organization and the age of the security policy. The results of this test are represented by Table 13.

When analyzing the results of the statistical tests for total breach count, no statistically significant relationships were observed. Both of the p-values from the analyses, shown in Table 12 and Table 13, were greater than .05, indicating no statistically significant associations. The results of the analysis indicated no evidence of statistically significant associations between the age of the information security policy and the incidence of information security breaches. Additionally, there was no evidence of a statistically significant relationship between the age of policy and the severity of breaches.

Hypothesis two was disconfirmed. This research did not observe the weak significance between variables that Doherty and Fulford (2005) observed. However, the results corroborated the overall findings of Doherty and Fulford (2005) which rejected its hypothesis two due to no indication of strong significance being observed. Tables representing the findings of Doherty and Fulford (2005) are located in Appendix E.

The third research question represents the question “Does the frequency of information security policy updates have an effect on the frequency and severity of information security breaches?” Hypothesis three is derived from the third research question. Hypothesis three predicted that organizations that had frequent information security policy updates would have fewer and less severe security breaches.

Table 14. Results of Levene's Test for Equality of Variances

	F	Sig.
Incidence	2.534	.115
Severity	3.759	.055

Table 15. Relationship Between the Frequency of Information Security Policy Updates and the Incidence of Security Breaches by Total Breach Count

		t	df	Sig. (2- tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference		
								Lower	Upper
Incidence	Equal variances assumed	.123	96	.902	.197	1.607	-2.992	3.387	

Table 16. Relationship Between the Frequency of Information Security Policy Updates and the Severity of Security Breaches by Total Breach Count

		t	df	Sig. (2- tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference		
								Lower	Upper
Severity	Equal variances assumed	.010	96	.992	.030	2.960	-5.846	5.906	

There were a total of five categories respondents might have chosen as responses to represent their organizations. This author compressed the categories into two categories of less than one update per year and the other, one or more updates per year. This author utilized t-tests to explore the statistical relationships. The results of the t-tests are represented in Table 15 for the incidence of breaches and Table 16 for the severity of breaches. The results of the t-tests yielded p-values that were greater than .05 for both the sets of t-tests. As such, there is no indication of statistically significant relationships between update frequency of the information security policy and security breaches in terms of either severity or frequency. Hypothesis three was disconfirmed. This analysis

corroborated the findings from Doherty and Fulford (2005) which also found no strong evidence of significant relationship between the two variables.

The fourth research question is represented by the question “Does the range of issues covered by an information security policy have an effect on the frequency and severity of information security breaches?” Hypothesis four is derived from the fourth research question. Hypothesis four predicts that organizations with information security policies covering broad scopes would have fewer and/or less severe security breaches.

Table 17. Relationship Between the Range of Issues Covered by the Information Security Policy and the Incidence of Security Breaches by Total Breach Count

Correlation		Scope
Incidence	Pearson Correlation	.115
	Sig. (2-tailed)	.242

Table 18. Relationship Between the Range of Issues Covered by the Information Security Policy and the Severity of Security Breaches by Total Breach Count

Correlation		Scope
Severity	Pearson Correlation	-.085
	Sig. (2-tailed)	.386

For this dissertation the scope of policy coverage was defined as a listing of 12 potential separate issues that that might be covered in policy. The Survey respondents were presented with a list of 12 distinct topics and were asked to indicate which items are covered within their organization’s information security policy. The count or sum of the categories provided by each of the respective respondents was used to derive a continuous variable that described how broadly the scope of the information security

policy covered security related issues. Respondents' answers were summed to create a score within the range of 0-12.

The analysis was performed so that each issue was given a value of one if any of the categories of policy or standard was present. Therefore an issue is either covered or not. The highest possible score was 12 and the lowest was zero. Correlation tests were used for both frequency of breaches and severity of breaches. The result of the correlation test for the relationship between the range of issues covered by the policy and the incidence of security breaches is depicted in Table 17. Additionally, the result of the correlation test for the relationship between the range of issues covered by the policy and the severity of security breaches is depicted in Table 17. The p-values were greater than .05 for both incidence and severity. Therefore, hypothesis 4 was disconfirmed. These findings corroborated the results found by Doherty and Fulford (2005).

The fifth research question represents the question of “Does the successful adoption of success factors in an information security policy have an effect on the frequency and/or severity of information security breaches?”. Hypothesis five covered the prediction that organizations that had policies based on a wide variety of best practices would have fewer and/or less severe security breaches.

Table 19. Relationship Between the Successful Adoption of Success Factors and the Incidence of Security Breaches by Total Breach Count

Correlation		Success
Incidence	Pearson Correlation	-.162
	Sig. (2-tailed)	.097

Table 20. Relationship Between the Successful Adoption of Success Factors and the Severity of Security Breaches by Total Breach Count

Correlation		Success
Incidence	Pearson Correlation	-.162
	Sig. (2-tailed)	.097

This section of the research revolved around the impact of the adoption of 10 best practice areas on breaches. The best practices were derived from ISO17799. The survey instrument was used ask the respondents about the importance of each area. They also inquired as to how successful the respondents believed their home organization was in adoption of the 10 areas.

This dissertation utilized correlations to explore the relationship between adoption of best practices and the frequency and severity of breaches. The result of the correlation test for the relationship between the successful adoption of success factors and the incidence of security breaches is depicted in Table 19. The result of the correlation test for the relationship between the successful adoption of success factors and the severity of security breaches is depicted in Table 19. The p-values were greater than .05 for both frequency and severity, hypothesis five was therefore disconfirmed. This analysis corroborated the findings of Doherty and Fulford (2005), which found no indications of strong evidence to support the hypothesis.

Research question six represents the question “Does a formal education and awareness program that is administered to the workforce in the information security policy result in a reduction of security breaches in terms of severity and frequency?” Security awareness is believed to be an important facet of an effective information security program and is

cited as such in entries in the literature (Rezgui & Marks, 2008; Wiles, 2008; Wright, 2008). As is the case with other assertions regarding information security, there is little in the form of empirical evidence that supports the claims. Hypothesis six predicted that organizations with an information security awareness program would experience fewer security breaches or that the breaches that did occur would be less severe than organizations without security awareness programs.

Table 21. Relationship Between the Existence of an Information Security Awareness Program and the Incidence of Breaches by Total Breach Count

		t	df	Sig. (2- tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference		
								Lower	Upper
Incidence	Equal variances assumed	.122	102	.903	.157	1.293	-2.408	2.723	

Table 22. Relationship Between the Existence of an Information Security Awareness Program and the Severity of Breaches by Total Breach Count

		t	df	Sig. (2- tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference		
								Lower	Upper
Severity	Equal variances assumed	-.202	102	.840	-.476	2.359	-5.154	4.202	

This research question focused on the existence of security awareness programs within the surveyed organizations. Survey respondents were asked: does the information security awareness program exist? There were two choices for potential respondents.

Yes, indicating a formal security awareness program exists. The other choice being no, a security program does not exist.

Two t-tests were utilized to explore the relationship between the existence of the awareness program and the incidence and severity of breaches. The result of the t-test that examines the relationship between the existence of an information security awareness program and the incidence of breaches is depicted by Table 21. The result of the t-test that examines the relationship between the existence of an information security awareness program and the severity of breaches is depicted by Table 22. The p-values were greater than .05 for both sets of relationships. There was no indication of a significant relationship between the existence of a security awareness program and either the incidence or severity of breaches. Hypothesis 6 was disconfirmed.

Research question seven is represented by the question “Does an organization that has a wider mandatory scope of coverage for its information security awareness program have fewer and/or less severe security breaches?” Hypothesis seven predicted that organizations that had wider mandatory coverage of information security awareness programs would have fewer and/or less severe security breaches.

Table 23. Relationship Between the Information Security Awareness Program Scope of Coverage and the Incidence of Breaches by Total Breach Count

Correlation		Coverage
Incidence	Pearson Correlation	-.044
	Sig. (2-tailed)	.655

Table 24. Relationship Between the Information Security Awareness Program Scope of Coverage and the Severity of Breaches by Total Breach Count

Correlation		Coverage
Severity	Pearson Correlation	-.036
	Sig. (2-tailed)	.713

Employees must be made aware of their information security roles and responsibilities. In regards to information security, training and awareness is used to inform workforce members about the approaches an organization has implemented. Employees are then able to receive the fundamentals of the security program via formal training mechanisms (Knapp et al., 2009). According to Beutement and Sasse (2009) an effective information security policy depends on an entity's employees. According to NIST publication 800-16 Information technology security training requirements, federal agencies cannot have a successful information security program without adequately training their workforce. The guide indicates that all employees need instruction on security fundamentals. The guide advocates for role based training (van Niekerk & von Solms, 2008).

This dissertation asked respondents to indicate which workforce categories are required to take information security awareness training. The respondents were presented with three employee categories, students, and not sure as potential answers. The results for each response were assimilated into a coverage score. This researcher derived the coverage scope by reviewing the responses for each category of employee and student (Faculty, Staff, Contractors and Students). This researcher assigned one point for each category represented in the response. The potential score ranged from 0-4.

Correlation tests were conducted to analyze the relationship between the coverage of the awareness program, as defined by the coverage score and both the severity and frequency of breaches. First, the results were tested for normality by reviewing the Kurtosis and Skewness statistics. After the assumption of normality was observed as met, the correlation analyses were performed. The result of the correlation that examines the relationship between the scope of awareness coverage and the incidence of breaches is depicted by Table 23. The result of the correlation that examines the relationship between the scope of awareness coverage and the severity of breaches is depicted by Table 24. The p-values were greater than .05 for both incidence and severity. This being the case, there was no statistically significant relationship indicated between the awareness coverage score and either the frequency or severity of breaches. Based on the absence of an indication a statically significant relationship between the variables hypothesis seven was disconfirmed.

Research Question eight is represented by the question “Does the existence of documented consequences for failure to follow policy result in a reduction of security breaches in terms of severity or frequency?” Many works in the literature highlight the importance of the consistent enforcement of information security policies (Baker & Wallace, 2007; Hoonakker et al., 2008; Knapp et al., 2009). The studies do not offer empirical evidence that supports the assertion. Hypothesis eight predicts that organizations with documented consequences for policy violations would have fewer and/or less severe security breaches.

Table 25. Relationship Between the Existence of Documented Consequences for Policy Violations and the Incidence of Breaches by Total Breach Count

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F.	Sig.	t	df	Sig.	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Incidence	Equal variances assumed	.001	.982	-.812	97	.419	-1.076	1.325	-3.706	1.555

Table 26. Relationship Between the Existence of Documented Consequences for Policy Violations and the Severity of Breaches by Total Breach Count

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F.	Sig.	t	df	Sig.	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Severity	Equal variances assumed	.001	.973	.139	97	.890	.364	2.616	-4.829	5.556

Two t-tests were conducted on the resultant data in order to explore the impact of the existence of documented consequences for policy violations on breaches. The results of the t-test that explored the relationship between the documented consequences for policy violations and the incidence of breaches are depicted in Table 25. The results of the t-test that explored the relationship between the documented consequences for policy violations and the severity of breaches are depicted in Table 26. The p-values were greater than .05 for both incidence and severity. Therefore, the t-tests were found to be statistically non-significant for the relationships between the incidence and the severity of breaches and

the adoption of documented consequences for policy violations. As a result, hypothesis eight was disconfirmed.

Research question nine is represented by the question “Do organizations with greater levels of enforcement consistency experience fewer and/or less severe security breaches?” Hypothesis nine, which is derived from research question nine, predicted that organizations with greater levels of enforcement consistency would experience fewer and/or less severe security breaches.

Table 27. Relationship Between the Scope of Consistent Enforcement of Information Security Policy and the Incidence of Breaches by Total Breach Count

Correlation		Scope of Coverage
Incidence	Pearson Correlation	-.010
	Sig. (2-tailed)	.918

Table 28. Relationship Between the Scope of Consistent Enforcement of Information Security Policy and the Severity of Breaches by Total Breach Count

Correlation		Scope of Coverage
Severity	Pearson Correlation	.099
	Sig. (2-tailed)	.311

Knapp et al. (2009) suggests that policy enforcement should be a consistent activity and that when policy is violated corrective action should occur. Policy should be a deterrent for bad actions and provide a sense that punishment looms when bad activity is perpetrated (Knapp et al.). Workforce members should be made aware when enforcement activities are utilized (McKenna, 2010). Beutement and Sasse (2009) suggests that

policy enforcement must be consistent. Sanctions are only effective when they are consistently applied whenever the policy is not followed (Beautement & Sasse, 2009). All workforce members should be covered by a policy and its sanctions in order for the policy to be sound. The policies should be comprehensive, have associated training, and sanctions should be swiftly applied to ward against violations (Hu, Xu, Dinev, & Ling, 2011).

Respondents were asked to rate their organizations' respective enforcement processes according to the extent to which they either agreed or disagreed with the statement *"Information Security Policy is consistently enforced for the organization (i.e. sanctions are applied consistently for faculty, staff, and students)."* The potential responses were derived from a five point Likert scale ranging from "strongly disagree to strongly agree."

The results of the Likert scale were converted to a score by granting each organization one point for each covered employee/student group. The points were summed to create a total score for each institution. This score was used to represent the perceived enforcement consistency for each institution. A correlation test was conducted to analyze the relationship between the scope of enforcement consistency and incidence of breaches. The results of this correlation are presented in Table 27. A second correlation explored the relationship between the scope of enforcement consistency and severity of breaches. These results are presented in Table 28. The corresponding p-values were greater than .05 for both incidence and severity. No statistically significant relationships between the variables were indicated. Therefore hypothesis nine was disconfirmed.

Exploratory Questions

The following section presents the quantitative breakdown of the responses from additional questions asked of the survey respondents. These results were presented to give the reader visibility into the additional questions that were asked in order to present context to the primary research questions and hypotheses based questions from the survey instrument. Additionally, this data is presented in Appendix G. The data in Appendix G. is sorted and categorized according to Carnegie Classification data.

Research questions six and seven focused on the impact of information security awareness efforts on breaches. Research Questions eight and nine explored the relationships between enforcement efforts and breaches. As stated previously, there were no statistically significant relationships indicated between either awareness or enforcement efforts and the frequency or impact of information security breaches. This being stated, the questions and responses portrayed in tables 29 through 35 give the reader a view into the state of awareness programs and enforcement efforts at the responding institutions. One position that could be drawn from the data is that awareness programs and consistent enforcement efforts are not widely used in higher education.

One way to communicate employee information security responsibilities is an information security awareness training program. Security training allows the employees to receive the fundamentals of the security program via formal training mechanisms (Knapp et al., 2009). According to the data discovered in this dissertation, formal awareness programs are not heavily used in colleges and universities. Approximately 55% of responding institutions reported having a formal information security awareness program. Many institutions (44%) required information security awareness training only

once for their members. Additionally, just over half of the responding institutions (53%) required training on an at least biennial basis.

Enforcement efforts and sanctions are only effective when they are consistently applied whenever the policy is not followed (Beautement & Sasse, 2009). Workforce members should be made aware when enforcement activities are utilized (McKenna, 2010). In terms of enforcement efforts, only 66% percent of responding institutions indicated having documented consequences for violations of policy. Additionally, 38% of respondents indicated that they did not believe their organization consistently enforced its policies.

For the data represented in Table 29, survey respondents were asked if their institution had a formal and documented security awareness program. This table gives the results sorted by the respondent's responses of yes, no, and not sure in regards to the existence of an information security policy at their institution. While more than half of responding organizations (55%) indicated having formal information security awareness programs, nearly 43% of responding organizations indicated not having a formal program. This was far from the level of prevalence (roughly 92.5%) of security policies adopted by institutions.

Table 29. Responses to the Question “Does an Information Security Awareness Program Exist?”

N=106	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Total	58	55%	46	43%	2	2%

The next table, Table 30, focuses on the responses to the question centered on how often is awareness training required? Less than half of the responding institutions (44%)

required information security awareness training only once for their members. Just more than half of the responding institutions (53%) required training on an at least biennial basis.

Table 30. Responses for the Question “How often is Awareness Training Required?”

N=59	Every 6 Months		Annually		Every Two Years		Only Once		Not Sure	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Total	0	0%	27	46%	4	7%	26	44%	2	3%

The next table, Table 31, presents the responses to the question “when information security awareness training is presented, how is it delivered?” The greatest concentrations of respondents (70%) indicated delivering training via web based methods. This was followed by in person delivery at 60%.

Table 31. Responses to the Question “How is Information Security Awareness Training Delivered?”

N=106	Web Based		Email Based		Paper handouts or mailers		Videos		Facilitated during in person presentations		Not Sure	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Total	74	70%	32	30%	26	25%	31	29%	64	60%	9	8%

Table 32, presents the responses to the question Responses for the question “Do documented consequences exist for failure to comply with policy?” Only 62% percent of responding institutions indicated having documented consequences for violations of policy.

Table 32. Responses for the Question “Do Documented Consequences Exist for Failure to Comply with Policy?”

N=106	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Total	66	62%	33	31%	7	7%

Table 33, focuses on the responses to the question where respondents were asked to indicate the strength to which they agreed or disagreed that their institution’s policies were consistently enforced. Here only 62% percent of responding organization indicated being at least neutral as to whether or not they agreed that their organization consistently enforced its policies. Additionally, 38% percent of responding agencies were within the “disagree to strongly disagree” response columns in regards to making users aware of enforcement activities.

Table 33. Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution’s Policies Were Consistently Enforced

N=106	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Total	10	9%	31	29%	26	25%	37	35%	2	2%

Table 34, focuses on the responses to the question where respondents were asked to indicate the strength to which they agreed or disagreed that their institution made users aware of enforcement activities. These results closely mirrored the results of the previous question in that 62% of respondents were either neutral, agreed, or strongly agreed that their organization made users aware of enforcement activities. While approximately 37% disagreed or strongly disagreed with that sentiment.

Table 34. Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution Made Users Aware of Enforcement Activities

N=106	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Total	13	12%	27	25%	34	32%	29	27%	3	3%

Table 35, focuses on the responses to the question where respondents were asked to indicate the strength to which they agreed or disagreed that their institution's compliance activities are visible to users. Again, these results aligned with the results of the previous two questions in that 66% of respondents were either neutral, agreed, or strongly agreed that their organization's enforcement activities were visible to users. While approximately 35% disagreed or strongly disagreed with that enforcement activities were visible to users.

Table 35. Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Compliance Activities are Visible to Users

N=106	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Total	7	7%	30	28%	22	21%	44	42%	3	3%

Summary of Results

This chapter depicted the data collected via the survey instrument, the statistical test used to determine significance between the dependent and independent variables, and results of the analysis. The results from nine hypothesis and associated research questions were described. The hypotheses were the results of a mixture of five hypotheses from Doherty and Fulford (2005) and four new hypotheses from this research as culled from the literature.

The data collected for this research effort was captured via an online survey hosted by Qualtrics. The research effort built upon a previously validated survey from Doherty and Fulford (2005). The additional questions used in the survey were subjected to a review and validation process that saw three researchers and one information security professional review the entire survey and make comments regarding their ability to understand and complete the survey. The comments and concerns of the review panel were then encapsulated in a revised version of the survey. The survey was then distributed to potential respondents.

The revised survey was attempted by 253 respondents and 106 valid surveys were presented for data analysis. No human demographic data was requested from the respondents, but organizational demographic data was captured and presented in tables one through five. The demographic data was presented for four Carnegie Foundation categories (Carnegie Classification, Student Enrollment, Funding Control, and Region).

For the hypotheses that were created by Doherty and Fulford (2005), the hypotheses were tested via correlation tests and t-tests. Hypothesis one was not testable by this

research. This was due to a lack of responses by organizations that reported having no information security policies. Therefore, this study was neither able to confirm nor disconfirm hypothesis one. Hypothesis two predicted that organizations that had more mature security policies would have fewer and/or less severe security breaches. This study relied on two correlation tests to test hypothesis two. Both of the p-values from the analyses were greater than .05, indicating no statistical significant associations between the age of the information security policy and the severity and frequency of information security breaches. Hypothesis two was disconfirmed. Hypothesis three predicted that organizations that had more frequent information security policy updates would have fewer and/or less severe security breaches than those with less frequent updates. This research relied upon two t-tests to explore the statistical relationships for hypothesis three. The analysis yielded p-values that were greater than .05 which indicated no statistically significant relationships between update frequency of the information security policy and security breaches in terms of either severity or frequency. Hypothesis three was disconfirmed. Hypothesis four predicted that organizations that had information security policies of broad scope would have fewer and/or less severe security breaches. This dissertation added one additional topic to the existing list of 11 issues covered by Doherty and Fulford (2005). Therefore, the final “Scope” score had a possible range of scores of zero to 12. The analysis was performed so that each issue was given a value of one if any of the categories of policy or standard was present. Correlation tests were utilized for both the incidence of breaches and the severity of breaches. Since the p-values were greater than .05 for both frequency and severity, hypothesis four was disconfirmed. Hypothesis five covered the prediction that organizations that had

policies based on a wide variety of best practices would have fewer and/or less severe security breaches. Two correlations were used to explore the relationship between adoption of best practices and the frequency and severity of breaches. For both the Importance and Success Factors, the p-values were greater than .05, as such, there is no statistically significant relationship between the adoption of best practices and either the frequency or severity of breaches. Hypothesis five was disconfirmed.

Hypothesis six predicted that organizations with an information security awareness program would experience fewer security breaches or that the breaches that did occur would be less severe than organizations without security awareness programs. Two t-tests were utilized to explore the relationship between the existence of the awareness program and both the incidence and severity of breaches. The p-values were greater than .05 for both sets of relationships. Hypothesis six was disconfirmed. Hypothesis seven predicted that organizations that have wider mandatory coverage of information security awareness programs would have fewer and/or less severe security breaches. Two correlation tests were conducted to analyze the relationship between the scope of awareness program coverage and the severity and frequency of breaches. The resultant p-values were greater than .05. As such, there is no statistically significant relationship between the variables. Therefore hypothesis seven was disconfirmed. Hypothesis eight predicted that organizations with documented consequences for policy violations would have fewer and/or less severe security breaches. Two t-tests were conducted on the resultant data. The t-tests failed to indicate a statistically significant relationship between the incidence or severity of breaches and the adoption of documented consequences for policy violations. Therefore Hypothesis eight was disconfirmed. Hypothesis nine predicted that

organizations with greater levels of enforcement consistency would experience fewer and/or less severe security breaches. A correlation test was conducted to analyze the relationship between the perceived consistency of enforcement and both the severity and frequency of breaches. No statistically significant relationships were indicated between the variables. Therefore, hypothesis nine was disconfirmed.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

This chapter illustrates the conclusions formed by this author's review and analysis of the nine research questions of this dissertation. The chapter goes on to highlight the implications of this research in regards to advancing the body of knowledge. Strengths and limitations of the research are also discussed. Additionally, recommendations for future research are discussed. Finally, the chapter and dissertation conclude with a general summary.

Conclusions

Doherty and Fulford (2005) conducted research into understanding the relationships between information security policies and the frequency and severity of information security breaches. The study focused on the perceived importance of the information security policy and its roles in making organizations more secure. Doherty and Fulford (2005) explored this perception and attempted to see if there was indeed a significant relationship between policies and breaches. They formulated and tested a set of hypotheses centered on the information security policy reducing the incidence and severity of information security breaches.

Doherty and Fulford theorized that a number of policy aspects could influence security breaches. There were five primary aspects studied. Does an information security policy exist for the organization in question? If an information security policy exists, how long has it been in place? How often is the information security policy updated? Does the

information security policy have sufficient scope? Has the organization based its security approach on a set of established best practices? Ultimately, the study determined that no strong significant statistical relationship existed between the covered aspects of the information security policy and the frequency or severity of security breaches.

In an attempt to advance the body of knowledge, a total of nine research questions were addressed over the course of this dissertation. The questions were comprised of the original five from Doherty and Fulford (2005) and an additional four from this dissertation. The new questions focused on aspects of information security awareness and information security policy enforcement. All nine hypotheses were tested via a mixture of correlation tests and t-tests. As was the case with Doherty and Fulford (2005), no statistically significant relationships were indicated between the dependent and independent variables.

Research Questions

The first research question was “Are higher education institutions that have formal information security policies likely to have less security breach incidents in terms of severity or frequency than those without?” (Doherty & Fulford, 2005, p. 25)? Doherty and Fulford hypothesized the organizations that had information security policies would have fewer and/or less severe security breaches. In order obtain information from respondents, this research utilized a survey question from Doherty and Fulford’s original survey instrument. Respondents were asked to answer to the question: Does your organization have a documented information (IT, Cyber) security policy? Out of the 106 viable

responses, only eight organizations indicated not having a documented information security program. Therefore hypothesis one could not be tested.

Even though hypothesis one could not be tested, it is interesting to note that the eight respondents that indicated not having security policies account for approximately 7.54% of all respondents. A full 92.45% of respondents indicated having a documented information security policy. There is potential corroboration of this high level of policy implementation by data from the 2012 EDUCAUSE Core Data Survey. The 2012 Core Data survey information security module had 646 responding institutions. Among the questions focused on the existence of various policy provisions, only three percent of responding agencies indicated having none of the provisions covered by the questions. The remaining 97% of responding agencies indicated having at least one policy among the nine policy areas covered by the EDUCAUSE questions (EDUCAUSE, 2012).

The second research question was “Does the age of the information security policy result in a reduction of security breaches in terms of severity and frequency (Doherty & Fulford, 2005, p. 25)?” Hypothesis two, again from Doherty and Fulford theorized that organizations that had more mature security policies would have fewer and/or less severe security breaches. As the age of the policy increased, the frequency or severity of breaches would decrease. Survey respondents for this dissertation were asked the question “In years, how long has your organization actively used a documented information security policy (Doherty & Fulford, 2005, p. 25)?” The results of the analysis indicated no evidence of statistically significant associations between the age of the information security policy and the severity and frequency of information security breaches. Hypothesis two was disconfirmed.

The third research question “Does the update frequency of the information security policy result in a reduction of security breaches in terms of severity and frequency (Doherty & Fulford, 2005, p. 26)?” Hypothesis three predicted that organizations that had frequent information security policy updates would have fewer and/or less severe security breaches. Respondents were asked the question “Approximately how often is the policy updated?” Data Analysis indicated no statistically significant relationships between update frequency of the information security policy and security breaches in terms of either severity or frequency. Hypothesis three was disconfirmed.

Research question four asks “Does having a broad scope of issue coverage in the information security policy result in a reduction of security breaches in terms of severity and frequency (Doherty & Fulford, 2005, p. 26)?” From this question Doherty and Fulford formed hypothesis four, which supposes that organizations that had information security policies of broad scope would have fewer and/or less severe security breaches. Respondents for this dissertation were asked to use a table in the survey instrument to indicate the security issues covered in their respective IT security policies. No statistically significant relationships were observed during analysis. Hypothesis four was disconfirmed.

Research question five asks “Does the adoption of best practice factors in the information security policy result in a reduction of security breaches in terms of severity and frequency (Doherty & Fulford, 2005, p. 26)?” Hypothesis five covered the prediction that organizations with policies based on a wide variety of best practices would have fewer and/or less severe security breaches. Respondents were again asked to use a table in the survey instrument, but this instance, to indicate the importance of best

practice factors and the extent to which their organization was successful in adopting them. No statistically significant relationships were observed during analysis. Hypothesis five was disconfirmed.

Research question six asks “Does a formal information security education and awareness program result in a reduction of security breaches in terms of severity and frequency?” Hypothesis six predicted that organizations with an information security awareness program would experience fewer security breaches or that the breaches that did occur would be less severe than organizations without security awareness programs. Respondents were asked “Does your institution have a formal and documented security awareness program (i.e. implemented with policies and procedures)?” There were no statistically significant relationships observed between the dependent and independent variables associated with the hypothesis. Hypothesis six was disconfirmed.

Research question seven asks “Does an organization that has a wider mandatory scope of coverage for its information security awareness program have fewer and/or less severe security breaches?” This researcher formulated Hypothesis seven, which predicted that organizations that had wider mandatory coverage of information security awareness programs would have fewer and/or less severe security breaches. Respondents were asked to answer the question “Security awareness training is mandatory for which of the following?” The question was a multiple select question that had faculty, student, staff, and contractors as possible selections. There were no observed statistically significant relationships between the awareness coverage score and either the frequency or severity of breaches. Hypothesis seven was disconfirmed.

Research question eight asked “Does the existence of documented consequences for policy violations result in a reduction of security breaches in terms of severity or frequency?” This researcher formulated hypothesis eight, which predicted that organizations with documented consequences for policy violations would have fewer and/or less severe security breaches. Respondents were asked the question “Does your organization have documented consequences for failure to comply with its information security policy?” There were no statistically significant relationships observed between the incidence or severity of breaches and the adoption of documented consequences for policy violations. Hypothesis eight was disconfirmed.

Research question nine asks “Do organizations with greater levels of enforcement consistency experience fewer and/or less severe security breaches?” This researcher advanced Hypothesis nine, which predicted that organizations with greater levels of enforcement consistency would experience fewer and/or less severe security breaches. Respondents were asked to use a Likert scale to indicate the strength to which they agreed or disagreed with the statement “Information security policy is consistently enforced for the organization (i.e. sanctions are applied consistently for faculty, staff, and students).” There were no statistically significant relationships indicated between the variables. Hypothesis nine was disconfirmed.

Discussion of Results

This dissertation adds additional empirical evidence to the body of knowledge regarding the effectiveness of information security policies, policy enforcement, and awareness efforts. The results indicated that there were no statically significant

relationships between the three types of controls and breaches. Doherty and Fulford (2005) described some potential reasons for the lack of relationships in regards to information security policies. Those researchers pointed to difficulties in raising awareness, enforcement difficulties, inadequate resourcing, failure to tailor policies, and policy complexity as potential clues for why policies did not impact breaches. They did not address awareness and enforcement efforts as those concepts were not within the scope of their research.

Potential reasons why information security awareness and enforcement efforts do not appear to impact breaches are available in the literature. These reasons might include failure to base awareness training on appropriate behavioral theories, reliance on lecture based study, and lack of technical controls to aid in enforcement. Perhaps security program modifications that incorporate these aspects could increase the effectiveness of policies, awareness, and enforcement efforts.

Failure to base awareness training on appropriate behavioral theories could lead to ineffective awareness training. If the training is not effective in changing behavior due to inappropriate content, breaches will not be reduced. Human beings do not function like machines with predictable patterns when presented with standard information (Ashenden, 2008). There are studies that attempt to increase knowledge of the rationales behind complaint and non-compliant behaviors. Compliance research that studies these behaviors is based on the premise that human beings are complicated (Kolkowska & Dhillon, 2013). Security awareness programs should be based on appropriate behavior modification theories.

Kahn, et al (2011) suggested that many information security awareness programs are based on interactions that stem from the knowledge-attitude-behavior (KAB) model. However, there are other models like theory of reasoned action (TRA) and theory of planned behavior (TPB) that can also impact the behaviors of learners (Khan, Alghathbar, Nabi, & Khan, 2011). Additionally, Kolkowska and Dhillon (2013) asserted that not only was an understanding of security concepts and values needed, but that organizational power dynamics must also be understood by leaders and employees for awareness and compliance to be successful. Ifinedo (2013) suggested a combination of TPB and the protection motivation theory (PMT) might effectively increase the success of awareness and compliance efforts. Research is needed to study the effectiveness of awareness methods and the underlying theories on which these approaches are based.

The questions of this dissertation that centered on awareness delivery were focused on lecture based approaches. However, active learning in the form of case studies, and labs may be more effective. Case studies provide a more interactive learning opportunity where a student participates in the discussion to reinforce the concepts of the lesson. Students are more likely to retain information when the exploration of a topic is performed in conjunction with active learning techniques (Ayyagari & Tyks, 2012). Group discussions were found to be the most effective means for changing behaviors in one 2011 study. The discussions were more effective than email, newsletters, posters, lectures, and other methods (Khan et al., 2011).

Lack of technical controls may play a role in the ineffectiveness of the controls studied by this dissertation. Unlike policies and awareness efforts which are management and operational controls, technical controls deal with technologies like firewalls,

biometrics, encryption, and others (Breier & Hudec, 2013). This dissertation did not delve into the technical controls deployed by colleges and universities in support of policies, awareness, and enforcement efforts. Technical controls are interwoven into information security programs. Human and organizational factors can affect their use, but they are important nonetheless (Kraemer et al., 2009). Perhaps, higher education institutions do not deploy technical controls effectively and this leads to reduced effectiveness of the management and technical controls this dissertation studied.

Strengths

This research analyzed the relationship between information security policies, security awareness training, and information security policy enforcement and the frequency and severity of information security breaches. There were no statistically significant relationships indicated by the analysis performed by this research. The research corroborated the findings from Doherty and Fulford (2005) in U.S. higher education institutions. In addition to validating the research questions posed by Doherty and Fulford this research also extends four questions extracted from the literature. The new questions focused on aspects of information security awareness and information security policy enforcement.

This research provides information on how institutions of higher education implement, disseminate, and enforce their information security policies. The results of the survey responses are also presented in categorical form sorted by Carnegie Foundation categories in Appendix G. Organizations can be ranked according to category for comparison purposes. Interested parties can use the results of the survey to benchmark organizations

against peer institutions. Categories such as enrollment, funding source, region, Carnegie Classification, and size and setting were used to present information in the dissertation. This data also served to describe the respondent pool without needing to publish the names of the institutions.

Limitations

One of the limitations of this survey was its relatively low response rate. Information security surveys are plagued with low response rates (Kotulic & Clark, 2004). This survey achieved a response rate of 7.22%. A total of 106 completed and qualified surveys were received from the sample population. This low response rate allowed for the possibility of substantially different responses from the organizations that did not respond to the survey (Sheehan, 2001). Organizations may have elected not to participate due to having high incidences of breaches or not having information security policies. Some organizations without appropriate security policies or security controls may have chosen not to respond to the survey for fear of publishing their lack of controls. Conversely, organizations that believed their security policies and controls to be adequate may have chosen to respond in greater quantities than those without adequate controls.

Dillman et al (2009) suggests that surveys can obtain higher responses rates by gaining the support of a known sponsor. The original intent of this research was to survey EDUCAUSE member institutions. EDUCAUSE is a nonprofit association that describes its mission as the advancement of higher education by promoting the intelligent use of information technology. The member organizations are comprised of more than 2,200 universities, colleges, and other education focused entities. EDUCAUSE declined to

participate in the study citing a full research agenda for the year and potential survey fatigue for its members and the EDUCAUSE Center for Applied Research (ECAR). This is important as survey fatigue could be significant to the low rate of survey response received by this and similar security based surveys. Additionally, the lack of a survey sponsor could have contributed to the low response rates (Dillman et al., 2009). This being said, the survey did obtain a similar response to the Doherty and Fulford (2005) and Heikkila (2009) efforts.

Additional limitations dealt with the formation of the dependent variable of incidence of breaches from the original study. Doherty and Fulford did not request responses that would yield a precise number for the incidence of breaches. The questions used in the original research gave respondents the choice between eight categories of breaches. The questions also captured the incidences of breaches as four ranges. The ranges were 0, 1-5, 6-10, and greater than 10. The last category, of greater than 10 does not allow for fine measurement of a number of breaches that exceeds 10 breaches. The way the question was asked had a potential for masking relevant information. Additionally, since the responses are within ranges, they do not allow for the calculation of an actual mean or standard deviation for the number of incidents. The incidence variable was however continuous which allowed for its use in correlations.

Additionally, rather than executing eight different tests, one for each category of breach types, this dissertation utilized one test for the sum of breach incidences for each hypothesis. This method avoids the need for statistical correction methods such as Bonferroni corrections or others. In essence, a total score is derived by adding the incidences from each of the eight categories. There is a potential here for respondents

having the same score that represents divergent numbers due to the differences in the ranges. For instance, one respondent may have had more instances of malware related breaches, but fewer instances of theft of resources, while still others may have fewer instances of other types of breaches and still have the same final score. This method does however allow for the measurement of the change in the number of breaches. As the variable increases or decreases, so too does the incidence of breaches increase or decrease respectively. Additionally, tests for normality indicated the distributions were acceptable for testing.

Table 36. Descriptive Statistics for Incidence and Severity

	N	Minimum	Maximum	Mean	Std. Deviation
Incidence	106	8	40	16.17	6.556
Severity	106	8	48	21.95	12.323

Table 37. Skewness and Kurtosis for Incidence and Severity

	N	Skewness		Kurtosis	
		Statistic	Std. Error	Statistic	Std. Error
Incidence	106	1.421	.235	2.466	.465
Severity	106	.707	.235	-.720	.465

Table 36 and 37 demonstrate that the assumption of normality is met for both dependent variables. In the case of the incidence variable, the kurtosis is high, but it is still acceptable. This is consistent with the use of ranges instead of actual numbers when requesting incidence responses. At any rate, the resulted responses met the condition for analysis.

Implications

This work has expanded the amount of empirical data available regarding information security policies. The work also highlights organizational practices for information security awareness. Finally this research adds to the body of knowledge in regards to the enforcement of information security policies. The advances contain potential implications for future research as well as future professional practices.

Information security policies are widely believed to be important aspects of an effective information security program (Höne & Eloff, 2002b). According to the findings of this dissertation, polices are widely used in higher education. Approximately 92.5% of responding organizations claim to have a formal information security policy. Even with the high utilization of policies, information security breaches still occur at higher education institutions (Ayyagari & Tyks, 2012). Additionally, this research found no statistically significant relationships between many aspects of policy implementation and maintenance and the severity or frequency of breaches. Perhaps the existence of policy is not enough to sufficiently curtail breaches. Additional studies should be performed to better understand how breaches can be reduced. Organizations may choose to augment their policies with additional technical, physical, and administrative controls.

This research found that there were no statistically significant relationships between the existence of information security awareness programs and the frequency or impact of information security breaches. This being said, there were some interesting data points observed. First, only about 55% of responding institutions reported having a formal information security awareness program. Many institutions (44%) required information security awareness training only once for their members. Slightly more than half of the

responding institutions (53%) required training on an at least biennial basis. This data implies there is room for additional coverage of formal information security awareness programs and potentially a requirement to attempt alternative training methods to achieve a reduction of the occurrences and impact of security breaches.

This research advances the body of knowledge in regards to the consistent enforcement of information security policies. Even though no statistically significant relationships were indicated between the enforcement of information security policies, some interesting observations were made. First, only 66% percent of responding institutions indicated having documented consequences for violations of policy. Also, only 62% percent of responding institutions' responses ranged from neutral to strongly agree that their organization consistently enforced its policies. Additionally, 38% percent of responding agencies were within the "disagree to strongly disagree" response columns in regards to making users aware of enforcement activities. Here, as well as, with awareness efforts, there is room for higher education organizations to elevate enforcement activities. Different approaches based on behavioral theories may also be required.

Recommendations

A study of the impact of information security policies could be conducted in health care organizations, military units, retail businesses, or other forms of industry. Doherty and Fulford (2005) concluded with a call for additional research on the effectiveness of the information security policy in reducing the occurrence and severity of security breach on organizations. The paper characterized the need for follow-up studies in this vein as

urgent. Other studies call for additional research regarding the effectiveness of the information security policy on improving the security of an organization. Goel and Chengular-Smith (2010) discussed the need for more empirical research on the effectiveness of various forms of security policies. Perhaps, this study could also focus on the incidence of breaches as an actual number instead of as ranges of breaches. This would allow for the fine measurement of the number of breaches reported.

An additional research study could seek to ascertain how information security policies affect the behaviors of employees or as is the case in higher education, faculty, staff, students, and contractors. Bulgurcu, Cavusoglu, and Benbasat (2010) recommended additional research in to the effectiveness of the information security policy in improving security by affecting changes in employee behaviors. The research could attempt to ascertain if there is a correlation between the existence of an organizational information security policy and changes in employee behaviors in regards to increased prevalence of encryption, reduced non-work related internet browsing, or less reported malware infections among others.

Another potential area of study might attempt to characterize the prevalent behavioral theories used as a foundation for higher education information security programs. As discussed earlier, there are various theories and methodologies that can be leveraged to form security awareness programs (Crossler et al., 2013; Ifinedo, 2012; Kolkowska & Dhillon, 2013). It might be novel to attempt to catalogue the forms that are in use in higher education and to attempt to explore how effective the approaches are at instilling compliance within an organization. The study may also attempt to understand if there are formal attempts to base these program on established theories.

Another area of study could focus on what types of technical controls organizations develop and implement to enforce information security policies. For example, a survey could be deployed to attempt to see how encryption policy requirements are met at agencies that have a requirement to encrypt sensitive data. Burdon, Reid and Low (2010) suggested that breach notification laws have resulted in an increase in the implementation of encryption technologies. The survey could also attempt to understand if encryption policies and technologies are being deployed to take advantage of safe harbor provisions.

Summary

This dissertation attempted to address the lack of empirical data regarding the effectiveness of information security policies, information security awareness, and information security policy enforcement on the severity and frequency of information security breaches. Many articles in the literature suggest that the information security policy is an important information security control (Doherty et al., 2009; Doherty & Fulford, 2005; Doherty & Fulford, 2006; Fulford & Doherty, 2003; Höne & Eloff, 2002a, 2002b). Even though much of the literature points to the security policy as very important, few studies offer any empirical data to support the assertion (Doherty et al., 2009; Doherty & Fulford, 2005; Fulford & Doherty, 2003). In regards to empirical research, a 2008 literature review of 1280 information security related papers found that only 8.1% of papers reviewed offered any empirical findings. Of the myriad of topics covered by the review, only nine dealt with security awareness and education (Warkentin & Willison, 2009). This dissertation attempted to provide some empirical data regarding

the impact policies, security awareness, and policy enforcement have on breaches in the higher education arena.

This dissertation studied the impact of information security policies on breaches put forward by Doherty and Fulford (2005), as well as, added new study goals. These new goals sought to highlight the impact of security awareness programs on the frequency and severity of security breaches. Finally, the study attempted to discern if the consistent enforcement of information security policies has an impact on the frequency or severity of security breaches. The nine research questions explored by this dissertation are listed below:

- A. Are higher education institutions that have formal information security policies likely to have less security breach incidents in terms of severity or frequency than those without (Doherty & Fulford, 2005, p. 25)?
- B. Does the age of the information security policy result in a reduction of security breaches in terms of severity or frequency (Doherty & Fulford, 2005, p. 25)?
- C. Does the update frequency of the information security policy result in a reduction of security breaches in terms of severity or frequency (Doherty & Fulford, 2005, p. 26)?
- D. Does having a broad scope of issue coverage in the information security policy result in a reduction of security breaches in terms of severity or frequency (Doherty & Fulford, 2005, p. 26)?
- E. Does the adoption of best practice factors in the information security policy result in a reduction of security breaches in terms of severity or frequency (Doherty & Fulford, 2005, p. 26)?

- F. Does a formal awareness program result in a reduction of security breaches in terms of severity or frequency?
- G. Does an organization that has a wider mandatory scope of coverage for its information security awareness program have fewer and/or less severe security breaches?
- H. Does the existence of documented consequences for policy violations result in a reduction of security breaches in terms of severity and frequency?
- I. Do organizations with greater levels of enforcement consistency experience fewer and/or less severe security breaches?

The data collected for this research effort was captured via an online survey hosted by Qualtrics. The research effort built upon a previously validated survey from Doherty and Fulford (2005). This researcher crafted additional research questions based on the literature. Additional survey questions derived from the four new research questions were subjected to a review, validation, and modification process that included three researchers and one information security professional.

The study targeted senior IT and information security professionals at various colleges and universities. This researcher contacted 1,468 distinct institutions and compiled a total of 106 valid surveys for analysis. This accounted for a responses rate of 7.22%. The web survey was distributed electronically. The web hosting solution allowed for the downloading of data for analysis in various formats. Dr. Rachel MacNair, a statistical consultant, retained for assistance with the statistical computations, executed the statistical test. The results of the computations were used by the author of this dissertation

to determine significance between the dependent and independent variables. The results from nine hypothesis and associated research questions were described. The hypotheses were the result of a mixture of five hypotheses from Doherty and Fulford (2005) and four new hypotheses from this research as culled from the literature.

For the hypotheses that were created by Doherty and Fulford (2005), the hypotheses were tested via correlations and t-tests. This researcher was unable to test Hypothesis one due to a lack of responses by organizations indicating having no information security policies. Therefore, this dissertation was neither able to confirm or deny hypothesis one.

The results of the remaining hypotheses are described below:

- Hypothesis two predicted that organizations that had more mature security policies would have fewer and/or less severe security breaches. The results of the analysis indicated no statistical significant associations between the age of the information security policy and the severity and frequency of information security breaches. Hypothesis two was disconfirmed.
- Hypothesis three predicted that organizations that had frequent information security policy updates would have fewer and/or less severe security breaches. The analysis indicated no statistically significant relationships between update frequency of the information security policy and security breaches in terms of either severity or frequency. Hypothesis three was disconfirmed.
- Hypothesis four predicted that organizations that had information security policies of broad scope have fewer and/or less severe security breaches. Results of the analysis indicated no statistically significant relationships between the scope of information

- security policies and the frequency or severity. Hypothesis four was disconfirmed four.
- Hypothesis five covered the prediction that organizations that had policies based on a wide variety of best practices would have fewer and/or less severe security breaches. There was no indication of statistically significant relationships between the adoption of best practices and either the frequency or severity of breaches. Hypothesis five was disconfirmed.
 - Hypothesis six predicted that organizations with an information security awareness program would experience fewer security breaches or that the breaches that did occur would be less severe than organizations without security awareness programs. Analysis of the results of the statistical computations indicated no statistically significant relationships between the existence of information security awareness programs and the frequency or severity of breaches. Hypothesis six was disconfirmed.
 - Hypothesis seven predicted that organizations that have wider mandatory coverage of information security awareness programs would have fewer and/or less severe security breaches. A correlation test was conducted to analyze the relationship between the variables. The analysis of the statistical results indicated no statistically significant relationships between the scope of awareness program coverage and the severity or frequency of breaches. Hypothesis seven was disconfirmed.
 - Hypothesis eight predicted that organizations with documented consequences for policy violations would have fewer and/or less severe security breaches. Analysis of the tests failed to indicate any statistically significant relationships between the

incidence or severity of breaches and the adoption of documented consequences for policy violations. Hypothesis eight was disconfirmed.

- Hypothesis nine predicted that organizations with greater levels of enforcement consistency would experience fewer and/or less severe security breaches. No statistically significant relationships between the variables under study were indicated. Hypothesis nine was disconfirmed.

This work added to the literature by expanding the amount of empirical data available regarding information security policies. This dissertation also added some illumination on higher education organizational practices for information security awareness. Finally, this research adds to the body of knowledge in regards to the enforcement of information security policies. The advances contain potential implications for future research as well as future professional practices.

Some interesting data points were observed in regards to information security awareness. Primarily, approximately 55% of responding institutions reported having a formal information security awareness program. Approximately 44% of responding organizations required information security awareness training only once during affiliation for their members. Less than half of the responding institutions (47%) required training on an annual basis. One could interpret this data as a call for additional coverage of formal information security awareness programs.

Regarding the enforcement of information security policies, only 62% percent of responding institutions indicated having documented consequences for violations of policy. Also, only 65% percent of responding institution's responses ranged from neutral to disagree that their organization consistently enforced its policies. Additionally, 70%

percent of responding agencies were within the neutral to strongly disagree response column in regards to making users aware of enforcement activities. This suggests there is room to elevate enforcement activities at colleges and universities.

Information security policies are widely believed to be important aspects of an effective information security program (Höne & Eloff, 2002b). According to the findings of this research, policies are heavily used. Roughly, 92.5% of responding organizations indicated using information security policies. As this research found no statistically significant relationships between many aspects of management and operational controls associated with information security policies and awareness, perhaps the existence of policy, policy enforcement efforts, and training are not enough to sufficiently curtail breaches. Additional research is needed to further understand how breaches can be reduced. As a practical application of the results of this dissertation, organizations may choose to augment their policies with additional technical and physical controls.


Appendices

A. IRB Approval



MEMORANDUM

To: Stanie Waddell, M.S.

From: Ana I. Fins, Ph.D.
Chair, Institutional Review Board  Signature

Date: October 26, 2012

Re: A Study of the Effect of Information Security Policies on Informatino Security Breaches in Higher Education Institutions (Protocol No.: Fins 2012-07)

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair (954-262-5369) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

Institutional Review Board
3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-5369 • Fax: (954) 262-3977 • Email: irb@nsu.nova.edu • Web site: www.nova.edu/irb

B. Survey Instrument

TextA.

Overview: The following survey is designed to capture information regarding your institution's use of information security policies, security awareness training, and policy enforcement. The survey will also ask questions pertaining to the frequency and impact of information security breaches your organization has experienced over the past two years. The goal of the study is to attempt to detail the statistical relationship between information security policies and information security breaches in higher education. The study is designed to be answered by someone familiar with your organizations information security program. Please answer the questions to the best of your abilities and remember that only anonymized results will be used in the resulting reports. It is my hope that all of us will be able to benefit from the information that results from this study. This is a relatively short survey of 15 questions. The survey should take less than 15-20 minutes to complete. For the purposes of this study, a breach is the unauthorized access, alteration, or destruction of personally identifiable data that results in a notification of affected individuals. The definitions of the various forms of breaches considered in this study can be found in the table below:

TextB.

Type of Breach	Description of Type of Breach
Computer Malware	Computer software that has the ability to replicate itself on computer systems. Malware that results in the unauthorized access, alteration, or destruction of personally identifiable information.
Hacking incident	Unauthorized electronic access, alteration, or destruction of organizational computers or data by outside parties. This category is typified by compromises that result when software or system vulnerabilities are exploited or security controls are defeated.
Unauthorized access	The deliberate abuse (access, alteration, or destruction) of systems and the data contained therein by individuals that do not have legitimate access to the systems. Excludes hacking. Includes compromises that result from social engineering, phishing, shoulder surfing, and identity management and access control failures.
Theft of resources	Theft of increasingly valuable hardware, software, and information assets. For example, the loss or theft of unencrypted laptops, drives, or backup tapes.
Computer-based fraud	Information systems, especially financial systems, are compromised by individuals who seek to defraud an organization. Individuals use these systems to defraud the organization or its employees, students, or customers. Failure of separation of duties, as well as, unauthorized charges, check runs, and account transfers are examples of this category.
Human error	The misconfiguration, accidental posting, or accidental destruction of data by computer users.
Force Majeure	Damage to computing facilities or data resources caused by phenomena such as earthquakes, floods, or fires.
Damage by employees	Compromises caused by disgruntled employees. These actions are separate and distinct from accidental actions.

Text1. Please answer these brief questions that provide some background about your organization.

QA1. Please enter the institution that you are providing information about. This information is only being used to ensure that there are no duplicate institutions represented in the cumulative results of the study. No institution names will be attributed to any survey responses when the results of the study are finalized.

Note: *These responses are coded as survey identifiers in the data file in order to de-identify the data.*

Text2. Please provide information regarding your organizations use of information security policies.

D1. Carnegie Basic Classification added after the survey was closed (for classification only)

D2. Enrollment Carnegie Basic Classification added after the survey was closed (for classification only)

D3. 2010 Size and Setting added after the survey was closed (for classification only)

D4. Region added after the survey was closed (for classification only)

D5. Carnegie Classification added after the survey was closed (for classification only)

D6. Funding Control added after the survey was closed (for classification only)

Q1. Does your organization have a documented information (IT, Cyber) security policy?

- Yes (1)
- No (2)
- Not Sure (3)

Q2. In years, how long has your organization actively used a document information security policy (If not sure please leave blank)?

Q3. Approximately how often is the policy updated?

- Less frequently than every 2 years (1)
- Every 2 Years (2)
- Every year (3)
- Every 6 months (4)
- More frequently than every 6 months (5)
- Not Sure (6)

Q4. How is the policy disseminated to faculty, staff, and students (Please check all that apply)?

	Faculty (1)	Staff (2)	Students (3)
Electronically (1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Printed Hardcopy (2)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not Sure (3)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q5. Are faculty, staff, and students, required to affirm that they have read, understand, and agree to abide by the policy?

	Yes (1)	No (2)	Not Sure (3)
Faculty (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Staff (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Students (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q6. Using the table below, please indicate the security issues covered in your IT security policy below. If the issues are only covered by policy please choose "Policy Document Only." If there is no policy covering the issue, but standards or procedures exist, please choose "Stand-alone Procedure or Standard Only." If you supplement your policies with procedures or standards please choose "Policy Document and Supplementary Procedure or Standard." If you do not explicitly cover an issue through your policy or a separate standalone standard, please choose "Not documented." If you are not sure please choose "Not Sure."

	Policy Document Only (1)	Stand-alone Procedure or Standard Only (2)	Policy Document and Supplementary Procedure or Standard (3)	Not Sure (4)	Not Documented (5)
Disclosure of Information (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Access Control (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Viruses, Worms, & Trojans (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Software Development (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Contingency Planning (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Encryption (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile Computing (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Personal Usage of IT (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Physical Security (9)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Violations and Breaches (10)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Internet Access (11)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use of Social Media (12)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q7. Using the table below, please indicate the importance of each of the following factors and the extent to which your organization is successful in adopting them.

	How important do you believe the following factors to be for the successful implementation of IT security in your organization on a scale of 1-5 with 1 being the least important and 5 being most important:					How successful do you believe your organization has been in adopting each of these factors on a scale of 1-5 with 1 being the unsuccessful and 5 being very successful:				
	Not Important 1	2	3	4	Very Important 5	Not successful 1	2	3	4	Very Successful 5
Ensuring security policy reflects the organization's business objectives (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<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 your organization's culture (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Visible commitment from management (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A good understanding of security requirements (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Effective marketing of security to all workforce members (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Distribution of guidance on IT security policy to all workforce members (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Comprehensive measurement system for evaluating performance in security management (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provision of feedback system for suggesting policy improvements (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Text4. Please provide some information on how your organization conducts information security awareness.

Q8. Does your institution have a formal and documented security awareness program (i.e. implemented with policies and procedures)?

- Yes (1)
- No (2)
- Not Sure (3)

Q9. Security awareness training is mandatory for which of the following (check all that apply)?

- None (1)
- Faculty (2)
- Staff (3)
- Students (4)
- Contractors (5)
- Not Sure (6)

Logic2. Display Q10. If None Is Selected

Q10. If training is mandatory how often is it required?

- Every 6 Months (1)
- Annually (2)
- Every Two Years (3)
- Only Once (4)
- Not Sure (5)

Q11. When Information security awareness training is presented, how is it delivered? (Please check all that apply)

- Web based (1)
- Email based (2)
- Paper handouts or mailers (3)
- Videos (4)
- Facilitated during in person presentations (5)
- Not Sure (6)

Text 4. Please provide information about how your organization enforces information security policies.

Q12. Does your Organization have documented consequences for failure to comply with its information security policy?

- Yes (1)
- No (2)
- Not Sure (3)

Q13. Please use the following Likert scale to indicate the strength to which you agree or disagree with each of the following two statements:

	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
Information Security Policy is consistently enforced for the organization (i.e. sanctions are applied consistently for faculty, staff, and students) (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Workforce members are made aware of enforcement activities (including employee sanction)? (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Compliance efforts (audits, reviews, logging, etc...) are visible to the workforce? (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Text4. Please provide some information regarding the frequency and severity of information security breaches experienced by your organization.

Q14. Please record in the table below the approximate number of IT security breaches that your organization has experienced in the past two years, and indicate the severity of the worst breach of each type, using the scale provided. For clarification please see the definitions of each type of breach location in the table below. For the purposes of this study breaches can affect confidentiality, integrity, and/or availability of data. Breaches should only be counted when they result in the notification of affected individuals under a breach notification or privacy and security law. Examples of such laws include: HIPAA, GLBA, the various state identity theft protection and breach notification laws, and others.

Type of Breach	Description of Type of Breach
Computer Malware	Computer software that has the ability to replicate itself on computer systems. Malware that results in the unauthorized access, alteration, or destruction of personally identifiable information.
Hacking incident	Unauthorized electronic access, alteration, or destruction of organizational computers or data by outside parties. This category is typified by compromises that result when software or system vulnerabilities are exploited or security controls are defeated.
Unauthorized access	The deliberate abuse (access, alteration, or destruction) of systems and the data contained therein by individuals that do not have legitimate access to the systems. Excludes hacking. Includes compromises that result from social engineering, phishing, and shoulder surfing and identity management and access control failures.
Theft of resources	Theft of valuable hardware, software, and information assets. For example, the loss or theft of unencrypted laptops, drives, or backup tapes.
Computer-based fraud	Information systems, especially financial systems, are compromised by individuals who seek to defraud an organization. Individuals use these systems to defraud the organization or its employees, students, or customers. Failure of separation of duties, as well as, unauthorized charges, check runs, and account transfers are examples of this category.
Human error	The misconfiguration, accidental posting, or accidental destruction of data by computer users.
Force Majeure	Damage to computing facilities or data resources caused by phenomena such as earthquakes, floods, or fires.
Damage by employees	Compromises caused by disgruntled employees. These actions are separate and distinct from accidental actions.

	Incidence of Breaches					Severity of Worst Breach						Approximate Number of Affected Individuals in the Most Severe Breach from Each Category
	0	1-5	6-10	>10	Not Sure	Fairly Insignificant 1	2	3	4	Highly Significant 5	Not Sure	
Computer Malware (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Quantity of Affected Records
Hacking Incident (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Unauthorized Access (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Theft of Resources (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Computer Based Fraud (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Human Error (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Force Majeure (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Intentional Damage by Employees (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Q15. How would you classify the level of centralization of IT resources at your university (On a scale of 0-10 with 5 being equally distributed between central IT and departmental IT)?

	Totally Decentralized 1	2	3	4	Equally Distributed 5	6	7 (8)	8 (9)	9 (10)	Totally Centralized 10
Centralization of IT (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

C. Permission to use Carnegie Classification Data

To: publications@carnegiefoundation.org

Dear Carnegie Foundation Representative,

I am a PhD candidate at Nova Southeastern University. I am completing a dissertation in information systems as part of my PhD requirements. I would like to use a subset of foundation classification data from 2011 as part of the breakdown for my survey data. I would like to use the following fields:

- Basic Classification
- Size and Setting Classification
- Geographic Region
- Control of Institution
- Enrollment

The data will be used to categorize approximately 120 US Universities that responded to a survey on information security in higher education institutions. I will make proper attribution to the Carnegie Foundation for the data that is used. Please respond to this email with a determination on my use of the data. Thank you in advance.

-Stan Waddell, ABD
Nova Southeastern University

To: [Stanie Waddell](#)

You have our permission to use the data. Good luck on your dissertation.

All the best,
Gay Clyburn

*Gay M. Clyburn
Associate Vice President, Public Affairs and Continuing Programs
Secretary to the Board of Trustees
Carnegie Foundation for the Advancement of Teaching
(office) 650 566-5162
(cell) 650 333-6974
www.carnegiefoundation.org*

D. Permission to Reprint Tables from Doherty and Fulford (2005)

Wednesday, May 15, 2013 1:39 PM
Jan Travers [jtravers@igi-global.com]

To: Stanie Waddell

Dear Stan, it won't be a problem to grant this permission for your thesis purposes, however we have to know which tables you wish to use and you will be required to label them with the IGI Global source of publication and include the wording, "Reprinted by permission of the publisher"

Jan Travers

(Ms) Jan Travers
Director of Intellectual Property and Contracts
IGI Global - Disseminator of Knowledge Since 1988
701 E Chocolate Avenue
Hershey Pennsylvania 17033-1240, USA
Tel: 717.533-8845 x112; Fax: 717.533-8661
E-mail: jtravers@igi-global.com
www.igi-global.com

Friday, May 17, 2013 1:39 PM
Jan Travers [jtravers@igi-global.com]

To: Stanie Waddell

You replied on 5/17/2013 6:24 PM.
Thanks Stanie, I'll record this in our copyright records. Good luck with your thesis.

Jan

(Ms) Jan Travers
Director of Intellectual Property and Contracts
IGI Global - Disseminator of Knowledge Since 1988
701 E Chocolate Avenue
Hershey Pennsylvania 17033-1240, USA
Tel: 717.533-8845 x112; Fax: 717.533-8661
E-mail: jtravers@igi-global.com
www.igi-global.com

E. Findings tables from Doherty and Fulford (2005)

Table 2. The incidence and severity of security breaches

Type of Breach	Incidence of Breaches				Severity of Worst Breach					
	Approximate number of breaches in last two years				Fairly Insignificant		Highly Significant		Mean value	
	0	1-5	6-10	> 10	1	2	3	4	5	
Computer virus	6	111	23	77	45	65	47	35	19	2.59
Hacking incident	142	66	1	5	42	21	10	5	4	1.92
Unauthorized access	106	83	13	10	32	42	21	5	7	2.23
Theft of resources	50	123	24	19	43	52	48	20	8	2.38
Computer-based fraud	187	23	0	2	15	10	3	6	2	2.15
Human error	41	85	19	65	32	61	43	23	10	2.48
Natural disaster	160	54	2	1	16	24	9	11	5	2.52
Damage by employees	185	28	0	0	20	8	7	2	2	1.82

Reprinted by permission of the publisher (see Appendix D.) from *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 29, by N.F. Doherty and H. Fulford.

Table 3. The relationship between the adoption of InSPy and the incidence and severity of security breaches

Type of Breach	Incidence of Breaches (Chi-Squared Analysis)			Severity of Worst Breach (One-Way ANOVA)			
	Pearson Value	Deg. of Freedom	Two-Sided Prob.	Yes	No	F Ratio	F Prob.
Computer virus	0.730	3	0.878	2.59	2.69	0.215	0.644
Hacking incident	5.733	3	0.111	1.92	1.72	0.422	0.518
Unauthorized access	3.090	3	0.378	2.23	2.00	0.730	0.395
Theft of resources	1.905	3	0.607	2.38	2.51	0.429	0.513
Computer-based fraud	1.892	2	0.300	2.15	2.25	0.036	0.851
Human error	5.388	3	0.144	2.48	2.67	0.743	0.390
Natural disaster	6.469	3	0.089	2.52	2.32	0.361	0.550
Damage by employees	0.003	1	1.000	1.82	2.30	1.210	0.279

Note: A chi-squared test was used to test the association between the four categories of incidence (0, 1-5, 6-10, >10) and the two classes of InSPy existence (yes, no), while ANOVA was used to compare the mean severity of breaches and the two classes of InSPy existence.

Reprinted by permission of the publisher (see Appendix D.) from *Information Resources Management Journal* article, "Do Information Security Policies Reduce the

Incidence of Security Breaches: An Exploratory Analysis," p. 31, by N.F. Doherty and H. Fulford.

Table 4. Relationship between the age of the InSPy and the incidence/severity of security breaches

Type of Breach	Incidence of Breaches (One-Way ANOVA)						Severity of Worst Breach (Correlation)	
	0	1-5	6-10	>10	F Ratio	F Prob.	Pearson Value	Two-Sided Significance
Computer virus	2.0	3.7	3.0	5.1	2.3	.08	-0.05	0.501
Hacking incident	3.7	4.7	5.0	5.0	.77	.51	-0.05	0.718
Unauthorized access	3.5	3.9	4.5	10.1	6.4	.00**	-0.08	0.443
Theft of resources	4.1	3.7	3.4	7.27	3.7	.01*	-0.20	0.025*
Computer-based fraud	3.9	6.14	-	3.00	2.8	.07	-0.13	0.513
Human error	3.9	3.5	3.7	4.9	1.2	.31	-0.00	0.963
Natural disaster	4.1	3.8	2.8	-	.23	.80	-0.15	0.335
Damage by employees	7.8	8.9	-	-	2.9	.09	-0.19	0.332

*Note: * Result significant at the 5% level; ** Result significant at the 1% level*

Reprinted by permission of the publisher (see Appendix D.) from *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 31, by N.F. Doherty and H. Fulford.

Table 5. Relationship between the frequency of updating InSPy and the incidence/severity of security breaches

Type of Breach	Incidence of Breaches (Chi-Squared Analysis)			Severity of Worst Breach (One-Way ANOVA)			
	Pearson Value	Degree of Freedom	Two- Sided Prob.	< Once a Year	≥Once a Year	F Ratio	F Prob.
Computer virus	3.157	3	0.368	2.42	2.75	2.71	0.101
Hacking incident	1.679	3	0.642	2.00	1.92	0.065	0.799
Unauthorized access	3.108	3	0.375	2.21	2.25	0.030	0.864
Theft of resources	2.219	3	0.528	2.35	2.42	0.117	0.733
Computer-based fraud	1.098	2	0.577	2.08	2.20	0.052	0.821
Human error	5.253	3	0.154	2.67	2.42	1.467	0.228
Natural disaster	3.237	2	0.198	2.29	2.72	1.450	0.235
Damage by employees	1.198	1	0.274	1.73	1.87	0.087	0.770

Reprinted by permission of the publisher (see Appendix D.) from *Information Resources Management Journal* article, "Do Information Security Policies Reduce the

Incidence of Security Breaches: An Exploratory Analysis," p. 32, by N.F. Doherty and H. Fulford.

Table 6. Relationship between the range of issues covered by the InSPy and the incidence/severity of security breaches

Type of Breach	Incidence of Breaches (One-Way ANOVA)						Severity of Worst Breach (Correlation)	
	0	1-5	6-10	>10	F Ratio	F Prob.	Pearson Value	Two-Sided Significance
Computer virus	8.0	7.8	7.6	8.4	.79	.49	0.05	0.530
Hacking incident	8.0	7.9	10.0	6.5	.41	.75	-0.04	0.779
Unauthorized access	7.9	8.0	7.9	9.4	.86	.46	0.15	0.169
Theft of resources	7.4	8.0	8.2	9.3	2.4	.10	-0.05	0.536
Computer-based fraud	7.8	9.3	-	5.00	3.4	.04*	0.31	0.122
Human error	8.1	7.9	7.8	8.2	.29	.88	0.02	0.838
Natural disaster	7.9	8.5	3.5	-	3.8	.02*	0.24	0.105
Damage by employees	7.8	8.9	-	-	2.9	.09	0.08	0.678

Note: Result significant at the 5% level

Reprinted by permission of the publisher (see Appendix D.) from *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 32, by N.F. Doherty and H. Fulford.

Table 7. One-way ANOVA between the successful adoption of success factors and the incidence/severity of security breaches

Type of Breach	Incidence of Breaches (One-Way ANOVA)						Severity of Worst Breach (Correlation)	
	0	1-5	6-10	>10	F Ratio	F Prob.	Pearson Value	Two-Sided Significance
Computer virus	3.17	2.95	2.85	2.85	0.42	0.74	0.031	0.699
Hacking incident	2.94	2.93	2.50	1.55	3.05	0.03*	0.120	0.365
Unauthorized access	2.99	2.82	2.76	2.75	1.01	0.39	-0.070	0.529
Theft of resources	2.87	2.89	3.01	2.91	0.40	0.75	-0.149	0.097
Computer-based fraud	2.89	2.87	-	2.40	0.27	0.76	0.305	0.138
Human error	2.98	2.87	3.12	2.81	0.99	0.39	-0.189	0.035*
Natural disaster	2.92	2.82	3.20	-	0.50	0.60	0.171	0.255
Damage by employees	2.91	2.86	-	-	0.09	0.76	-0.088	0.655

*Note: * Result significant at the 5% level*

Reprinted by permission of the publisher (see Appendix D.) from *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 33, by N.F. Doherty and H. Fulford.

F. Initial Survey Solicitation Notice

Dear <first name>,

Ever wished there was more research available regarding information security in higher education? Well, here is your chance to help add to the body of knowledge. I am conducting a survey of information security in academic institutions to provide information regarding the **impact of information security policies on computer security breaches** at America's colleges and universities. This survey is part of my doctoral program at the School of Computer and Information Sciences at Nova Southeastern University.

- This short survey will require approximately 15 minutes of your time. Participation is voluntary. You may choose not to participate or to stop at any time. This study **will collect no data that can identify you directly or indirectly like IP addresses. Only cumulative and anonymized data will be published** as part of the survey results. A summary report of the findings of this survey will be sent to each institution that completes the survey. The results should help illustrate many aspects of information security in academic institutions

Participating in the study:

To complete the study on-line, simply click on the link provided below and complete the survey.

By clicking on the link below and answering the survey questions, you are agreeing to participate in the study entitled, "A Study of the Effect of Information Security Policies on Information Security Breaches in Higher Education Institutions".

[Click Here to Take the Survey](#)

Or copy and paste the URL below into your internet browser:

https://survey.us2.qualtrics.com/WRQualtricsSurveyEngine/?Q_SS=cvvgYKYDIZr6zd3_0MtIdnVWDUgOryJ&_1

This short survey is divided into five sections. Most of the questions can be answered by simply clicking on the appropriate box.

Qualtrics, a secure survey hosting company located in Provo, Utah is hosting this survey. Qualtrics has SAS 70 Certification and meets federally regulated privacy standards.

This survey may be best completed by a member of your information security function. If you determine that another professional in your institution is better suited to participate in the study, please forward this email or contact me directly.

If you have any queries, please email me at [stanie at nova dot edu](mailto:stanie@nova.edu), or call me at 919-883-1900. Please leave a message and I will return your call. For questions/concerns about your rights as a research participant, contact:

Human Research Oversight Board (Institutional Review Board or IRB)

Nova Southeastern University

(954) 262-5369/Toll Free: 866-499-0790

IRB@nsu.nova.edu

Sincerely,

Stan Waddell, PMP, CISSP, C|CISO ABD Nova Southeastern University

A CISO in higher education for more than 7 years

G. Expanded Exploratory Questions Tables

Responses to the Question “Does an information security awareness program exist?” (by Carnegie Classification)

Carnegie Classification	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Associate's Colleges	1	1%	0	0%	0	0%
Baccalaureate Colleges—General	3	3%	6	6%	0	0%
Baccalaureate Colleges—Liberal Arts	2	2%	4	4%	0	0%
Baccalaureate/Associate's Colleges	3	3%	2	2%	1	1%
Doctoral/Research Universities— Extensive	20	19%	9	8%	0	0%
Doctoral/Research Universities— Intensive	6	6%	5	5%	1	1%
Master's Colleges and Universities I	17	16%	13	12%	0	0%
Master's Colleges and Universities II	0	0%	1	1%	0	0%
Specialized Institutions—Medical schools and medical centers	2	2%	0	0%	0	0%
Specialized Institutions—Other separate health profession schools	1	1%	1	1%	0	0%
Specialized Institutions—Schools of art, music, and design	0	0%	1	1%	0	0%
Specialized Institutions—Schools of business and management	1	1%	1	1%	0	0%
Specialized Institutions—Schools of engineering and technology	0	0%	1	1%	0	0%
Specialized Institutions—Teachers colleges	0	0%	1	1%	0	0%
Specialized Institutions—Theological seminaries and other specialized faith- related institutions	2	2%	1	1%	0	0%
Total	58	55%	46	43%	2	2%

Responses to the Question “Does an information security awareness program exist?” (by Funding Source)

Funding Source	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Public	37	35%	24	23%	0	0%
Private not-for-profit	21	20%	21	20%	1	1%
Private for-profit	0	0%	1	1%	1	1%
Total	58	55%	46	43%	2	2%

Responses to the Question “Does an information security awareness program exist?” (by Student Enrollment)

Enrollment	Yes		No		Not Sure	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Less than 1000	4	4%	7	7%	1	2%
1000-2999	9	8%	5	5%	1	2%
3000-9999	13	12%	11	10%	0	0%
10000-19999	15	14%	12	11%	0	0%
20000-29999	5	5%	9	8%	0	0%
greater than 30000	12	11%	2	2%	0	0%
Total	58	55%	46	43%	2	2%

Responses to the Question “Does an information security awareness program exist?” (by Region)

Region	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Far West AK CA HI NV OR WA	6	6%	5	5%	0	0%
Great Lakes IL IN MI OH WI	8	8%	8	8%	0	0%
Mid East DE DC MD NJ NY PA	6	6%	2	2%	1	1%
New England CT ME MA NH RI VT	5	5%	2	2%	0	0%
Outlying areas AS FM GU MH MP PR PW VI	0	0%	1	1%	1	1%
Plains IA KS MN MO NE ND SD	5	5%	8	8%	0	0%
Rocky Mountains CO ID MT UT WY	0	0%	4	4%	0	0%
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	19	18%	12	11%	0	0%
Southwest AZ NM OK TX	9	8%	4	4%	0	0%
Total	58	55%	46	43%	2	2%

Responses for the Question “How often is awareness training required?” (by Carnegie Classification)

Carnegie Classification	Every 6 Months		Annually		Every Two Years		Only Once		Not Sure	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Associate's Colleges	0	0%	1	2%	0	0%	0	0%	0	0%
Baccalaureate Colleges—General	0	0%	2	3%	0	0%	2	3%	0	0%
Baccalaureate Colleges—Liberal Arts	0	0%	1	2%	0	0%	1	2%	1	2%
Baccalaureate/Associate's Colleges	0	0%	2	3%	0	0%	2	3%	1	2%
Doctoral/Research Universities—Extensive	0	0%	9	15%	2	3%	5	8%	0	0%
Doctoral/Research Universities—Intensive	0	0%	3	5%	0	0%	3	5%	0	0%
Master's Colleges and Universities I	0	0%	5	8%	2	3%	10	17%	0	0%
Master's Colleges and Universities II	0	0%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Medical schools and medical centers	0	0%	2	3%	0	0%	0	0%	0	0%
Specialized Institutions—Other separate health profession schools	0	0%	0	0%	0	0%	2	3%	0	0%
Specialized Institutions—Schools of art, music, and design	0	0%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Schools of business and management	0	0%	1	2%	0	0%	0	0%	0	0%
Specialized Institutions—Schools of engineering and technology	0	0%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Teachers colleges	0	0%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Theological seminaries and other specialized faith-related institutions	0	0%	1	2%	0	0%	1	2%	0	0%
Total	0	0%	27	46%	4	7%	26	44%	2	3%

Responses for the Question “How often is awareness training required?” (by Funding Source)

Funding Source	Every 6 Months		Annually		Every Two Years		Only Once		Not Sure	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Public	0	0%	17	29%	4	7%	17	29%	1	2%
Private not-for-profit	0	0%	10	17%	0	0%	9	15%	0	0%
Private for-profit	0	0%	0	0%	0	0%	0	0%	1	2%
Total	0	0%	27	46%	4	7%	26	44%	2	3%

Responses for the question “How often is awareness training required?” (by Student Enrollment)

Enrollment	Every 6 Months		Annually		Every Two Years		Only Once		Not Sure	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Less than 1000	0	0%	2	3%	0	0%	3	5%	0	0%
1000-2999	0	0%	5	8%	0	0%	3	5%	2	3%
3000-9999	0	0%	4	7%	1	2%	7	12%	0	0%
10000-19999	0	0%	6	10%	0	0%	7	12%	0	0%
20000-29999	0	0%	4	7%	2	3%	3	5%	0	0%
greater than 30000	0	0%	6	10%	1	2%	3	5%	0	0%
Total	0	0%	27	46%	4	7%	26	44%	2	3%

Responses for the Question “How often is awareness training required?” (by Region)

Region	Every 6 Months		Annually		Every Two Years		Only Once		Not Sure	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Far West AK CA HI NV OR WA	0	0%	1	2%	0	0%	4	7%	0	0%
Great Lakes IL IN MI OH WI	0	0%	4	7%	0	0%	4	7%	0	0%
Mid East DE DC MD NJ NY PA	0	0%	0	0%	0	0%	2	3%	0	0%
New England CT ME MA NH RI VT	0	0%	3	5%	0	0%	2	3%	0	0%
Outlying areas AS FM GU MH MP PR PW VI	0	0%	0	0%	0	0%	0	0%	1	2%
Plains IA KS MN MO NE ND SD	0	0%	3	5%	0	0%	1	2%	1	2%
Rocky Mountains CO ID MT UT WY	0	0%	0	0%	0	0%	2	3%	0	0%
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	0	0%	10	17%	2	3%	9	15%	0	0%
Southwest AZ NM OK TX	0	0%	6	10%	2	3%	2	3%	0	0%
Total	0	0%	27	46%	4	7%	26	44%	2	3%

Responses to the Question “How is information security awareness training delivered?” (by Carnegie Classification)

Carnegie Classification	Web Based		Email Based		Paper handouts or mailers		Videos		Facilitated during in person presentations		Not Sure	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Associate's Colleges	1	1%	0	0%	0	0%	1	1%	0	0%	0	0%
Baccalaureate Colleges—General	1	1%	1	1%	1	1%	2	2%	6	6%	2	2%
Baccalaureate Colleges—Liberal Arts	2	2%	3	3%	0	0%	1	1%	2	2%	1	1%
Baccalaureate/Associate's Colleges	4	4%	2	2%	1	1%	1	1%	4	4%	2	2%
Doctoral/Research Universities—Extensive	28	26%	9	8%	8	8%	14	13%	19	18%	0	0%
Doctoral/Research Universities—Intensive	10	9%	4	4%	3	3%	3	3%	8	8%	0	0%
Master's Colleges and Universities I	21	20%	11	10%	12	11%	9	8%	19	18%	2	2%
Master's Colleges and Universities II	0	0%	0	0%	0	0%	0	0%	0	0%	1	1%
Specialized Institutions—Medical schools and medical centers	2	2%	0	0%	0	0%	0	0%	1	1%	0	0%
Specialized Institutions—Other separate health profession schools	2	2%	0	0%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Schools of art, music, and design	0	0%	1	1%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Schools of business and management	1	1%	0	0%	1	1%	0	0%	2	2%	0	0%
Specialized Institutions—Schools of engineering and technology	1	1%	0	0%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Teachers colleges	0	0%	0	0%	0	0%	0	0%	0	0%	1	1%
Specialized Institutions—Theological seminaries and other specialized faith-related institutions	1	1%	1	1%	0	0%	0	0%	3	3%	0	0%
Total	74	70%	32	30%	26	25%	31	29%	64	60%	9	8%

Responses to the Question “How is information security awareness training delivered?” (by Funding Source)

Funding Source	Web Based		Email Based		Paper handouts or mailers		Videos		Facilitated during in person presentations		Not Sure	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Public	50	47%	18	17%	18	17%	21	20%	35	33%	2	2%
Private not-for-profit	24	23%	14	13%	8	8%	10	9%	29	27%	5	5%
Private for-profit	0	0%	0	0%	0	0%	0	0%	0	0%	2	2%
Total	74	70%	32	30%	26	25%	31	29%	64	60%	9	8%

Responses to the Question “How is information security awareness training delivered?” (by Student Enrollment)

Enrollment	Web Based		Email Based		Paper handouts or mailers		Videos		Facilitated during in person presentations		Not Sure	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Less than 1000	6	6%	4	4%	0	0%	0	0%	5	5%	3	3%
1000-2999	6	6%	2	2%	2	2%	4	4%	7	7%	3	3%
3000-9999	15	14%	9	8%	9	8%	6	6%	18	17%	1	1%
10000-19999	22	21%	9	8%	6	6%	11	10%	21	20%	2	2%
20000-29999	11	10%	5	5%	6	6%	4	4%	8	8%	0	0%
greater than 30000	14	13%	3	3%	3	3%	6	6%	5	5%	0	0%
Total	74	70%	32	30%	26	25%	31	29%	64	60%	9	8%

Responses to the Question “How is information security awareness training delivered?” (by Region)

Region	Web Based		Email Based		Paper handouts or mailers		Videos		Facilitated during in person presentations		Not Sure	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Far West AK CA HI NV OR WA	9	8%	2	2%	3	3%	1	1%	6	6%	0	0%
Great Lakes IL IN MI OH WI	9	8%	6	6%	7	7%	6	6%	11	10%	1	1%
Mid East DE DC MD NJ NY PA	9	8%	4	4%	3	3%	6	6%	8	8%	0	0%
New England CT ME MA NH RI VT	5	5%	3	3%	0	0%	2	2%	6	6%	0	0%
Outlying areas AS FM GU MH MP PR PW VI	0	0%	0	0%	0	0%	0	0%	0	0%	2	2%
Plains IA KS MN MO NE ND SD	8	8%	3	3%	4	4%	3	3%	4	4%	4	4%
Rocky Mountains CO ID MT UT WY	2	2%	1	1%	1	1%	1	1%	3	3%	0	0%
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	23	22%	12	11%	7	7%	12	11%	18	17%	1	1%
Southwest AZ NM OK TX	9	8%	1	1%	1	1%	0	0%	8	8%	1	1%
Total	74	70%	32	30%	26	25%	31	29%	64	60%	9	8%

Responses for the Question “Do documented consequences exist for failure to comply with policy?” (by Carnegie Classification)

Carnegie Classification	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Associate's Colleges	1	1%	0	0%	0	0%
Baccalaureate Colleges— General	5	5%	3	3%	1	1%
Baccalaureate Colleges— Liberal Arts	3	3%	2	2%	1	1%
Baccalaureate/Associate's Colleges	4	4%	2	2%	0	0%
Doctoral/Research Universities—Extensive	18	17%	8	8%	3	3%
Doctoral/Research Universities—Intensive	6	6%	6	6%	0	0%
Master's Colleges and Universities I	18	17%	10	9%	2	2%
Master's Colleges and Universities II	1	1%	0	0%	0	0%
Specialized Institutions— Medical schools and medical centers	2	2%	0	0%	0	0%
Specialized Institutions—Other separate health profession schools	2	2%	0	0%	0	0%
Specialized Institutions— Schools of art, music, and design	1	1%	0	0%	0	0%
Specialized Institutions— Schools of business and management	2	2%	0	0%	0	0%
Specialized Institutions— Schools of engineering and technology	0	0%	1	1%	0	0%
Specialized Institutions— Teachers colleges	0	0%	1	1%	0	0%
Specialized Institutions— Theological seminaries and other specialized faith-related institutions	3	3%	0	0%	0	0%
Total	66	62%	33	31%	7	7%

Responses for the Question “Do documented consequences exist for failure to comply with policy?” (by Funding Source)

Funding Source	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Public	37	35%	21	20%	3	3%
Private not-for-profit	27	25%	12	11%	4	4%
Private for-profit	2	2%	0	0%	0	0%
Total	66	62%	33	31%	7	7%

Responses for the Question “Do documented consequences exist for failure to comply with policy?” (by Student Enrollment)

Enrollment	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Less than 1000	8	8%	4	4%	0	0%
1000-2999	10	9%	3	3%	2	2%
3000-9999	17	16%	6	6%	1	1%
10000-19999	13	12%	12	11%	2	2%
20000-29999	7	7%	6	6%	1	1%
greater than 30000	11	10%	2	2%	1	1%
Total	66	62%	33	31%	7	7%

Responses for the Question “Do documented consequences exist for failure to comply with policy?” (by Region)

Region	Yes		No		Not Sure	
	Frequency	%	Frequency	%	Frequency	%
Far West AK CA HI NV OR WA	6	6%	4	4%	1	1%
Great Lakes IL IN MI OH WI	12	11%	2	2%	2	2%
Mid East DE DC MD NJ NY PA	6	6%	2	2%	1	1%
New England CT ME MA NH RI VT	5	5%	2	2%	0	0%
Outlying areas AS FM GU MH MP PR PW VI	1	1%	0	0%	1	1%
Plains IA KS MN MO NE ND SD	6	6%	5	5%	2	2%
Rocky Mountains CO ID MT UT WY	1	1%	3	3%	0	0%
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	21	20%	10	9%	0	0%
Southwest AZ NM OK TX	8	8%	5	5%	0	0%
Total	66	62%	33	31%	7	7%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Policies Were Consistently Enforced (by Carnegie Classification)

Carnegie Classification	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Associate's Colleges	1	1%	0	0%	0	0%	0	0%	0	0%
Baccalaureate Colleges—General	0	0%	5	5%	2	2%	2	2%	0	0%
Baccalaureate Colleges—Liberal Arts	1	1%	0	0%	1	1%	4	4%	0	0%
Baccalaureate/Associate's Colleges	0	0%	3	3%	0	0%	2	2%	1	1%
Doctoral/Research Universities—Extensive	2	2%	5	5%	7	7%	15	14%	0	0%
Doctoral/Research Universities—Intensive	2	2%	3	3%	4	4%	3	3%	0	0%
Master's Colleges and Universities I	2	2%	11	10%	8	8%	8	8%	1	1%
Master's Colleges and Universities II	0	0%	0	0%	0	0%	1	1%	0	0%
Specialized Institutions—Medical schools and medical centers	0	0%	1	1%	0	0%	1	1%	0	0%
Specialized Institutions—Other separate health profession schools	0	0%	1	1%	1	1%	0	0%	0	0%
Specialized Institutions—Schools of art, music, and design	0	0%	0	0%	1	1%	0	0%	0	0%
Specialized Institutions—Schools of business and management	0	0%	1	1%	0	0%	1	1%	0	0%
Specialized Institutions—Schools of engineering and technology	1	1%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Teachers colleges	0	0%	0	0%	1	1%	0	0%	0	0%
Specialized Institutions—Theological seminaries and other specialized faith-related institutions	1	1%	1	1%	1	1%	0	0%	0	0%
Total	10	9%	31	29%	26	25%	37	35%	2	2%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Policies Were Consistently Enforced (by Funding Source)

Funding Source	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Public	7	7%	17	16%	14	13%	22	21%	1	1%
Private not-for-profit	3	3%	14	13%	12	11%	14	13%	0	0%
Private for-profit	0	0%	0	0%	0	0%	1	1%	1	1%
Total	10	9%	31	29%	26	25%	37	35%	2	2%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Policies Were Consistently Enforced (by Student Enrollment)

Enrollment	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Less than 1000	1	1%	3	3%	6	6%	2	2%	0	0%
1000-2999	1	1%	6	6%	1	1%	6	6%	1	1%
3000-9999	2	2%	9	8%	8	8%	5	5%	0	0%
10000-19999	1	1%	8	8%	6	6%	12	11%	0	0%
20000-29999	2	2%	3	3%	2	2%	6	6%	1	1%
Greater than 30000	3	3%	2	2%	3	3%	6	6%	0	0%
Total	10	9%	31	29%	26	25%	37	35%	2	2%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Policies Were Consistently Enforced (by Region)

Region	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Far West AK CA HI NV OR WA	1	1%	3	3%	1	1%	6	6%	0	0%
Great Lakes IL IN MI OH WI	2	2%	8	8%	1	1%	4	4%	1	1%
Mid East DE DC MD NJ NY PA	0	0%	2	2%	4	4%	3	3%	0	0%
New England CT ME MA NH RI VT	1	1%	1	1%	1	1%	4	4%	0	0%
Outlying areas AS FM GU MH MP PR PW VI	0	0%	1	1%	0	0%	0	0%	1	1%
Plains IA KS MN MO NE ND SD	1	1%	1	1%	6	6%	5	5%	0	0%
Rocky Mountains CO ID MT UT WY	0	0%	2	2%	1	1%	1	1%	0	0%
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	4	4%	9	8%	9	8%	9	8%	0	0%
Southwest AZ NM OK TX	1	1%	4	4%	3	3%	5	5%	0	0%
Total	10	9%	31	29%	26	25%	37	35%	2	2%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution Made Users Aware of Enforcement Activities? (by Carnegie Classification)

Carnegie Classification	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Associate's Colleges	0	0%	0	0%	1	1%	0	0%	0	0%
Baccalaureate Colleges—General	0	0%	2	2%	4	4%	3	3%	0	0%
Baccalaureate Colleges—Liberal Arts	1	1%	0	0%	2	2%	2	2%	1	1%
Baccalaureate/Associate's Colleges	1	1%	1	1%	1	1%	2	2%	1	1%
Doctoral/Research Universities—Extensive	1	1%	9	8%	9	8%	10	9%	0	0%
Doctoral/Research Universities—Intensive	2	2%	4	4%	1	1%	5	5%	0	0%
Master's Colleges and Universities I	5	5%	10	9%	10	9%	5	5%	0	0%
Master's Colleges and Universities II	1	1%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Medical schools and medical centers	0	0%	0	0%	2	2%	0	0%	0	0%
Specialized Institutions—Other separate health profession schools	0	0%	0	0%	1	1%	0	0%	1	1%
Specialized Institutions—Schools of art, music, and design	0	0%	0	0%	1	1%	0	0%	0	0%
Specialized Institutions—Schools of business and management	0	0%	0	0%	0	0%	2	2%	0	0%
Specialized Institutions—Schools of engineering and technology	1	1%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Teachers colleges	0	0%	0	0%	1	1%	0	0%	0	0%
Specialized Institutions—Theological seminaries and other specialized faith-related institutions	1	1%	1	1%	1	1%	0	0%	0	0%
Total	13	12%	27	25%	34	32%	29	27%	3	3%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution Made Users Aware of Enforcement Activities? (by Funding Source)

Funding Source	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Public	8	8%	16	15%	19	18%	17	16%	1	1%
Private not-for-profit	4	4%	11	10%	15	14%	12	11%	1	1%
Private for-profit	1	1%	0	0%	0	0%	0	0%	1	1%
Total	13	12%	27	25%	34	32%	29	27%	3	3%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution Made Users Aware of Enforcement Activities? (by Student Enrollment.)

Enrollment	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Less than 1000	2	2%	1	1%	6	6%	2	2%	1	1%
1000-2999	2	2%	2	2%	5	5%	4	4%	2	2%
3000-9999	3	3%	11	10%	7	7%	3	3%	0	0%
10000-19999	2	2%	9	8%	6	6%	10	9%	0	0%
20000-29999	3	3%	2	2%	4	4%	5	5%	0	0%
Greater than 30000	1	1%	2	2%	6	6%	5	5%	0	0%
Total	13	12%	27	25%	34	32%	29	27%	3	3%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution Made Users Aware of Enforcement Activities? (by Region)

Region	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Far West AK CA HI NV OR WA	1	1%	3	3%	4	4%	3	3%	0	0%
Great Lakes IL IN MI OH WI	4	4%	6	6%	2	2%	3	3%	1	1%
Mid East DE DC MD NJ NY PA	0	0%	3	3%	4	4%	2	2%	0	0%
New England CT ME MA NH RI VT	2	2%	1	1%	2	2%	2	2%	0	0%
Outlying areas AS FM GU MH MP PR PW VI	0	0%	0	0%	1	1%	0	0%	1	1%
Plains IA KS MN MO NE ND SD	1	1%	3	3%	5	5%	3	3%	1	1%
Rocky Mountains CO ID MT UT WY	0	0%	3	3%	1	1%	0	0%	0	0%
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	3	3%	6	6%	10	9%	12	11%	0	0%
Southwest AZ NM OK TX	2	2%	2	2%	5	5%	4	4%	0	0%
Total	13	12%	27	25%	34	32%	29	27%	3	3%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Compliance Activities are Visible to Users (by Carnegie Classification)

Carnegie Classification	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Associate's Colleges	0	0%	1	1%	0	0%	0	0%	0	0%
Baccalaureate Colleges—General	1	1%	3	3%	4	4%	1	1%	0	0%
Baccalaureate Colleges—Liberal Arts	2	2%	2	2%	0	0%	1	1%	1	1%
Baccalaureate/Associate's Colleges	0	0%	3	3%	1	1%	2	2%	0	0%
Doctoral/Research Universities—Extensive	1	1%	4	4%	4	4%	19	18%	1	1%
Doctoral/Research Universities—Intensive	1	1%	3	3%	3	3%	5	5%	0	0%
Master's Colleges and Universities I	1	1%	11	10%	8	8%	10	9%	0	0%
Master's Colleges and Universities II	0	0%	0	0%	0	0%	1	1%	0	0%
Specialized Institutions—Medical schools and medical centers	0	0%	0	0%	1	1%	1	1%	0	0%
Specialized Institutions—Other separate health profession schools	0	0%	0	0%	1	1%	1	1%	0	0%
Specialized Institutions—Schools of art, music, and design	0	0%	0	0%	0	0%	1	1%	0	0%
Specialized Institutions—Schools of business and management	0	0%	1	1%	0	0%	1	1%	0	0%
Specialized Institutions—Schools of engineering and technology	1	1%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Teachers colleges	0	0%	1	1%	0	0%	0	0%	0	0%
Specialized Institutions—Theological seminaries and other specialized faith-related institutions	0	0%	1	1%	0	0%	1	1%	1	1%
Total	7	7%	30	28%	22	21%	44	42%	3	3%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Compliance Activities are Visible to Users (by Funding Source)

Funding Source	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Public	3	3%	15	14%	13	12%	28	26%	2	2%
Private not-for-profit	4	4%	15	14%	9	8%	14	13%	1	1%
Private for-profit	0	0%	0	0%	0	0%	2	2%	0	0%
Total	7	7%	30	28%	22	21%	44	42%	3	3%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Compliance Activities are Visible to Users (by Student Enrollment)

Enrollment	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Less than 1000	1	1%	5	5%	1	1%	4	4%	1	1%
1000-2999	1	1%	5	5%	4	4%	4	4%	1	1%
3000-9999	3	3%	9	8%	6	6%	6	6%	0	0%
10000-19999	0	0%	6	6%	5	5%	15	14%	1	1%
20000-29999	1	1%	1	1%	6	6%	6	6%	0	0%
Greater than 30000	1	1%	4	4%	0	0%	9	8%	0	0%
Total	7	7%	30	28%	22	21%	44	42%	3	3%

Responses for the Question Where Respondents Were Asked to Indicate the Strength to Which They Agreed or Disagreed That Their Institution's Compliance Activities are Visible to Users (by Region)

Region	Strongly Disagree		Disagree		Neither Agree nor Disagree		Agree		Strongly Agree	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Far West AK CA HI NV OR WA	1	1%	2	2%	2	2%	6	6%	0	0%
Great Lakes IL IN MI OH WI	1	1%	5	5%	3	3%	7	7%	0	0%
Mid East DE DC MD NJ NY PA	0	0%	3	3%	1	1%	4	4%	1	1%
New England CT ME MA NH RI VT	2	2%	4	4%	0	0%	1	1%	0	0%
Outlying areas AS FM GU MH MP PR PW VI	0	0%	0	0%	1	1%	1	1%	0	0%
Plains IA KS MN MO NE ND SD	2	2%	3	3%	4	4%	2	2%	2	2%
Rocky Mountains CO ID MT UT WY	0	0%	1	1%	1	1%	2	2%	0	0%
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	1	1%	9	8%	7	7%	14	13%	0	0%
Southwest AZ NM OK TX	0	0%	3	3%	3	3%	7	7%	0	0%
Total	7	7%	30	28%	22	21%	44	42%	3	3%

Responses for the Question Where Respondents Were Asked to Classify the Level of Centralization of IT Resources at Their University (by Carnegie Classification)

Carnegie Classification	Totally Decentralized		2		Equally Distributed		4		Totally Centralized	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Associate's Colleges	0	0%	1	1%	0	0%	0	0%	0	0%
Baccalaureate Colleges—General	0	0%	2	2%	2	2%	1	1%	4	4%
Baccalaureate Colleges—Liberal Arts	0	0%	0	0%	0	0%	2	2%	4	4%
Baccalaureate/Associate's Colleges	0	0%	1	1%	2	2%	2	2%	1	1%
Doctoral/Research Universities—Extensive	1	1%	7	7%	13	12%	8	8%	0	0%
Doctoral/Research Universities—Intensive	0	0%	3	3%	3	3%	6	6%	0	0%
Master's Colleges and Universities I	0	0%	3	3%	3	3%	17	16%	7	7%
Master's Colleges and Universities II	0	0%	0	0%	0	0%	0	0%	0	0%
Specialized Institutions—Medical schools and medical centers	0	0%	0	0%	0	0%	2	2%	0	0%
Specialized Institutions—Other separate health profession schools	0	0%	0	0%	1	1%	1	1%	0	0%
Specialized Institutions—Schools of art, music, and design	0	0%	0	0%	0	0%	1	1%	0	0%
Specialized Institutions—Schools of business and management	0	0%	0	0%	0	0%	0	0%	2	2%
Specialized Institutions—Schools of engineering and technology	0	0%	0	0%	0	0%	1	1%	0	0%
Specialized Institutions—Teachers colleges	0	0%	0	0%	0	0%	0	0%	1	1%
Specialized Institutions—Theological seminaries and other specialized faith-related institutions	0	0%	0	0%	0	0%	0	0%	3	3%
Total	1	1%	17	16%	24	23%	41	39%	22	21%

Responses for the Question Where Respondents Were Asked to Classify the Level of Centralization of IT Resources at Their University (by Funding Source)

Funding Source	Totally Decentralized		2		Equally Distributed		4		Totally Centralized	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Public	1	1%	13	12%	15	14%	28	27%	4	4%
Private not-for-profit	0	0%	4	4%	8	8%	13	12%	18	17%
Private for-profit	0	0%	0	0%	1	1%	0	0%	0	0%
Total	1	1%	17	16%	24	23%	41	39%	22	21%

Responses for the Question Where Respondents Were Asked to Classify the Level of Centralization of IT Resources at Their University (by Student Enrollment)

Enrollment	Totally Decentralized		2		Equally Distributed		4		Totally Centralized	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Less than 1000	0	0%	0	0%	2	2%	3	3%	6	6%
1000-2999	0	0%	1	1%	3	3%	3	3%	8	8%
3000-9999	0	0%	3	3%	3	3%	14	13%	4	4%
10000-19999	0	0%	6	6%	7	7%	10	10%	4	4%
20000-29999	0	0%	3	3%	3	3%	8	8%	0	0%
Greater than 30000	1	1%	4	4%	6	6%	3	3%	0	0%
Total	1	1%	17	16%	24	23%	41	39%	22	21%

Responses for the Question Where Respondents Were Asked to Classify the Level of Centralization of IT Resources at Their University (by Region)

Region	Totally Decentralized		2		Equally Distributed		4		Totally Centralized	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Far West AK CA HI NV OR WA	0	0%	5	5%	3	3%	3	3%	0	0%
Great Lakes IL IN MI OH WI	0	0%	1	1%	3	3%	7	7%	5	5%
Mid East DE DC MD NJ NY PA	0	0%	1	1%	2	2%	5	5%	1	1%
New England CT ME MA NH RI VT	0	0%	1	1%	1	1%	2	2%	3	3%
Outlying areas AS FM GU MH MP PR PW VI	0	0%	0	0%	2	2%	0	0%	0	0%
Plains IA KS MN MO NE ND SD	0	0%	0	0%	1	1%	7	7%	5	5%
Rocky Mountains CO ID MT UT WY	0	0%	2	2%	2	2%	0	0%	0	0%
Southeast AL AR FL GA KY LA MS NC SC TN VA WV	1	1%	4	4%	8	8%	13	12%	5	5%
Southwest AZ NM OK TX	0	0%	3	3%	2	2%	4	4%	3	3%
Total	1	1%	17	16%	24	23%	41	39%	22	21%

Reference List

- Adler, M. P. (2006). A Unified Approach to Information Security Compliance. *Educause Review*, 46-60.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289. doi: 10.1016/j.cose.2006.11.004
- Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives*, 22(2), 171-192.
- Arnesen, D. W., & Weis, W. L. Developing an effective company policy for employee internet and email use. *Communications*, 11(2), 53-65.
- Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, 13(4), 195-201.
- Ayyagari, R., & Tyks, J. (2012). Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education*, 11.
- Baker, S., & Schneck-Teplinsky, M. (2010). Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US
- Cybercrimes: A Multidisciplinary Analysis. In S. Ghosh & E. Turrini (Eds.), (pp. 239-263): Springer Berlin Heidelberg.
- Baker, W. H., & Wallace, L. (2007). Is information security under control? *IEEE Security and Privacy*, 5(1), 36-44.
- Barboza, S., Epps, S., Byington, R., & Keene, S. (2010). HIPAA goes to school: Clarifying privacy laws in the education environment. *The Internet Journal of Law, Healthcare, and Ethics*, 6(2). Retrieved from http://www.ispub.com/journal/the_internet_journal_of_law_healthcare_and_ethic/s/volume_6_number_2_39/article/hipaa-goes-to-school-clarifying-privacy-laws-in-the-education-environment.html
- Beautement, A., & Sasse, A. (2009). The economics of user effort in information security. *Computer Fraud & Security*, 2009(10), 8-12.

- Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management*. Paper presented at the Proceedings of the 2001 Workshop on New Security Paradigms, Cloudcroft, New Mexico.
- Breier, J., & Hudec, L. (2013). On identifying proper security mechanisms *Information and Communicatiaon Technology* (pp. 285-294): Springer.
- Burdon, M. (2010). Contextualizing the tensions and weaknesses of data breach notification and information privacy law. *Santa Clara Computer and High Technology Law Journal*, 27(1).
- Burdon, M., Reid, J., & Low, R. (2010). Encryption safe harbours and data breach notification laws. *Computer Law & Security Review*, 26(5), 520-534. doi: 10.1016/j.clsr.2010.07.002
- Campana, J. (2008). How safe are we in our schools. Retrieved from <http://www.jcampana.com/JCampanaDocuments/EducationSectorDataBreachStudy.pdf>
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431-448.
- Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment*: Sage Publications.
- Carnegie Foundation. June 24, 2013). The Carnegie Classification of Institutions of Higher Education Retrieved 2013, from <http://classifications.carnegiefoundation.org/>
- Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3), 438-458.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32(0), 90-101. doi: <http://dx.doi.org/10.1016/j.cose.2012.09.010>

- Culnan, M. J., & Carlin, T. J. (2009). Online privacy practices in higher education: making the grade? *Commun. ACM*, 52(3), 126-130. doi: 10.1145/1467247.1467277
- Custer, W. L. (2010). Information security issues in higher education and institutional research. *New Directions for Institutional Research*, 2010(146), 23-49. doi: 10.1002/ir.341
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207. doi: 10.1016/j.cose.2009.09.002
- Denning, D. E. R. (1999). *Information warfare and security* (Vol. 4): Addison-Wesley Reading MA.
- Dillman, D. A., Smyth, J. D., & Christian, L. M. (2009). *Mail and Internet surveys: The tailored design method* (3rd Ed ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.
- Dodge, A. (2009). Educational Security Incidents (ESI) Year in Review. Retrieved from http://www.adamdodge.com/esi/files/esi_yir_2009.pdf
- Doherty, N. F., 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, 449-457.
- Doherty, N. F., Anastasakis, L., & Fulford, H. (2010). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management*, In Press, Corrected Proof. doi: 10.1016/j.ijinfomgt.2010.06.001
- Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches : An exploratory analysis. *Information Resources Management Journal*, 18(December), 21-39.
- Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1), 55-63.

- EDUCAUSE. (2012). *2012 Core Data Service*. <http://www.educause.edu/research-and-publications/research/core-data-service/access-data>. Retrieved from: <http://www.educause.edu/research-and-publications/research/core-data-service/access-data>
- Ekelhart, A., Fenz, S., & Neubauer, T. (2009, 5-8 Jan. 2009). *AURUM: A Framework for Information Security Risk Management*. Paper presented at the System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on.
- Ernst & Young. (2010). Borderless security: Ernst & Young's 2010 global information security survey *Global Information Security Survey* (pp. 24): Ernst & Young.
- Fritsche, G. D. (2009). *Desktop data management and security*. Paper presented at the Proceedings of the 37th annual ACM SIGUCCS fall conference, St. Louis, Missouri, USA.
- Fulford, H., & Doherty, N. (2003). The application of information security policies in large UK-based organizations: An exploratory investigation. *Information Management & Computer Security*, 11(3), 106-114.
- Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems*, 3(2), 112-126.
- Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216-230. doi: 10.1108/09685221111173049
- Gaunt, N. (1998). Installing an appropriate information security policy. *International journal of medical informatics*, 49(1), 131-134.
- Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4), 281-295. doi: 10.1016/j.jsis.2010.10.002
- Greenberg, P. (2011, 12-21-2011). Security Breach Legislation 2011 Retrieved 02-10, 2012, from <http://www.ncsl.org/issues-research/telecommunications-information-technology/security-breach-legislation-2011.aspx>

- Gritzalis, D. (1997). A baseline security policy for distributed healthcare information systems. *Computers & Security*, 16(8), 709-719. doi: 10.1016/s0167-4048(97)00009-6
- Guttman, B., & Roback, E. A. (1995). *An introduction to computer security: the NIST handbook*. DIANE Publishing.
- Hanson, J. (2008). Liability for consumer information security breaches: Deconstructing FTC complaints and settlements. *Washington Journal of Law, Technology & Arts*, 4(4).
- Hasan, R., & Yurcik, W. (2006). *A statistical analysis of disclosed storage security breaches*. Paper presented at the Proceedings of the Second ACM Workshop on Storage Security and Survivability, Alexandria, Virginia, USA.
- Heikkila, F. M. (2009). *An Analysis of the Impact of Information Security Policies on Computer Security Breach Incidents in Law Firms*. (Doctor of Philosophy in Information Systems), Nova Southeastern University.
- Hilley, S. (2007). IT security breaches not behind most ID theft: GAO. *Computer Fraud & Security*, 2007(8), 6-10. doi: 10.1016/s1361-3723(07)70101-x
- Höne, K., & Eloff, J. H. P. (2002a). Information security policy -- what do international information security standards say? *Computers & Security*, 21(5), 402-409. doi: 10.1016/s0167-4048(02)00504-7
- Höne, K., & Eloff, J. H. P. (2002b). What makes an effective information security policy? *Network Security*, 2002(6), 14-16. doi: 10.1016/s1353-4858(02)06011-7
- Hong, K. s., Chi, Y. p., 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.
- Hoonakker, P., Carayon, P., Deb, J., Desoki, R. E., & Veeramani, R. (2008). The Use of Focus Groups to Examine Human Factors in Computer and Information Security. In L. Sznelwar, F. Mascia & U. Montedo (Eds.), *Human Factors in Organizational Design and Management* (Vol. IX, pp. 377-382). Santa Monica, CA: IEA Press.

- Hosack, B., Twitchell, D. P., & Sagers, G. (2009). Effects of Education on User Compliance with Security Policies : Ignore or Comply ?
- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Commun. ACM*, 54(6), 54-60. doi: 10.1145/1953122.1953142
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95. doi: <http://dx.doi.org/10.1016/j.cose.2011.10.007>
- ISO/IEC. (2000). ISO/IEC 17799:2000 - information technology - code of practice for information security management. Switzerland.
- ISO/IEC. (2005). ISO/IEC 27002:2005 - information technology - security techniques - code of practice for information security management. Switzerland.
- Israel, G. D. (2011). Strategies for obtaining survey responses from extension clients: Exploring the role of e-mail requests. *Journal of Extension*, 49(3).
- Johns, M. L. (2010). *Health information management technology, an applied approach* (Third ed.). Chicago, IL: American Health Information Management Association.
- Jones, R., & Stallings, T. J. (2010). Network security in two-year colleges. *Journal of Computing Sciences in Colleges*, 25(5), 83-88.
- Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, 24(3), 246-260. doi: 10.1016/j.cose.2004.08.011
- Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26), 10862-10868.
- Kiel, J. M., & Knoblauch, L. M. (2010). HIPAA and FERPA: Competing or collaborating? *Journal of Allied Health*, 39(4), 161E-165E.

- Knapp, K. J., Franklin Morris Jr, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7), 493-508. doi: 10.1016/j.cose.2009.07.001
- Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36.
- Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 33(0), 3-11. doi: <http://dx.doi.org/10.1016/j.cose.2012.07.001>
- Kolkowska, E., Hedström, K., & Karlsson, F. (2009). *Information Security Goals in a Swedish Hospital*. Paper presented at the Security, Assurance and Privacy: Organizational Challenges Proceedings of the 8th Annual Security Conference Discourses in Security Assurance & Privacy, Las Vegas, NV, USA.
- Kotulic, A. J., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information and Management*, 41(5), 597-607.
- Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7), 509-520. doi: 10.1016/j.cose.2009.04.006
- Kvavik, R. B., Voloudakis, J., Caruso, J. B., & Pirani, J. A. (2003). *Information Technology Security: Governance, Strategy, and Practice in Higher Education (Vol. 5)*: ECAR.
- Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). *Employees' Information Security Awareness and Behavior: A Literature Review*. Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.
- McKenna, B. (2010). Keeping it real: Updating your security policy in 2010. *Infosecurity*, 7(2), 18-21. doi: 10.1016/s1754-4548(10)70036-x
- Meers, E. B., & Meade, D. S. (2008). FTC's Red Flag Rule Likely to Affect Colleges. *NACUBO Initiatives News* Retrieved 02-08, 2012, from

http://www.nacubo.org/Initiatives/Initiatives_News/FTCs_Red_Flag_Rule_Likely_to_Affect_Colleges.html

Monroe, M. C., & Adams, D. C. (2012). Increasing response rates to web-based surveys. *Journal of Extension*, 50(6).

Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Review*, 24(6), 540-554. doi: 10.1016/j.clsr.2008.07.001

NIH CIT. (2012, 02-22-2012). Using the NIH Guide for Identifying Sensitive Information Retrieved 02-22, 2012, from datacenter.cit.nih.gov/interface/interface241/PIIguide.html

NIST. (2010a). *Guide for Applying the Risk Management Framework to Federal Information Systems. Special Publication 800-37* Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.

NIST. (2010b). *Risk Management Guide for Information Technology Systems. Special Publication 800-37*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.

Papadaki, M., & Furnell, S. (2010). Vulnerability management: an attitude of mind? *Network Security*, 2010(10), 4-8. doi: 10.1016/s1353-4858(10)70124-0

Peppard, J. (2007). The conundrum of IT management. *European Journal of Information Systems*, 16(4), 336-345.

Ponemon Institute. (2011). Perceptions About Network Security Survey of IT & IT security practitioners in the U.S.

Qualtrics Crushes 2012 With Record Client Growth and More Than A Billion Surveys Served. (2013). Retrieved May 15, 2013, from <http://www.marketwatch.com/story/qualtrics-crushes-2012-with-record-client-growth-and-more-than-a-billion-surveys-served-2013-01-31>

Regan, P. M. (2009). Federal Security Breach Notifications: Politics and Approaches. *Berkeley Technology Law Journal*, 24(3), 1101-1130.

- Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7-8), 241-253. doi: 10.1016/j.cose.2008.07.008
- Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8), 816-826. doi: 10.1016/j.cose.2009.05.008
- Roberds, W., & Schreft, S. L. (2009). Data breaches and identity theft. *Journal of Monetary Economics*, 56(7), 918-929. doi: 10.1016/j.jmoneco.2009.09.003
- Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives *Berkeley Technology Law Journal*, 24(3), 1062-1102.
- Roster, C. A., Rogers, R. D., Hozier, G. C., Baker, K. G., & Albaum, G. (2007). Management of marketing research projects: Does delivery method matter anymore in survey research? *Journal of Marketing Theory and Practice*, 15(2), 127-144.
- Satoh, N., & Kumamoto, H. (2009). Analysis of information security problem by probabilistic risk assessment. *International Journal of Computers*, 3(3), 337-347.
- Schwartz, P. M., & Janger, E. J. (2007). Notification of data security breaches. *Michigan Law Review*, 105, 913-972.
- Shaw, A. (2010). Data breach: From notification to prevention using PCI DSS. *Columbia Journal of Law and Social Problems*, 43(4), 517-562.
- Sheehan, K. B. (2001). E-mail Survey Response Rates: A Review. *Journal of Computer-Mediated Communication*, 6(2), 0-0. doi: 10.1111/j.1083-6101.2001.tb00117.x
- Siegel, P. M. (2008). Data breaches in higher education: From concern to action. *EDUCAUSE Review*, 43(1), 72-73.
- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, 43(2), 64-71.

- Sotto, L. J., Treacy, B. C., & McLellan, M. L. (2010). Privacy and data security risks in cloud computing. *Electronic Commerce & Law Report*, 15(186).
- Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, 2006(10), 7-11. doi: 10.1016/s1361-3723(06)70430-4
- van Niekerk, J., & von Solms, R. (2008). *Bloom's taxonomy for information security education*. Paper presented at the Information Security South Africa ISSA Johannesburg South Africa Johannesburg South Africa
- von Solms, R., van der Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. *Information & Management*, 26(3), 143-153. doi: 10.1016/0378-7206(94)90038-8
- von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security*, 23(4), 275-279. doi: 10.1016/j.cose.2004.01.013
- Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198. doi: 10.1016/j.cose.2004.01.012
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101.
- Whitman, M. E., & Mattord, H. J. (Eds.). (2011). *Principles of Information Security* (4th ed.). Boston, MA: Course Technology.
- Wieland, J. (2010). HIPAA: the new enforcement culture. *Medical Lab Observer*, 42(11).
- Wiles, J. (2008). Developing an Effective Security Awareness Program *Techno Security's Guide to Securing SCADA* (pp. 137-169). Burlington: Syngress.
- Williams, P. A. H. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report*, 13(4), 207-215. doi: 10.1016/j.istr.2008.10.009

Wright, C. (2008). Assessing Security Awareness and Knowledge of Policy *The IT Regulatory and Standards Compliance Handbook* (pp. 161-194). Burlington: Syngress.

Wuensch, K. L. (2001, June 04, 2001). Choosing an Appropriate Bivariate Inferential Statistic Retrieved June 01, 2012