

Exploring Information Technology Security Requirements for Academic Institutions  
to Reduce Information Security Attacks, Breaches, and Threats

Dissertation Manuscript

Submitted to Northcentral University

Graduate Faculty of the School of Business and Technology Management  
in Partial Fulfillment of the  
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

by

KEVIN J. MISENHEIMER

Prescott Valley, Arizona  
July 2014

UMI Number: 3638473

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 3638473

Published by ProQuest LLC (2014). 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

Approval Page

Exploring Information Technology Security Requirements for Academic Institutions  
to Reduce Information Security Attacks, Breaches, and Threats

By

KEVIN J. MISENHEIMER

Approved by:



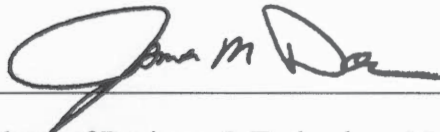
8/15/14

Chair: Dr. Michael Shriner, Ph.D.

Date

Committee Member: Dr. Lawrence R. Ness, Ph.D.

Certified by:



8/19/2014

Dean of School of Business & Technology Management: Dr. Jim Dorris, Ph.D. Date

## Abstract

With most organizations involved in a complex computing environment, managing and protecting information has become a primary concern. The success or failure of many organizations is contingent upon the levels of information technology (IT) and the protection of data. The securing of this information is a major challenge. Incidents of information security attacks, breaches, and threats and the costs associated with these incidents continue to be on the rise. The focus of this study was to examine the computer and information technology security needs and requirements of colleges and universities in order to provide information that may help administrators reduce or eliminate potential information security attacks, breaches, and threats and provide a foundation for future research into these critical issues from the perspectives of IT personnel within institutions of higher education. The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved computer and information security and reduced attacks, breaches, and threats among institutions of higher education. Perspectives gathered from IT personnel from colleges and universities throughout the state of North Carolina were examined. The sample of institutions included community colleges, and private and public colleges and universities that offer associates, bachelors, masters, and doctoral degrees within the state of North Carolina. There were a total of 13 interview participants from 12 distinct and separate institutions of higher education that were included in this study. In-depth open-ended interviews were conducted with at least one member of the institution's IT department to collect data for the study. Ten thematic categories were used to conduct this research and all relate to how institutions of higher

education may be involved in computer and information security. Participants revealed various types of attacks, breaches, and threats that are common to colleges and universities and that a major way to avoid having computers and information compromised is through training, educating, and making users aware of their responsibilities. Recommendations for future research include narrowing the units of analysis down to certain colleges or universities and analyzing how the increase usage of mobile devices on institution networks and the security risks involved.

## Acknowledgements

The dissertation process was certainly a difficult journey, but I had the good fortune of having a supportive dissertation committee. I would like to thank Dr. Michael Shriner, the final chair of my dissertation committee, for being a great coach, being supportive, and providing advice that helped me complete this journey. I would like to thank my previous dissertation committee chairs, Dr. Gene Fusch and Dr. Karin Klenke, for the amount of work they did in helping me accomplish this goal. I would like to thank my dissertation committee member and subject matter expert, Dr. Lawrence Ness for all the knowledge and help he provided me on completing this process.

I would like to thank all the research participants involved in this study. Without their willingness to participate in the research, this would not have been possible. A special thanks goes to the people I work with whom kept me focused on completion and encouraged me. Finally, this was a challenging process in my life and from start to finish I would like to thank my family who were always supportive and encouraging to me. Thank God for giving me the wisdom and strength needed to complete this big task.

## Table of Contents

Chapter 1: Introduction.....	1
Background.....	3
Statement of the Problem .....	5
Purpose of the Study.....	6
Theoretical Framework.....	7
Research Questions.....	11
Nature of the Study.....	12
Significance of the Study.....	15
Definition of Key Terms.....	18
Summary.....	23
Chapter 2: Literature Review.....	26
Documentation.....	27
The Need for Computer, Network, and Information Security.....	27
Importance of Computer, Network, and Information Security .....	31
Management's Concern for IT Security .....	33
Analysis of Risks Associated With Security Breaches and Risk Management .....	40
Information Security Awareness and Training.....	46
Information Security Statistics .....	53
Computer and Information Security Implementations .....	56
Information Security at Institutions of Higher Education .....	73
Summary.....	78
Chapter 3: Research Method.....	81
Research Methods and Design .....	84
Population.....	94
Sample .....	94
Materials/Instruments .....	97
Data Collection, Processing, and Analysis.....	102
Assumptions .....	115
Limitations.....	115
Delimitations .....	116
Ethical Assurances.....	117
Summary.....	120
Chapter 4: Findings.....	122
Results .....	126
Evaluation of Findings.....	169
Summary.....	179

Chapter 5: Implications, Recommendations, and Conclusions .....	181
Implications .....	185
Recommendations .....	190
Conclusions .....	193
References.....	197
Appendices.....	213
Appendix A: Interview Questions Guide .....	214
Appendix B: Dissertation Participation Permission Request Letter.....	217
Appendix C: Dissertation Participation Introduction Letter.....	218
Appendix D: Informed Consent Form.....	219
Appendix E: Information Technology Security Requirements Recommended .....	221
Appendix F: Permission to Use Computer and Information Security Threats Table..	222
Appendix G: Permission to Use Security Incidents and End –Effects Table.....	223
Appendix H: Permission to Use Traditional Risk Management Process Table .....	226
Appendix I: Permission to Use The Goal Setting Process Table .....	228
Appendix J: Permission to Use Risk Factors by Percentages Table .....	229
Appendix K: Permission to Use Top 10 Computer and Information Security Threats for 2010 Table .....	232
Appendix L: Permission to Use Four Security Actions Table .....	234
Appendix M: Permission to Use Types of Attacks Experienced from 2006-2010 Table .....	235
Appendix N: Permission to Use Cognitive Skills of Users as Relating to Information Security Table.....	237
Appendix O: Permission to Use Information / Computer Security and Privacy Concerns Table .....	239
Appendix P: Permission to Use Distribution of Information Security Policy Use Table .....	242
Appendix Q: Permission to Use Ten Stage Security Management Strategy Model Figure.....	243
Appendix R: Permission to Use Information Security Awareness Program Lifecycle Figure.....	245
Appendix S: Permission to Use Information Security Planning Involves Planning at Various Levels Figure .....	247
Appendix T: Permission to Use Performance Pyramid Framework Figure .....	249
Appendix U: Permission to Use A Strategic Framework for Effective Information Security Figure .....	250
Appendix V: Permission to Use Information Security Framework Figure .....	251



## List of Tables

Table 1	<i>Computer and Information Security Threats</i>	29
Table 2	<i>Security Incidents and End-Effects</i>	37
Table 3	<i>Traditional Risk Management Process</i>	42
Table 4	<i>The Goal Setting Process</i>	45
Table 5	<i>Risk Factors by Percentages</i>	46
Table 6	<i>Top 10 Computer and Information Security Threats for 2010</i>	48
Table 7	<i>Four Security Actions</i>	52
Table 8	<i>Types of Attacks Experienced from 2006-1010</i>	55
Table 9	<i>Cognitive Skills of Users as Relating to Information Security</i>	59
Table 10	<i>Information / Computer Security and Privacy Concerns</i>	68
Table 11	<i>Distribution of Information Security Policy Use</i>	71
Table 12	<i>Participant Demographics</i>	124
Table 13	<i>Major Thematic Categories and Sub-thematic categories</i>	127
Table 14	<i>Types of Computer and Information Security Attacks</i>	131
Table 15	<i>Types of Plans Participant Institutions Currently Have in Place</i>	144
Table 16	<i>Top Three Major Risks of Information Security Attacks, Breaches, Threats</i>	153
Table 17	<i>Top IT Security Issue at Your Institution</i>	155
Table 18	<i>Best Security Practices and Tools-Hardware</i>	157
Table 19	<i>Best Security Practices and Tools-Software</i>	159

## List of Figures

<i>Figure 1. Ten Stage Security Management Strategy Model.....</i>	36
<i>Figure 2. Information Security Awareness Program Lifecycle.....</i>	40
<i>Figure 3. Information Security Planning Involves Planning at various Levels.....</i>	57
<i>Figure 4. Performance Pyramid Framework. ....</i>	61
<i>Figure 5. A Strategic Framework for Effective Information Security. ....</i>	65
<i>Figure 6. Information Security Framework.....</i>	77

## Chapter 1: Introduction

The success or failure of many organizations is contingent upon the levels of information technology (IT) and information protection (Jo, Kim, & Won, 2011). The key purpose of information security is to protect information and specifically, the integrity, confidentiality, authenticity and availability of data through an organization's network and communication channels (Koskosas, Kakoulidis, & Siomos, 2011). Throughout the first decade of the 21<sup>st</sup> century and into the second decade, information security attacks on organizations were increasing day by day and it was necessary to take appropriate actions to safeguard against these malicious attacks (Taluja & Dua, 2012). Information security breach incidents and costs associated with these incidents continue to be on the rise in 2012 (Zafar, Ko, & Osei-Bryson, 2012).

Information security was one of the greatest challenges facing management (Ramachandran & Ramachandran, 2012). It was found that individuals were put at direct risk of harm by criminals when their personal and confidential information was not appropriately secured (Gillon et al., 2011). Due to a more open academic environment and a rise in network connectivity, cybercriminals were increasingly looking at colleges and universities as a point from which to launch their attacks (Alwi & Fan, 2010; Kumari, Debbarma, & Shyam, 2011; Mensch & Wilkie, 2011; Perkel, 2010; Spanier, 2010). Web 2.0 technologies that included social networking sites had also increased organization's exposure to information security risks and increased vulnerabilities to data breaches (Almeida, 2012). Between 2005 and 2012, educational institutions had experienced the most reported information security issues as compared to any other

industry (Ayyagari & Tyks, 2012).

Although information security was critical for organizations to survive, as of 2011 a number of incidents were still being reported of critical information loss (Koskosas et al., 2011). At the end of the first decade of the 21<sup>st</sup> century, IT security on campuses was continually improving and yet this type of security threat remained a challenge with numerous internal and external concerns (Grummon, 2010). Between 2005 and 2011, computer and IT security threats to educational institutions increased considerably (Maskari, Saini, Raut, & Hadimani, 2011). One reason for the increase in threats and vulnerabilities was the evolution of wireless networking found on many college campuses and gave rise to serious security issues (Likhar, Yadav, & Keshava, 2011). With the increase in IT security threats and intrusions during the first decade of the 21st century, it was critical that IT departments developed a comprehensive security program (Liu & Ormaner, 2009). Information security threats required development of more adaptive and responsive defensive systems (Taluja & Dua, 2012). Network security at institutions of higher education was a critical issue in the first decade of the 21st century as well as into the second decade (Kumari, et al., 2011). The focus of this research was to examine the computer and IT security needs and requirements for institutions of higher education operating within the state of North Carolina.

Colleges and universities possess considerable amounts of employee and student information that needs to be protected and secured and potential security vulnerabilities exist because of this information (Jones, 2008). Managers have faced various information security challenges due to uncertainties in new technologies, obsolescence of

their security processes, and overall needs for changes in security requirements (Abbas, Magnusson, Yngstrom, & Hemani, 2011). As of 2009, the field of computer, network, and information systems security had become a new arena for risk management, threat, and consideration for the IT professional (Herath & Rao, 2009). Through an in-depth qualitative research study, an examination of the unique IT security needs of colleges and universities within the state of North Carolina was conducted.

The remainder of Chapter 1 contains the background on why the research topic is relevant and the presentation of the problem statement describing the problem to be addressed. Included in the chapter are the purpose statement that describes the intent of the study, theoretical framework, research questions that are used to guide the research, a brief background of the methodology plan, nature of the study, significance of the study, and a list of relevant definitions to ensure clarity. A summary of the chapter is also included.

## **Background**

Information security is the way of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, inspection, or destruction (Susanto & Almunawar, 2012). Innovative security threats and attacks are continually being fashioned and deployed by cybercriminals to exploit weaknesses that organizations have not yet uncovered (Jourdan, Rainer, Marshall, & Ford, 2010).

Network security at colleges and universities has been a critical issue in the first decade of the 21st century as well as into the second decade (Kumari et al., 2011). Identity theft, data breaches, and data exposure type crimes have been increasing and are motivated by financial gains (Ramachandran & Ramachandran, 2012).

Computer and information security threats and intrusions are motivating IT management in organizations to acclimate to a more complete and comprehensive security program (Liu & Ormaner, 2009). The U.S. Cost of Data Breach report released in March 2011 showed that the number of data breaches had increased and the costs associated with these breaches were on the rise (Zafar et al., 2012). During the years 2005 through 2009, 549 data breach incidents were reported at educational institutions exposing on average 10.4 million records (Collins et al., 2011). Information technology (IT) security management encompasses a blend of expectation, discovery, and reaction type processes along with a chain of actions that necessitate continual monitoring and control activities used to lessen the chance of information security attacks (Issa-Salwe & Ahmed, 2011; Sehgal et al., 2011).

Based on recent published literature on IT security requirements, there is a general consensus for each organization to include certain and specific IT security requirements (see Appendix E) (Kimwele, Mwangi, & Kimani, 2011). It is essential that management ensure the organization's resources like databases and operating systems are secure (Ramachandran & Ramachandran, 2012). Numerous colleges and universities have added security challenges, such as relaxed working environments, less formalized policies and procedures, additional vulnerabilities, and employees that are assigned many different tasks (Ayyagari & Tyks, 2012; Susanto, Almunawar, & Tuan, 2012). Research conducted by Garrison and Ncube (2011) found that educational institutions are more likely to experience an information security breach over other types of organizations including business/financial, medical, and federal, state, and local governments.

Therefore, the research findings from this study are of great importance to IT management within institutions of higher education.

### **Statement of the Problem**

Information security is a foremost concern for IT management since hackers are directing their targets toward colleges and universities to steal and compromise computing resources, property, and data (Perkel, 2010). The specific problem addressed in this study is the increase in information security breaches impacting institutions of higher education (Ayyagari & Tyks, 2012; Collins et al., 2011; Perkel, 2010; Susanto, Almunawar, Tuan, Aksoy, & Syam, 2011). The costs associated with data breaches have increased and continue to motivate IT departments to implement new security of information protection measures (Hoadley, Deibel, Kistner, Rice, & Sokhey, 2012). Raising awareness concerning information security issues faced by academic institutions is important because the majority of reported breaches in 2011 have occurred in an educational environment (Ayyagari & Tyks, 2012).

In 2010, educational institutions reported 65 security breach incidents that lead to the exposure of over 1.6 million records (Collins, Sainato, & Khey, 2011). The majority of data breaches since 2005 have occurred in educational environments and information security is a leading concern for institutions of higher education because hackers are targeting colleges and universities to steal computing resources, property, and data (Ayyagari & Tyks, 2012; Perkel, 2010).

A gap in literature exists on IT security requirements for colleges and universities. Researchers have found IT security an important concern for organizations, but very few

have focused on the specific needs of a college or university and due to increases in IT security breaches in educational environments, researchers have recommended that the needs of colleges and universities for the improvement of IT security be explored in more depth (Abbas et al., 2011; Fisher & Shorter, 2013; Guo, Yuan, Archer, & Connelly, 2011; Ma, Schmidt, & Pearson, 2009; Mensch & Wilkie, 2011; Werlinger, Muldner, Hawkey, & Beznosov, 2010). The importance of computer and network security at institutions of higher education has never been higher due to the numbers of breaches and costs associated with breaches (Kumari et al., 2011).

### **Purpose of the Study**

The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. There were a total of 13 participants as holistic units of analysis selected from 12 distinct and separate colleges and universities within the state of North Carolina. The institutions were derived from a population of more than 220 institutions of higher education in the state of North Carolina and the IT personnel selected from these institutions. Face-to-face, one-on-one, in-depth interviews were conducted with 13 personnel working in the IT departments of 12 separate and distinct academic institutions for a total of 13 interview participants in order to gather data relevant to fulfilling the purpose of this study. The interview participants were IT professionals working in and having responsibility over IT security.

The goal of this study was to explore what aspects of computer and information security are not only important but what are required to be implemented for maximum



computer, network, and information security. Information technology (IT) management and university administrators could use the detailed information gathered from this study to help and aid in designing, implementing, or verifying appropriate and required IT security tools, processes, procedures, systems and strategies.

### **Theoretical Framework**

This qualitative holistic multiple case study was supported by examining different IT management theories that align with the research. A comprehensive theory explaining computer and information security in institutions of higher education does not exist, and further research is necessary to define such specific and definite implementations of such for optimal protection (Ayyagari & Tyks, 2012; Collins et al., 2011). Nevertheless, considerable research exists in the broader area of computer, network, and information securities and the multiple approaches and uses of tools, techniques, processes, and certain procedures to follow (Abbas et al., 2010; Anand, Saniie, & Oruklu, 2012; Kumari et al., 2011; Wallace, Lin, & Cefaratti, 2011; Werlinger, Hawkey, & Beznosov, 2009). Connecting the emergent theory to existing literature enriches the internal validity, generalizability, and theoretical level of theory building (Eisenhardt, 1989). Theory developed from case study research is likely to have significant strengths like innovation, testability, and empirical validity, which arise from the close association with empirical evidence (Eisenhardt, 1989).

Complexity Leadership Theory (CLT) is a theoretical perspective this study was based on. At its basic level, CLT is about leadership in and of complex adaptive systems or CAS (Uhl-Bien & Marion, 2009). Complexity Leadership Theory is a change model of leadership that assists management in understanding how to design robust,

dynamically adapting organizations (Uhl-Bien & Marion, 2009). Complex adaptive systems dynamics represents the self-organizing mechanisms through which complex systems develop and change their internal structure instinctively and adaptively to survive with their environment (Uhl-Bien & Marion, 2009). Information flow can occur when interacting adaptive leaders imagine and effectively advance new ideas, capabilities, opportunities, and possibilities within a dynamic context of CAS (Uhl-Bien & Marion, 2009).

The CLT theory has suggested a bottom up approach to be used to conceptualize IT use processes, in hopes to embrace the nature of technology, achieving a more holistic analysis of the active role IT plays in the entire organization (Nan, 2011). The CLT theory suggests that in recent years, more researchers have come to the realization that the uses and consequences of information technology are often created through self-orchestrated interactions among users, new available technologies, and institutional needs rather than commanded by organizational policies or management's decisions or intentions (Nan, 2011). This theory supported this study by the use of implementing information security technology by looking at what the users' needs are and looking at the information flow throughout the organization or educational institution.

The theory building process depends on past literature and empirical observation or experience as well as on the insight of the theorist (Eisenhardt, 1989). The theoretical foundation used in this study rested upon several different approaches in computer and information security implementations. Some researchers specify that the technological tools, such as the hardware and the software, are the best approaches to implementing the

needed security within the organization (Wallace et al., 2011). Other researchers have suggested that although the technological tools are important, more importantly is awareness and training of the users within the organization as to know how to look for and avoid any instances of computer and information security breaches (Chander & Kush, 2011; Fielden, 2011; Wolf, Haworth, & Pietron, 2011). Still, other researchers, such as Fielden, provided for a holistic view of information security which is an evolving dynamic system made up of the following: purpose and role of information security, changing technologies, information security management, societal trends, human elements, and interaction and complexity.

The overall goal and objectives for an information security strategy is to help organizations with its risk management in reducing the risk exposure (Kayworth & Whitten, 2010). In addition, by implementing this type of framework and theory, management may better understand the importance of the relationship between information security and risk management. However, Koskosas (2011) stated that applying risk management approaches seems inadequate in managing information security risks and generally the IT department's performance in managing risks remains limited. The data generated in this study provided a deeper understanding of the computer and information security implementations recommended by professionals working in these institutions. Other benefits of this study included an effort to share the findings of this study and could be used to help develop guidelines and/or a road map for information technology and security professionals to use at their colleges and universities or other educational related organizations.

To better understand the linkages between IT security and systems theory and how it relates to information security framework, Fielden's (2011) holistic view framework was used to support this study. Fielden has presented a holistic model of information security used as a framework that includes the following six clusters: purpose and role of information security, societal trends, human elements, changing technologies, information security management, and complexity and interactions. The basis of this theory is that information security situations and research requires various different points of views as information security has progressed from computer scientists to include politics, economics, civil society, and the individual (Fielden, 2011). Systems theory of IT is about integrating technology at various levels by both the organization and the individual and that organizational and individual benefits derived from technology are contingent upon this level of integration (Fadel, 2012).

The duality of technology model is another supporting theory that was used in this study to examine how technology is changed and put in place by the people within the organization. This model builds on previous research that found technology to be the outcome of strategic choice and social actions (Orlikowski, 1992). The duality of technology examines the interaction between technology and organizations and suggests technology is a product of human action, while it also assumes structural properties (Orlikowski, 1992). Meaning, technology is physically constructed by individuals working in a given social context but is socially constructed by individuals through different meanings they attach to it and the various features they emphasize and use (Orlikowski, 1992).

The results of this study were expected to contribute theory in the field of computer and information security. This study contributed by adding additional support to the Complexity Leadership Theory. CLT is about leadership in and of complex adaptive systems and the results of this study showed that the IT department personnel deal with the complexity of information technology and information security and need to be leaders in initiating any and all available options in order to keep data safe and confidential. This study added to theory by presenting a need of leadership that assists management in understanding how to design robust, dynamically adapting organizations. This study also contributed to the theory of Complex Adaptive Systems by showing the importance through which colleges and universities change their internal structure instinctively and adaptively to survive with their environment. In other words, to keep data safe, secure, and confidential and to allow only authorized personnel access to the data. Additionally, the results of this study contributed to the duality of technology theory which suggests technology is part of human interaction. This study presented that for the best and most optimal environments in which computer and information security is protected, there needs to be a human element in the mix and not just implementation of technological tools.

### **Research Questions**

Colleges and universities hold enormous amounts of personal information from students, parents, and employees such as income tax returns, employment history, salary, loans, credit information, admissions records, and medical files (Jones, 2008). The research questions were postulated to obtain an understanding of what a sample of IT

professionals working in IT departments in institutions of higher education warrants as being necessary to protect and secure information, resources, assets, and other data. To better understand the IT security tools, policies, procedures, and systems that are recommended by the IT personnel, the following research question was used to ascertain the IT security needs from 12 institutions of higher education which were located throughout the state of North Carolina.

**Q1.** What IT security components within academic institutions potentially contribute to improved IT security and reduce or eliminate possible information security attacks, breaches, and threats?

The research question used in this qualitative holistic multiple case study helped identify the IT security needs for colleges and universities, as perceived by a sample of IT personnel within colleges and universities. The research question was focused toward addressing the purpose of the proposed study, which was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. The results of the study may be useful for informing management of colleges, universities, and other educational institutions, the current IT security practices and, ultimately, helping to minimize the risk of IT security attacks, breaches, and threats.

### **Nature of the Study**

The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. Qualitative research for this case study included 13 volunteer participants from institutions of higher education IT

departments purposively selected from among IT personnel working in colleges and universities within North Carolina. A qualitative research method was used in this study, in which information about the experiences of currently employed IT personnel at colleges and universities was collected through conducting in-depth, face-to-face, open-ended interviews. Shank (2006) defined qualitative research as a form of systematic empirical inquiry into meaning. Qualitative data is a source of well-grounded, rich descriptions and explanations of processes in identifiable local contexts (Miles & Huberman, 1994). The use of a qualitative method is justified because of the need for in-depth information from the research participants (Patton, 2002). Because of the minimum amount of relevant research data on computer and information security implemented at colleges and universities, this study was conducted in order to discover more comprehensive information regarding the topic (Collins et al., 2011).

A qualitative research method is appropriate for this study focusing on a need for data that includes research participant's experience, knowledge, thinking, intuition, reflection, and judgment on the complex issues surrounding the unique needs of this population within an institution of higher education (Wengraf, 2001). A qualitative case study is suitable for this study because the design is used to enlighten those situations in which the intervention being evaluated has no clear, single set of outcomes (Yin, 2009). A multiple case study allows the researcher to analyze within each setting and across settings and in addition, allows the examining of several cases in order to understand the similarities and differences between the cases (Baxter & Jack, 2008). Qualitative case study issues reflect complex, situated, and problematic relationships that pull attention to

both ordinary experience and disciplines of knowledge (Stake, 2006).

This holistic multiple case study was patterned after Yin's (2009) process and procedures for conducting human science research. The steps to be included are (a) planning; (b) designing; (c) preparation; (d) data collection; (e) analyzing; and (f) results sharing (Yin, 2009). A multiple case study was appropriate for this research because case study issues reflect complex, situated, problematic relationships that pull attention to both the ordinary experience and also to the disciplines of knowledge (Stake, 2006). Stake (2006) suggests an important reason for conducting a multiple case study is to examine how the phenomenon being studied performs in different environments.

A digital recording device was used in order to capture the participant's answers and comments to the research questions. The recorded face-to-face interviews of the research participants was transcribed and then analyzed to understand results and compare responses (Patton, 2002). Field notes was taken after the interview sessions to record any descriptions of participants' actions and any other important information or happenings that came from conducting the interview session (Groenewald, 2004).

After the analysis of the data collected during the study, it was determined what critical measures of information security needs should be used in developing and implementing an information security portfolio for institutions of higher education within the state of North Carolina. This information was collected from the various IT managers and employees at different colleges and universities throughout North Carolina. Data was gathered by interviewing information technology and IT security professionals that have hands-on experience securing and supporting hardware and software applications in



their currently employed position in institutions of higher education and any previous organizations they may have been employed.

Thematic analysis was used to find themes and/or patterns in the information acquired from the participants and were used as (a) a way of seeing, (b) a way of making sense out of the data, (c) a way of analyzing information, and (d) a way of converting qualitative information into quantitative data such as word frequencies (Boyatzis, 1998). NVivo10 software was used in this case study to help identify, track, and organize frequently occurring thematic categories and patterns that emerges from the data from each case study. By conducting analyses with NVivo10 software, this increased the thoroughness of the qualitative data analysis procedures and enhanced the accuracy of the coding (Leech & Onwuegbuzie, 2011). Overlapping data analysis with data collection provided a jump start in analysis, and more importantly, allowed for full advantage of flexible data collection (Eisenhardt, 1989).

### **Significance of the Study**

The central purpose of information security is to protect the information and the data that is found on organization's networks and telecommunication channels (Koskosas et al., 2011). Information security is one of the greatest challenges facing management (Ramachandran & Ramachandran, 2012). The amount of information security attacks being experienced by organizations increase day by day (Taluja & Dua, 2012). Researchers have discovered a high number of computer and information security attacks, breaches, and threats in institutions of higher education and noted the potential costs associated with them (Meade, 2009, Kuzma, 2011). Despite a growing number and assortment of information security threats, management within many organizations

continue to neglect implementing information security policies and procedures (Jourdan et al., 2010). The significance of network and information security at institutions of higher education has been crucial for the first decade of the 21<sup>st</sup> century and leading into the second decade (Kumari et al., 2011).

The higher education industry has been quite susceptible to risks and encompasses a wealth of valuable information on millions of personal records linked to students, faculty, and alumni (Collins, Sainato, & Khey, 2011). Computer and IT security threats to educational institutions have considerably increased over the previous few years (Maskari et al., 2011). Academic institutions have become prime targets for hackers due to campuses having abundant computers, servers, and other computing resources, along with highly powered networks (Anonymous, 2010). Economic conditions, stagnant or shrinking security related budgets and a perceived lack of skilled and trained information security resources are increasing concerns for an organization's IT management (Farrell, 2010). Collins et al. (2011) reports that previous attempts to study the amount of information security breaches occurring at institutions of higher education have been inadequate. Researchers have indicated that more empirical studies are needed in order to develop and enhance the challenges of information security at academic institutions (Chang & Wang, 2011).

This holistic multiple case study was significant in several unique and different ways. First, the effectiveness of computer, network, and information security implementations for colleges and universities had yet to be explored from the position of the IT professionals working within these academic institutions. In reviewing research

on IT security, the majority of the studies focused on the needs of for-profit business organizations (Hagen & Albrechtsen, 2009; Smith, 2009; Styles & Tryfonas, 2009; Tarn, Raymond, Razi, & Han, 2009). The unique insights gathered by conducting this study provided additional, updated, and corrective needs for information security implementations for within institutions of higher education. This study investigated the various different attitudes, aspects, challenges, practices, procedures, policies, and strategies described by the participants dealing on a day-to-day basis with computer and information security at institutions of higher education.

Second, all types of security breaches are costly when dealing with computers, networks, or the information itself. Throughout the first decade of the 21st century, the importance of network security at institutions of higher education remained critical due to the numbers of breaches and costs associated with information security breaches (Kumari et al., 2011). This study helped in determining the best technical tools such as hardware and software protections, along with aiding in implementing the security awareness and training processes and procedures that will maximize returns on investment for institutions of higher education. New security threats are constantly being created and deployed by cybercriminals to exploit weaknesses that organizations have not yet discovered (Jourdan et al., 2010).

Lastly, this study contributed to the existing body of knowledge. The results of the study revealed relationships between the participants' perspectives about computer and information security for colleges and universities compared to theories described in the literature review section of this study. Other relationships was identified and noted

regarding current and related computer and information security theories (Fadel, 2012; Fielden, 2011; Kayworth & Whitten, 2010; Nan, 2011; Orlikowski, 1992; Uhl-Bien & Marion, 2009). While CLT has not been applied in the context of IT, this study made a contribution given the importance context plays in qualitative research. The research was conducted to identify the required types of IT security tools, processes, training and procedures, and other necessary items for institutions of higher education. This study extended and expanded on the literature for needed computer, information, and network securities required by colleges, universities, and various other types of academic institutions of education. The unique insights from the IT professionals actually working in the field of security at these North Carolina colleges and universities provided new and additional insights and information regarding further research needed in this area. Results from this study will influence future research within areas of educational institutions such as budgeting and information security and whether there is a correlation, risks associated with different levels of information security implemented, and costs associated with computer and information security attacks, breaches, or threats within academic institutions of higher education.

### **Definition of Key Terms**

The following terms are essential to the topic of computer and information security as well as the effective use of security methods, tools, procedures, and training or on the research on the topic. Definitions clarify commonly misunderstood terms used in unique ways within this study. Any terms without citations were defined based on related terms and knowledge acquired from work experience.

**Access control lists.** An access control list is a security safeguard that is applied

to an object or a list of employees allowed to access a computer resource and determines what functions a user can perform (Katzan, 2010).

**Access control policy.** An access control policy is a document explaining aspects of an organization's access policies regarding information technology usage (Katzan, 2010).

**Attacks.** An intentional or unintentional act to take advantage of a vulnerability to compromise information or a system (Whitman & Mattord, 2012).

**Authentication.** Authentication is the system, processes, and procedures of confirming the identity of a user logging into a computer network by using passwords, digital certificates, smart cards, and biometrics (Murray, 2010).

**Bastion host.** A bastion host is a dedicated firewall or computer used to prescreen data coming into the organization's network and is usually open and exposed to attack (Ahamed, 2010).

**Breach incident.** An information security breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an unauthorized individual (Whitman & Mattord, 2012).

**Bring-your-own-device (BYOD).** BYOD is where employees and others in an organization are bringing and using their personal mobile devices such as laptops, tablets, and smartphones versus using organization supplied devices (Patten & Harris, 2013).

**Business continuity planning.** Business continuity planning includes specific processes and procedures that guide organizations in preparing for disruptive events (Omar, Alijani, & Mason, 2011).

**Cryptography.** Cryptography is the science of writing in secret code used to not only protect data from theft or alteration, but also can be used for user authentication (Guynes, Wu, & Windsor, 2011).

**Contingency planning.** A contingency plan is a plan implemented to help management of an organization to better handle different situations to reduce losses and help to ensure safe and stable operation of a network system (Ma, Zou, & Li, 2011).

**Cybercrime.** Cybercrime is a term commonly used to describe fraudulent activities and crime committed using the Internet (Figg, 2008).

**Data custodian.** A data custodian is an employee responsible for the storage, maintenance, and protection of the organization's information (Morris, Tuttle, & Essic, 2009).

**Denial-of-service (DoS).** A denial-of-service refers to attacks that prevent authorized users from accessing system resources by overloading or crashing the computer system or network (Rudman, 2014).

**Disaster recovery planning.** Disaster recovery planning focuses on technology recovery in the event of a disaster (Nollau, 2009).

**Dumpster diving.** Dumpster diving involves digging through trash dumpsters or bins to find recording media that may hold valuable information (Figg, 2008).

**Encryption.** Encryption is the process of converting an original message into a form unreadable by unauthorized persons (Zhou, Zhang, Wei, & Zhou, 2010).

**Enterprise information security policy.** An enterprise information security policy is a document that provides the strategic direction, scope, and tone for an

organization's security efforts (Xing, Xue, & Li, 2010).

**Firewall.** A firewall is a host that intercedes access to a network, allowing and prohibiting certain types of access on the basis of a pre-configured security policy (Surisetty & Kumar, 2011).

**Hackers.** Hackers are individuals who attempt to gain unauthorized access to information systems, networks, and/or other resources (Warren & Leitch, 2010).

**Incident response plan.** An incident response plan is a documented procedure to assist in dealing with a security incident that can include but is not limited to unauthorized access, malicious code, network probes, and denial of service attacks (Liu & Ormaner, 2009).

**Information security.** Information security is the protection of data and other information from unauthorized observation, modification, or interference (Sehgal et al., 2011).

**Information technology (IT).** Information technology enables the storage and transportation of information from one organizational unit to another (Whitman & Mattord, 2010).

**Information technology (IT) personnel.** Information technology personnel are those technology professionals that support the organizational objectives of the organization by supplying and supporting information technology (Whitman & Mattord, 2010).

**Intrusion.** An intrusion is a deliberate unauthorized attempt to break in, manipulate or misuse any type of valuable property (Jonnalagadda & Mallela, 2011).

**Intrusion detection system/software.** An intrusion detection system or software looks for unauthorized Internet users and includes necessary tools to monitor critical networks, identify attacks or intrusions, and take immediate corrective action (Liu & Ormaner, 2009).

**Malware (malicious logic/software).** Malware or malicious logic/software is a set of instructions that cause a website's security policy to be disrupted (Lazovic & Simic, 2011).

**Network security.** Network security involves the safeguarding of an organization's data networking devices, connections and contents, and the ability to use the network to achieve the organization's data communication tasks (Chen, Kataria, & Krishnan, 2011).

**Phishing.** Phishing is a scam by which someone fraudulently obtains and uses a person's personal or financial information by cheating users to provide this information (Lungu & Tabusca, 2010).

**Risk management.** Risk management consists of the identification of risks or threats, the application of security measures, and monitoring of those measures for effectiveness (Saleh, Refai, & Mashhour, 2011).

**Safeguard.** A safeguard is a security mechanism, policy, or procedure that can effectively counterattack, reduce risk, resolve vulnerabilities, and normally improve the security of an organization (Anderson & Agarwal, 2010).

**Security management.** Security management is the operational activities, posture, and compliance requirements as it related to computer security (Enescu, Enescu,



& Sperdea, 2011).

**Security threat.** A security threat is a condition of vulnerability that may lead to an information security being compromised (Issa-Salwe & Ahmed, 2011).

**Security countermeasure.** A security countermeasure refers to a process or method used to expose, stop, or reduce losses associated with specific information security threats (Issa-Salwe & Ahmed, 2011).

**Spyware.** Spyware refers to a type of Trojan software that monitors activity and collects information on the targeted computer information system (Gurung, Luo, & Liao, 2009).

**Virus (computer).** A computer virus is a destructive, sometimes viscous, self-replicating computer code that can infect computer files, systems, and networks (Ou, 2013).

**Vulnerability management.** Vulnerability management includes each element of the IT infrastructure being systematically managed for vulnerabilities and security risks (Liu & Ormaner, 2009).

### **Summary**

From 2008 until 2011, computer and IT security threats to educational institutions have considerably increased (Maskari et al., 2011). Economic conditions, stagnant or shrinking security related budgets and a perceived lack of skilled and trained information security resources have increased concerns for an organization's IT management (Farrell, 2010). Information security has been a major concern for institutions of higher education because hackers are targeting colleges and universities to steal computing resources, property, and data (Perkel, 2010). Ma, Schmidt, and Pearson (2009) have found that

organizations should develop a framework that outlines the separate components of IT security and what each component entails. Research studies in IT security by Ransbotham and Mitra (2009) suggested the need for IT management in organizations to implement multiple sources of IT security such as technological tools, proper user training programs, and gain support from top management to better deal with IT security issues.

The problem addressed in this qualitative holistic multiple case study is the increase in information security breaches impacting institutions of higher education (Ayyagari & Tyks, 2012; Collins et al., 2011; Perkel, 2010; Susanto, Almunawar, Tuan, Aksoy, & Syam, 2011). There is a gap in the literature regarding IT security requirements for colleges and universities where there have been too few researchers studying actual data on organizational data breaches within the past three years (Collins et al., 2011). Researchers have found IT security an important concern for organizations, but very few have focused on the specific needs of a college or university which leads to the specific problem of that due to increases in IT security breaches in educational environments, researchers have recommended that the needs of colleges and universities for the improvement of IT security be explored in more depth (Abbas et al., 2011; Fisher & Shorter, 2013; Guo, Yuan, Archer, & Connelly, 2011; Ma, Schmidt, & Pearson, 2009; Mensch & Wilkie, 2011; Werlinger, Muldner, Hawkey, & Beznosov, 2010).

In order to obtain a deeper understanding of the unique needs of information security within institutions of higher education, qualitative research in the form of a holistic multiple case study with 13 participants was conducted. A qualitative research

method was used in the study, in which information about the experiences of currently employed IT personnel at colleges and universities across the state of North Carolina was collected through conducting in-depth, face-to-face, open-ended interviews. Qualitative data, such as that obtained through a qualitative multiple case study, is a source of well grounded, rich descriptions and explanations of processes in identifiable local contexts (Miles & Huberman, 1994). For data measurement to be most meaningful, research participants cannot have data gathering instruments that impose on them a perspective based on the researcher's preconceptions (Fisher & Stenner, 2011).

## Chapter 2: Literature Review

The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. This study offered the recommended computer and information security strategies, tools, policies, procedures, and systems that IT security professionals would implement at their college or university. Chapter 2 contains the literature review presentation of the research study. The goal of the literature review was to present and discuss related issues and findings of previous studies pertinent to this study.

This focus of this study was to collect the best of IT security based tools, practices, processes, procedures, and systems that should be implemented at academic institutions in order to increase information security and decrease attacks, breaches, and threats. Personnel working in the IT departments of colleges and universities within the state of North Carolina were chosen for this study. This literature review highlights the areas included in recent computer and information security principles, applications, tools, systems, and theories. It is organized into the following seven sections: general concern for information security, information security and importance, information security statistics, management's concerns for IT security, analysis of the risks associated with security breaches, information security awareness and training, and concludes with a summary of the literature review. These themes and generalizations were important to the literature review. The literature review is an important part of conducting research and examining theories and explanations of the research topic.

## **Documentation**

The strategy used to create the literature review began with the examination of the problem and the purpose of the proposed research. Several key words were identified and noted as relevant to the goals of the study. These key words lead to the development and organization of the literature review. Seminal and scholarly books, journal articles, and other research documents were reviewed through the Northcentral University library, and other online publication websites. These books, articles, and peer-reviewed content from the past several years were evaluated as well as other writings pertinent to the proposed study. The search strategy included the utilization of several databases, such as ProQuest, EBSCOhost and Google Scholar, to discover past and current research on the unique needs of IT security at institutions of higher education.

A literature review is a means of demonstrating an author's knowledge about a certain field of study and should provide a foundation for understanding a phenomenon prior to conducting a research study (Randolph, 2009). It is recommended that an author be cautious and avoid developing literature-induced preconceptions regarding what the research may reveal, which could impede research impartiality (Corbin & Strauss, 2007). The researcher should take into consideration what is learned within the literature, though it should not be the only basis for developing an entire conceptual framework (Randolph, 2009).

## **The Need for Computer, Network, and Information Security**

As of the start of the second decade of the 21<sup>st</sup> century, the significance of network and information security at institutions of higher education has been a crucial concern (Kumari et al., 2011). Information security threats require a more responsive and

defensive information security system (Taluja & Dua, 2012). The higher education industry has been quite susceptible and encompasses a wealth of valuable information on millions of personal records linked to students, faculty, and alumni (Collins et al., 2011). Computer and IT security threats to educational institutions have considerably increased over the previous few years (Maskari et al., 2011). Academic institutions have become prime targets for hackers due to campuses having abundant computers, servers, and other computing resources, along with highly powered networks (Anonymous, 2010). New security threats are constantly being created and deployed by cybercriminals to exploit weaknesses that organizations have not yet discovered (Jourdan et al., 2010).

In 2012, the numbers of information security attacks are increasing daily and represent a necessity to take appropriate actions and steps in order to safeguard the organization (Taluja & Dua, 2012). In spite of an increasing amount and variety of information security threats, IT management continued to neglect implementing information security policies and procedures (Jourdan et al., 2010). Information and other assets in organizations are subject to an increasing range of attacks, threats, and vulnerabilities (Beebe & Rao, 2010). This important information and valuable assets must be protected in order to avoid the loss of confidentiality, integrity, and availability (Alwi & Fan, 2010). Confidentiality ensures computer related assets are accessed by authorized users only, where integrity assures that data cannot be modified by unauthorized users and availability ensures that assets and data are accessible to authorized users at appropriate times (Kruger, Drevin, & Steyn, 2010). By thwarting unauthorized access, organizations can attain greater confidence in data and system

integrity (Zissis & Lekkas, 2012). Any loss or leakage of information can not only cause a huge financial loss but also a loss of credibility, therefore keeping data, information, knowledge, and other assets is a big concern for all types of organizations (Chander & Kush, 2011). Individuals are put at direct risk of harm by criminals when their personal and confidential information is not secured appropriately (Gillon et al., 2011).

Cyber-attacks can be categorized into targeted attacks and untargeted attacks, where targeted attacks are designed to damage a specific communication system or an organization's information assets (Shim, 2012). Untargeted cyber-attacks are aimed at many potential victims, hoping to contaminate as numerous computer and network systems as possible (Shim, 2012). Even when management has implemented firewalls, virus protection software, intrusion detection systems, and other more advanced technologies, the organization's computers, networks, and information are not completely safe (Jourdan et al., 2010). Events, such as information security breaches, have a wide-ranging negative impact on organizations (Zafar, Ko, & Osei-Bryson, 2012). As displayed in Table 1, there are various different types of information security threats to be aware of. Security issues can be classified into: system availability, which means that all available components are available to support users' requirements; data integrity, which means that information, is not altered in a way to make it invalid; and data privacy, which means that information, is seen only by their intended audience (Guynes, Wu, & Windsor, 2011).

Table 1

*Computer and Information Security Threats*

---

Type	Examples
Deliberate Software Attacks	Viruses, Worms, Macros, Denial of service
Technical Software Failures/Errors	Bugs, Coding problems, Unknown loopholes
Acts of Human Error/Failure	Accidents, Employee/User mistakes
Deliberate Acts of Espionage/Trespass	Unauthorized access and/or data collection
Deliberate Acts of Sabotage/Vandalism	Destruction of information or systems
Technical Hardware Failures/Errors	Equipment failure
Deliberate Acts of Theft	Illegal confiscation of information or equipment
Compromises to Intellectual Property	Piracy, Copyright infringement
Quality of Service Deviations from Service Providers	Power and WAN service issues
Technological Obsolescence	Antiquated or out-of-date technologies
Deliberate Acts of Information Extortion	Blackmail for information disclosure

*Note:* Adapted from “E-Learning and Information Security Management,” by N. Alwi and I. Fan, 2010, *International Journal of Digital Society (IJDS)*, 1, pp. 151-152. Reprinted with permission.

Information security breaches are usually classified into certain categories depending on what type of breach it is or the effect it has. The following categories are typically used: breaches of information confidentiality, which are breaches that allow unauthorized users access to confidential information; breaches connected to information availability, which are breaches that prevent authorized users of information to have access to such information; and breaches of information integrity, which are breaches that



compromise the reliability and/or validity of a database (Gordon, Loeb, & Zhou, 2011). Other IT professionals categorize with different terminology, but the end result is close to being the same. New types of security breaches and vulnerabilities exist with the increasing use of Web 2.0 applications such as collaboration and communications to social media websites (Almeida, 2012).

### **Importance of Computer, Network, and Information Security**

The number one objective of information security is to protect information and specifically, the integrity, confidentiality, authenticity, and availability of data through an organization's network (Koskosas et al., 2011). Information security has been one of the greatest challenges facing management (Ramachandran & Ramachandran, 2012).

Management of organizations should be aware of the importance of computer and information security policies and refining these policies or creating new ones as new threats emerge (Anand et al., 2012). The information security environment have been continuously evolving and new threats to an organization are emerging frequently (Kolb & Abdullah, 2009). Understanding the amount of information stored in databases, the increasing use of wireless and other technologies, and the importance of keeping data out of the hands of unauthorized individuals all contribute to the awareness that management need to implement the technical and nontechnical controls such as procedures, processes, training, technologies, systems, and strategies concerning computer and information security (Abbas et al., 2010; Wallace et al., 2011; Werlinger et al., 2009). Changing information security requirements is of substantial importance due to the fact that organizations must simultaneously provide information to their employees, customers,

business partners, and governmental entities while protecting it from inappropriate access, use, and disclosure (Cline, Guynes, & Nyanoga, 2010).

A number of studies have reported incidents where critical information has been compromised and this reason continues to create an increasing interest to study information security (Koskosas et al., 2011). Computer and information security, in the first decade of the 21<sup>st</sup> century, have attracted the attention of researchers, professionals, journalists, legislators, governments, businesses, organizations, and citizens (Jourdan et al., 2010). Justifiably, security breaches draw tremendous attention, nonetheless it is difficult to calculate the exact amount of damages or losses caused by them (Shim, 2012). This negative publicity should increase awareness and drive IT management to invest in computer and information security, but many IT professionals encounter major difficulty in convincing management to invest in security projects (Jourdan et al., 2010). Based on published literature on IT security requirements, there has been a general consensus for each IT manager to include certain and specific IT security requirements (see Appendix E) (Kimwele, Mwangi, & Kimani, 2011).

The development of computer networking, through the use of the Internet, has changed the stand alone method of computing and has also increased the risk and opportunity of networks being breached (Folorunso, Akinwale, & Ikuomola, 2010). Computer and information security awareness has been an essential issue that IT management as well as all persons should be concerned with as data is transported around the world (Chen, Medlin, & Shaw, 2008). Technological controls and solutions are effective after users are familiar and skilled at using them; therefore, computer and

information security awareness can be more significant than the technology itself in certain circumstances and situations (Chen et al., 2008).

Advances in technology have changed the way IT leaders work with computer and information security within organizations (Goyal, 2012). Areas of technology management include content management, data management, information access, meeting legal requirements, privacy issues, accountability, user training, employee penetration/manipulation, outside hackers, and disaster recovery (Smith, Koohang, & Behling, 2010). Most leaders within IT departments tend to focus more on the technical controls/issues of IT security that include the policies and explicit tools that can be implemented within the business environment but lacks nontechnical controls/areas of education, training, and contingency planning (Wallace et al., 2011).

### **Management's Concern for IT Security**

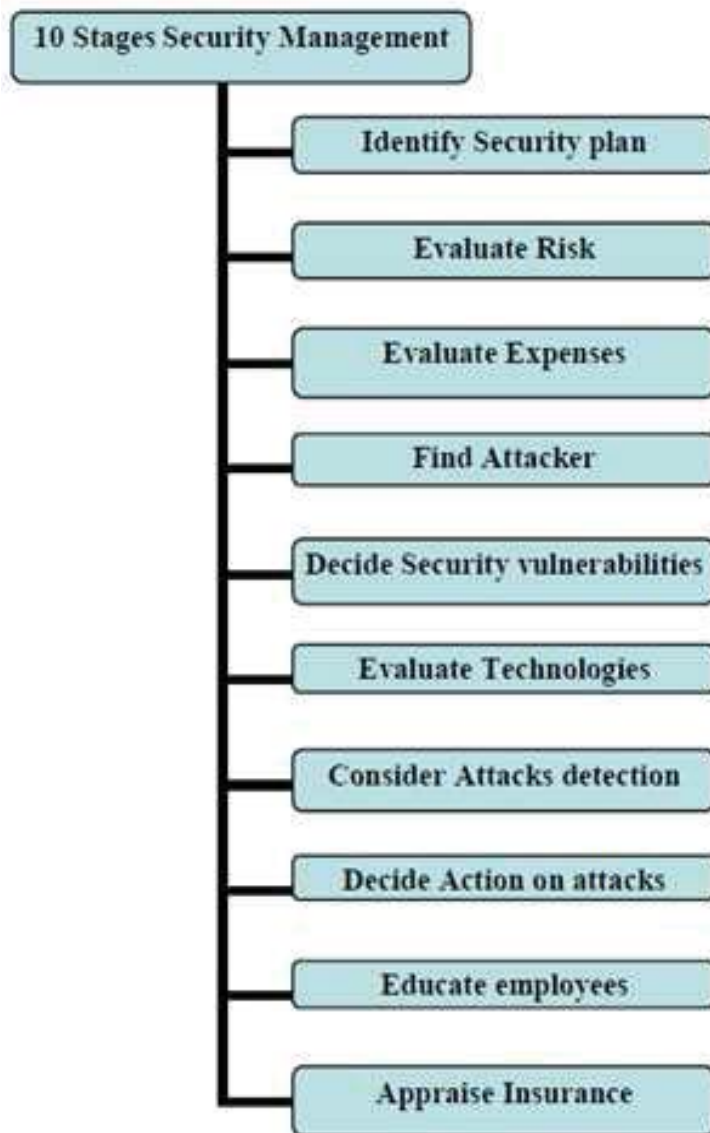
Management has articulated less confidence about future information security concerns, noting that security incidents are increasing both in terms of number and complexity (Koskosas et al., 2011). Dramatic changes in the complexities of information systems, connectedness, and economic value have been reasons to the increase in security concerns (Ransbotham, Mitra, & Ramsey, 2011). Attacks on the network computing systems could be devastating and negatively affect the entire organization (Reddy & Prasad, 2012). Securing the IT infrastructure and the data contained therein is one of the most crucial and critical components of managers of IT (Luftman & Zadeh, 2011). Weaknesses are still apparent on the technical side (technical controls) of IT security and many organizations lack certain nontechnical controls such as security policies,

procedures and training (Herath & Rao, 2009b). Implementing new information security objectives often is interpreted by upper-level management as an unnecessary expenditure or a decision that can be put on hold (Saleh, 2011). In order to produce valuable, relevant information security plans, the information security manager must understand the objectives and strategies of the organization in order to create information security plans that fit the organization (Young & Windsor, 2010). The Sarbanes-Oxley Act of 2002 was passed to focus management on the importance of internal controls and how management is responsible for implementing information security controls to promote reliability and integrity (Walters, 2007).

One of the most critical steps in the information security planning process is obtaining top management support because it is through this support that acknowledgment of the importance of information security planning is communicated throughout the organization (Young & Windsor, 2010). Information security has changed greatly over time in recognizing the importance and the need for an organization's IT management to have security related plans, procedures, systems, and strategies in place (Wolf et al, 2011). Management is creating contingency plans to prepare for events that may cause an interruption in operations (Ologunde, & Akinlolu, 2012). Contingency plans help management prepare for unexpected events and can consist of major areas which include a business impact/risk analysis, an incident response plan, a disaster recovery plan, and a business continuity plan (Omar et al., 2011). Management in various organizations began to increase their investments in information security by continually adapting and implementing a variety and more diversified

security solutions (Shim, 2012).

Problematic issues are unavoidable in the twenty-first century, but it does not mean solving them is impossible (Khodarahmi, 2009). A number of existing security models, security methods, countermeasures and security metrics are unable to provide adequate protection (Chander & Kush, 2011). More than ever before, anticipating the future is imperative and therefore, critical for management to identify and analyze the available situations susceptible to risks (Pearce, Zeadally, & Hunt, 2010). Management should examine the areas of potential risk, the probability of an event taking place, the potential level of disruption, impact on employees and customers, and the financial impact of interrupted operations (Khodarahmi, 2009). According to Amancei (2011), there are certain methods management can implement in order to reduce risk associated with any type organization: (a) implementation of security controls, (b) improving procedures, (c) changing the environment by reducing exposure to vulnerabilities, (d) implementation of early detection methods to catch a threat when it happens and to reduce potential damage that this may cause, (e) update continuity plan to address how the organization can continue if a specific threat appears, and (f) security awareness training sessions where and when applicable. Security management can be broken down into 10 separate and distinct stages as shown in Figure 1 (Tyagi & Srinivasan, 2011).



*Figure 1.* Ten Stage Security Management Strategy Model. Adapted from “Ten-Stage Security Management Strategy Model for the Impacts of Security Threats on E-Business,” by N. Tyagi and S. Srinivasan, 2011, *International Journal of Computer Applications*, 21, p. 3. Reprinted with permission.

To ensure data remains protected, scholars in the field use information security metrics to create, implement, and improve security systems to keep data safe not only when it is stored, but also when it is being transmitted or received over a network or the

Internet (Chander & Kush, 2011). Phishing is one of the most important threats for both individuals and organizations and has been found that on any given day, the average amount of phishing attempts world-wide are approximately 8 million (Lungu & Tabusca, 2010). As shown in Table 2, IT management must be aware of the various types of security incidents and the end-effects of each and the cause to the organization (Shirtz & Elovici, 2011).

Table 2

*Security Incidents and End-Effects*

Incident	End-effects
Virus and malware	Performance degradation, servers or workstation damage, information leakage
Financial fraud or phishing	Financial loss, information leakage
Laptop/mobile device theft or loss	Information leakage, information lost
Telecom fraud, spyware	Financial loss, information leakage
Bots	Information leakage, performance degradation, systems damage
Unauthorized access (inside or outside)	Information leakage, financial loss, reputation loss, network and systems damage
System penetration	Information leakage, financial loss, reputation loss, network and systems damage
Spam mail	Performance degradation

*Note:* Adapted from “Optimizing Investment Decisions in Selecting Information Security Remedies,” by D. Shirtz and Y. Elovici, 2011, *Information Management & Computer Security*, 19, p. 105. Reprinted with permission.

The attention given to computer and information security theory has developed greatly and has included increasingly complex issues and increased exposure to attacks (Issa-Salwe & Ahmed, 2011). This theory has grown from using very few technical controls/tools to an entire company-wide approach to protecting information, assets, and resources. Interest has turned to social and organizational factors that may have an influence on information security development and management (Koskosas et al., 2011b). Information security management has developed into being a part of the organization’s overall comprehensive framework (Saleh & Alfantookh, 2011). To better prepare for the challenges of securing information, IT management has developed organizational structures and operational procedures surrounding technology (Cline, Guynes, & Nyanoga, 2010). Managing this technology and securing information is a crucial strategic objective (Smith et al., 2010). This philosophy is important because information has become and continues to be the lifeblood of modern organizations (Smith et al., 2010).

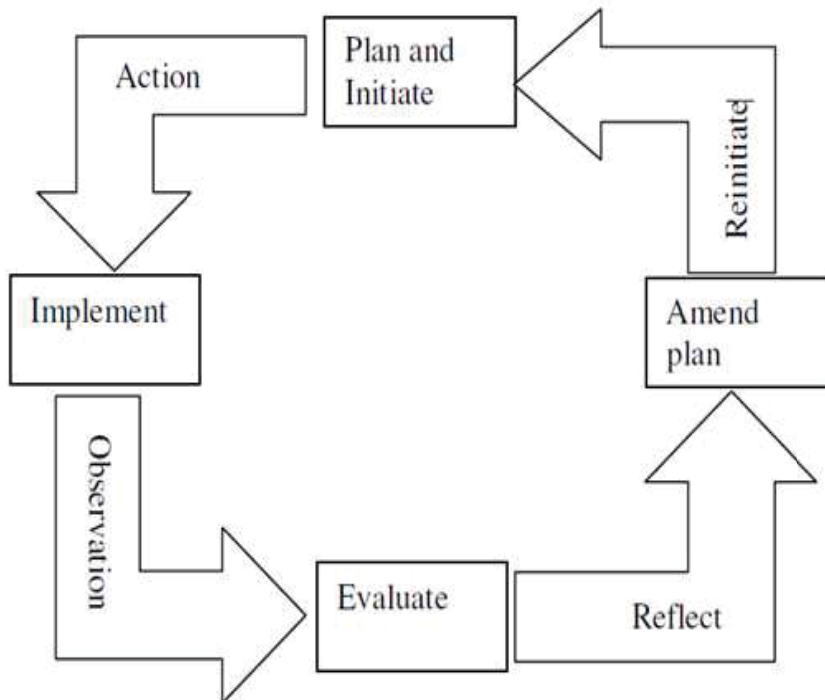
Information technology managers across various organizations are periodically surveyed and asked to select the most important technology issues they are facing (Luftman & Zadeh, 2011). According to Smith et al. (2010), the top five concerns for IT managers are privacy issues, data management, meeting legal requirements, hackers, and information access. Five other concerns of IT professionals are content management, accountability, disaster recovery, employee penetration, and staff training (Smith et al.,



2010). What is unique about this empirical study is that most of the top areas of concern have something relating to computer, network or information security. Many of these concerns are not only the responsibility of IT managers, but also the responsibility of all employees in the organization (Spears & Barki, 2010).

Thirty-two information security professionals across a diverse set of organizations were asked to identify if their organization's management or audit team regularly conducts some type of information security risk analysis (Jourdan et al., 2010). Additionally, the researchers of this study wanted to learn about the analysis organizations undergo to allocate their security resources (Jourdan et al., 2010). Organizations that do not take advantage of using multiple methods of information technology to assist in being competitive are actually allowing their organizations to become less competitive due to increased vulnerabilities (Fielden, 2011). Security professionals responded by listing financial losses, risks to infrastructure, legal and regulatory requirements, and damage to the organization's brand or image as the top four factors of risk analysis (Jourdan et al., 2010).

The IT management/staff must be constantly aware of new risk potentials and how to effectively reduce and eliminate their danger to the organization (Benson & Rahman, 2011). It is important that management take a proactive approach in providing a reasonable, cost-effective framework using risk management as the basis for securing the information system (Issa-Salwe & Ahmed, 2011). For an information security program to be effective, it must be evaluated on a regular basis and updates and revisions implemented as shown in Figure 2 (Kimwele, Mwangi, & Kimani, 2011).



*Figure 2. Information Security Awareness Program Lifecycle. Adapted from “Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs),” by M. Kimwele, W. Mwangi, & S. Kimani, 2011, *International Journal of Computer Science and Security (IJCSS)*, 5, p. 49. Reprinted with permission.*

### **Analysis of Risks Associated With Security Breaches and Risk Management**

Risk analysis on information security is essential in many organizations (Amancei, 2011). Information security risk management is a crucial element in ensuring long-term organizational success (Anand et al., 2012; Fenz, Ekelhart, & Neubaur, 2011). Risk analysis can be defined as the process that management takes to examine threats facing their IT assets and weaknesses of those assets (Jourdan et al., 2010). Information security is implemented in order to ensure business continuity and to accordingly minimize business risk (Alwi & Fan, 2010). Most information security professionals have used certain types of risk analysis or risk management as a tool to justify the cost of

security controls as well as investing in new information technologies (Jourdan et al., 2010). Balancing risk and cost is part of the management process of the IT personnel (Benson & Rahman, 2011). As revealed in Table 3, a measure of an effective security policy is one that begins with an evaluation of the potential security risks as well as an overall risk management assessment (Anand et al., 2012; Beebe & Rao, 2010).

Table 3

*Traditional Risk Management Process*

Steps	Description
Asset Identification and Classification	Determine what the organization needs to protect and to what extent.
Threat Identification and Classification	Determine who and what represent risks to those assets.
Vulnerability Identification and Classification	Determine the organization's weaknesses and how they relate to assets from Step 1 and threats from Step 2.
Risk Assessment	Quantitatively or qualitatively determine the risk of each vulnerability (considering asset value, threat probability, loss estimates, and vulnerability exposure).
Controls and Countermeasures Identification	Design preventative solutions (controls) to mitigate risks to the extent deemed desirable/acceptable, considering cost and operational impact.
Controls and Countermeasures Implementation	Put controls in place institutionally.
Re-evaluation	Continually examine the effectiveness of current controls and reconsider changes to mission, assets, threats, and vulnerabilities to identify appropriate changes.

*Note:* Adapted from "Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process," by N. Beebe and V. Rao, 2010, *Communications of the Association for Information Systems*, 26, p. 332. Reprinted with permission.

Managers who are serious about defending their organization's information need to ensure that an in-depth organizational information security risk analysis is being conducted (Jourdan et al., 2010). The IT management team must always be familiar of inerrant security threats from inside and outside the organization while mitigating the possible threats with an incidence response plan, a disaster recovery plan, and a continuance plan which documents and enforces policies among all personnel (Benson & Rahman, 2011). Even though management has seen firsthand how important this part of the contingency planning is, security incident response is still in its early stages (Werlinger et al, 2009). The incident response plan includes a comprehensive set of processes and procedures that anticipate, identify, and mitigate the effects of an unforeseen incident that might compromise information resources and assets (Liu & Ormaner, 2009). Moreover, management of organizations do not have adequate incident response plans in place, and those that did, reported plans had not been regularly updated (Hurley-Hanson & Giannantonio, 2009).

The next part of the contingency plan is the disaster recovery plan. Information technology disaster recovery planning is the set of procedures which IT management follow in order to improve their ability to resume IT services following a disaster (Kadlec & Shropshire, 2010). To help alleviate the effect of security threats, information security management is a very essential part of a successful organization's strategic plan (Ma et al., 2009). Information security management needs to hold themselves accountable for updating and implementing the necessary requirements to protect the organization and

related stakeholders (Abbas et al., 2010). The use of best practice guidelines, information security standards, and expert knowledge can support management in the risk assessment and numerous challenges of IT security management, but a great amount of investment in time and money is required (Fenz et al., 2011; Werlinger et al., 2009).

The last area of contingency plans is business continuity plans. Business continuity plans are action plans, complete with tools and resources needed to continue the processes necessary to keep an organization operating after a disruption (Sobel, 2009). This type of plan is an ongoing process that must develop with the organization and its environment (Sobel, 2009). Having and updating a business continuity plan can help organizations lessen operational losses in the event of a catastrophe or serious disruption (Sobel, 2009). The business continuity plan is a broader plan that covers all aspects of the organization including process, technical, physical, human, and focuses on keeping the organization viable in the event of a disaster (Nollau, 2009). As a result of there being no such thing as a perfect security, every organizations management team must identify the value of the information assets within the organization and determine an acceptable level of risk (Young, 2010).

Goal setting is a significant, central, and integral part of the process at the stage of risk planning and risk management (Koskosas et al., 2011). The decisions management makes are which risks to mitigate, to what extent, what types of countermeasures to employ, and to what cost, are all strategic in nature (Beebe & Rao, 2010). Risk analysis can be a straightforward methodology that follows certain stages that include asset identification/valuation, threats assessment, vulnerabilities assessment, existing/planned

safeguard assessment, and risk management (Jourdan et al., 2010). Table 4 presents the critical phases the IT management team needs to put in place in order to prepare for risk management as it relates to information security.

Table 4

*The Goal Setting Process*

Phases and Steps	Description
<b><u>1st Phase: Project initiation phase</u></b>	
<b>Step 1:</b>	Selection of members for the project team
<b>Step 2:</b>	Explanation of the method to the members of the team and planning of the 'security risk activities'
<b>Step 3:</b>	Physical security (external)
<b>Step 4:</b>	Control of users' activities into networks
<b>Step 5:</b>	Systems security (internal)
<b><u>2nd Phase: Execution phase</u></b>	
<b>Step 1:</b>	Identification of risks
<b>Step 2:</b>	Pre-selection of identified risks
<b>Step 3:</b>	Final risk identification and selection via a joint security project management group meeting
<b>Step 4:</b>	Control and Security
<b>Step 5:</b>	Risk monitoring
<b><u>3rd Phase: Evaluation phase</u></b>	
<b>Last Step:</b>	Compiling a security management evaluation report

*Note:* Adapted from "A Model Performance to Information Security Management," by I. Koskosas, K. Kakoulidis, and C. Siomos, 2011, *International Journal of Business and Social Science*, 2, p. 49. Reprinted with permission.

Information provided by Jourdan et al. (2010) in a qualitative and quantitative based study in which 32 Certified Information Systems Security Professionals were asked what risk factors they

consider or take into account the most when planning their respective information security strategies. Table 5 lists the most common factors and each percentage accordingly. Considering the dangers and expenditures associated with security incidents, it is critical for management to take this risk analysis process seriously in order to secure their valuable information assets (Jourdan et al., 2010). One very interesting point found in this study is that several of the security professionals indicated that they used insurance to protect their information assets.

Table 5

*Risk Factors by Percentages*

When developing risk factors for your organization's risk analysis, which factors does your organization focus on the most?

Risk Factors	Yes	No
Legal, regulatory, or statutory requirements	78.13%	21.88%
Loss of consumer confidence	75.00%	25.00%
Damage to organization's image/brand	78.13%	21.88%
Financial losses	93.75%	6.25%
Risks to infrastructure	81.25%	18.75%
Risks of possible lawsuits	71.88%	28.13%
Business requirements for information confidentiality, integrity, and availability	75.00%	25.00%
Other	25.00%	75.00%

*Note:* Adapted from "An Investigation of Organizational Information Security Risk Analysis," by Z. Jourdan, R. Rainer, T. Marshall and F. Ford, 2010, *Journal of Service Science*, 3, p. 38. Reprinted with permission.

### **Information Security Awareness and Training**

The goal of information security awareness should be to achieve a long term embrace in the attitude of employees towards security, while encouraging a cultural and



behavioral change within an organization (Susanto & Almunawar, 2012). Constructive behavior by end users and IT system administrators can improve the effectiveness of information security (Koskosas et al., 2011b). Security awareness consists of disseminating accurate, current, and appropriate knowledge of policy to individuals explaining to them the threats they need to be aware of as well as the appropriate actions to take upon encountering a threat (Wolf et al., 2011). Organizational networks are exposed to a wide variety of information security threats (Reddy & Prasad, 2012). Investing significant resources into implementing different technologies or technical controls designed to protect both data and the IT infrastructure from threats are necessary and serve a valuable role in protecting information, but alone they are inadequate (Jourdan et al., 2010). Becoming too reliant on one security element, such as security technologies, can place the organization at risk due to the large percentage of security breaches that are results of other areas or weakness such as error in human behaviors (Fielden, 2011). Table 6 includes the most common computer and information security threats found in a study by Perimeter E-Security (Jo, Kim, & Won, 2011).

Table 6

*Top 10 Computer and Information Security Threats for 2010*

Top 10	Security Threat
1	Malware of many methods to install malware on systems, including the use of client-side software vulnerabilities
2	Malicious insiders who expose critical information of an organization
3	Exploited vulnerabilities such as data breaches, worms, viruses, malware, and a host of other attack types
4	Careless employees who are duped or fall prey to social engineering type attacks and malicious employees
5	Mobile devices such as iPhone and laptop that exposed sensitive data because of stealing, public disclosure, or iPhone worm
6	Social networking such as Facebook, MySpace, Twitter and others have changed the way people communicate with each other but that can be grounds for SPAM, scams
7	Social engineering by cyber criminals and phishing is a popular method for doing just that
8	Zero-day exploits to compromise a system based on a known vulnerability but no patch or fix exists, and it has become a very serious threat to information security
9	Cloud computing security threats such as abuse and nefarious use, malicious insiders, and data loss and leakage
10	Cyber espionage to act obtaining secrets without the permission of the holder of the sensitive information

*Note:* Adapted from “Advanced Information Security Management Evaluation System,” by H. Jo, S. Kim and D. Won, 2011, *KSII Transactions on Internet and Information Systems (TIIS)*, 5, p. 1203. Published by Perimeter E-Security. Reprinted with permission.

Earlier research studies examining security awareness effectiveness has shown inconclusive results (Wolf et al., 2011). One theory within the research of computer and information security is the user's effectiveness in protecting information (Shropshire, Warkentin, & Johnston, 2010; Lacey, 2010; Kimwele, Mwangi, & Kimani, 2011). Often, the people working in the organization are considered to be the final and most important line of defense when dealing with information security (Benson & Rahman, 2011). The occurrence of information security breaches caused by internal users may be reduced if greater emphasis were placed on threats to information security that can occur when employees handle information in their day-to-day activities (Spears & Barki, 2010). Most users within the university are unconscious about information security (Kumari et al., 2011). The theory of utilizing end users as a line of defense is something management should contemplate using as a part of the overall information security strategy (Spears & Barki, 2010).

This theory is extremely beneficial for management to consider as a recent survey of 2,100 IT security administrators found that employees rarely consider organizational security threats in their everyday business communications (Steffee, 2010). The 2,100 IT security professionals explained that employees tend to ignore IT security threats when downloading Internet applications, browsing the Web, clicking on and opening links, streaming videos, using peer-to-peer file sharing sites and engaging in social networking sites (Steffee, 2010). Many experienced security experts emphasize the fact that employees within an organization are generally considered to be the weakest link in the information security chain (Benson & Rahman, 2011).

Part of this theory embraces the idea that users may not fully understand what they should do to implement security processes (Lacey, 2010). Employees do not always know what to look for in their day-to-day activities concerning the aspects of information security (Hagen & Albrechtsen, 2009). Numerous employees face the task daily to prevent security breaches within the systems and networks that sometimes exceed their level of understanding and knowledge (Shropshire et al., 2010). In order to for management to properly implement nontechnical controls such as a security policy, it must first be developed, analyzed, tested, and taught to every employee as this can have a negative impact on the entire network (Benson & Rahman, 2011). Organizations need direction in creating an information security awareness program or implementing a suitable information security culture (Veiga & Eloff, 2010). When IT managers strive to align the actions of the end users to the goals of information security, an increased level of success is achieved in the organization (Johnston & Warkentin, 2010).

Organizational efforts to manage information security are usually focused on vulnerabilities in technological assets such as hardware, software, and networking, and other sources of vulnerabilities, such as people, policies, processes, and culture are ignored (Spears & Barki, 2010). Keeping information protected is the responsibility of the IT security department as well as users within the organization (Styles & Tryfonas, 2009). Some research studies suggested that employees' failures to follow information security policies are the cause of the majority of breaches in information security (Lacey, 2010; Steffee, 2010; Shropshire et al., 2010). Employees should not only be aware of what their roles and responsibilities are in shielding information resources, but also how

they should respond to any potential security threats or issues (Werlinger, Hawkey, & Beznosov, 2009). The goal is to protect the company's information resources, and the implementation of security awareness programs for users will help achieve this goal (Styles & Tryfonas, 2009). Management is responsible for establishing computer security policies, however if the employees and end users do not understand the importance of these practices and are not willing to follow, then these efforts are in vain (Herath & Rao, 2009). The organization's management as well as the employees should be involved in the entire process of information security as displayed in Table 7 (Shropshire et al., 2010).

Table 7

*Four Security Actions*

Action	Description	Controls
Deterrence (Organizational action)	Security awareness programs and policies designed to convey information about risks to end users, and to reveal possible security threats.	Education programs, system use guidelines, counter-measure awareness training, warnings about sanctions for violations.
Prevention (Organizational or Individual action)	Active countermeasures with the inherent ability to enforce security policies and to prevent unauthorized system use.	Electronic locks, password access controls, automatic logoff features.
Detection (Organizational or Individual action)	Proactive actions taken to report suspicious activities. This stage includes detective actions taken after a system breach.	Virus scanner software, SPAM/malicious email detection services, anti-malware programs, firewalls, port scanners.
Remedy / Recovery (Organizational action)	Solutions taken after a system has been compromised. Includes steps taken to reprimand system abusers.	Verbal reprimands, loss of privileges, system restoration processes.

*Note:* Adapted from “Impact of Negative Message Framing on Security Adoption” by J. Shropshire, M. Warkentin, and A. Johnston, 2010, *The Journal of Computer Information Systems*, 51, p. 43. Reprinted with permission.

As evidenced by a study conducted by Wolf et al. (2011), there were several conclusions with information security awareness and its effectiveness and how direct behavioral measurement does provide and accurate assessment of an individual’s security compliance. This study measured the behavior of end users by examining the actual end user passwords to see if user was compliant in changing it regularly and changing to the

required format and usage. The study found that if users were left to voluntarily comply with security issues, in this case, updating and changing passwords, that there would be a sixty percent compliance rate. The overall results of the study provide that it is best to use hardware or software measures to implement and enforce security related policies and procedures (Wolf et al., 2011).

### **Information Security Statistics**

The reliance by organizations upon information technology has increased dramatically, as technology has developed and progressed (Koskosas et al., 2011). With an increase in the amount of information that can be shared and stored electronically, information is exposed to a growing number and a wider variety of threats and vulnerabilities (Alwi & Fan, 2010). The United States Federal Government has initiated a much stronger stance on cyber security and has made it an integral part of the national security system (Grummon, 2010). Average losses within United States organizations, which include colleges and universities, due to security incidents for 2009 were around \$234,244 per occurrence, while for the same study in 2010, the average losses reported were around \$100,000 but many chose not to disclose (CSI, 2010). The Ponemon Institute's annual study for 2010 reported an average cost of an entire data breach for a firm was \$7.2 million (Zafar, Ko, & Osei-Bryson, 2012). There are roughly 350 million attempts to break into Pennsylvania State University computers each month and multiply that by every other college and university, the number of attacks and the amount of risks is overwhelming for institutions of higher education (Spanier, 2010).

The Computer Security Institute's Computer Crime and Security Survey

(2010/2011) annually reports the most current types of security attacks experienced by organizations, including educational institutions. The leading security attack reported is malware infection with 67% of organizations reporting this type of attack (CSI, 2010). The other major types of attacks were being fraudulently represented as a sender of phishing messages at 39%, laptop or mobile device theft at 34%, bots/zombies within the organization at 29%, and insider abuse of Internet access or email at 25% (CSI, 2010). The complete listing is revealed in Table 8. For institutions of higher education are to remain competitive, management needs to invest in technology equipment, software, and security precautions (Spanier, 2010).

An organization's information must be protected in order to avoid the loss of its confidentiality, integrity, and availability (Alwi & Fan, 2010). During the years 2005 through 2009, 549 data breach incidents were reported at educational institutions exposing on average 10.4 million records (Collins et al., 2011). A recent survey conducted by The Association for Information Communications Technology Professionals in Higher Education (ACUTA) asked its members about their institution's security (Landsman, 2009). The respondents of the survey showed confidence in their network security systems; however, 47% of respondents reported significant security breaches; 71% of those institutions reported limited damage resulting in minor exposure of confidential information and some public embarrassment (Landsman, 2009). This survey suggests the importance of having an information security policy, procedures, systems, and strategies in place at any organization especially with the growth that institutions of higher learning have experienced recently.



Table 8

*Types of Attacks Experienced from 2006-1010*

Type of Attack	2006	2007	2008	2009	2010
Malware infection	65%	52%	50%	64%	67%
Bots / zombies within the organization	---	21%	20%	23%	29%
Being fraudulently represented as sender of phishing messages	---	26%	31%	34%	39%
Password sniffing	---	10%	9%	17%	12%
Financial fraud	9%	12%	12%	20%	9%
Denial of service	25%	25%	21%	29%	17%
Extortion or blackmail associated with threat of attack or release of stolen data	---	---	---	3%	1%
Web site defacement	6%	10%	6%	14%	7%
Other exploit of public-facing Web site option	---	---	---	6%	7%
Exploit of wireless network	14%	17%	14%	8%	7%
Exploit of DNS server	---	6%	8%	7%	2%
Exploit of client Web browser	---	---	---	11%	10%
Exploit of user's social network profile	---	---	---	7%	5%
Instant messaging abuse	---	25%	21%	8%	5%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	42%	59%	44%	30%	25%
Unauthorized access or privilege escalation by insider	---	---	---	15%	13%

(continued)

System penetration by outsider	---	---	---	14%	11%
Laptop or mobile hardware theft or loss	47%	50%	42%	42%	34%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	---	---	8%	6%	5%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	---	---	4%	6%	5%
Theft of or unauthorized access to PII or PHI due to all other causes	---	---	8%	10%	11%
Theft of or unauthorized access to intellectual property due to all other causes	---	---	5%	8%	5%

*Note:* 2010 CSI Computer Crime and Security Survey: 149 Respondents. Where (---) is listed, this type of attack was not asked in that year. Adapted from “2010 CSI Computer Crime and Security Survey” by Computer Security Institute, 2011, p. 17. Reprinted with permission.

### **Computer and Information Security Implementations**

The constantly changing business environment has created new vulnerabilities where criminals are adapting to and exploiting these new vulnerabilities and as a result, cybercrime has become more common (Susanto & Almunawar, 2012). There are numerous information security methods available and under development so that data stays safe and protected (Chander & Kush, 2011). Much of the past research on information security focused on the specific technological aspects and how it impacted the principles of confidentiality, integrity, and availability, but an area receiving far too little attention is the effectiveness of information security at the organizational level (Young & Windsor, 2010). Organizational awareness is the basis for information security programs; by making all levels of the organization aware of security issues, users

are better able to protect themselves and the organization as a whole (Wolf et al., 2011).

Leaders of an organization that fosters and encourages collective exchange between

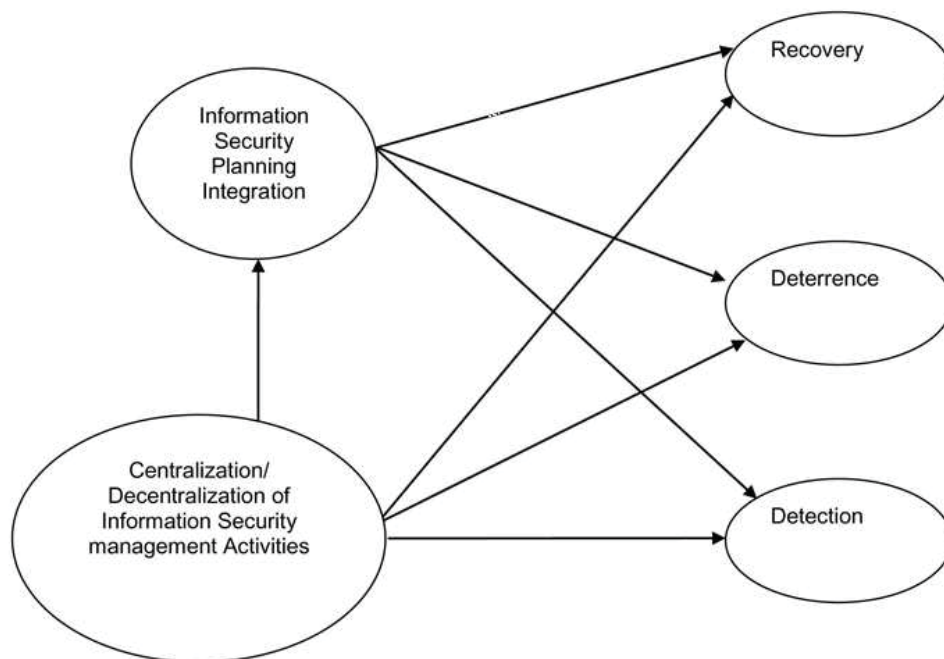
management, end users and the information security function is in a position to

theoretically manage information security in a more effective manner (Young, 2010).

The research model shown in Figure 3, relates information security planning and its goals

to allow such planning to be conducted at all levels of the organization (Young &

Windsor, 2010).



*Figure 3. Information Security Planning Involves Planning at Various Levels. Adapted from “Empirical Evaluation of Information Security Planning and Integration,” by R. Young and J. Windsor, 2010, *Communications of AIS*, 2010, p. 251. Reprinted with permission.*

Computer and information security has become a major concern not only for the

IT department, but for executives of the organization (Kayworth & Whitten, 2010). Despite the economic downturn over the past three years, most organizations have spent more on information security this year than in the previous year (Susanto & Almunawar, 2012). Much of management's effort is being expanded and focused in developing and enforcing information security policies and assessing strategies (Young, 2010). Although many organizations have invested significantly in information security and privacy practices in recent years, in various circumstances, these practices have not become embedded in the way people do things (Gillon et al., 2011). Not only does the challenge of securing data, assets, and other information include technical solutions, but also includes entire processes to change the way things are done within the organization (Gillon et al., 2011). There are several benefits gained through improved communication and collaboration which include top management commitment, greater visibility of the information security function, more aligned business and security plans, less implementation difficulties, better utilization of resources, and higher user acceptance (Young, 2010). The question remains as to what is the most effective organizational approach or strategy for information security (Kayworth & Whitten, 2010).

The entire IT system is dependent upon the success of each of its component's functions, and the interconnection among them, while experiencing a deficiency might allow information security to be compromised (Sehgal et al., 2011). Information security depends on technical, as well as social and organizational aspects which together communicate and interrelate so that management can control and navigate the organization towards providing expected information security services with desired

quality (Monfelt, Pilemalm, Hallberg, & Yngström, 2011). Intrusion Detection Systems (IDS) have been vigorously investigated by researchers for the past two decades and is one of the successful solutions of a defense system for an organization (Stiawan, Idris, Salam, & Abdullah, 2012). As presented in Table 9, the protection of information and other assets relies on the success of the usual technical controls but there is also becoming a huge dependence on human factors such as human behaviors and human knowledge (Kruger et al., 2010).

Table 9

*Cognitive Skills of Users as Relating to Information Security*

Cognitive Category	Cognitive Action	Explanation
Knowledge of facts, processes, procedures, and concepts (what someone needs to know)	Recall, recognize, calculate, derive information from graphs or tables, measure, classify and sort	When people do not have reasonable access to a knowledge or facts base in information security, focused information security reasoning becomes difficult.
Understanding and application of knowledge	Choose, suggest, develop a model, solve problems, and implement solutions	Representation of information security ideas forms the basis of perceptions and communication in information security and is a basic prerequisite for a successful information security environment.
Reasoning (focus on solving problems in unknown situations)	Analyze, generalize, integrate, defend solutions	Reasoning in information security requires logical and systematically, including intuitive and inductive, thinking processes. People should be able to implement expertise in different

contexts.

---

*Note:* Adapted from “A Vocabulary Test to Assess Information Security Awareness” by H. Kruger, L. Drevin, and T. Steyn, 2010, *Information Management & Computer Security*, 18, p. 320. Reprinted with permission.

Most networks are implemented with the information security systems pointing outside the organization, whereas, security mechanisms are often more effective and efficient if the system is inwardly secure (Enescu, Enescu, & Sperdea, 2011). Information technology (IT) security approaches too often focus on the narrow, technically oriented solutions, while ignoring the social aspects of risks and the informal structures within the organization (Koskosas et al., 2011b). Most information security failures emerge from human error, carelessness, or malevolence and unless management can fundamentally change the way employees approach security and privacy, and make it a higher priority for them, failures are likely to continue (Gillon, 2011). As shown in Figure 4, this reflects a need for IT management to adopt a social organizational view, which includes factors such as trust, culture, and communication in order to achieve the best performance for IT security processes and implementations (Koskosas et al., 2011).



*Figure 4. Performance Pyramid Framework. Adapted from “A Model Performance to Information Security Management,” by I. Koskosas, K. Kakoulidid, and C. Siomos, 2011, *International Journal of Business and Social Science*, 2, p. 50. Reprinted with permission.*

Historically, organizations have focused on the technology aspect of information security strategy that emphasizes the primary role of technology in designing effective security solutions (Kayworth & Whitten, 2010). The significance of quality data, the emphasis on information security as a business process, and having a greater respect for the role of users and social interactions in the security design process are all important components of a successful information security strategy and program (Chander & Kush, 2011). For a new approach to information security, there needs to be a shift in emphasis from processes and procedures towards people (users), relationships, and the flow of information (Lacey, 2010).

A number of research scholars have written on the numerous various topics

surrounding computer and information security. There is an ongoing discussion and debate about which information security management system an organization would be most beneficial to implement. The question also remains as to what is the most effective organizational approach or strategy for information security (Kayworth & Whitten, 2010). There has been some skepticism or reservation by information security professionals in disclosing too much about their respective organizations and this may hamper research in this field (Jourdan et al., 2010). Monfelt et al. (2011) concurred with the theory of using various information security methods, tools, implementations to better equip the organization to protect its assets and other information and suggest using a 14-layered framework in information security management and communication. The 14-layered framework is broken down into seven technical aspects and seven social aspects of information security and communication within an organization. The seven technical aspects of the framework consists of (a) physical medium, (b) link, (c) network, (d) transport, (e) session, (f) presentation coding, and (g) application. The seven social aspects of the information security communication framework includes (a) adaptation, (b) organizational, (c) managerial, (d) legal, (e) ethical, (f) cultural, and (g) SWOT (Monfelt et al., 2011).

There are many different approaches to implementing information security in an organization that range from specific technical tools, differing software and hardware, and implementing training and awareness programs. Wallace et al. (2011) conducted an extensive investigation into the IT controls that organizations have implemented for information security compliance. Of the 13,000 emailed surveys to individuals for



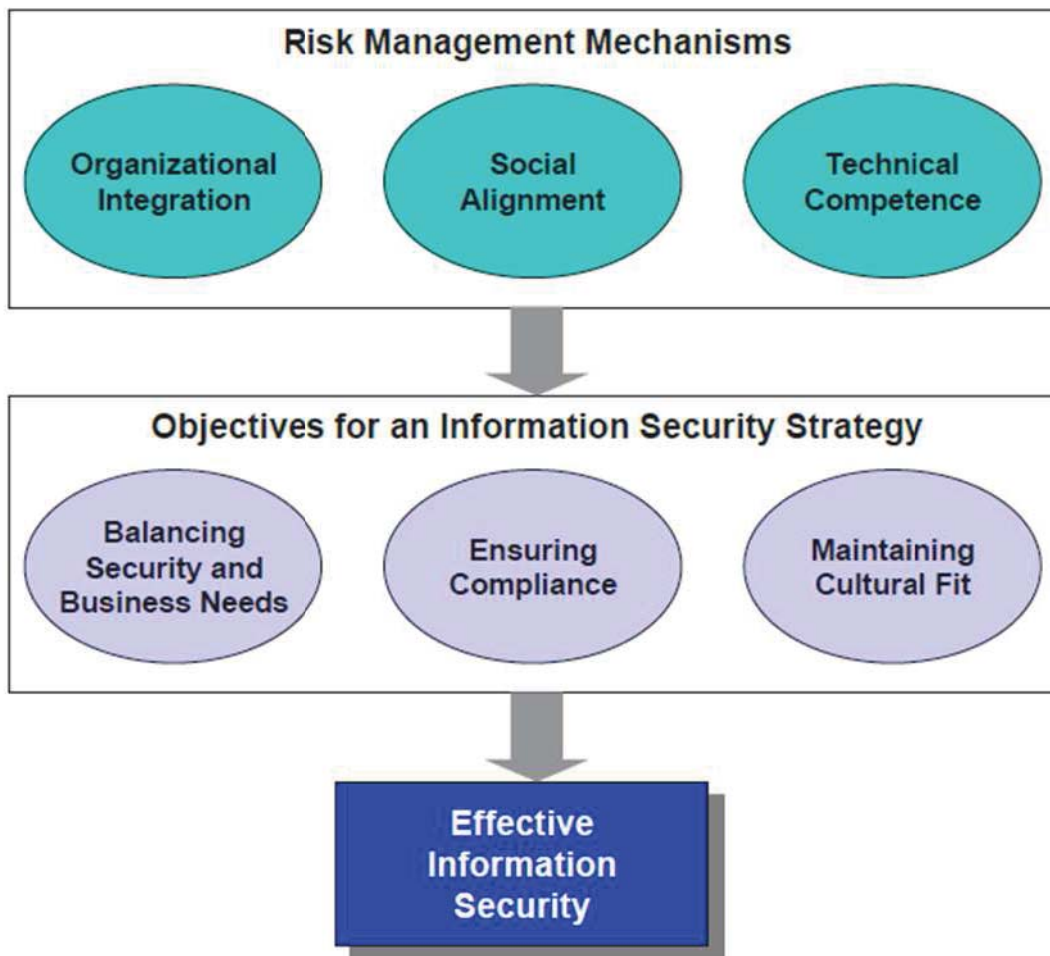
compliance issues within organizations, 881 replied to the survey. The top 10 most commonly implement information security controls were: (a) using antivirus software on workstations, (b) authenticating remote users access the organization's network, (c) using IT to protect networks from unauthorized access, (d) maintaining network security through use of IT, (e) keeping antivirus updated, (f) enforcing a secure log-on process when providing access to information services, (g) enforcing security procedures regarding password selection and use, (h) restricting access rights to applications, (i) regularly backing up essential business information and software, and (j) restricting and controlling system privileges (Wallace et al., 2011). The results of this one investigation showed a reliance on numerous security implantations that are used by IT professionals in order to protect their organization although the majority of these controls were technology based and did not incorporate users' security awareness and training options.

In a separate study, Guo et al. (2011) used the composite behavior model that suggests that intention is the immediate cause of behavior and intention is influenced by attitude toward behavior, which in turn is determined by the following antecedents: (a) habit (the sequences of a person's behavior that have become automatic), (b) attitude toward target (attitude toward the specific target that is the object of a behavior), (c) utilitarian outcomes (either rewards or punishment that one presumes from engaging in the behavior), (d) normative outcomes (the approval or disapproval by significant others of the behavior), and (e) self-identity outcomes (either affirmations or repudiations of one's self-concept that are expected to follow from engaging in the behavior). The behavioral intentions of users and how this relates to information security violations is

what was measured in this research. In total, 306 end users were surveyed regarding behaviors that are affected by information security violations and practices. One of the most important discoveries from this research was that end users often lack security knowledge and skills and may view security as irrelevant to their jobs (Guo et al., 2011). However, through this study, it was found that security risk is an important factor that can influence users' behavioral decision (if they know enough about the event or incident). The results of the study proposed a shift in information security management strategy may be necessary to one that is more user-centered, which raised the question what should information security management do to help end users do their job, while at the same time being better equipped to improve security (Guo et al., 2011).

Based on the study of Kayworth and Whitten (2010), several primary objectives for an information security strategy were discovered by interviewing numerous information security executives and managers. The three primary objectives, as shown in Figure 5, all security managers must address regardless of the organizational structure is: balancing the need to secure information assets against the need to enable the organization, ensuring compliance, and maintaining a cultural fit (Kayworth & Whitten, 2010). Information security management must find the balance that fits their organization where enough protection is obtained but also does not hinder business operations. The second objective must be followed to make sure the design and implementation of information security policies comply with numerous external legal requirements and the third objective found was to ensure that the values concerning information security align with those values adopted by the management of the

organization.



*Figure 5. A Strategic Framework for Effective Information Security. Adapted from “Effective Information Security Requires a Balance of Social and Technology Factors,” by T. Kayworth and D. Whitten, 2010, *MIS Quarterly Executive*, 9, p. 166. Reprinted with permission.*

In a study conducted by Young and Windsor (2010), it was noted that the majority of organizations’ management are choosing to view information security strictly from a cost-benefit or risk analysis perspective. The data was collected using a mail survey from 119 information security and/or IT managers. The findings of this study

suggested that organizations with more sophisticated information security planning processes push the responsibilities of many of the information security activities down the organizational ladder but that how management chooses to structure the information security management activities does not impact the effectiveness of information security recovery strategies. However, findings did reveal how management chose to structure information security management activities does impact the effectiveness of detection and deterrence strategies (Young & Windsor, 2010). Other notable discoveries from this study revealed that organizational management was not placing a heavy focus of information security on developing aware and responsible information users and that the overall goal of information security is mainly to demonstrate compliance with laws and regulations (Young & Windsor, 2010).

As reflected in a study by Cline et al. (2010), the three information security executives that were interviewed believed that a proactive information security strategy would deliver considerable positive benefits and recommend their managers investigate the advantages of having a proactive (internally driven) versus reactive (externally driven) strategic approach to information security. Table 10 presents numerous information security ideas generated by the information security executives in which management may use to analyze how proactive they are within the areas presented. The findings also present the major concern management will have with negative consequences of a security breach, but often view security issues as secondary. One more important discovery was that the executives thought it to be important to investigate the characteristics of an organization's culture that must be adhered to in order to

establish and maintain successful governance of its information security strategies (Cline et al., 2010).

Table 10

*Information / Computer Security and Privacy Concerns*

Construct	Ideas About Information Security
Environmental Conditions & Changes	<p data-bbox="862 447 1203 478"><u>Representative Legislation</u></p> <ul style="list-style-type: none"> <li data-bbox="862 485 1308 552">☐ Health Insurance Portability and Accountability Act (HIPAA)</li> <li data-bbox="862 558 1154 590">☐ Sarbanes-Oxley Act</li> <li data-bbox="862 596 1349 663">☐ National Information Infrastructure Act of 1996</li> <li data-bbox="862 669 1203 701">☐ U.S. Patriot Act of 2001</li> <li data-bbox="862 707 1390 774">☐ Corporate Information Security Act of 2003</li> <li data-bbox="862 781 1154 812">☐ Privacy Act of 2003</li> <li data-bbox="862 819 1357 886">☐ Federal Information Security Act of 2002</li> </ul> <p data-bbox="862 926 1203 957"><u>Technology vulnerabilities</u></p> <ul style="list-style-type: none"> <li data-bbox="862 963 1317 1031">☐ Generally inadequate technology standards for secure computing</li> <li data-bbox="862 1037 1273 1068">☐ Wi-Fi protocol security flaws</li> <li data-bbox="862 1075 1357 1142">☐ Wireless Equivalent Privacy (WEP) vulnerabilities</li> </ul> <p data-bbox="862 1182 1219 1213"><u>Information systems threats</u></p> <ul style="list-style-type: none"> <li data-bbox="862 1220 1219 1251">☐ Denial-of-service attacks</li> <li data-bbox="862 1257 1219 1289">☐ Unauthorized data access</li> <li data-bbox="862 1295 1162 1327">☐ Web-site penetration</li> <li data-bbox="862 1333 1325 1365">☐ Theft/disclosure of customer data</li> </ul>
Organizational Conditions & Changes	<p data-bbox="862 1430 1162 1461"><u>Electronic criminal acts</u></p> <ul style="list-style-type: none"> <li data-bbox="862 1467 1065 1499">☐ Identify theft</li> <li data-bbox="862 1505 1065 1537">☐ Internet fraud</li> <li data-bbox="862 1543 1268 1610">☐ Phishing - soliciting personal information through e-mail</li> <li data-bbox="862 1617 1219 1648">☐ Other fraudulent schemes</li> </ul> <p data-bbox="862 1654 1284 1686"><u>Secure distributed corporate data</u></p> <ul style="list-style-type: none"> <li data-bbox="862 1692 1154 1724">☐ N-Tier architectures</li> <li data-bbox="862 1730 1219 1761">☐ Across supplier networks</li> <li data-bbox="862 1768 1260 1799">☐ Across outsourced networks</li> </ul>

## Managerial Cognition

### Data assurance

- Accuracy
- Unauthorized Use
- Organizational Culture
- Internal Software Vulnerabilities
- Inadequate internal security controls
- Software bugs/errors/omissions/back doors

### Managerial concerns

- Competitive threats
- Legal penalties
- Asset protection
- Privacy protection

### Perceived security priorities for 2004

- Security review and assessment
- Security policies and standards
- Incident response teams

## Managerial Actions

### Managerial oversight

- Setting, maintaining, and implementing security policies, procedures, and standards
- Increased hiring of certified security professionals
- Increased training

### Installation of security hardware

- Biometrics
- Smart cards
- Firewall applications/VPNs/ intrusion detection systems (IDSs)
- Intrusion Prevention Systems (IPSs)

### Installation of security software

- Certificate authorities
- Single sign-on
- Provisioning
- Access controls
- Secure e-mail
- Encryption
- Enterprise security management
- Vulnerability assessments

- E-mail scanning
- Web filtering
- Audit software

#### Acquisition of security services

- Consulting
- Digital forensics
- Disaster recovery/business continuity
- Executive recruitment
- Managed security services
- Penetration testing
- Outside audit services

#### Changes in the Content of Strategy

#### Risk Management

- Contingency/disaster recovery plans
- Continuity plans
- Insurance
- Audits

#### Organizational Outcomes

#### Loss Prevention

- Reduce unauthorized access
- Reduce service attacks
- Reduce loss of data
- Reduce unauthorized disclosure
- Improve data accuracy

---

*Note:* Adapted from “The Impact of Organizational Change on Information Systems Security,” by M. Cline, C. Guynes, and A. Nyanoga, 2010, *Journal of Business & Economics Research*, 8, pp. 61-62. Reprinted with permission.

From the work of Young (2010), it becomes apparent that many different information security policies and procedures are used by management to increase the securing of information and other assets belonging to the organization. Table 11 presents research findings collected from 119 information security and IT managers on information security policy use. It was found in the study that management was better off fashioning explicit policies to address specific information security concerns within the



organization as this may increase user awareness and promote more consistent organizational behavior. This study also presented the importance of developing information security policies while promoting collaborative exchange between the organization's information security function, management, and end users of information systems (Young, 2010). Additionally, having end user contribution in the information security policy development and implementation process may lead to increased acceptance and ownership thus improving the effectiveness of the information security policies and the detection, deterrence, and recovery strategies that the policies address. In the end, it is the user who must adhere to the information security policies.

Table 11

*Distribution of Information Security Policy Use*

Policy	Used	Percent
Access Control Policy and Procedures	114	95.8
Identification & Authentication Policy and Procedures	104	87.4
Physical and Environmental Protection Policy and Procedures	102	85.7
Contingency Planning Policy and Procedures	97	81.5
Security Awareness and Training Policy and Procedures	96	80.7
System Maintenance Policy and Procedures	94	79.0
Audit and Accountability Policy and Procedures	93	78.2
Media Protection Policy and Procedures	92	77.3
Configuration Management Policy and Procedures	89	74.8
Personnel Security Policy and Procedures	89	74.8
Incident Response Policy and Procedures	86	72.3
System and Communication Protection Policy and Procedures	85	71.4
Systems and Information Integrity Policy and Procedures	82	68.9
Security Planning Policy and Procedures	81	68.1
Risk Assessment Policy and Procedures	80	67.2
System and Services Acquisition Policy and Procedures	72	60.5
Certification, Accreditation & Security Policy and Procedures	48	40.3

---

*Note:* Adapted from “Evaluating the Perceived Impact of Collaborative Exchange and Formalization on Information Security” by R. Young, 2010, *Journal of International Technology & Information Management*, 19, pp. 25-26. Reprinted with permission.

## **Information Security at Institutions of Higher Education**

In researching this topic, much information was found on the various needs for IT security effectiveness (Anand et al., 2012). The importance of network security at institutions of higher education has never been higher than during the first decade of the 21<sup>st</sup> century (Kumari et al., 2011). Colleges and universities possess large amounts of information from students, parents, and employees such as income tax returns, employment history, salary, loans, credit information, admissions records, and medical files (Jones, 2008). The higher education industry is quite vulnerable and contains a wealth of valuable information on millions of personal records linked to students, faculty, and alumni (Collins et al., 2011). The majority of data breaches from 2005 through 2011 have occurred in an educational or academic environment (Ayyagari & Tyks, 2012).

Computer and IT security threats to educational institutions have considerably increased from 2008 to 2011 (Maskari et al., 2011). In 2010 alone, educational institutions reported 65 security breach incidents which lead to the exposure of over 1.6 million records (Collins et al., 2011). Academic institutions have become prime targets for hackers due to campuses having abundant computers, servers, and other computing resources, along with highly powered networks (Anonymous, 2010). Wireless networking capabilities, which are abundant on most college campuses, have raised serious security issues (Likhar et al., 2011). Economic conditions, stagnant or shrinking security related budgets and a perceived lack of skilled and trained information security resources are increasing concerns for an organization's IT management (Farrell, 2010).

Providing IT security on a shoestring budget is always difficult and many small

colleges and universities management are challenged with balancing cost and effectiveness (Ayyagari & Tyks, 2012). Most organization's management has an idea of how much of their IT budget is spent directly on information security (Young & Windsor, 2010). Management at colleges and universities have additional security challenges, such as relaxed working environments, less formalized policies and procedures, and employees that wear several different hats that have various different job responsibilities (Ayyagari & Tyks, 2012).

Compliance with information security standards is highly recommended to ensure all information is safe (Susanto et al., 2012). Any leakage of information can cause the organization to suffer financial and economic loss, but also credibility; therefore, keeping the data, information, and knowledge secure and confidential is a major concern (Chander & Kush, 2011). With leaner and tighter budgets for schools, making hard decisions on areas to reduce expenditures is very important (Donlevy, 2011). The U.S. Cost of Data Breach report released in March 2011 showed that the number of data breaches has increased and the costs associated with these breaches are on the rise (Zafar et al., 2012). The increase climbed 7% from the year before to an average of \$7.2 million per security breach incident (Zafar et al., 2012). Security threats and intrusions are driving organizations to adapt a more full comprehensive computer and information security program (Liu & Ormaner, 2009). Managing and monitoring computer and information security requires a commitment from not only IT management but everyone in the organization.

Colleges and universities are more vulnerable than corporations regarding IT

security because of the amounts of accessible data, lack of security policies, and unsecured wireless networks (Jones, 2008). Cyber security incidents have been known to reduce visitors to an organization's website but on the other hand these incidents have also been used to increase the size of IT budgets (Davis, Garcia & Zhang, 2009). Information security management involves a combination of anticipation, detection, and response processes along with a series of actions that require constant monitoring and control activities used to reduce the chance of information security attacks (Issa-Salwe & Ahmed, 2011). Completely preventing security attacks, breaches of security, and attempts of unauthorized access is unrealistic at this time (Jonnalagadda & Mallela, 2011).

The number of computers networked within an organization along with computers networked through the Internet to other organizations, has increased the information system's exposure to security threats and breaches (Reddy & Prasad, 2012). New threats are constantly being created and deployed by cybercriminals to exploit weaknesses that organizations have not yet discovered (Jourdan et al., 2010). Facilitating awareness concerning information security issues facing educational institutions is very important because the majority of reported security breaches occur in an educational setting (Ayyagari & Tyks, 2012). The increase in security threats with the increase in unauthorized access to computers and networks even further the need for educational institutions to prepare themselves to fight against this phenomenon (Spanier, 2010).

The focus and overall objective of Kruger's et al. (2010) research study of 44 students at a university was to investigate the feasibility of using a vocabulary test to

assess information security awareness. Based on the results of the vocabulary test, the majority of the students had a reasonable knowledge concerning e-mail security, computer viruses, spyware, and spam, but a surprising number of them, around 11% did not know what the term phishing meant and 25% did not understand the term security incident. Most of the students were not sure where to report a security incident and almost half of them (48%) did not comprehend what was meant by using a strong password and many of them were willing to give their passwords away under certain circumstances (Kruger et al., 2010). The results did show that using a security related vocabulary test can make a contribution to help students identify and become more aware of information security related issues and one way to address the need of students and employees lacking the necessary information security knowledge and responsibilities is to design and implement a suitable information security awareness program (Kruger et al., 2010).

The information security standards certification (ISO 27001) suggested implementing an entire information security management system that consists of the following areas of concentration: (a) an information security policy, (b) communications and operations management, (c) access control, (d) information system acquisition, development, and maintenance, (e) organization of information security, (f) asset management, (g) information security incident management, (h) business continuity management, (i) human resource security, (j) physical and environmental security, and (k) compliance (Susanto & Almunawar, 2012). Whether managers are working with information security in a small business, large corporation, college or university, or any

type of organization, there is much included in the overall challenge to secure computers, networks, and information. Institutions of higher education need to have a general approach to information security. Figure 6 represents an entire information security framework approach that should be made known to management (Fielden, 2011).

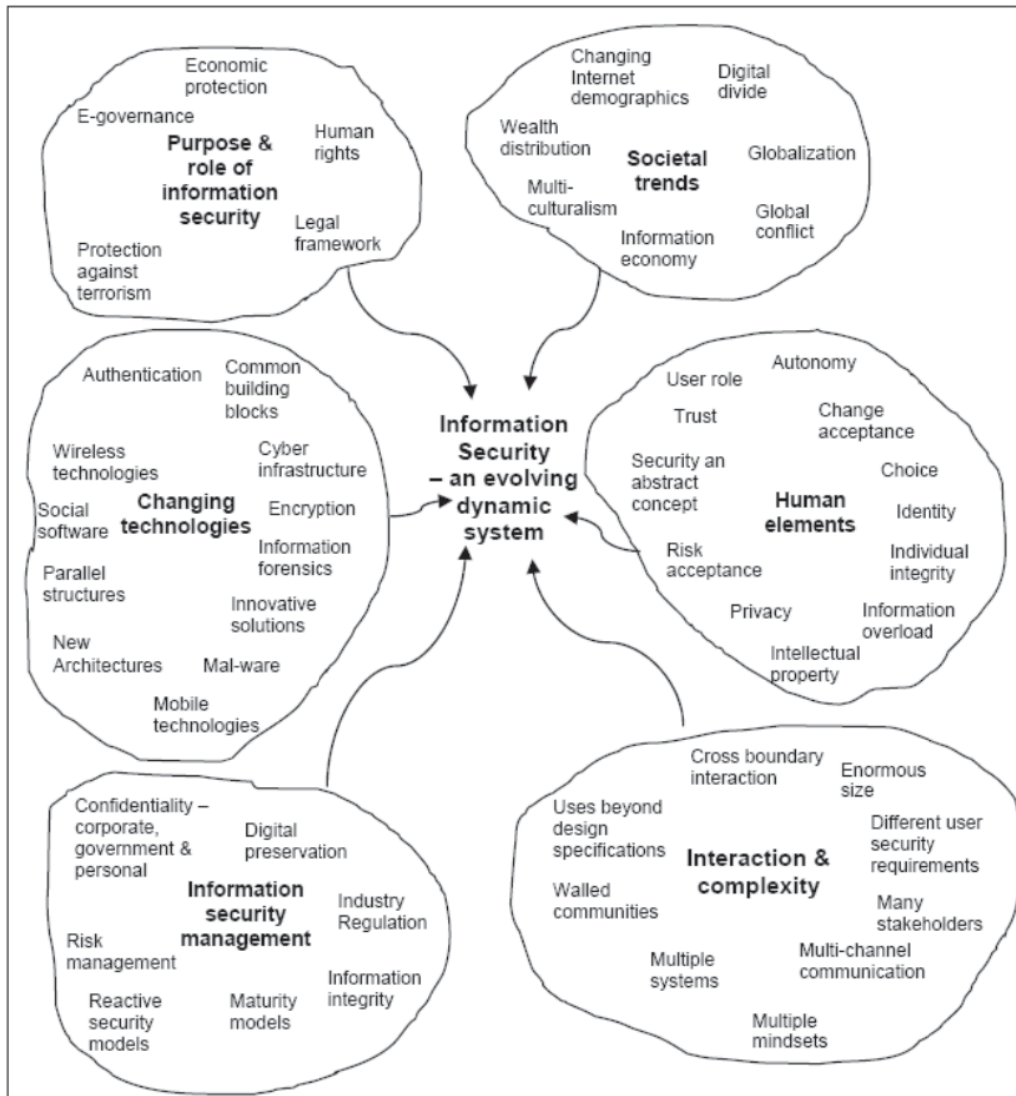


Figure 6. Information Security Framework. Adapted from "An Holistic View of Information Security: A Proposed Framework," by K. Fielden, 2011, *International Journal for Infonomics*, 4, p. 2. Reprinted with permission.

## Summary

Information security has a very important role in supporting the activities throughout an organization and therefore, the attention information security receives from management should be one of top priority (Susanto & Almunawar, 2012). Though a number of information security approaches have been developed over the years that reactively minimize security threats such as technical checklists, risk analysis, and evaluation methods, there is a need to establish mechanisms to proactively manage IT security (Koskosas et al., 2011). Management must take advantage of technology initiatives to drive changes and improve operations, productivity, and performance (Wang, 2010). Sufficiently deployed information systems provide the means to increase the effectiveness and efficiency of organizational processes (Monfelt et al., 2011). Computer information security has become a major concern of the 21<sup>st</sup> century and management should focus on proactive measures to help counter security attacks (Stiawan et al., 2012). Knowledgeable users can be the first line of defensive against a security breach whereas technological tools are effective only after the users are skillful at using them in their day-to-day activities (Chen et al., 2008). Some IT professionals are even stating that security awareness and training can be more of a crucial factor than security technologies in contributing to the success of information security (Chen et al., 2008).

The process of IT security management and improvement is less about revolutionary leaps and more about the changing of daily organizational habits, taking action that is regular and stable, and keeping information security improvement as a



constant primary concern (Enescu et al., 2011). A quality security awareness program will provide users with sufficient understanding to evaluate adverse consequences of security problems as well as take the appropriate actions to avert and correct security breaches (Chen et al., 2008). One of the best ways to be proactive is to have a combination of security tools, policies, crisis-response procedures, systems, strategies, and user education and training programs within the organization (Tyagi & Srinivasan, 2011). A goal of this study is to evaluate what computer and information security practices, procedures, security tools, policies, systems, strategies, and training the management at colleges and universities would recommend implementing to increase IT security and reduce attacks, breaches and threats.

There are numerous information security threats that have impacted on institutions of higher learning that concerns the protection of users, information, assets, and other resources (Maskari, et al., 2011). There is a great need for IT departments within all organizations to be well equipped to handle the numerous information security threats that exist and continue to be an ongoing critical issue for management (Abbas, et al., 2011; Kim & Cha, 2012; Ryan, Mazzuchi, Ryan, Lopez de la Cruz, & Cooke, 2012). The more organizations rely on information systems to survive, the greater the need to maintain the confidentiality, availability, integrity, and authenticity of data moving through an organization's network (Koskosas et al., 2011). Current and future information security threats require development of more adaptive and responsive information security systems (Taluja & Dua, 2012). Looking to the future, it is likely that information security will become increasingly important topic for research and

instruction as technology becomes more universal, risks around information grow, and more criminals gain value by the exploitation of confidential and personal information (Gillon, 2011).

### Chapter 3: Research Method

The problem needing to be addressed is the increase in information security breaches impacting institutions of higher education (Ayyagari & Tyks, 2012; Collins et al., 2011; Perkel, 2010; Susanto, Almunawar, Tuan, Aksoy, & Syam, 2011). Researchers have found IT security an important concern for organizations, but very few have focused on the specific needs of a college or university which leads to the specific problem of that due to increases in IT security breaches in educational environments, researchers have recommended that the needs of colleges and universities for the improvement of IT security be explored in more depth (Abbas et al., 2011; Fisher & Shorter, 2013; Guo, Yuan, Archer, & Connelly, 2011; Ma, Schmidt, & Pearson, 2009; Mensch & Wilkie, 2011; Werlinger, Muldner, Hawkey, & Beznosov, 2010)..

The costs associated with data breaches have increased and continue to motivate IT departments to implement new security of information protection measures (Hoadley, Deibel, Kistner, Rice, & Sokhey, 2012). Raising awareness concerning information security issues faced by academic institutions is important because the majority of reported breaches in 2011 have occurred in an educational environment (Ayyagari & Tyks, 2012).

The U.S. Cost of Data Breach report released in March 2011 showed that the number of data breaches had increased and the costs associated with these breaches were on the rise (Zafar et al., 2012). In 2010, educational institutions reported 65 security breach incidents which lead to the exposure of over 1.6 million records (Collins, Sainato, & Khey, 2011). During the years 2005 through 2009, 549 data breach incidents were

reported at educational institutions exposing on average 10.4 million records (Collins et al., 2011). The majority of data breaches since 2005 have occurred in educational environments and information security is a leading concern for institutions of higher education because hackers are targeting colleges and universities to steal computing resources, property, and data (Ayyagari & Tyks, 2012; Perkel, 2010).

A gap in literature exists on IT security requirements for colleges and universities. Researchers have found IT security an important concern for organizations, but very few have focused on the specific needs of a college or university (Abbas et al., 2011; Guo, Yuan, Archer, & Connelly, 2011; Ma, Schmidt, & Pearson, 2009; Werlinger, Muldner, Hawkey, & Beznosov, 2010). The importance of network security at institutions of higher education has never been higher due to the numbers of breaches and costs associated with breaches (Kumari et al., 2011).

The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. There are over 4,000 distinct colleges and universities that make up this educational system throughout the United States of America and 220 located in North Carolina alone. In this study, a total of 13 participants were involved. Interviews were conducted with 13 members from within IT departments of 12 separate and distinct colleges and universities in order to gather data relevant to fulfilling the purpose of this study (Stake, 2006; Yin, 2009). A holistic multiple case study design was chosen for this study to focus on 13 participants as holistic units of analysis from 12 separate colleges and universities (Stake, 2006; Yin, 2012). The

detailed information gathered from the multiple case study on the diverse and unique needs of the universities IT personnel could be used by university administrators to design, implement, or verify appropriate and needed IT security systems and strategies.

The research question was created to obtain an understanding of what a sample of the university's IT department warrants as being necessary to implement concerning reduction of information security attacks, breaches, and threats in hopes of protecting resources, assets, and data. To better understand the IT security tools, policies, procedures, and systems that are recommended by the IT personnel, the following research questions were used to ascertain the security measures needed from 13 IT personnel from 12 separate and distinct colleges and universities. The goal was to conduct face-to-face, one-on-one interviews with a member in an IT department involved in or responsible for IT security at their North Carolina academic institution. The central research question of this study was focused on the following:

**Q1.** What IT security components within academic institutions potentially contribute to improved IT security and reduce or eliminate possible information security attacks, breaches, and threats?

Interview questions were used in this study to focus on the participants' perceptions of IT securities and the processes and procedures involved with the need to implement such measures in order to achieve organizational IT security effectiveness. The interview guide/protocol is located in Appendix A and lists the specific interview questions that were asked of the research participants.

This holistic multiple case study involves research methods designed to examine participants' comprehensive perspectives. The purpose of this chapter is to describe the research that took place with this multiple case study and the methods and procedures used to establish and gather the research needed. Chapter 3 includes discussions on the research method and design, as well as the participants, data collection and analysis, methodological assumptions and limitations, and ethical assurances.

### **Research Methods and Design**

In order to obtain a deeper understanding of the unique needs of information security within institutions of higher education, qualitative research in the form of a holistic multiple case study with 13 total participants was conducted. The unit of analysis (13 participants) was selected using purposeful sampling (Yin, 2009). Thirteen participants were interviewed with face-to-face, one-on-one communications. A qualitative research method was used in this study, in which information about the experiences of currently employed IT personnel at colleges and universities was collected through in-depth, open-ended interviews. Shank (2006), among other authors such as Yin (2009) and Denzin and Lincoln (2008), defined qualitative research as a form of systematic empirical inquiry into meaning. Qualitative data is a source of well grounded, rich descriptions and explanations of processes in identifiable local contexts (Miles & Huberman, 1994). The use of a qualitative method is justified because of the need for in-depth information from the research participants (Patton, 2002; Yin, 2009). Qualitative researchers press for understanding the complex interrelationships among all the data collected from the participants (Stake, 1995). The use of a holistic multiple case study

was appropriate for this study because even though the research boundary is within the State of North Carolina, all interview participants were employed within an IT department at a separate and distinct college or university operating within the State of North Carolina.

Quantitative research methods are used for testing hypotheses, especially with large samples, allowing the development of sophisticated fundamental models and easily allow replication across research situations, however, they are inadequately suited to help comprehend the implications management would attribute to the success or failure of their organizations (Klenke, 2008). Much of an organization's success or failure will come partially from the implementations and use of technology to achieve organizational goals and objectives. Qualitative interviewing is a basic mode of inquiry and the primary method a researcher can use to investigate the experiences and knowledge of the individual people who make up the organization and carry out the process itself (Seidman, 2013). Qualitative inquiry research studies are especially important when the processes being studied are nearly invisible and not observable (Rubin & Rubin, 2012). Qualitative research engages in purposive or theoretical sampling, meaning the researcher intentionally chooses participants who can contribute an in-depth, information-rich understanding of the phenomenon under examination (Klenke, 2008). The goal of theoretical sampling is to select cases which are likely to replicate or extend the emergent theory (Eisenhardt, 1989).

With a qualitative study one can preserve sequential flow, determine exactly which events led to which consequences, and develop productive explanations (Miles &

Huberman, 1994). Qualitative research data is gathered from the participants' perspectives and intended to capture the voice of the research participants. (Klenke, 2008). Conducting a qualitative research study has an advantage over a quantitative approach in that qualitative researchers often collect data in the field and at the site where the participants actually experience the issue or problem being examined (Patton, 2002). Significant resources should be invested in qualitative research studies, documentation, and descriptions of a phenomenon, whereas few resources might be invested in substantiating the meaning of the numbers presumed to represent something quantitatively (Fisher & Stenner, 2011). The findings from qualitative studies have a quality of being understood with concrete meaning, more than just pages of summarized numbers as in a quantitative study (Miles & Huberman, 1994). Unlike quantitative research methods, qualitative methods generally do not examine relationships between variables through standardized measures; qualitative methods explore a phenomenon in depth (Patton, 2002). A qualitative research design is flexible and can and should be changing to match the dynamics of the evolving research process (Klenke, 2008). Another advantage of using a qualitative research method is that as the researcher's knowledge increases, through the interviews and other data collection methods, the research design can be modified to further increase the topic knowledge (Wengraf, 2001).

Qualitative research methods yield a wealth of detailed information about a small number of participants and cases and provide depth and detail through direct citation and careful description of situations, events, interactions, and observed behaviors (Klenke, 2008). Qualitative inquiry methods begin with the premise that the viewpoint of others is



meaningful, knowledgeable, and able to be made clear (Denzin & Lincoln, 2008; Patton, 2002; Yin, 2009).

A qualitative case study method is appropriate to use when (a) researchers are asking how or why questions, (b) the researcher has little or no control over events, and (c) the research focus is on a contemporary phenomenon within a real-life context (Yin, 2009). Qualitative case study issues reflect complex, situated, and problematic relationships that bring attention to both ordinary experience and disciplines of knowledge (Stake, 2006). In a qualitative case study, the researcher looks for greater understanding and appreciation of the issue being studied and the uniqueness and complexity of it (Stake, 1995). A multiple case study research design allows the researcher to explore differences within and between cases and to also make comparisons (Yin, 2009). By asking in-depth questions of select participants from more than one academic institution, and by exploring differences and comparisons among cases, a holistic multiple case study design is selected as the preferred research method for this study (Yin, 2009).

This holistic multiple case study was patterned after Yin's (2009) process and procedures for conducting human science research. The steps to be included are (a) planning; (b) designing; (c) preparation; (d) data collection; (e) analyzing; and (f) results sharing (Yin, 2009). Yin suggested that evidence from multiple-case designs is often considered more convincing, and the overall study is therefore considered as being more robust. Semi-structured interview questions were used as the method in this holistic multiple case study to gain in-depth understanding of participants' perceptions,

perspectives, knowledge, and experiences with the phenomenon under study (Creswell, 2009).

Yin (2009) stated that once a significant finding or discovery is uncovered from a single experiment an insistent priority would be to replicate this finding or discovery by conducting a second, third, and even more experiments. Researchers should apply replication logic in multiple case studies to interpret discoveries across cases and determine whether research discoveries support broader patterns of conclusions (Yin, 2012). Only with such replications would the original finding or discovery be robust (Yin, 2009).

Yin (2009) asserted that sample selection of cases in a multiple case study should be based on replication logic. The selection of multiple cases for this study was based on replication logic as select criteria was used to identify prospective colleges and universities in the state of North Carolina and replicated for each case (Yin, 2009). Yin (2012) stated that theoretical replication should be used in multiple case studies so that the disposition of each case will produce varying or contrasting results. In replication logic, cases which confirm developing relationships heighten confidence in the validity of the relationships (Eisenhardt, 1989).

By using qualitative interviewing, researchers can communicate with those who have knowledge of and/or experience with the problems of interest (Rubin & Rubin, 2012). The use of qualitative semi-structured interviews allows flexibility in that the interviewer can modify the order and details of how topics and questions are presented (Wengraf, 2001). This cedes some control to the respondent over how the interview

proceeds, but because respondents are asked the same questions, this makes possible a comparison across interviews (Bernard & Ryan, 2010).

A qualitative inquiry allows the researcher to design the interview sessions by using semi-structured process that suggests a certain degree of standardization of interview questions, and a certain degree of openness of response by the interviewer (Wengraf, 2001). The questions are specific in nature and relate to the overall research question and research purpose of the study. Conducting interviews can help reconstruct events researchers have never experienced and by putting together responses from separate interviewees, researchers can create representations of complex practices (Rubin & Rubin, 2012). In this holistic multiple case study an interview guide was prepared to ensure that the same basic lines of inquiry have been pursued with each participant interviewed (Patton, 2002). The researcher remains free to shape the conversation within a particular subject area, to word questions freely and to establish a conversational style but with the focus on a particular subject matter that has been predetermined (Patton, 2002). Having an interview guide with the interview questions prepared ahead of time helps make interviewing a number of different people more systematic and all-inclusive by delimiting in advance the issues to be explored (Patton, 2002).

Each interview question must be aligned with the problem and purpose statement, the research questions, and congruent with the theoretical framework (Wengraf, 2001). The interview protocol provides a framework within which the researcher will develop questions, sequence these questions, and make decisions about which information to pursue in greater depth (Patton, 2002). In-depth interviewing allows for the examination

of complex matters of the real world by exploring multiple perspectives toward an issue (Rubin & Rubin, 2012). Using an interview guide with interview questions makes sure that the researcher has carefully decided how to best use the limited time available in an interview session (Patton, 2002). Conducting interviews as an approach to data gathering allows researchers to see differing perspectives gathered from all angles which lead to more thoughtful and nuanced conclusions (Rubin & Rubin, 2012).

When using in-depth qualitative interviewing, researchers talk with those who have the knowledge and experience concerning the problem being investigated (Rubin & Rubin, 2012). Personal interviews allow the researcher to add impromptu questions to gain even further information or an understanding of the phenomenon being studied (Yin, 2009). Through these types of interviews, the researcher can explore in detail the experiences, motives, and opinions of the participants in an effort to view perspectives on the phenomenon being researched (Rubin & Rubin, 2012). Planning the interviewing sessions with the research participants is of utmost importance (Rubin & Rubin, 2012). Options such as starting with minimal intervention so as to build up knowledge of, and rapport with, the participant, then shift to a more investigative style, and then end with a much more relaxed and conversational mode (Wengraf, 2001).

Two important steps in deriving scientific evidence in a qualitative research study are to develop a set of questions to guide the interview process and to conduct face-to-face interviews (Stake, 2006). Information should be obtained from the research participants based on what they think and feel about the topic without any preconceived ideas or viewpoints from the researcher (Groenewald, 2004). Qualitative researchers

listen to hear the meaning of what participants tell them and then the researcher cannot figure out the meaning, follow-up questions to gain clarity and precision are asked (Rubin & Rubin, 2012). Qualitative research questions have certain characteristics that include seeking to reveal the qualitative factors in experience and do not seek to predict or to determine underlying relationships (Seidman, 2013).

A set of open-ended interview questions was used (see Appendix A) that was asked of all participants in a semi-structured interview format that allowed for follow-up questions to be asked (Rubin & Rubin, 2012). This unstructured or semi-structured interviewing process often can provide greater breadth of information than do other types of interviews given its qualitative nature (Denzin & Lincoln, 2008). This type of interview is used when the researcher is looking for rich and detailed information and not simply a yes or no answer to the research question (Rubin & Rubin, 2012). To receive fresh commentary about the subject matter, the interviewer must be careful in wording of the questions in order to avoid asking leading questions that might bias the participants answers (Yin, 2009). There are several major reasons and benefits for the use of open-ended interviews: (a) the exact instrument used in the evaluation is available for examination by those who will use the outcomes of the study, (b) the interview is highly focused so that participants time is used efficiently, and (c) analysis is facilitated by making responses easy to find and compare (Patton, 2002).

Denzin and Lincoln (2008) claimed the focus of interviews is moving to incorporate the *hows* of people's lives (the constructive work involved in producing order in everyday life) as well as the *whats* (the activities of everyday life). All of the questions

in the interview were grammatically concise, clearly and precisely worded, easy to understand, and as unbiased as possible. The interview questions have been field tested with one IT professional working in network security for a college, one IT professional that is a CIO of IT at a college, one IT faculty member who teaches computer and information security, one faculty member who teaches English, and a professional from the Communications field. None of the individuals in the field test was interviewed for the qualitative multiple case study. NCU's policies on field tests are as follows and each one was achieved for this study: (a) to have experts in the field review a draft of the interview questions for a qualitative study to ensure for its credibility and dependability, (b) the sample population of a field test is not the same as the study population as the dissertation study, (c) the majority of the time, the field test involves experts in the field and this reduces the risks of the study tremendously, (d) a separate IRB review is not needed for field tests, (e) experts reviewed the interview questions to make sure it captures the key concepts being studied, the questions make sense, the questions were not awkwardly phrased, and (f) the "findings" from the field test were used to refine and revise interview question items.

The interview protocol included questions that were correlated directly towards answering the research question of this study. Miles and Huberman (1993) stated that the researcher should put information into different arrays, making a matrix of categories and placing evidence or research findings within these categories. Yin (2009) added it is important to do this and by doing so allows the researcher to put the evidence in some preliminary order. Yin also suggested that all empirical research studies, including case

studies, have a story to communicate. The required analytic strategy is the researcher's guide to crafting this story, and only rarely will your data do the crafting for you (Yin, 2009). Stake (1995) said the patterns will be known in advance, drawn from the research questions, and should serve as a template for the analysis. For the most important data, using pre-established codes will be useful but to go through the data looking for new ones (Stake, 1995). The coding categories will usually be made before any data are collected and only rarely will important assertions result from surfing through the data (Stake, 1995). For these reasons listed, the interview questions contained pre-established themes, codes, and/or categories that were used to directly answer the research question.

Boyatzis (1998) added that themes may be initially generated inductively from the raw information or generated deductively from theory and prior research. This type of thematic analysis enables researchers to use a wide variety of types of information in a systematic manner that increases accuracy or sensitivity in understanding and interpreting observations in their research (Boyatzis, 1998). A good thematic code is one that captures the qualitative richness of the phenomenon and is usable in the analysis, interpretation, and presentation of the research (Boyatzis, 1998). Miles and Huberman (1994) stated the method they prefer when it comes to creating codes is that of creating a provisional "start list" of codes prior to fieldwork. The list of potential codes may come from the conceptual framework, list of research questions, hypothesis, problem areas, and/or key variables that the researcher may bring to the study (Miles & Huberman, 1994). Dey (1993) suggested the term category which indicates another type of coding and stated that the application of names to passages of text is not arbitrary but involves a

deliberate and thoughtful process of categorizing the content of the text. The concepts of categories or codes may originate from the research literature, previous studies, topics in the interview schedule, hunches the researcher has about what is going on, and so on (Gibbs, 2007). Gibbs also added it is possible to create a collection of codes without using them to code the data and encouraged the researcher to build up a list of key thematic ideas before coding any text. King (1998) recommended the construction of a template which is a hierarchical arrangement of potential codes.

### **Population**

There are over 4,000 distinct colleges and universities that make up this educational system throughout the United States of America and 220 located in North Carolina alone. Public academic institutions including senior academic colleges, community colleges and private academic institutions were chosen for this study. The academic institutions varied in size such as the number of students whereas, some colleges and universities had a small student population (under 5,000 students) and some colleges and universities had larger student populations (over 20,000 students). Participants were not selected from colleges and universities outside the state of North Carolina due to resource constraints. In this study, a total of 13 participants were involved. Interviews were conducted with 13 members from within IT departments of 12 separate and distinct colleges and universities in order to gather data relevant to fulfilling the purpose of this study (Stake, 2006; Yin, 2009).

### **Sample**

Purposeful sampling was used for this multiple case study. Purposeful sampling focuses on selecting information-rich participants who will best bring to light the



questions under study (Patton, 2002). The goal of purposeful or theoretical sampling is to select cases which are likely to replicated or extend the emergent theory (Eisenhardt, 1989). The first standard in selecting cases should be to maximize what the researcher can learn (Stake, 1995). The researcher's sampling strategies should align with purpose of the study, questions being asked, and any constraints to be faced (Bernard & Ryan, 2010). Researchers need to avoid haphazard selection of participants and need to focus on a deliberate or purposeful selection or a randomized selection (Wengraf, 2001).

The participants that were included in this research were currently employed personnel working at a college or university physically located within the state of North Carolina. Each participant was currently working in the IT department of their academic institution with responsibility over the IT security of their institution. Twelve separate and distinct colleges and universities were visited and included in the study. The participants have responsibility in managing or supervising the department and responsibility dealing with computer, network, and/or information security. The benefits of a multiple case study will be limited if fewer than four cases are chosen, or more than 10 cases are chosen but balance and variation are essential and the opportunity to learn is of primary importance (Eisenhardt, 1989; Stake, 1995; Stake, 2006). Patton (2002) claimed there is no set rules for sample size and the number of samples should be chosen based on what the researcher wants to know, the purpose of the inquiry, what's at stake, what will be useful, what will have credibility, and what can be done with available time and resources. Yin (2009) stated that if six to 10 cases turn out as anticipated, then this would provide compelling support for the primary set of propositions. Patton (2002)

stated that when dealing with sample size and with all aspects of the research, it is ultimately subject to peer review, validation, and judgment and the researcher is obligated to discuss how the sample affected the findings, along with the strengths and weaknesses of the sampling procedures.

In selecting cases or participants to be included in the study, the researcher should consider those which are likely to lead to understandings, to assertions, and to even perhaps generalizations (Stake, 1995). Twelve colleges and universities were identified to be included in the study and written permission has been granted from the appropriate administrator or supervisor of the academic institution. An email was sent to the administrator asking for permission to contact a member of the IT department (see Appendix B). The written permission from the institutions was documented and attached to the IRB. Once permission was obtained and the IRB was approved, one prospective participant from each institution was contacted by telephone or e-mail in order to invite them to participate in the study and given a dissertation participation information letter (see Appendix C). Each participant interested in participating in the study was provided an informed consent form to authorize and return to the researcher (see Appendix D). Scheduled interviews with the 13 participants were conducted one-on-one and face-to-face to accommodate the participants and/or interviewer schedules. There were 13 interview participants contacted and written permissions granted for each by college and university administrators. This information was not be presented in the dissertation for privacy and ethical concerns but was listed in the IRB application for university review.

The opportunity to gain learning and understanding is the primary importance and therefore, balance and variety in selection of cases are essential (Stake, 1995).

Participants were referred to by a number rather than their name in this study in order to maintain participants' anonymity and confidentiality. Participants were not asked to reveal any proprietary or confidential information regarding their academic institution. Interview questions were designed to gain participants' perspectives about generalizations about IT security as it relates to colleges and universities. Interview sessions lasted on average 45-55 minutes for each participant. Participants had the option to decline any interview question or terminate the interview at any time.

Participants did not receive compensation or any other type of incentives to participate in this study. To avoid any kind of discrimination, prospective participants were not screened on factors such as age, gender, race, religion, ethnicity, or cultural background. Participants were offered to be given an electronic copy of the executive overview of the study once completed and approved. Selection criteria were used to ensure that participants met certain requirements in terms of industry related knowledge, experience, responsibility within the IT security department of their employer. Participant eligibility requirements were based on if they (a) are involved in or responsible for IT security, and (b) work for a college or university within the state of North Carolina.

### **Materials/Instruments**

Once participants are carefully chosen, the interviewer is the primary research instrument used in the study (Patton, 2002; Yin, 2009). Prior to collecting data from actual study participants, I conducted a field test to ensure that the basic interview design,

techniques, and structure were appropriate for the study (Seidman, 2013). The use of field tests in qualitative research provided a clear description of the focus of the study, permitting the researcher to concentrate on data collection on a narrow spectrum of proposed topics (Teijlingen & Hundley, 2001). Field tests assist the researcher in determining whether there are flaws, limitations, or other weaknesses within the interview protocol that should be revised prior to the implementation of the study (Teijlingen & Hundley, 2001). Using a pre-determined set of interview questions that have been field tested by experts, should increase the probability that all key topics were discussed.

In qualitative interviews, researchers inquire for more depth but on a narrower range of topics (Rubin & Rubin, 2012). Once the first interview was conducted, no major modifications to the interview guide protocol were made. Two questions were added to the interview guide after the third interview was conducted in order to gain a better understanding of a certain topic that surfaced at one institution. Any major modifications made to the interview protocol, even after expert panel review; could make it difficult to compare data collected from earlier interviews to data collected from later interviews, thus lessening the validity and meaningful interpretation of the results (Seidman, 2013). The questions used in the interviews were planned in advance, organizing them so they are interrelated to one another to acquire the information needed to complete the study (Rubin & Rubin, 2012). Conducting in-depth interviews can be extensive in nature and very time consuming because it takes skill and experience on the part of the interviewer (Klenke, 2008).

The interview guide has been field tested with a total of five professionals that include a professional in the field of English, one in Communications, and three professionals within the field of Information Technology and Security. Field testing the interview protocol is conducted in order to confirm that questions are appropriate and unlikely to cause risk or discomfort to participants. Modifications to the interview questions based on the field test participants' feedback have been made and were documented in the IRB according to NCU's requirements. A meeting has taken place with the field test participants where changes recommended were discussed and implemented in the interview protocol. Due to performing the field test, the number of questions was reduced from 36 to 25. After additional review and analysis of the interview protocol, the number of questions was once again reduced to a final total of 17 questions. However, after the third interview, there were two additional questions added to the interview protocol due to information surfacing from a particular institution and an experience they had. Approval was received to add the additional questions to the interview guide and start asking the additional questions with the fourth participant.

The field test participants helped narrow down the questions by eliminating questions that were redundant, awkwardly worded, or not related or necessary. It was determined that the interview questions would likely provide valuable insight and information relevant to the research questions being asked. Grammar was also checked and several items changed to be grammatically correct and more easily understood. Bernard and Ryan (2010) stated to use the data gathered in early interviews to keep expanding the analysis to assist in later interviews. Due to the more subjective nature of

in-depth interviewing, analyzing and interpreting the data is a more complex task than with structured surveys (Klenke, 2008). While time consuming, the potential information to be gathered from the interviews was very valuable when determining the unique information security needs for institutions of higher education.

The interview protocol included questions that were correlated directly towards answering the research question of this study. Miles and Huberman (1993) stated that the researcher should put information into different arrays, making a matrix of categories and placing evidence or research findings within these categories. Yin (2009) added it is important to do this and by doing so allows the researcher to put the evidence in some preliminary order. Stake (1995) said the patterns will be known in advance, drawn from the research questions, and should serve as a template for the analysis. The coding categories will usually be made before any data are collected and only rarely will important assertions result from surfing through the data (Stake, 1995). Boyatzis (1998) added that themes may be initially generated inductively from the raw information or generated deductively from theory and prior research. Miles and Huberman (1994) stated the method they prefer when it comes to creating codes is that of creating a provisional “start list” of codes prior to fieldwork. The concepts of categories or codes may originate from the research literature, previous studies, topics in the interview schedule, hunches the researcher has about what is going on, and so on (Gibbs, 2007). King (1998) recommended the construction of a template which is a hierarchical arrangement of potential codes. For these reasons listed, the interview questions contained pre-established themes, codes, and/or categories that were used to directly answer the

research question.

Informal conversation was used throughout the interviews to relax the participants and encourage a conversational dialogue while conducted in such a way the desired research data were collected. The researcher provided a consistent list of questions that was evaluated during the interviews, and during any post-interview follow-ups that were essential for clarification (Corbin & Strauss, 2007). Transcriptions of the interviews were sent to each of the participants to solicit feedback regarding any content discrepancies or errors as this is a form of triangulation which aided in reliability and validity (King & Horrocks, 2010). Interview participants were given a dissertation participation information letter and an informed consent form, which includes consent to audio recording agreement (see Appendix C and D) before the interviews were conducted. A high-quality digital recording device was used to record the face-to-face interviews once permission was granted by the participant and to the interviewer. Notes were taken as needed during each of the interviews or shortly thereafter in order to retain any needed information as to help assist in transcribing or analyzing the interview. Transcriptions were analyzed and compared with field notes to assess any errors or omissions during transcription. This type of in-depth interviewing has the benefit of allowing participants to describe what is meaningful or important to them, using their own words rather than being limited to predetermined sets of answers or categories (Klenke, 2008).

Researchers should use field notes to capture what will be heard, observed, and different thoughts and experiences as data is collected and reflected upon (Bloomberg & Volpe, 2012; Groenewald, 2004). There are several advantages and disadvantages of

taking notes during and after an interview session. Notes taken during an interview can help to formulate additional questions but may be a distraction, while looking over notes before transcribing may give early insights to the possibility of additional interviews (Patton, 2002). During the interviews, field notes were taken on thoughts, ideas, and did result in the addition of two more interview questions. Taking notes on what is said will facilitate later analysis and notes serve as a backup in the event of losing recorded data (Patton, 2002). Taking notes after conducting interviews and during fieldwork allows ideas and observations to surface and represents that beginning of data analysis (Gibbs, 2007).

Researchers also find it beneficial to keep a reflective research diary or journal in which they record their ideas, conversation topics, information about the research process, and anything else relevant to the research project and data analysis (Gibbs, 2007). A research journal was kept during the proposal stage, research stage, and analysis stage of the study. The research journal includes many ideas, topics of discussion, notes on communications with dissertation chair and graduate school representatives, and listed an outline of the next steps and what is involved in the next process of the research.

### **Data Collection, Processing, and Analysis**

Data collection in a qualitative holistic multiple case study may include a variety of methods such as: interviews, focus groups, direct observations, and written documents (Patton, 2002). For qualitative research studies, the most common method of data collection is interviews because interviews can provide a deeper understanding of a



phenomenon based on the experiences of the people directly involved in the phenomenon under examination (Wengraf, 2001). For this research study, data collection was completed by conducting interviews with 13 participants. Interviews allow the researcher to comprehend a phenomenon from the perspective of the participants (Bloomberg & Volpe, 2012; Patton, 2002). With the qualitative interviewing research method, the interviewer is considered to be the principal data gathering tool (Klenke, 2008). The use of open-ended questions used during the interviews will provide the researcher the ability to explore and probe for additional information (Denzin & Lincoln, 2008). Listed in Appendix A is the research questions that were used for the face-to-face interviews conducted in this study.

The qualitative interview usually begins with a social conversation designed at creating a relaxed and trusting atmosphere (Wengraf, 2001). It was the goal of the interviewer to conduct these interviews in comfortable surroundings in a conversation-like manner. Qualitative interviewing requires concentrated listening, an admiration for and curiosity about people's experiences and perspectives, and the ability to ask about what is not yet understood (Rubin & Rubin, 2012). For each of the interviews, a secure, quiet place was found and this is where the interview was conducted. For most of the participants, interviews took place in their office but for several participants the interviews were conducted in a conference room. A social conversation which included general introductions and information about the institution was first conducted with each participant. I asked each question slowly and spoke clearly and repeated the question if needed. Then, I concentrated on listening and clarifying any of the questions.

Once the IRB approval was received, an initial phone call was made or an email was sent to each of the potential participants individually. This information was obtained by conducting an Internet search on each of 12 academic institutions throughout the state of North Carolina. More than 12 was originally researched and permission granted to ensure at least 12 would offer their permission. The names of individuals working in the IT department were sought. The Chief Information Officer (CIO), Chief Technology Officer (CTO), or another manager within the IT department had already been identified, communicated with, received permission from, and documented in the IRB. The selected interview participant was contacted and an explanation of research intentions, procedures, and documentations such as consent and information forms was provided to each.

Memos were written throughout the research process and are used to make notes to the researcher concerning the data or any other applicable topic regarding the research or analysis (Gibbs, 2007). Groenewald (2004) presented four types of notes in his research, observational notes, theoretical notes, methodological notes, and analytical memos. Observational notes are used to record the events that happen during the interview process (Groenewald, 2004). Theoretical notes are used to help with deriving meaning of certain things whereas methodological notes are used as reminders or instructions for the researcher (Klenke, 2008). All four types of field notes were used to help ensure the reliability of the data gathered for the study. Analytical notes are used to summarize the events of an entire day about what was learned about concepts and patterns emerging from the data (Groenewald, 2004).

Each of these types of notes was used at some point throughout the entire

research process. The observational notes were used to record things that may have happened during the research process such as the need to clarify something or where we conducted the interview. Theoretical notes were used for the researcher to go back and look up certain words or phrases the participant may have used in regards to technical jargon during the interview. Methodological notes were used to make notes of where the institution, building, office, and participant was located and at what time they were available and any other instructions that were given such as checking in at the front desk or reception area. Analytical notes were used after each interview was conducted and summarized the interview process and noted any areas of significance. A research journal was also used to record and document thoughts, ideas, decisions, communications with committee chair, NCU policies and procedures, and other related information throughout the entire research process.

A unique identifier or number was assigned to each of the participants in order to maintain privacy throughout the study. Neuendorf, (2002) presented a comprehensive method of analysis that incorporates the complete transcription of each of the participant's interview. Specific steps were followed to group, analyze, and construct information taken from the data gathered during the interview stage of the research process. The steps of data analysis include: (a) collecting the raw data, (b) organizing the raw data, (c) reading data in its entirety, (d) coding or categorizing the data, (e) identifying themes or categories, (f) correlating the themes or categories, and (g) interpreting the meaning of the themes or categories (Creswell, 2009). There are certain advantages that exist for the researcher to perform the transcription of the interviews.

Transcribing the interviews allowed the researcher to begin the analysis and careful listening to tapes, reading, and checking of the transcript, allows the researcher to become very familiar with the content (Gibbs, 2007)

The challenge that exists at this stage of research is in making sense of the massive amounts of data that have been collected, identifying what is significant, and constructing a framework for communicating the core of what the data reveal (Bloomberg & Volpe, 2012; Patton, 2002). Once the researcher has completed conducting the research and collecting data, the focus becomes concluding analysis in which the researcher has two primary sources to consult in forming the analysis: (a) the research questions that were generated during the design phase of the study and prior to any fieldwork, and (b) analytical insights and interpretations that became evident during the data collection process (Patton, 2002).

Microsoft® Excel spreadsheets were used to record and organize participants contact information, to schedule interviews, and keep track of days and times interviews were conducted. Information such as the dates and locations of the interviews and other information needed was kept on this spreadsheet. These spreadsheet files were stored on a home computer and backed up to an external hard drive. This information is maintained in a safe environment at all times and the information kept confidential.

Interview sessions were digitally recorded by an electronic recording device. These recorded interview sessions were then transcribed into Microsoft® Word documents, organized by the participant number (participant names are not on this document), and was uploaded into NVivo10 qualitative software for purposes of coding,

categorizing, and analysis. Computer software programs, such as NVivo10, are available that can assist in classifying interview answers and counting specific key words, which may permit for some form of quantitative analysis (Klenke, 2008). The data organization provided by using the NVivo10 computer software program assisted in categorizing the data and identifying relationships in the data to develop emerging theory (Bazeley, 2007).

NVivo10 qualitative software, along with other similar software such as Atlas.ti, MAXQDA, and HyperRESERACH were all compared and analyzed. Comparisons were based on the cost of the product, amount of time the product can be used, tutorials available on the product's website, the ease of creating a new project, the process of coding, user-friendliness of the software and ease of navigation. The decision was made to adopt NVivo10 qualitative software due to its outstanding software capabilities, online help and support, and functionality it provides it assisting the qualitative researcher.

After conducting each interview, the recorded findings were taken from the audio recorder and transcribed to text data. Since the researcher is the one who conducted the interviews, and transcribing is such an important and lengthy process, the researcher did the transcribing as well (Wengraf, 2001). Hand written field notes were used by the researcher during the interview sessions to capture detailed description of participants' actions and to compare to transcriptions of each participant to look for errors or discrepancies (Creswell, 2009). Reliability of the findings was ensured by having participants evaluate their own transcribed interviews to ascertain that the transcripts accurately reflect what the participants voiced in the current research study (Gibbs, 2007; Yin, 2009). Further triangulation occurred in this study by providing participants'

interview transcripts and requesting feedback regarding accuracy and validity of transcriptions of their specific interview (Creswell, 2009).

After the data from this multiple case study had been collected and detailed transcripts of the interviews printed out, all data was coded by the researcher and entered into NVivo10. NVivo10 was developed by QSR International and intended to organize, store, and classify qualitative data (Leech & Onwuegbuzie, 2011). By conducting analyses with NVivo10 software, this increased the thoroughness of the qualitative data analysis procedures (Leech & Onwuegbuzie, 2011). Also by using the NVivo10 computer program, specific words and phrases were extrapolated from the transcriptions, which helped with understanding the results of the study. Computer coding means having software analyze a set of text or data, counting key words or phrases for hopes of finding patterns (Neuendorf, 2002).

Case folders were created in NVivo10 to assign numerical identification to each of the participants' transcriptions. Coding provided several benefits in the organization, processing, and analysis of qualitative data (Boyatzis, 1998; Gibbs, 2007). Qualitative analysis, allowed the researcher to transform this data into findings (Patton, 2002). Using a cross-group comparison was a very powerful tool for classifying patterns in data (Bernard & Ryan, 2010). Additionally, once all the data were organized in computer files, the researcher looked for individual concepts, themes, events, and other meanings that point to the research question and then placed an appropriate description data label next to each piece of data unit to allow future retrieval of the coded items (Klenke, 2008). A manual review of each transcript was read and reviewed several times over to assist in

the data gathering and theory generation. This process helped with identifying research data and categorizing said data as well as using the qualitative analysis computer assisted software program NVivo10.

Data were analyzed in hopes of converging upon a particular finding by using different sorts of data and data gathering strategies (Gibbs, 2007; Shank, 2006). The beliefs and biases of the researcher were set aside during the process of data collection, analysis, and interpretation (Bloomberg & Volpe, 2012; Patton, 2002). Even with just a few interviews conducted with the participants in the research study, patterns started to develop and formulation of hypotheses can begin (Bernard & Ryan, 2010). One of the most common methods of qualitative analysis is thematic analysis and this approach was very useful when analyzing data from interviews (Bernard & Ryan, 2010).

Using thematic analysis, data uncovered from the research participants was placed into categories and reported statistically through procedures commonly understood and accepted (Wolcott, 2009). Thematic analysis allowed codes to be grouped into patterns and then can also be used to find a theme in the information acquired from the participants and was used as (a) a way of seeing, (b) a way of making sense out of the data, (c) a way of analyzing information, and (d) a way of converting qualitative information into quantitative data (Boyatzis, 1998). When a pattern is located, the researcher will have good reason to suspect that something systematic is creating that pattern, or themes, and that these themes are emerging from the data (Shank, 2006). Boyatzis lists certain criteria that good codes should include: (a) a label, (b) a definition of what the theme is about, (c) a description of how to determine when the theme

appears, (d) a description of any qualifications or exclusions to identifying the theme, and (e) examples to eliminate any confusion while searching for the themes. Coding is a way of indexing or grouping the text in order to define it and establish a framework of thematic ideas about it (Gibbs, 2007). The process of qualitative data analysis and synthesis is an ongoing one, involving continual consideration about the findings and asking analytical questions (Bloomberg & Volpe, 2012).

Concerning qualitative research, one of the most common validation strategies is triangulation (Shank, 2006). Data triangulation, or triangulation of sources, includes gathering data from several different sources which were used in this research study (Denzin, 1970; Patton, 2002). Triangulation for a multiple case study strives to assure that the researcher has the picture as clear and suitably meaningful as it can be, relatively free from researcher biases, and not likely to mislead the reader (Stake, 2006). Using multiple methods or approaches of data gathering, or triangulation, allows the researcher to secure an in-depth understanding of the phenomenon being researched (Denzin & Lincoln, 2008). Stake asserts that triangulation is mostly a process of repetitious data gathering and critical review of what is being said.

In a qualitative study, triangulation produces the results by looking at how knowledge might be obtained from different perspectives (Shank, 2006). The most significant benefit in using multiple sources of evidence collection is the development of converging lines of inquiry, which is a process of triangulation and corroboration (Yin, 2009). Credibility of the research was improved through the use of triangulation in data collection using multiple data sources (Shank, 2006). The research methods of inquiry



for this study consisted of one-on-one, face-to-face, in person interviews. Triangulation provided a public inspection of the research process, and helps add validity, credibility, and confidence to the research study (Patton, 2002; Shank, 2006). Triangulation was achieved by using and then comparing the data retrieved from the different data gathering methods that included conducting one-on-one, face-to-face, in person interviews.

Triangulation allowed for a public examination of the process and helped add validity and confidence in the study as well (Shank, 2006). Also by providing vigilant step-by-step documentation of the analysis offers other researchers access to procedures and an implicit affirmation of the value of the research (Bloomberg & Volpe, 2012).

Stake (2006) suggested that triangulation is the effort used to assure that the right information and interpretations have been obtained. The use of triangulation helps lead either to confirmation that the data collected means what we think it means or to ideas about how the data would be interpreted differently by different people (Stake, 2006). The sources of data that were triangulated are the field notes taken after the interviews, the digital recordings of the interview sessions and the transcriptions taken from conducting the face-to-face, one-on-one, in person interviews. The transcripts obtained from conducting qualitative interviews produced large amounts of material in which the researcher must condensed, categorized, and interpreted to make meaningful (Klenke, 2008). Any case findings or conclusions are more likely to be convincing and truthful if founded on several diverse sources of information (Yin, 2009).

Dependability in a qualitative study refers to the ability to know where the data is coming from, how it was collected, and how it is used (Shank, 2006). The fundamental

strategy for warranting dependability is an audit trail that shows a clear and continuous path between the collection of data and its use (Shank, 2006). Dependability was increased by documenting all steps, processes, and procedures to provide an audit trail for review by other researchers (Miles & Huberman, 1994; Patton, 2002). If other researchers use the same procedures and processes documented in this study, they should collect similar findings and potentially make comparable conclusions based on the results gathered.

To enhance the validity and credibility and to clarify the data gathered from the research participants, each participant was given the opportunity to review the interview notes and transcripts of the actual interview (Bernard & Ryan, 2010; Denzin & Lincoln, 2008). Capturing the interview participants' perspectives on the phenomenon being researched was the main goal of transcription. One way of making sure an accurate description of the perception has been captured was to ask the respondents to review the transcript to make sure it is correct (Bloomberg & Volpe, 2012; Gibbs, 2007).

Participants clarified the data by confirming their answers or correcting any feedback that was recorded or transcribed in error. Allowing the interview participants to review the transcript recorded by the researcher allowed the respondents to confirm the transcript is acceptable, convincing, and credible (Gibbs, 2007). By using triangulation, the researcher used different sources of data in order to validate the findings (Denzin, 1970; Denzin & Lincoln, 2008; Patton, 2002).

The trustworthiness was evident in this research study. Trustworthiness is simply the degree to which the given research findings can be depended upon and trusted

(Shank, 2006). The trustworthiness of the data is tied directly to the trustworthiness of the researcher who collected and analyzed the data and their proven competence (Patton, 2002). Competence is then substantiated by using the verification and validation procedures essential to establish the quality of analysis and building a track record of quality work (Bloomberg & Volpe, 2012; Patton, 2002). Competence in the field along with proven competence in gathering and analyzing data has been accomplished and demonstrated personally. A detailed audit trail of all interviews was produced and notes preserved as well as any other documents collected during the study.

Transferability is the degree to which results of a qualitative research study can be transferred to a different setting or used with a different population (Bloomberg & Volpe, 2012; Shank, 2006). The establishment of transferability relies on the researchers to use adequate and detailed description in presenting and documenting all of the relevant details of the research process (Shank, 2006). An audit trail was documented to include all processes used in data gathering for the proposed study. Interview notes, field notes, research notes, and recordings were maintained but kept confidential. With this information in hand, another researcher can decide whether or not the process can be transferred to another setting or population (Bloomberg & Volpe, 2012; Shank, 2006).

Triangulation is the primary strategy engaged to control bias and establish valid schemes. The greater the agreement between different data sources on a particular issue, the more reliable the interpretation of the research (Denzin & Lincoln, 2008). Using multiple methods of data collection such as one-on-one, face-to-face in-person interviews lead to more valid, reliable and diverse data (Yin, 2009). Researcher bias is a possible

threat to validity and must be kept out of the process of data collection and analysis (Bloomberg & Volpe, 2012; Denzin & Lincoln, 2008). Therefore, qualitative researchers must be able to bracket personal values and pre-existing knowledge of the field by ascertaining the positions from which they are conducting the research (Klenke, 2008). Predispositions and biases were reduced by recording the interviews and taking detailed notes so multiple evaluations of what the participants stated may be reviewed. Controlling or bracketing researcher predispositions requires that the researcher recognizes that qualitative research is not value neutral (Klenke, 2008).

Credibility in qualitative research is partially achieved by showing that the researcher has communicated with people who are informed and knowledgeable about the research concerns (Rubin & Rubin, 2012). The interviewees chosen for this research study was asked prior to the interview if they have the credentials in both education and work experience within the IT field. The participants were currently employed in the IT department at the academic institutions. Credibility also comes from showing readers how carefully the researcher carried out the research and being able to report your findings in a transparent manner (Bloomberg & Volpe, 2012; Gibbs, 2007; Rubin & Rubin, 2012). To accomplish this, the interview notes, interview transcripts, and interview recordings were kept so if anyone wishes to check the data, they may do so (confidentiality is still to be maintained). In credible research, the data is consistent and cohesive instead of scattered and contradictory and deals with the degree of believability of the research findings (Shank, 2006). Credibility was improved by multiple data sources revealing to the researcher the same or similar information (Yin, 2009).

### **Assumptions**

The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. Several assumptions were being made for this research study. The first assumption was that the researcher must always be conscious of the fact that the work is always limited and empowered by the selection of participants, data, and methods to be used (Bloomberg & Volpe, 2012; Patton, 2002). Another assumption included in this study was that the participants are knowledgeable through their completed and continuing education and work experience related to IT security so that their answers given were true and reliable. Even though the researcher will make the assumption that the participant is trying to be as truthful as they can, there is a potential for errors to be made (Wengraf, 2001).

Other assumptions in this study include the participants understanding of the research procedures and assurance of confidentiality which was evidenced by their signed informed consent. The study participants shared their knowledge, perspectives, and perceptions based on their personal working experiences with the problem of interest. The main assumption of this research study pertained to the honesty and accurate reflections of the participants. However, by interviewing a number of participants, the researcher attempted to connect their experiences (answers to questions) and checked the comments of one participant against those of others (Seidman, 2013).

### **Limitations**

This study contains certain limitations, some of which were related to the common critiques of the qualitative research methodology in general and some which

were specific to this study's research design (Bloomberg & Volpe, 2012). One limitation of the study was that additional research will not be replicated at a future date to compare results with original findings. Interview limitations could include possible distorted responses due to personal bias, anger, anxiety, politics, and lack of awareness, along with recall error, reactivity of the interviewee to the interviewer, and self-serving purposes (Bloomberg & Volpe, 2012; Gibbs 2007; Patton, 2002). When conducting qualitative research, there was the possibility of limiting the study by introducing researcher bias and predispositions into the study. Another limitation of the study was the quality of information obtained during an interview is largely reliant on the interviewer (Patton, 2002). Being open and transparent reduced the probability that personal bias was introduced.

Since analysis ultimately rests with the thinking and choices of the researcher, qualitative studies in general are limited by researcher subjectivity, researcher bias, assumptions, interests, perceptions, and needs (Bloomberg & Volpe, 2012). Multiple methods of data collection such as face-to-face, in-depth interviews, as well as multiple participant groups, such as 12 different colleges and universities, reduced the possibility of a biased outcome. Limitations to the study included the limited size of the sample and the narrowing of the participants to colleges and universities only within the state of North Carolina. Because a small sample was used, other researchers may incur difficulty in generalizing the findings from this research to institutions of higher education across the nation or from a global perspective.

### **Delimitations**

A number of delimitations was apparent in the study and is discussed in order to provide transparency in terms of the choices made with regard to the design of this study. First the total number of participants being interviewed one-on-one, face-to-face and in person was limited to 13 individuals from 12 separate and distinct colleges and universities. One participant from each of the 12 selected colleges and universities was selected for one-on-one, face-to-face, in person interviews. There were two participants interviewed at the same academic institution because both participants were involved with information security. There were 12 separate and distinct colleges and universities visited, so this study was a good predictor of what these academic institutions' unique IT security needs are, but the results and data may not be used to generalize what all colleges and universities may need with regards to IT security. Another related delimitation is the boundary set for just public or private universities within the state of North Carolina. The study findings cannot be generalized to be appropriate for other colleges and universities outside of the state North Carolina or for-profit colleges and universities within the state or outside the state.

### **Ethical Assurances**

The most important aspect of ethics in research is to minimize the harm or cost and to maximize the benefit or value (Gibbs, 2007). It is important to communicate research intent, purpose and expectations to participants before conducting any interviews (Bloomberg & Volpe, 2012; Patton, 2002). Prior to conducting the interviews, participants and college and university administrators were made aware the purpose of the research study, data collection procedures, ethical standards, and the informed

consent process (Rubin & Rubin, 2012; Shank, 2006). Ethical concerns in research consist of several categories, informed consent (receiving permission by the participant after truthfully informing them about the research), protection from harm (physical, emotional, or any other kind), and the right to privacy (protecting the identity of the participant) (Denzin & Lincoln, 2008; King & Horrocks, 2010, Patton, 2002; Shank, 2006). As part of the ethical standards, participants were informed of their right to privacy, confidentiality, informed consent, and adequate protection of their information (Gibbs, 2007; Rubin & Rubin, 2012).

Another aspect of ethical research includes voluntary participation where the participants are not forced or coerced in the study and may withdraw from the study at any time (Klenke, 2008). Prior to the data collection process, the approval of the Institutional Review Board (IRB) was received. The IRB is an institution that ensures that researchers are conducting studies with integrity and protects the interest and integrity of the prospective participants in research studies (Rice, 2011; Rubin & Rubin, 2012). To protect the privacy of the participants, only the researcher has access to the digital tape recordings and the interview transcripts. Each digital tape recording and interview transcript was assigned a unique number to represent the names of the participants and institution. The real names of the participants or academic institution does not appear on any of the digital tape recordings or interview transcript files. The assigned unique numbers and the corresponding real names were recorded on a separate file which will remain confidential and no access will be allowed to these particular files. Participants were assured that their responses and actions would be reported in a fashion that would



not be traceable to them. Due to qualitative data being so rich and detailed, there is always a danger that confidentiality may be breached, so anonymity is especially important at all stages of the research process (Gibbs, 2007).

Prior to the data collection process, each participant and college or university administrator was given a dissertation participation information letter (see Appendix C) and an informed consent form (see Appendix D). The dissertation information sheet included a description of the study and an overview of the interview process. The informed consent form contained a brief description of the study, potential risks involved, terms regarding confidentiality, and the contact information of the researcher. The choice to withdraw at any time during the study was emphasized. Participants could withdraw from the study by contacting the researcher, and the participant would have been removed from the sample. All contents of the informed consent form were verbally explained to the participants and if the participants agreed with all the terms, he or she was asked to sign the consent forms. Before the interviews took place, the participants were given an opportunity to ask questions or express concerns about the research.

Participants were reasonably expected to be honest due to being highly sensitive information being asked during the interview. To help assure this, the interview was conducted privately and behind closed doors in a secured office with no interruptions and out of view of others. Participants and institutions were referred to by a number rather than their name in this study in order to maintain participants' anonymity and confidentiality. College and university names were also kept confidential and privacy protected just as the participants in the study were. Participants were not be asked to

reveal any proprietary or confidential information regarding their academic institution. Participants did not receive compensation or any other type of incentives to participate in this study. To avoid any kind of discrimination, prospective participants were not screened on factors such as age, gender, race, religion, ethnicity, or cultural background. Strict adherence to the guidelines of Northcentral University's Institutional Review Board and the ethical guidelines of the American Psychological Association was maintained during the entire research study.

### **Summary**

By conducting qualitative research in the form of a holistic multiple case study, data concerning recommended computer and information security tools, measures, methods, and training for institutions of higher education was discovered. The focus of this study was on what IT security measures were recommended to be implemented by these participants employed by colleges and universities to assist in protecting people, networks, computers, and information along with other assets and to achieve an overall reduction in information security attacks, breaches, and threats. Data collected through conducting interviews were used to record and document common thematic categories and patterns recommended and implemented by IT professionals employed at these institutions.

The research gained from this qualitative holistic multiple case study presented what employees of institutions of higher education perceived as being important to implement to protect information, networks, assets, and resources, from security attacks, breaches, and threats, as well as, assess the effectiveness of IT security implementations such as contingency planning and user awareness and education. The information

collected from this study can be used by IT departments when analyzing security measures and programs at other colleges and universities and other educational and academic institutions. Additionally, the common thematic categories and patterns determined based on the findings of the data could be used to develop a security implementation plan for other non-profit organizations such as hospitals, schools, municipalities, and associations.

## Chapter 4: Findings

The purpose of this chapter is to present the results, evaluation of findings, and a summary of the research conducted. This chapter begins with the purpose of the research study and revisits the main research question with which this study was based upon. The results section presents the findings and analysis of the 13 in-depth, face-to-face, semi-structured interviews, which were conducted on IT employees of colleges and universities within the state of North Carolina. The results presented are based on these 13 participants' experiences of working in the IT departments in these institutions of higher education. The evaluation of findings section presents briefly what the findings of the research study means. Chapter 4 concludes with a discussion that summarizes the key points discussed in the chapter.

The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. There were a total of 13 participants as holistic units of analysis selected from 12 distinct and separate colleges and universities within the state of North Carolina. Each of these participants were employed by the institution and worked in the IT department. At one institution, there were two participants interviewed. In-depth, face-to-face, semi-structured interviews were conducted to gain information for this study. Purposeful sampling of the colleges and universities within the state of North Carolina were based on institutions from the community college base, four year private colleges and universities, and four year public colleges and universities.

The breakdown of the colleges and universities that participated in the study included six community colleges, four private universities, and two public universities. Two participants were interviewed from one university due to both individuals working in the field of information security at that institution. Limited uses of demographic questions were asked of the participants in this study. Only the participants' title, gender, numbers of years working in the field of IT, and the educational background which may have included degrees and certifications were asked. Table 12 provides information of the interview participants' demographics and characteristics.

Table 12

*Participant Demographics*

Participants/Title	Gender	Educational Background	Years in IT
1 Chief Information Officer	Male	Bachelors	14
2 Senior Security Analyst	Female	Masters	16
3 Chief Information Security Officer	Male	Masters	24
4 Director of Computing Services	Male	Bachelors	31
5 Manager of Infrastructure Services/IT	Male	Bachelors	26
6 Information Technology Manager	Male	Bachelors	21
7 Network Manager	Male	Associates	28
8 Director of Information Services	Male	Masters	12
9 Chief Technology Officer	Male	Doctorate	21
10 Network Administrator II	Female	Associates	22
11 Network/Security Manager	Male	Masters	14
12 Chief Information Security Officer	Male	Masters	23
13 Information Technology Director	Male	Doctorate	21

All 13 participants had one or more certifications in the field of computer and information technology. Each participant was interviewed one-on-one and face-to-face, at their institution. On average the interviews lasted from 40-50 minutes. All of the participants answered all the questions and none were opposed to being recorded by an

audio-recording device. Each participant provided rich data for the study. Once the interviews were completed, the digitally recorded interviews were manually transcribed by the researcher into Microsoft Word documents to ensure anonymity and accuracy of responses. These documents were stored on a secured laptop and backed up on a secured storage device. Once the transcripts were transcribed into the Word document, it was then emailed as an attachment to the participant in order to review for accuracy, completion, and reliability. Most participants did not respond, two participants made some clarifications, and the remaining participants accepted the submission. Data analysis was performed manually on the transcripts as well as use of NVivo10 software was used to help analyze data and document thematic categories in answering the research question.

The research questions were postulated to obtain an understanding of what a sample of IT professionals working in IT departments in institutions of higher education warrants as being necessary to protect and secure information, resources, assets, and other data. To better understand the IT security tools, policies, procedures, and systems that are recommended by the IT personnel, the following research question was used to ascertain the IT security needs from 12 institutions of higher education which were located throughout the state of North Carolina.

**Q1.** What IT security components within academic institutions potentially contribute to improved IT security and reduce or eliminate possible information security attacks, breaches, and threats?

The research question to be used in this qualitative holistic multiple case study

helped identify the IT security needs for colleges and universities, as perceived by a sample of IT personnel within colleges and universities. The research question is focused toward addressing the purpose of the proposed study, which is to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. The results of the study may be useful for informing management of colleges, universities, and other educational institutions, the current IT security practices and, ultimately, helping to minimize the risk of IT security breaches.

### **Results**

An interview protocol that consisted of 19 interview questions was used to gather responses from the 13 participants to answer the research question. Interviews were conducted in order to answer what IT security components within academic institutions potentially contribute to improved IT security and reduce or eliminate possible information security attacks, breaches, and threats. Prior to conducting any research study interviews, a field test was conducted on the interview questions with one IT professional working in network security at a college, one IT professional that is a CIO at a college, one IT faculty member who teaches computer and information security, one faculty member who teaches English, and a working professional within the field of communications. None of the individuals in the field test was interviewed for the qualitative multiple case study. The benefits of conducting a field test are as follows: (a) to have experts in the field review a draft of the interview questions for a qualitative study to ensure for its credibility and dependability, (b) the majority of the time, the field



test involves experts in the field and this reduces the risks of the study tremendously, (c) experts will review the interview questions to make sure it captures the key concepts being studied, the questions make sense, the questions are not awkwardly phrased, and (d) the “findings” from the field test are used to refine and revise interview question items.

Ten themes or categories were established prior to any fieldwork and these themes were used to record the data received by the participants. Manually reading through the interview transcripts and using qualitative analysis software NVivo10, categories and themes were documented. Then, categories were organized using NVivo10 software. Approximately 10 major categories or themes emerged with several having sub-categories and are presented in Table 13.

Table 13

*Major Thematic Categories and Sub-thematic categories*

Major Thematic Categories	Sub-Thematic Categories
Defining and Identifying Terms	Attacks, Breaches, Threats
Common Types	Attacks, Breaches, Threats
Users' Responsibilities	N/A
Written Policies and Updating Them	N/A
Types and Benefits of Having Plans	N/A
Training	N/A
Top Major Risks	N/A

Top IT Security Issues	N/A
Best Information Security Practices/Tools Implementation	Hardware, Software, Procedures, Training
	N/A

---

**Defining and identifying terms.** Three interview questions were dedicated to gathering data on the definitions of attacks, breaches, and threats. Each participant was asked in a separate question to give how their institution would define each of them. These interview questions were asked of all 13 participants based on their own perspectives as it relates to their institution and all 13 provided definitions for each category.

Participant 1 defined attacks as “anything that tries to penetrate or bring our systems down to a stand-still or get student, employee, or faculty data.” Participant 2 added that “attacks are incidents that cause a negative impact on the system or network or on a user experience.” Other participants gave answers that concentrated on the unauthorized attempts to access information or information systems whether internally or externally. Two participants’ focused the definition of an attack as something unwanted and downloaded on machines without users’ knowledge. Participants 8 and 11 focused on attacks as “anything that disrupts the confidentiality, integrity, or availability of information” and “would prohibit users from doing their job.” Two participants stated that there is not a true formalized definition.

The second term or definition associated with computer and information security is breach or breaches. Several diverse definitions were provided by the participants who

include a majority focusing on unauthorized access into the systems or network and having data or other resources compromised or exposed. Participant 10 stated “a security breach is one of the earlier stages of security attacks by a malicious intruder such as hackers.” This participant also stated “security breaches happen when the security policies, procedures, and our systems are violated and depending on the nature of the incident, they can range from lowest to highly critical.” Participant 8 added that a breach could even be “an internal user leaking or losing their password and leaking information or passing information to an outside entity that could cause an attack.”

Finally, the third term or definition included in this theme is threats. The main area of conformity among the participants’ definitions focused on weaknesses or vulnerabilities within the computer and information system of the institution. Participants 3, 4, 8, and 12 all responded about how threats are the vulnerabilities within the system that hackers are constantly searching for because this then would be the start of an attack and possibly a breach. Participant 12 stated “in general I am not as worried about the threats as I am the vulnerabilities because I don’t necessarily care who is coming after me, I know if it is vulnerable and it’s on the Internet, somebody will find it and try to exploit it.” Participant 1 defined threats as “any attempt to collect information that can be used to bypass any of our security measures.” Participant 10 defined threats as “the potential of the occurrence of a harmful event such as an attack or a potential cause of an unwanted incident that may result in harm to our system or organization.” Participant 2 added threats are “everything bad that could happen...long list.”

Being able to identify and define the terms associated with computer and information security such as what exactly is considered an attack, breach or threat is very important to improving IT security. The first step in reducing or eliminating computer and information security attacks, breaches, and threats is to have a good understanding of what they each involve and what makes them dangerous and a potential risk for colleges, universities, and all organizations. Many of the participants presented various definitions of what an attack, breach, and threat are when talking about computer and information security.

**Common types of attacks, breaches, and threats.** This was another theme that had subcategories within it. Just as the definitions of the terms were broken down, the various kinds of attacks, breaches, and threats were also broken down and asked of all participants. Each of the 13 participants provided the major types of attacks, breaches, and threats that are most common for their institution. Attacks were the first subcategory, breaches the second subcategory, and threats were the third subcategory. For the first subcategory, table 14 illustrates the major attacks as presented by the participants. The column to the right lists how many participants stated that actual attack has happened at their institution.

Table 14

*Types of Computer and Information Security Attacks*

Types of Attacks (Participants Terminology)	# Times Reported by Participants
Phishing Attacks	8
Email Attacks	3
Denial of Service Attacks	2
Log in by Brute Force Passwords Attacks	2
Webserver/Web Application Attacks	2
PHP Remote Code Execution Attempts	2
Viruses	2
Unpatched System Attacks	1
Malware Infection	1
Scareware	1
Internet Born Attacks	1
Automated Malicious Software Attacks	1
Spyware Scenarios	1
Adware Scenarios	1
Website Attacks	1
Malicious Websites	1
Hi-jacking Attacks	1
Probes for FTP Servers	1
Spamming	1

Several of the participants shared a common answer for the second subcategory concerning the types of computer and information security breaches that have been most common at their institution. Accidental disclosure of data was a popular response and 6 of the 13 participants mentioned this type of breach had occurred at their institution. Various participants mentioned that many of the breaches do occur internally and not necessarily always originate outside the institution from an external user or intentional hacker.

The third subcategory within this theme is the common types of threats. When asked what computer and information security threats are most common for your institution, participant 2 stated “Anything you can think of. We have such a wide attack surface, we have every operating system possible, every type of mobile device on the network, networks are generally wide open and we have users all over the country and the all over the world.” Participants 3, 6, and 12 also expressed concern over threats to research data and intellectual property owned by the institution. Participant 5 explained that “most common security threats here are by far the unsolicited emails that try to attempt to get people to give information, those emails represent about 95% of all emails sent to an institution and only about 5% get in.” Participant 8 was concerned over threats of trusting the operating system is a concern and if you put trust in your firewalls and they are not doing the job they are supposed to do, then there are threats regarding this. Participant 8 suggestion is to pick the best equipment and software you can for your institution’s needs. Participant 13 took a total opposite approach to the way they view threats and stated “most of the threats would be internal.”

Being aware and knowledgeable of the many various types of attacks, breaches, and threats that are currently being used to attempt to do harm or are actually causing harm to an organization should increase the likelihood of an institution's IT department to be able to put together a computer and information security strategy in which to reduce or eliminate computer and information security attacks, breaches, and threats. This area of computer and information security is constantly changing as more and more types of attacks, breaches, and threats are being created daily and used to gain unauthorized access to an organization's systems and data.

**Users' responsibilities.** The topic of discussion about users' responsibilities, which include faculty, staff, and students, is one that took much time to respond to and discuss by each of the participants. Numerous participants' responses were several paragraphs long and included much information about policies and handbooks for both employees and students. This theme helped focus on the research question what IT security components within academic institutions potentially contribute to improved IT security and reduce or eliminate possible information security attacks, breaches, and threats. All 13 participants believe to some extent that protection of the college's or university's computers, information, data, and other assets resides somewhat on the faculty, staff, and students of the institution, in other words, the users.

Included in this area of focus were several responses on academic freedom where the participants stated educational institutions such as colleges and universities have this understood code of academic freedom, where there is more computing freedom, which means less control and restrictions on computer usage. For example, several participants

stated that their institution cannot do any content filtering on the activity that is moved through the Internet. Reasons listed commonly deal with nursing, biology, and healthcare students needing access to certain websites and resources that may be identified and/or blocked as pornographic content. Many of the participants stated there is no content filtering due the culture that surrounds academic and research freedom at their institution. Participant 7 stated “Something that might be considered pornography, you can’t block that because health sciences needs that, like in biology class. So you can’t just block all nudity let’s say.” Participant 13 gave a very specific example of how at their institution they do lite content filtering and one time a group of nursing students needed to order life-like mannequins from an adult toy store because these mannequins were more life-like than the ones at the medical products store. Participants 10, 11, and 12 all stated they have tried to implement content filtering but because of academic freedoms and the culture at their institution, they were not successful and told not to block information.

All 13 participants felt that users are to be held responsible to some degree for information security on their work computers. Participant 1 commented “before you can hold them responsible you have to make sure they have informed knowledge that there is a policy and that they are required to uphold it. They have to know what the policies are and there has to be a clear outlined policy that your institution follows...that’s the real trick there is you have to follow it.” Participant 10 contributed “users must understand the importance of securing passwords, encryption keys, and PIN numbers and keeping those confidential...using careful practices when accessing the Internet and email, they



must understand the critical nature of this and if they do not follow these policies, they could possibly have to deal with certain implications of data loss or possibly disciplinary action.” This particular participant brings up a common point among several of the participants and that is disciplinary action.

As far as disciplinary action taken against the users, 6 out of 13 participants referenced this as a possibility when users disregard institution owned policy on computer and information security. These participants stated that this type of incident would be handled by the Human Resources Department and not by IT, for the faculty and staff of the institution. Participant 11 commented “we do have policies in place and there is some enforcement but there is really no ramifications for violating these policies. It’s a ticket, sometimes an incident report but nothing, no punishment or sanctions have been imposed upon the individual that causes the problems.”

This interview question did ask the participants to break their responses down between employees of the institution (faculty, staff, and researchers) and students of the institution. Participant 2, 5, 7, 8, 9, 12 specifically mention a distinction between students and reference a student handbook that lists computer and information security requirements. If students are found in violation of these policies, they are often referred to the student honor code or student honor board. Participant 12 stated “we have a requirement where students live on campus, so they have a home life that still runs over our network, so when they are in their academic area doing things it is different than when they are in their dorm doing things. We are trying to set up different mechanisms

to allow much more freedom to do things that would be unacceptable in a business environment, so what they do at home is different than what they do at work.”

Another key point presented by a majority of the participants is the very popular BYOD (Bring Your Own Device) trend happening at academic campuses across the state and the nation. This is where students as well as the faculty and staff and often members of the community bring mobile devices such as laptops, tablets, and smartphones onto campus and use the institution provided wireless network. I started asking participants if computer and information security issues were different with institution owned computers verses non-institution owned computers and received varying responses on how the IT Departments are working with the popular trend of BYOD. **Bring-your-own-device** was mentioned by 9 out of 13 participants as an information security concern for their IT department.

Participant 2 wants their institution to communicate to users and make it clear to them that there is a distinct difference between institutional managed machines and personal machines, between institutional accounts such as email and personal email accounts and make a distinction which ones should be used for which things. However, participant 6 added “I don’t see much of a difference in institution owned and non-institution owned because really my focus is on data and to me it doesn’t matter if the breach occurred on your personal machine or on one of our lab machines.” Participant 9 indicated “one distinction that we do make is you don’t have to abide by the university’s policies for your mobile devices as long as you don’t connect it to our network, or use our information system, but as soon as you do that, they fall under the university’s policy.”

Participant 10 agreed “we have to be more cautious with institution owned computers and we try and step back away from users computers and say we are not responsible for your computer and devices, however, we do have certain criteria they must meet such as they need to have anti-virus on their machine. What we have done now is we segregated the students off on their own network, which aids us in protecting our network.” Along the same thought, participant 11 adds “for our wired network, it has to be college owned equipment or the owner of that piece of equipment has to sign two contracts with us to gain access to the wired network, wireless network goes straight out to the Internet, it doesn’t access any of our inside, non-public resources.” Most of all the participants mentioned that their institution now has a separate wireless network in which students, guests, and the public may access.

Participant 3 commented on responsibility of users “I think everyone has personal responsibility to their system and data for which they are using. Some staff are more responsible or should be held more responsible than others for example, IT staff because of the nature of the access they have and their responsibility for maintaining the systems for which they are responsible.” Participant 5 agreed, “I feel and this is just a tech guy talking but I feel the bulk of the responsibility for the security of the data that we are entrusted with falls to us, it’s up to us to put in the right tools, appliances, and even create behavior models that prevent that.” Participant 13 added staff is held to a higher responsibility at their institution because of the access to sensitive information relating to HR, payroll, and finance areas. Participants 7, 9, and 13 mentioned their institution has a policy manual or handbook that each employee must read and attest to the fact they have

read the computer security related policies, understand these policies, and agree to abide by these policies. Then each employee must sign and date the document. Participant 4 believes training is the key to everything and states “I cannot make one policy that affects everybody. The culture of our university makes it difficult to apply any policies across the board.”

Much discussion took place in this area of computer and information security and many different viewpoints were exposed from the participants in how users should be held responsible to some degree of security on their machines. All participants feel that users are to be held to some degree of responsibility but the IT department currently faces many challenges involved with colleges and universities such as academic freedom and the popular trend of bring your own device (BYOD) on campus. Additionally, there are numerous challenges with not only the employees of the institution but with the students as well. Each of these components of user responsibility does need to be considered when composing a computer and information security strategy in which to reduce or eliminate attacks, breaches, and threats.

**Written policies and keeping them updated.** Another major area of discussion was concerning written policies and what should be included in them and how often are they updated. Some participants presented very basic attributes of discussion and others went more in-depth and gave specific responses. Participant 1, when asked about what should be included in a written policy concerning computer and information security for your institution, stated “All the standards that you’re holding the person accountable for. The policy is laid out and what the processes are and what it comes down to is having a

school adopted policy that everybody is aware of.” Participant 2 added “The main things I think would be making it clear that users of the network and users of institution owned systems have responsibilities and that if they don’t meet those responsibilities that there could be consequences and then give example.”

Participant 3 contributed “I think acceptable use is the approach that many schools have taken and certainly the approach we have taken.” Participant 4 stated “We don’t have a specific policy for security, we do have an acceptable use policy and it’s on the website, published in the student handbook, faculty handbook, and staff handbook.” Participant 6 explained “Policy should set the expectations that we as an institution should have for our users and also give users the expectation of how we are going to handle their information. One of the things I have seen over the years is that people are starting to become concerned with what we as an institution are doing with their data.” Participant 8 stated “As far as acceptable uses, make it clear these systems are for work purposes.” Participant 13 indicated “The biggest points for me is number one the computer is not yours. Number two, because it is not yours and it is a state owned machine, you have to follow the state guidelines of whatever the security is and whatever the retention policy is of information. Too many people really think it is their own computer and then get mad when we tell them we can’t do stuff.” Participant 10 presented a breakdown and listed these to be topics within the written policy: purpose and scope of the policy, guidelines for day-to-day security practices, clear emergency procedures, definition of responsibilities, appropriate and enforceable sanctions, and references to any other supplemental documents that you might need. Participant 12

commented “We have an ethical use guide which is a little bit different in that it describes what the user can and cannot do, what faculty and staff or students can and cannot do and presents a list of things no one can do.”

A common area of protection computer and information security was answered with protecting your passwords and never sharing usernames or passwords, which was given by participants 1, 3, 7, and 12. Participant 2 noted “Forwarding your institutional email to an external account could be a bad thing or bringing your personal machine on the network or using a personal machine to access institutional data could also be a bad thing.” Participant 4 stated “You can’t use our network for profit sharing ventures; we prohibit peer-to-peer file sharing. In a written policy there should be and heavily enforced an encryption requirement for any portable device, either the drive or the files be encrypted, again our culture at the moment makes it very challenging to push that forward.” Participant 7 added “Users should be made aware that at the end of the day they log off their computers and all of their work should be saved to the file server for nightly backups.” Participant 8 commented “You should not be downloading any software you shouldn’t be, talking about copyrighted things. Don’t download music or videos that could get the institution in trouble as a whole.” Participant 11 shared “We put in what we had to for PCI requirements and we also want nothing that contains sensitive or confidential information to be exposed or out in the open when you are not in your office. You have to put it away, lock your workstation.”

Additional conversation on how written and documented policies within their institution will help contribute to improved IT security in reducing or eliminating

information security attacks, breaches, and threats included the following comments from the participants. Participant 3 noted “I like to see some additional things like you should take simple steps to protect your computer systems and data. The last thing I will note is I think it is very important for an institution to have a data classification standard and then tie very specific security rules to those pieces so public to all the way up to sensitive with increasing levels of security.” Participant 12 explained “It talks about who is allowed to monitor activity on a network or a computer. The differentiation between what monitoring is and what an investigation is which is where we target an individual and we want to know what you did and why and who can authorize that.” Participant 5 commented “The easiest thing for a person who is looking to get sensitive information out of an organization is to go through someone’s human instincts to help. I think what needs to be written into the process is the fact to open people’s eyes to those things that people might not be aware of, like when do you shred trash. A lot of that information we take for granted in the higher ed world and that is very sensitive and can be used to do some big damage to peoples identity.” Participant 9 stated “The points I would like to see covered are user responsibility, so you have to say you have a responsibility to and play a part in securing the sensitive data of the university. Controls, I think you have to give the user some sense of controls they are responsible to deploy whether it be anti-virus or encrypting data, but it does need to be things they can do, you can’t tell them they need to put up a firewall because they can’t do that, but it’s the controls they have the capability to affect and implement. I think you have to give some background context

as to why you're doing it and so that may be explaining what the risks are but it also might be explaining what the legal requirements are for why we are doing it.”

Another interview question asked dealt with how often policies and procedures are evaluated and updated at their academic institution and how this contributes to improved information security. All 13 participants answered this question with at least once a year, some participants stated even more often than annually. Participant 1 indicated “As we have a problem. I mean it really should be yearly or at least bi-yearly thing but it doesn't happen in practice.” Participant 3 added “Update more as needed as environment changes, technology changes, process changes.” Participant 5 explained “We are constantly looking at security breaches or security threats as they come in. We are constantly looking at virus outbreaks and constantly looking at the processes that we need to control that information. I don't know if we put a time frame around it. Certainly we do it two times a year.” Participant 6 stated “The goal is annually, reality it slips. Some of our regulations require annually and we have to attest, PCI being one of them. You have to do it annually, so those ones are going to be annually because we have to attest to doing it annually which means some of the other ones are going to slip.” Participant 7 agreed “We probably officially look at that once a year but every day we talk about stuff like how we can implement DNS more secure or how to use subnetting to lessen broadcast environments or how to treat student access. We are constantly talking everyday about stuff and changing the way we do things and improve.”

Additionally on the topic of how often are IT policies at your institution updated and how this helps with reducing or eliminating information security attacks, breaches,



and threats, participant 8 noted “We have a program review and information services operations manual here locally that we try to update once a year. We try our best to do that. Again, we have a lean staff and we kind of do it when we can. If there is a threat or something evolves in our world, we can address it then. Participant 10 added “We do that every year and this has been working for us and appears to be an adequate time to allow for documentation of new technologies and changes that happen and focus on how those implantations went and any changes that need to be made as they happen throughout that year.” Participant 11 agreed “Once a year. It is in the policy that everything must be reviewed at least once a year. Firewall rules we review every six months and other areas we have to review more frequently because of PCI and we are trying to become fully PCI compliant.” Participant 12 contributed “We have a yearly cycle and if they haven’t been updated you get flagged to update them. Some we do more often as needed.” Participant 13 indicated “About every six months. We are doing it every six months because when I got here we really had no policies in place and as we get more and more stuff, we do it because we keep getting new stuff. Six months is about right.”

It is apparently clear that there is a need for an institution to have clearly written policies concerning computer and information security. By the overall analysis of the importance of policies, there seems that there is no cookie-cutter approach or a one-size-fits-all policy that could be implemented across the board for all colleges and universities. Many different topics were discussed on what should be included in a computer and information security policy, all of which will add to the overall security strategy in order

to help reduce or eliminate computer and information security attacks, breaches, and threats. The one main area of agreement among the participants is that there does need to be a written documented policy on computer and information security and it should be examined and updated at least annually.

**Types and benefits of having plans.** All 13 participants were asked about having an all-inclusive comprehensive IT security plan, a disaster recovery plan, and a business continuity plan. These documented plans and procedures are part of the IT security components within academic institutions that potentially contribute to improved IT security. Table 15 lists each participant and which plan their institution currently has in place or is in the process of developing.

Table 15

*Types of Plans Participant Institutions Currently Have in Place*

Participant	IT Security Plan	Disaster Recovery Plan	Business Continuity Plan
1	No	No	No
2	No	No	No
3	No	No	No
4	Developing	Yes	No
5	No	Yes	Yes
6	Developing	Developing	Developing
7	No	Developing	Yes
8	Yes	Yes	Yes

9	Yes	Developing	Developing
10	Yes	Yes	Yes
11	No	No	No
12	No	Yes	No
13	Developing	No	Yes

---

When participants were asked if your institution could have an all-inclusive comprehensive security plan put in place, these were the responses. Participant 1 stated “You’re not going to have an all-inclusive, there’s no way to protect against everything because everything is changing at the speed of light. You don’t know what the attack areas are going to be tomorrow and it’s probably something you haven’t thought about. It’s a best guess of here is what we’re most worried about and we’re going to take these measures and adapt as the environment changes.” Participant 2 added “Every department and school is its own business entity, so to have an institutional level, all you could probably do really is to say you should have these things or you must have these things and then let each department or school determine up front what the organizational unit would be and implement at that level.” Participant 3 agreed “You are not going to have a one size fits all plan, especially in higher ed. You have at least or an audience of at least three different types of people and actually probably four different types of people at a university setting. Faculty, staff, and students and I would argue researchers are separate and all with different needs.” Participant 6 explained “Going back to the all-inclusive comprehensive IT security plan, I think you need it especially in security because security

is one of those fields if nothing is going wrong, you don't notice it. So you need it before it goes wrong and same as business continuity and disaster recovery.”

Participant 10 contributed “A security policy should fulfill many purposes to protect people and information, set the expected rules of the behavior by users, system administrators, management, and security personnel. It authorizes security personnel to monitor, investigate, and define the consequences of a violation, help minimize risks, it helps to track compliance with regulations and legislation and an all-inclusive plan would benefit most by offering all the required elements of the plan to ensure complete coverage of all the aspects of the plan are met.” Participant 11 commented “I do not think an all-inclusive IT security plan is possible because we have been severely strained budget wise and skating by on as little money as we can.” Participant 12 indicated “No, you can't have an all-inclusive comprehensive security plan because too many things change and it would be out of date and you spend your life updating it. So you have high level guidance and you write specific guidance where necessary where more detail is needed.”

Concerning the other plans such as the disaster recovery plan and the business continuity plan, participant 1 added “Your security plan and your disaster recovery plan and your business continuity plan is not three separate things, its one big living, breathing document that is not an IT driven feature. That is not the decisions IT makes.”

Participant 3 stated “I think it's important to have a disaster recovery because people have to understand in a disaster what its role is in terms of bringing up systems. So if we have a disaster and we lose the main data centers on campus, the question is where are we going to bring the systems back up, what systems will be brought back up and in what

order. So it's like having a game plan so at least you have a general idea of what you are going to do and more importantly so the community knows."

Participant 5 explained "The fact that revenue is driven off student admission and student retention, keeping students on campus and engaged, those processes cannot break down because of a technology failure. We are more and more thinking about how to keep this campus up and technology savvy in times of disaster. Being able to move to a secondary site and bring it up and commerce can still happen on campus, this is a huge benefit to today's college." Participant 6 stated "Because security is risk, disaster recovery, business continuity, it's all risk and you have to say here's what it's going to cost us if we are down for however long, what can we do. Also a part of that is necessary to say is what's the risk of these various things because you only have so many hours to put towards developing a comprehensive plan, figuring out which ones are going to give us the biggest bang for the buck." Participant 7 explained "Now we are actually getting a consultant to come in and help us write our business continuity and disaster recovery plan. We don't have an official disaster recovery site, but we do have a site laid out. So we are in the process of getting some equipment to get that started. We have not had a disaster recovery site but it is something we really need."

Having in place an information security plan, a disaster recovery plan, and a business continuity plan is an important part of organization's overall strategy when it comes to computer and information security. As apparent in Table 15, only two of the institutions have all three implemented, while several other institutions are currently developing. Having these plans assists the IT personnel in contributing to improved IT

security and will allow for a smoother transition from thwarting any attempts to attack the systems to dealing with a successful attack, breach, or threat. Hopefully by initiating these plans, the IT department will be able to minimize any successful attack to the institution's computer information system and network.

**Training.** All 13 participants were asked to describe how their college or university trained users to be aware of computer and information security and if the users are trained to be proactive in implementing computer and information security procedures. Nine out of 13 participants stated their institution does offer some type of minimal computer security training, while four did not offer any.

When asked about a formalized computer and information security program, Participant 1 commented "That's something I wanted to look into but other demands on my time have kept it from becoming a priority. I think it's something a lot of institutions fall down on. My last institution we had a bit of an issue with formalized training on it. The institution before that, the same thing. There's no real standardized here's what you need to know and what your expected to uphold and we need to do better on that front especially in higher education." Participant 2 contributed "We don't have any sort of required training. The university IT Security office is always open for invitations and occasionally we have a series of problems or a serious problem in a department that we know about, then we will offer to come to a staff meeting or a departmental meeting or meet with a group of students. But the best results we seem to have for educational efforts are in person presentations."

Participant 3 stated “This is really tough because in higher ed it is very difficult to mandate additional training. We do require HIPAA training for those who have HIPAA access. We require PCI training for those who have PCI access, but we don’t have general security training. What we have found works best is face-to-face interactions with folks. Computer-based training is easier to implement. We find it to be less effective and mandatory training is difficult at best.” Participant 4 added “We regularly have informational sessions but they are not required to attend. I have tried repeatedly when new people are hired to have them forced to go through a training session with us or HR who are trained to tell them their responsibilities and things to watch out for, but again our culture doesn’t allow for that.”

Participant 5 indicated “What we do here is on the faculty and staff side of things as part of your HR introduction is sort of a really quick lesson about things you should and shouldn’t open, things you should and shouldn’t send out, and to report security breaches when you see them. That’s part of what the faculty and staff go through. Students on the other hand, I don’t think are educated as quite as well as we want them to be educated.” Participant 6 commented “We have a number of training like sessions for our students, it’s not required. It is required as you move up the ladder in how much access you have and what data you have access to. There are forms you have to sign off on, so there is some knowledge transfer. In addition there is computer cyber security awareness month. We do numerous talks for the whole month, 4-8 presentations throughout the month. Participant 7 stated “We have a knowledge base. We have a website here at the college and you can log in with your account ID name and password

and there is a knowledge base there and we have lots and lots of training classes. The helpdesk usually leads those classes and that's where we teach people how to mad drives and about security and how to use email. They are voluntary but I think certain deans make their people go. Certain department heads approach it different but is all voluntary." Participant 8 stated "Here recently, I think it was last fall, we subscribed to SANS, the [www.SANS.org](http://www.SANS.org) organization and doing the human training. So everybody, faculty and staff had to go through securing the human. There were videos talking about attacks, malware, phishing. We were proactive in that way and sometimes we are reactive."

Participant 9 added "We have a number of facts and help pages on the university website that indicate what users are supposed to do and will walk them through various aspects of security. We do a number of in-person outreach sessions and those are administered by the information security officer. Those tend to be more departmental and focused. Around 75% of the time the ISO has reached out to the departments saying you know we can do this for you and 25% of the time a department head will say I would like someone to come into my department and talk about information security and is usually in response to an incident." Participant 10 stated "Users are trained and told to contact the helpdesk immediately if they suspect a security risk. Classes are held to train on various subjects such as anti-virus software, securing their computer when away from the desk and protecting student information. That's a big one. It is mandatory and then there are some that are elective based but most that we do in our area are mandatory."



Participant 11 explained “Right now we do our bi-annually employee meetings. We have a speaker talking about a topic or a specific subject and right now we are primarily focusing on areas surrounding PCI. I would like to expand that with regular training maybe through a Blackboard course where the employees would go through the material and take a test that verifies they did read the material and understand it. The employee meetings are mandatory.” Participant 12 stated “Well we have an employee here in the department that goes to all the new employee orientations and gives them a briefing on here’s what’s going on. We have periodic reminders and communications, university-wide communications. We hold probably four computer security 101 classes a year and anyone can sign up for them. We hold them in the auditorium and here’s the things you need to be doing here at work and at home to protect yourself. Not mandatory but we do get pretty wide engagement.” Participant 13 added “We don’t. That’s a big beef with me and that’s one of the things we are pushing for staff development for next year.”

Training is an important piece of an institution’s overall computer and information security strategy. Nine out of 13 participants explained their institution did some type of training and four did no training when it comes to information security. The overall atmosphere of this discussion seemed as though all the participants wanted to some type of training for the users but faced challenges such as time constraints, budget constraints, manpower constraints, and not being able to mandate it for the faculty and staff of the institution. Even fewer participants could get any kind of training in this area for the students of the college or university. The trend seems to be moving from the IT

department to the human resources department when the new employee is first hired. HR having the responsibility to explain what is acceptable use concerning computer and information systems of the institution.

**Top major risks.** All 13 participants were asked to discuss the top three major risks a college or university could experience if a successful computer and information security attack, breach, or threat would occur. Knowing what the top and most potentially dangerous risks are is an important component of the overall information technology security focus on protecting the institution. Table 16 indicates the top three major risks proposed by each participant (P#).

Table 16

*Top Three Major Risks of Information Security Attacks, Breaches, Threats*

P#	Major Risk One	Major Risk Two	Major Risk Three
1	Loss of student data	Faculty/staff information	Loss of service
2	Financial	Political	PR
3	User accounts exposed	Data breach	System compromised
4	Reputation	Financial implications	Legal
5	Identity theft of social security number	Identity theft of credit card number	Identity theft relating to health information
6	Student data	PCI data	HIPPA
7	Lost/stolen data	Remote access to an administrative desktop	Loss of network
8	Downtime	Data loss	Identity theft areas of
9	Fundraising activities	Healthcare components	Decreased enrollment
10	Network failure/down	Loss of confidential info	Fines
11	Compromised info	Denial of service	Electrical out
12	Reputational loss	Legal risk	Intellectual property loss
13	Access to student info	Finance	Identity theft

Participant 4 commented “Once you experience a breach, you are under attack from everybody else who wants to cause a breach. You’ve got to go through the process of how this happened. It may have just been a network person who set a flag wrong and a kid searches for a social security number and holy smokes look what I found.”

Participant 7 stated “Internal threats are the biggest threats to a college. It isn’t the external people; you block them with a firewall. But once you get inside there’s no firewall other than the local firewall on a desktop and virus protection. But that’s where your biggest threat is, internally.” Participant 8 stated “Those things are the things that will get you in the news.”

By examining table 16 it is apparent there are many risks involved that an institution could experience if a successful information security attack, breach, or threat would occur. Many of these are experienced by colleges and universities and have been very detrimental to the ongoing mission of the institution. Knowing the effects of a successful attack, breach, and threat is very important to the overall computer and information security strategy of an organization and may cause IT personnel along with other users to be more aware of the possibilities of this happening.

**Top IT security issues.** This topic was discussed with participants four through 13 only as it was added after the third interview was conducted. This topic of discussion was needed to clarify and focus on one top major IT security issue and to discover what this issue was as it pertains to the participants’ institution. Table 17 presents the top issue as stated by each participant.

Table 17

*Top IT Security Issue at Your Institution*

Participant	Top IT Security Issues
4	The challenge of securing portable devices
5	Prevention of ID theft
6	Phishing and spear phishing
7	Lost or stolen data, data protection
8	Keeping malware out of the network
9	Distribution of data in various locations
10	Protecting a vast amount of confidential and secure data
11	Resistance to change because they have always done it this way before
12	Getting all the pocket ID departments on the same page and following and following good security standards
13	Social engineering

Participant 5 stated “Protecting that information we are entrusted with. We have to uphold that trust on our end.” Participant 6 added “I’ve seen some of the phishing that people have responded to and it’s almost embarrassing.” Participant 19 explained “The bulk of the breaches as I have seen in my career have dealt with data that is just not well protected by accident. It didn’t take a super genius to break into it.” Participant 12 commented “They have shadow IT or pocket IT whatever you want to call it and there’s groups floating around and getting all of them to understand what good security is and to

follow good security is a task.” Participant 19 added “It’s social engineering. What I mean by that is that we have so many passwords and we are working on this with Forefront Manager. I can walk into, I know right now, at least 20 offices and flip over their keyboard and see their passwords everywhere.”

As table 17 presents the top IT security issues as presented from the perspectives of the study participants, it suggests a theory of there not being a cookie-cutter approach or a one-size-fits-all approach to computer and information security. Many of the participants designated different security issues as their top concern for their institution and therefore will change or modify the approach of an overall computer and information security strategy. However, this is a good starting point for contributing to improved information security in hopes of reducing or eliminating possible information security attacks, breaches, and threats.

**Best information security practices and tools.** Much discussion concentrated and focused on computer and information security best practices and tools. This is a major component of the IT security strategy of each institution in which could be used to improve information security. Each question was different in that it asked about diverse best security practices and tools based on use of hardware, software, processes/procedures, and education/training programs at their institution. All 13 participants gave responses based on what they would recommend for an institution of higher learning to implement as it relates to best practices. Table 18 illustrates hardware tools which is the first segment within this theme.

Table 18

*Best Security Practices and Tools-Hardware*

Participant	Best Security Practices-Hardware
1	Biggest thing is to do your research on your hardware vendors. Don't overlook physical security.
2	Network tools looking for known malware. Being able to give metrics on network usage.
3	Network security appliances. IPS. Firewalls. IPFire for malware detection. Vulnerabilities scanners. Dedicated hardware for incident response like external drives.
4	Encrypted flash drives. Two-stage password so you have a device that changes your password.
5	Firewalls. Behavioral type intrusion detection and intrusion prevention systems.
6	For the most part, you just need to make sure you have people skilled in all the various areas. Segmenting your servers.
7	UTM device. Firewalls (local and external). Email spam security appliance. NAC solution. Internal windows and virus update service. SonicWall 8500. Virus scanning. Content filtering.
8	Firewalls. IPS. Anti-spyware services. Network access control systems.
9	Firewalls. VPN. Intrusion prevention. Intrusion detection.
10	Firewalls. Packet filtering gateways. VPN remote access. Intrusion detection. Virus detection. Spare hardware items. Failover devices. Web content filters.
11	Wireless sniffer. CISCO wireless LAN controllers. Log server with Splunk running on top of it. Intrusion prevention system.
12	Locks. Readers. Badge readers. Cameras.
13	Firewalls. SonicWall high availability unit. Aruba wireless piece.

Participant 1 stated “If I can lay my hands on your hardware, you are done, you can’t stop me. If I can put physical hands on a switch, no amount of security will keep me out. Being able to get to the server room and get to a switch or anything like that is the biggest breach that most IT departments overlook.” Participant 3 explained “First of all don’t buy hardware unless you have the manpower to run it, software too. Security professionals in the security field sometimes make the mistake of having the budget to buy something but then not the budget to run it. That’s a very important distinction.” Participant 9 added “When you don’t have a firewall in place or you don’t have other tools in place, you are relying on the weakest link to provide security for the university. Whereas you have a firewall in place and you can develop a cohesive firewall strategy. You can control some of that risk at the border. You can’t control all of it, no tool is 100 percent but I think firewalls offers you the ability to put more control and granular control in place that otherwise would be permitted.”

The next area of concentration was concerning best computer and information security practices and how this relates to software. All 13 participants were asked to share some of the best information security practices relating to software tools they would recommend for a college or university to implement or to include in the overall institution’s information technology strategy. Table 19 presents the main recommendations from each participant.



Table 19

*Best Security Practices and Tools-Software*

Participant	Best Security Practices-Software
1	Any kind of auditing software that will remotely look at the PC and say here's everything that's installed on it and will let you know when violations have occurred.
2	Centrally monitoring tools like Nagios. Symantec. Any sort of end-point protection. Multi-factor authentication.
3	Encase forensics tool kit. BackTrack. Nmap. Vulnerabilities scanner software like Nessus or Rapid7. Malware analysis websites such as Anubis and Urlquery. Netflow analysis.
4	Identity finder. Vulnerability assessment.
5	Anti-malware. Anti-virus.
6	Making sure the tools are kept up-to-date. Up-to-date software.
7	Network monitoring tools. Network troubleshooting tools like Wireshark. Network access controls. Virus scan engines like MacAfee. VPN access from the outside. IP Seg. Malware protection.
8	Application called Deep Freeze.
9	Whole disk encryption. Anti-virus software. Having a two factor. Vulnerability management.
10	Virus protection. Spyware/malware protection. Software firewalls. Keeping your browsers up-to-date. Updating your OS on a regular basis. Web content filters.
11	Nmap for port scanning. Ping sweep. Vulnerability scans with Nessus. Intrusion prevention systems. CISCO tools. A firewall. BackTrack. Kali Linux a security testing suite.
12	Next generation firewalls. System integrity monitor or homegrown monitoring. Good logs. Netflow analysis. Intrusion detection/prevention. Anti-virus. Some type of scanner. Microsoft system configuration manager. Secure development of open-source software and websites.

- 13 SonicWall software. SonicWall Extender. Anti-virus and malware software. Turn on port security on every port.
- 

Participant 1 commented “There’s not a very easy, here is the prescription for a good secure software environment because it is so dependent on what your needs are.”

Participant 4 stated “Yeah there are applications like identity finder. Things like that that can scan things on the network to look for confidential information and say that person has something they shouldn’t have on their machine. You need to go talk to them about that.” Participant 5 added “I think software tools are thought of as anti-malware, anti-virus. Those types of things, but we don’t drive them down to the students like we should or require them to the students like we should. We are very protected on university owned equipment but not so much on student owned.”

The third area of concentration when looking at best computer and information security practices focused on methods, processes, and procedures. Each of the 13 participants was asked what they recommend as some of the best security practices relating to methods, processes, and procedures to for a college or university to implement in order to reduce attacks, breaches, or threats. Participant 2 explained “For our institution what has been helpful has been building consensus. Being helpful and building consensus on what is good security. It has not worked to try to put in policy and then require people to follow policy. It also turns out to be, according to lawyers, a worse thing is to have a policy you don’t follow then to not have a policy. So we have a much more consensus based and assistance based than enforcement based.” Participant 3 stated

“The first thing I like is I like to have our team kind of focus on different areas so we have an operations team that is really focused on using our tool sets. I would say operational what are your methods and practices for looking at your tools and looking at the information being presented and then acting on that in terms of okay, we may have a security incident over here, let’s go investigate. I think another important method is how do we evaluate some of the services from a security perspective or what is IT doing in general and then how do we contribute to that. Then lastly is incident response, having a very well thought out incident response plan.”

Participant 4 commented “This goes back to your question about training. People need to know what their responsibilities are, that what they do impacts everybody else.”

Participant 5 explained “I will go back to what I said before, I do not think there is enough focus on the non-technical security things that we do. Throwing stuff away.

When you have the documents and you are finished putting it into the system, what do you do with that document. I think the best policy and procedures we could implement here is an educational process about the importance of shredding and destroying hard documents after done working with them.”

Participant 6 contributed “There’s the common things like making sure your software is up-to-date. Security should never be a charge service. The issues with that is that people will not tend to notify us until they absolutely have to because it will affect their budget. The big thing to catch this as quick as possible, so I tend to rely on logs. Basically monitoring and quick response on the hey this looks abnormal.”

Participant 7 stated “Communication and documentation. Keep information updated and current. So information is the key and getting it out there and getting people to understand.” Participant 8 added “I think it is going to be and we need to do a better job of this is least privileges. Make sure users can do what they only need to do because if they have more privileges than they need, they could potentially cause an outage or delete files. So I think this is what we need to do a better job at to secure our systems.” Participant 9 explained “I think that universities should have strong sets of policies and procedures, so administrative practices for information security. I also think universities should have strong concrete practices for incident response and incident management, so when the bad thing happens, how do you respond to it in a timely fashion.” Participant 10 added “Schedule user training on a regular basis as hardware, software, and applications are constantly changing and users need to have refreshers to keep them in the loop and makes them feel more comfortable.”

Participant 11 indicated “If it’s not in writing, it doesn’t exist. You have to have some sort of policy approved by the board of trustees that you can point back to and say we need to do these things. Network access control, unless your environment allows visitors to connect to your network. You have to have some kind of knack to ensure that unauthorized users are not connecting. Participant 12 stated “A best practice is pushing things from a central source, controlling these things from a central source. Universities are notorious for having pocket IT departments everywhere that may or may not follow what they’re supposed to be doing or what a best practice is. Bringing it in and whether

or not you do it centrally but the validation and control centrally is important. Having standard builds. Having standard ways of doing things.”

The final area of importance when asked about best computer and information security practices related to education, training, and awareness programs. Each of the 13 participants was asked to discuss the best practices they would recommend for a college or university to implement dealing with these types of best information security practices. All 13 participants gave a response to this area of best practices and how this could be used to help assist in improving IT security at their institution of higher education.

Participant 1 explained “Teach your users why you do this. There’s too many things coming out of IT that we just say do and don’t worry about anything else. If you take 10 minutes to explain to people why you’re doing something, they usually receive it a lot better and will work with you to try and make things better.” Participant 2 stated “I would say as much in-person training as is possible. To have a really approachable training team.” Participant 3 added “Number one, don’t boil the ocean. You’re not going to be able to train everybody, so figure out what your high risk areas are, as an example, HR, finance. Those are areas you can impact directly.” Participant 5 stated “This isn’t so much towards the students but towards the staff and faculty that we constantly look at help desk tickets. What’s the trending issues on those tickets and how can we educate the process. How do we educate those tickets to a lower number, especially if we see a trend, What we don’t do well in higher ed is to look at the tickets holistically and say wait a minute, that’s really just a central issue and we can train that away. Can’t just train

someone one time and let them work here for 10 years. But on a periodic basis let them know what a critical role they play in regards to everyone's security information."

Participant 6 stated "So on the training, I think it may seem wasteful to give the same training year after year, but you've got to keep it up, because you're getting a whole new group and people tend to forget. But your whole population is basically cycling every four years." Participant 7 indicated "Some of the things we do is go to road shows with security vendors to learn about new things. We do a lot of reading online. Some guys are members of groups that meet once a month. We don't have to force anyone to do this but most of the guys would take the initiative to learn those types of things. We have an ITS website and sometimes we put things up there and same thing on the student portals. You can advertise stuff and put links to topics and stuff like that." Participant 8 commented "That SANS securing the human was pretty good. There are videos that are kind of funny and anything from FERPA to credit cards was covered. It's a work at your own pace, so you watch the videos and then there is a quiz afterwards. But it probably needs to be done on a consistent basis because people seem to forget." Participant 9 stated "I've seen in my career that having those in person delivery mechanisms generate much more success than having people go through a web-based training. Being able to sit down in front of someone and say this is why we do it and here is the risk for when we don't do it, I mean you can see the light bulbs going on when you're delivering that type of message."

Participant 10 explained "It should be focused on the entire user population. Create some type of professional development courses for staff and faculty. Create IT

policies and procedures and enforce those. Recognize users that are at different levels of education and experience with information security. Communicate policies and procedures to respective groups and communicate those as they apply to their different groups and departments, staff, faculty, students, as well as public guests.” Participant 11 commented “Unfortunately I have been told no to training over here. It is difficult to come by. I was able to join a couple organizations and get free training through those organizations. The Internet Storm Center is my default home page and I get a lot of information from them.” Participant 12 stated “A lot of the university websites are ran out there in the pocket IT groups and they get together and talk about stuff and we show up at that meeting and say okay here’s the security concerns related to this.” Participant 13 indicated “Well unfortunately for higher ed, it would have to be mandatory. We have tried to do it within professional development days, come here and learn about this. We have actually started what’s called NewsFeed, it’s like an internal Facebook page. What we are trying to do is let people migrate to this and we are not forcing them to come to this page. I put self-help tips about computers, guidelines, I’m throwing things out there about once a week to get people to follow that NewsFeed. Trying to trick them into learning something instead of making them learn it. I would like to see a formal thing done but right now it’s just not going to happen.”

This theme of best information security practices was separated into four different categories: hardware, software, processes/procedures, and education/training programs. Participants provided what they thought was a best practice for a college or university to implement in each of the categories in order to help contribute to an improved IT security

strategy for their institution. Knowing the best practices and best tools to implement should reduce or possibly eliminate potential computer and information security attacks, breaches, and threats. Again, no one-size-fits-all approach was revealed as participants recommended a vast array of hardware, software, process, and training programs for a college or university to implement.

**Implementation.** The final theme dealt with implementation of a computer and information security awareness program and how it should be implemented at a college or university. All 13 participants were asked to discuss on how they would implement or what would be included in the process in order to implement a computer and information security awareness program at their college or university in hopes of creating a more aware environment of the importance of computer and information security.

Participant 1 commented “I guess the first thing to do is a review of policy and user expectations of what you are allowed and not allowed to do and then go into more detail of if you violate this is what happens.” Participant 2 explained “There are such different user groups, takes such different ways to reach them but I think you have to have lots of buy in and support at the senior most management level. Whether that’s policy or not you have to have people that really believe that it is important and can see the difference that it can make and to provide both the political backing and the monetary resources to either provide computer based training or people to do in person training and figure out who should be required and who should be encouraged to get training.”

Participant 3 added “It goes back to an earlier question is identify who your audience is going to be because again I don’t think you can implement one that crosses the entire



university at one time. So identify who your audience is going to be. Number two identify if there is computer based training. That would be useful. Number three I would work with stakeholders in each areas of the university. You have to make it personal. You have to tie it back to something they are doing and why does it matter to me and could it happen to you.”

Participant 4 stated “It starts with HR when someone comes in new but it’s also incumbent upon IT. All the schools, all the deans of the schools to insist that annually there is some sort of tech event that everyone is required to go to or during a faculty meeting we come in and explain these are the policies and regulations. I think it’s fairly easy to implement if you have the backing of the senior administration.” Participant 5 explained “The difference between employees and students is that you can require employees to sit down and go through a security program. There’s not a lot of requirement on the student side to go through a program or process to what needs to be secured.” Participant 6 indicated “We’ve got pieces and parts of it. One thing we are adding is required training for all staff on just basic awareness, security awareness training, PCI awareness and those sort of things to targeted groups. So keeping it fresh in people’s minds.”

Participant 7 stated “Advertise it. That’s the way we do things around here is we advertise it. You might start a month ahead, saying we are going to have these security classes, send out to all faculty and staff emails saying to read this, plan on attending. We have held classes that were mandatory.” Participant 8 agreed “I would say posters. Put posters on the boards, email. Constant email reminders to think about these things when

using your PC. The self-paced learning, do that annually.” Participant 9 stated “If i were going to start one I would start with policies that listed out what the end user is responsible for and I would build the training out of that policy and i would focus on in-person delivery where possible. Where not possible I would do the online training.”

Participant 10 explained “The policies and procedures should be communicated to staff and faculty at the institution at the time of hire and throughout the term of their employment with communication through email and training sessions if needed.

Students must be made aware of policies and procedures at the time they are registered and become students of the college and in some written form so they know what is expected of them and go ahead and explain in the beginning these are our network usage policy and this is what we expect you to follow.”

Participant 11 stated “Put it on a blackboard course. We give them what we want and it is recorded in the class. I would like to put up awareness brochures and posters in certain areas where that would be more beneficial reminding people about the need to think about security. I was trying to get something set up like once a semester a general security session where people can come in and ask questions.” Participant 12 added “I would get with the equivalent of corporate communications and work with them to what works at the university. If I had dollars, I would buy a program from one of the companies that sells information awareness programs where they provide you the updates and you just distribute them. At my last company we did that. We got posters and things to put on web pages, email alerts, little snippets, rolling questioners, funny things, and a good system.” Participant 13 explained “Well we tried it. We actually have a cyber-

information course and that program. Actually tried to do a campus-wide send out with posters, etc. They took it upon themselves to let everyone know what was going on. It was interesting for about a month and then it kind of lost its steam and that's where it was. But from a training thing to train people about information security, they do this training session when they are first hired. Once a year we have a blackboard information security training for about a half an hour. Its watch a video, click, watch a video, click and that's what we are doing now.”

Each of the participants gave their opinion on what it takes to implement a computer and information security awareness program. They realize the importance of making all users aware of the importance of information security and how this could help contribute to improved overall computer and information security for the institution. Some participants had already implemented such a plan that advertise or focused on an aspect of computer and information security while others have not implemented an across the board awareness program at their college or university. Participants did discuss it was more popular to do an awareness program that included the faculty and staff of the institution but as seen before, more difficult to reach the students or to require any type of computer and information security awareness training for the students of the college or university.

### **Evaluation of Findings**

The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. The interview questions were asked

to obtain an understanding of what a sample of IT professionals working in IT departments in institutions of higher education warrants as being necessary to protect and secure information, resources, assets, and other data. Additionally, this study was conducted to better understand the computer and information technology security tools, policies, procedures, and systems that are recommended by the IT personnel working at North Carolina colleges and universities. Researchers have found IT security an important concern for organizations, but very few have focused on the specific needs of a college or university and due to increases in IT security breaches in educational environments, researchers have recommended that the needs of colleges and universities for the improvement of IT security be explored in more depth (Abbas et al., 2011; Fisher & Shorter, 2013; Guo, Yuan, Archer, & Connelly, 2011; Ma, Schmidt, & Pearson, 2009; Mensch & Wilkie, 2011; Werlinger, Muldner, Hawkey, & Beznosov, 2010). A comprehensive theory explaining computer and information security in institutions of higher education does not exist, and further research is necessary to define such specific and definite implementations of such for optimal protection (Ayyagari & Tyks, 2012; Collins et al., 2011).

The theoretical foundation used in this study rests upon several different approaches in computer and information security implementations. The data generated in this study provided a deeper understanding of the computer and information security implementations recommended by professionals working in these institutions in an effort to share the findings of this study and help develop guidelines and/or a road map for

information technology and security professionals to use at their colleges and universities or other educational related organizations.

Complexity Leadership Theory (CLT) is a theoretical perspective this study was based on. At its basic level, CLT is about leadership in and of complex adaptive systems or CAS (Uhl-Bien & Marion, 2009). Complexity Leadership Theory is a change model of leadership that assists management in understanding how to design robust, dynamically adapting organizations (Uhl-Bien & Marion, 2009). Complex adaptive systems (CAS) dynamics represents the self-organizing mechanisms through which complex systems develop and change their internal structure instinctively and adaptively to survive with their environment (Uhl-Bien & Marion, 2009). Information flow can occur when interacting adaptive leaders imagine and effectively advance new ideas, capabilities, opportunities, and possibilities within a dynamic context of CAS (Uhl-Bien & Marion, 2009).

The CLT theory has suggested a bottom up approach to be used to conceptualize IT use processes, in hopes to embrace the nature of technology, achieving a more holistic analysis of the active role IT plays in the entire organization (Nan, 2011). The CLT theory suggests that in recent years, more researchers have come to the realization that the uses and consequences of information technology are often created through self-orchestrated interactions among users, new available technologies, and institutional needs rather than commanded by organizational policies or management's decisions or intentions (Nan, 2011). This theory supported this study by the use of implementing information security technology by looking at what the users' needs are and looking at

the information flow throughout the organization or educational institution. The findings in this study support the Complexity Leadership Theory in that the IT personnel along with management at these colleges and universities must be able to quickly adapt to rapidly changing technological environments in order to better maintain confidential data and improve computer and information security.

To better understand the linkages between IT security and systems theory and how it relates to information security framework, Fielden's (2011) holistic view framework was also used to support this study. Fielden has presented a holistic model of information security used as a framework that includes the following six clusters: purpose and role of information security, societal trends, human elements, changing technologies, information security management, and complexity and interactions. The basis of this theory is that information security situations and research requires many different points of views as information security has progressed from computer scientists to include politics, economics, civil society, and the individual (Fielden, 2011). Systems theory of IT is about integrating technology at various levels by both the organization and the individual and that organizational and individual benefits derived from technology are contingent upon this level of integration (Fadel, 2012).

The findings of this study were in alignment with Fielden holistic model of information security. The following thematic categories are representative of Fielden's research and theory in regards to having a holistic view of computer and information security: users' responsibilities, written policies, types and benefits of having plans, training, best information security practices/tools, and implementation. Each of these

thematic categories represent a different tactic in approaching to deal with computer and information security and management of the academic institutions do not just rely on one tactic alone.

The duality of technology model is another supporting theory that was used in this study to examine how technology is changed and put in place by the people within the organization. This model builds on previous research that found technology to be the outcome of strategic choice and social actions (Orlikowski, 1992). The duality of technology examines the interaction between technology and organizations and suggests technology is a product of human action, while it also assumes structural properties (Orlikowski, 1992). Meaning, technology is physically constructed by individuals working in a given social context but is socially constructed by individuals through different meanings they attach to it and the various features they emphasize and use (Orlikowski, 1992).

The results of this study were consistent with this research and the links well with the duality of technology theory. Technology is always changing, always updating, always improving, and at a rapid pace. Strategic choice is a major attribute of the duality of technology theory and in each of the colleges and universities, the IT department personnel, along with management; choose which piece of computer and information security technology they will implement. There was not a one-size-fits-all approach and this was even mentioned by a few of the participants, for implementing computer and information security technologies. Each institution's IT department and management

must assess their needs and their computer and information security requirements and implement from this data.

**Defining and identifying terms.** It is important to be able to define, identify, and understand the unique terms associated with computer and information security. The results of this study revealed that although there is some overlap in each of these categories, there are distinct differences when asked to define them specifically. Whereas most of the participants stated no conformity in an exact definition of attacks, breaches, and threats, they were all along the same lines of thought.

**Common types.** This study revealed that the most common type of computer and information security attacks are phishing. At this time phishing attacks are identified as a major security threat and are so common because it can attack universally and capture and retain the users' confidential information (Jose & Lakshuni, 2014). Eight out of the 13 participants stated that phishing attacks are the number one computer and information security attacks present at their institution of higher learning.

**Users' responsibilities.** All 13 participants felt that users are to be held responsible to some degree for information security on their work computers. Spears and Barki (2010) researched the topic and conducted a study that indicated user participation contributed to improved security control performance through greater awareness, and greater alignment between IS security risk management and the business environment. As far as disciplinary action taken against the users, 6 out of 13 participants referenced this as a possibility for when faculty and staff disregard institution policy. Also, 6 out of 13 participants mentioned a different process when it involves students' responsibilities.



**Written policies and keeping them updated.** The findings of this study revealed numerous computer and information security topics should be included in a written policy for a college or university. For securing a computer system, a well-defined security policy is needed and can be used as the framework within which an organization establishes required levels for securing the systems (Singh, Chauhan, & Chandra, 2013). A policy is a statement of information values, protection responsibilities and organization commitment for a system (Singh, Chauhan, & Chandra, 2013). Many of the participants feel that information regarding what is acceptable, an acceptably use policy, should be included in the institutional document concerning computer and information security. Also, 6 out of the 13 participants felt that information regarding repercussions should be included in a written policy when an employee of the institution ignores the accepted policy. Organizations construct information security policies to provide employees with guidelines concerning how to warrant information security while they utilize information systems in the course of carrying out their jobs (Bulgurcu, Cavusoglu, & Benbasat, 2010). All 13 participants stated that a policy for IT security should be updated at least annually.

**Types and benefits of having plans.** There are three different types of plans that organizations can implement in the area of computer, network, and information security which include an information security plan, a disaster recovery plan, and a business continuity plan. All participants were asked if it is possible to have an all-inclusive comprehensive security plan at their institution. Twelve out of the 13 participants felt that there could not be a one-size-fits-all plan implemented due to the nature of colleges

and universities which include academic freedom and a broad set of users, for example faculty, staff, and students. A security policy varies for each organization, a common policy standard cannot be defined and a security policy implemented for one organization may not be sufficient for another (Singh, Chauhan, & Chandra, 2013).

The second type of plan an organization could implement is a disaster recovery plan and only 5 out of the 13 participants stated their institution had one in place. Just 3 out of the 13 participants were in the midst of developing a disaster recovery plan at the time of the interview. IT disaster recovery planning is no longer an option (Mohamed, 2014). To guarantee the sustained delivery of information technology, organization must engage in IT disaster recovery planning (Mohamed, 2014).

The third type of plan an organization could implement in the security area is a business continuity plan. Organizations can suffer substantial losses as a result of unforeseen business disruptions and in order to restore the organization's critical functions and reduce the impacts of a disruption, it is essential to establish business continuity planning (Tan & Takakuwa, 2011). Only 5 out of the 13 participants currently have a business continuity plan implemented at their institution and 2 participants stated their institution is currently in the development stage.

**Training.** Participants were asked about training activities and if their institution provided computer and information security training to employees and to the students. Of the different information security policy compliance approaches, training is the most frequently recommended in the literature (Puhakainen & Siponen, 2010). Some IT professionals are even stating that security awareness and training can be more of a

crucial factor than security technologies in contributing to the success of information security (Chen et al., 2008). Nine out of the 13 participants; institutions do provide some type of minimal computer and information security training, while four of the institutions did not offer any of this type of training for their employees. These four participants did mention that this training is mandatory. Only 3 of the 13 participants mentioned any type of information security training offered for students.

**Top major risks.** Participants were asked to list the top three major risks their college or university could experience if a successful attack, breach, or threat would occur. Eight out of the 13 participants listed some form of loss of confidential data/loss of student data/identity theft as the most detrimental risk if a successful attack, breach, or threat would occur at their institution. Confidentiality refers to only authorized parties or systems having the ability to access protected data and organizations involved with any kind of personal data are mandated to follow a country's legal framework that warrants suitable privacy and confidentiality protection (Zissis & Lekkas, 2012).

**Top IT security issue.** The top information technology issues were very broad, in that only two of the participants stated data protection as their number one security issue at their institution. Resistance to change was one participants answer due to the challenge the IT department is experiencing in getting users to change their philosophy on computer and information security awareness and precautions. Other participants mentioned the culture of an intuition of higher education too aides in this resistance to change the way things are done when it involves computer and information security.

Research has shown that implementation of information security or related processes often experiences problems of power relations, political games, and resistance to change, often occurring as a result of norms or culture in an organization (Smith, Winchester, Bunker, & Jamieson, 2010).

**Best information security practices and tools.** The first area of concentration on computer and information security best practices and tools related to what hardware would each of the participants recommend for a college or university to implement. Having a firewall was the most common answer with 7 of the 13 participants recommending having these. Other popular recommendations included having some type of vulnerabilities scanner, intrusion detection system, and an intrusion prevention system. Literature evidence suggests that over 60% of organizations are implementing technical information security countermeasures, including anti-virus software, firewalls, anti-spyware software, virtual private networks, vulnerability management, encryption of data, and intrusion detection systems (Ahmad, Maynard, & Park, 2014).

The next area of computer and information security best practices and tools are in relation to software. All participants were asked what they would recommend for a college or university to implement in regards to software to help deter any attacks, breaches, or threats. Eight out of the 13 participants recommended having some type of anti-virus software and malware detection software. One of the most common thing used to avoid viruses is using the proper antivirus software to protect our computers from the virus itself, spyware, and other unwanted software such as malware (Ganeshkumar, Arivazhagan, & Sundaram, 2013).

**Implementation.** The final theme focused on implantation of a computer and information security awareness program at the participants' institution. An organization's approach to information security should focus on employee behavior, as the organization's success or failure may be contingent on the things that the employees may do or fail to do (Veiga & Eloff, 2010). In addition to training and continuous communication, the role of campaigns in improving employees' information systems security policy compliance should be studied since campaigns have proved successful in changing human behavior (Puhakainen & Siponen, 2010). Numerous participants responded that you have to go back to your audience and know what their needs are, to follow and enforce already adopted institutional policy on the matter, to communicate and advertise the importance of information security. An information security-aware culture will minimize risks to the organization and therefore organizations have need of a comprehensive framework to cultivate an information security-aware culture (Veiga & Eloff, 2010).

### **Summary**

The first part of this chapter presented the purpose, the research question, and the results of this qualitative holistic multiple case study. The purpose of this study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. In-depth, face-to-face, semi-structured interviews were conducted on current IT employees at institutions of higher learning in North Carolina in order to gain information for this study. Rich data were collected by conducting these interviews with 13 participants working at each

institution between January 2014 and March 2014. None of the participants refused to be recorded or to answer any of the interview questions. Findings are organized by thematic categories that include the data captured by the participants in order to answer the research question.

The second part of the chapter presented the results section. The results section presented the rich data obtained from conducting the 13 interviews and contained 10 thematic categories in relation to computer and information security at colleges and universities. The thematic categories included defining and identifying terms, common types, users' responsibilities, written policies and updating them, types and benefits of having plans, training, top major risks, top IT security issues, best information security practices and tools, and implementation.

The final section of this chapter includes the evaluation of the findings section. The evaluation of the findings section presents the meaning of the research conducted. Participants presented based on their experiences working in an IT department at a college or university what they felt regarding computer and information security. Participants provided their perspectives on the importance and the need for computer and information security awareness at their institution and the need for protecting institutional information and assets.

## Chapter 5: Implications, Recommendations, and Conclusions

Chapter 5 presents a discussion of the implications, recommendations, and conclusions of the study. Limitations are discussed and how they may have affected the interpretation of the results. The findings from this study are evaluated by describing how the results respond to the study problem, fit with the purpose, demonstrate significance, and contribute to the existing literature. Recommendations for practical applications of the results are provided for both researchers and practitioners. Recommendations for future research are discussed. This chapter is concluded with a summary of key points presented in the chapter.

Computer and information security is a principal concern for IT management since hackers are directing their targets toward colleges and universities to steal and compromise computing resources, property, and data (Perkel, 2010). The costs associated with data breaches have increased and continue to motivate IT departments to implement new security of information protection measures (Hoadley, Deibel, Kistner, Rice, & Sokhey, 2012). Due to a more open academic environment and a rise in network connectivity, cybercriminals were increasingly looking at colleges and universities as a point from which to launch their attacks (Alwi & Fan, 2010; Kumari, Debbarma, & Shyam, 2011; Mensch & Wilkie, 2011; Perkel, 2010; Spanier, 2010). Raising awareness concerning information security issues faced by academic institutions is important because the majority of reported breaches in 2011 have occurred in an educational environment (Ayyagari & Tyks, 2012).

The specific problem addressed in this study is the increase in information security breaches impacting institutions of higher education (Ayyagari & Tyks, 2012; Collins et al., 2011; Perkel, 2010; Susanto, Almunawar, Tuan, Aksoy, & Syam, 2011). A gap in literature exists on IT security requirements for colleges and universities. Researchers have found IT security an important concern for organizations, but very few have focused on the specific needs of a college or university and due to increases in IT security breaches in educational environments, researchers have recommended that the needs of colleges and universities for the improvement of IT security be explored in more depth (Abbas et al., 2011; Fisher & Shorter, 2013; Guo, Yuan, Archer, & Connelly, 2011; Ma, Schmidt, & Pearson, 2009; Mensch & Wilkie, 2011; Werlinger, Muldner, Hawkey, & Beznosov, 2010). The importance of computer and network security at institutions of higher education has never been higher due to the numbers of breaches and costs associated with breaches (Kumari et al., 2011).

The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. There were a total of 13 participants as holistic units of analysis selected from 12 distinct and separate colleges and universities within the state of North Carolina. Face-to-face, one-on-one, in-depth interviews were conducted with 13 personnel working in the IT departments of 12 separate and distinct academic institutions for a total of 13 interview participants in order to gather data relevant to fulfilling the purpose of this study. The interview participants were IT professionals working in and having responsibility over IT security. The goal of



this study was to explore what aspects of computer and information security are not only important but what are required to be implemented for maximum computer, network, and information security.

The use of a qualitative method is justified because of the need for in-depth information from the research participants (Patton, 2002). Because of the minimum amount of relevant research data on computer and information security implemented at colleges and universities, this study was conducted in order to discover more comprehensive information regarding the topic (Collins et al., 2011). A qualitative research method is appropriate for this study focusing on a need for data that includes research participant's experience, knowledge, thinking, intuition, reflection, and judgment on the complex issues surrounding the unique needs of this population within an institution of higher education (Wengraf, 2001). A qualitative case study is suitable for this study because the design is used to enlighten those situations in which the intervention being evaluated has no clear, single set of outcomes (Yin, 2009). A multiple case study will allow the researcher to analyze within each setting and across settings and allow the examining of several cases in order to understand the similarities and differences between the cases (Baxter & Jack, 2008).

Limitations on the study included some that were related to the common critiques of the qualitative research methodology in general and some which were specific to this study's research design (Bloomberg & Volpe, 2012). One limitation of the study was that additional research will not be replicated at a future date to compare results with original findings. This is a limitation because similar research findings in the future

could or could not match the results of this study. The knowledge produced might not generalize to other IT personnel or to other colleges and universities. The findings produced from this study might be unique or exclusive to the twelve cases included in this research.

Interview limitations could include possible distorted responses due to personal bias, anger, anxiety, politics, and lack of awareness, along with recall error, reactivity of the interviewee to the interviewer, and self-serving purposes (Bloomberg & Volpe, 2012; Gibbs 2007; Patton, 2002). When conducting qualitative research, there was the possibility of limiting the study by introducing researcher bias and predispositions into the study. The results of qualitative research are more easily influenced by the researcher's personal biases and idiosyncrasies. This researcher bias is a possible threat to validity and must be kept out of the process of data collection and analysis (Bloomberg & Volpe, 2012; Denzin & Lincoln, 2008). Researchers must be able to bracket personal values and pre-existing knowledge of the field by ascertaining the positions from which they are conducting the research (Klenke, 2008). Predispositions and biases were reduced by digitally recording the interviews and taking detailed notes of what the participants stated.

Another limitation of the study was the quality of information obtained during an interview is largely reliant on the interviewer (Patton, 2002). Since analysis ultimately rests with the thinking and choices of the researcher, qualitative studies in general are limited by researcher subjectivity, researcher bias, assumptions, interests, perceptions, and needs (Bloomberg & Volpe, 2012). Limitations to the study included the limited size

of the sample and the narrowing of the participants to colleges and universities only within the state of North Carolina. Because a small sample was used, other researchers may incur difficulty in generalizing the findings from this research to institutions of higher education across the nation or from a global perspective.

The most important aspect of ethics in research is to minimize the harm or cost and to maximize the benefit or value (Gibbs, 2007). Prior to conducting the interviews, participants and college and university administrators were made aware the purpose of the research study, data collection procedures, ethical standards, and the informed consent process (Rubin & Rubin, 2012; Shank, 2006). As part of the ethical standards, participants were informed of their right to privacy, confidentiality, informed consent, and adequate protection of their information (Gibbs, 2007; Rubin & Rubin, 2012). Prior to the data collection process, the approval of the NCU's Institutional Review Board was received. Participants were assured that their responses and actions would be reported in a fashion that would not be traceable to them. Before the interviews took place, the participants were given an opportunity to ask questions or express concerns about the research. College and university names were kept confidential and privacy protected just as the participants in the study were. Strict adherence to the guidelines of Northcentral University's Institutional Review Board and the ethical guidelines of the American Psychological Association was maintained during the entire research study.

### **Implications**

Institutions of higher education hold massive amounts of personal information from students, parents, and employees such as income tax returns, employment history,

salary, loans, credit information, admissions records, and medical files (Jones, 2008). To better understand the IT security tools, policies, procedures, and systems that are recommended by the IT personnel, the following research question was used to ascertain the IT security needs from 12 institutions of higher education which were located throughout the state of North Carolina.

**Q1.** What IT security components within academic institutions potentially contribute to improved IT security and reduce or eliminate possible information security attacks, breaches, and threats?

The research question used in this qualitative holistic multiple case study helped identify the IT security needs for colleges and universities, as perceived by a sample of IT personnel within colleges and universities. The research question was focused toward addressing the purpose of the proposed study, which was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. The results of the study may be useful for informing management of colleges, universities, and other educational institutions, the current IT security practices and, ultimately, helping to minimize the risk of IT security attacks, breaches, and threats.

A total of 10 thematic categories were identified regarding the exploration of information technology security requirements for academic institutions in order to reduce information security attacks, breaches, and threats by this research study. These thematic categories were used when interviewing those participants who are involved in the daily operations of an academic institution's IT department. The 10 thematic

categories include: defining and identifying terms, common types of attacks/breaches/threats, users' responsibilities, updated written policies, types and benefits of having plans, training, top major risks, top IT security issues, best information security practices/tools, and implementation. Numerous colleges and universities have added security challenges, such as relaxed working environments, less formalized policies and procedures, additional vulnerabilities, and employees that are assigned many different tasks (Ayyagari & Tyks, 2012; Susanto, Almunawar, & Tuan, 2012). Research conducted by Garrison and Ncube (2011) found that educational institutions are more likely to experience an information security breach over other types of organizations including business/financial, medical, and federal, state, and local governments.

An interesting finding in this study is that the participants all believed that dealing with computer and information security is a major challenge at their college or university. This current research is consistent with past research in ways such as academic environments are less formalized due to the openness of the institution and its culture of academic freedom (Ayyagari & Tyks, 2012; Susanto, Almunawar, & Tuan, 2012). The implication of this current research may suggest there is a unique challenge in institutions of higher education due to the nature of the organization and may be the reason why these institutions are more likely to experience a computer and information security breach over other organizations.

Another interesting finding of this study involved the widening approach of overall computer and information security management. Information security management has developed into being a part of the organization's overall comprehensive

framework (Saleh & Alfantookh, 2011). To better prepare for the challenges of securing information, IT management has developed organizational structures and operational procedures surrounding technology (Cline, Guynes, & Nyanoga, 2010). Managing this technology and securing information is a crucial strategic objective (Smith et al., 2010). This philosophy is important because information has become and continues to be the lifeblood of modern organizations (Smith et al., 2010). All the participants believed that user responsibility, written policies, documented plans, training, and implementing security awareness programs across campus is as important if not more important than the technical pieces such as firewalls, anti-virus software programs, or intrusion detection and prevention tools. Management in various organizations needs to begin to increase their investments in information security by continually adapting and implementing a variety and more diversified security solutions (Shim, 2012).

An additional key finding in this study was the number of institutions that do not have a comprehensive IT security plan, a disaster recovery plan, or a business continuity plan. With the increase in IT security threats and intrusions during the first decade of the 21st century, it was critical that IT departments developed a comprehensive security program (Liu & Ormaner, 2009). Contingency plans help management prepare for unexpected events and can consist of major areas which include a business impact/risk analysis, an incident response plan, a disaster recovery plan, and a business continuity plan (Omar et al., 2011). In order to produce valuable, relevant information security plans, the information security manager must understand the objectives and strategies of the organization in order to create information security plans that fit the organization

(Young & Windsor, 2010). This current research agrees with past research in that having these three different types of plans is an important part of the overall computer and information security strategy (Ologunde, & Akinlolu, 2012, Omar et al., 2011, Liu & Ormaner, 2009, Young & Windsor, 2010). Participants disagreed with whether or not there could be an all-inclusive one-size-fits-all comprehensive information security plan, but they all did agree some type of plan was needed and it is possible to have separate plans for the separate needs of the institution.

Additional findings of the study related to user training and having a well-educated faculty, staff, and students in the area of computer and information security awareness. Often, the people working in the organization are considered to be the final and most important line of defense when dealing with information security (Benson & Rahman, 2011). The occurrence of information security breaches caused by internal users may be reduced if greater emphasis were placed on threats to information security that can occur when employees handle information in their day-to-day activities (Spears & Barki, 2010). Most users within the university are unconscious about information security (Kumari et al., 2011). The theory of utilizing end users as a line of defense is something management should contemplate using as a part of the overall information security strategy (Spears & Barki, 2010). Participants believed in requiring computer and information security training but are faced with many challenges in doing this or providing this service to the entire student body and all the faculty, staff, researchers, and other personnel associated with the institution. Participants realized training users just in

the basics of what to look out for in dealing with computer and information security, that benefits will arise and may help reduce security attacks, breaches, and threats.

The findings revealed from this study responded to the study problem, fulfilled the purpose of the study, demonstrated significance, and contributed to the existing literature. The information security environment have been continuously evolving and new threats to an organization are emerging frequently (Kolb & Abdullah, 2009). Many diverse types of attacks, breaches, and threats were presented by the participants as having experienced within their academic institution. Changing information security requirements is of substantial importance due to the fact that organizations must simultaneously provide information to their employees, customers, business partners, and governmental entities while protecting it from inappropriate access, use, and disclosure (Cline, Guynes, & Nyanoga, 2010).

### **Recommendations**

This research case study revealed interesting facts about how IT personnel at North Carolina colleges and universities are involved in awareness of and reducing or eliminating computer and information security attacks, breaches, and threats. In addition to contributing to the body of scholarly knowledge regarding computer and information security in academic institutions, the results of this study can also be used for practical applications. The recommendations presented below are for practical applications as well as for future research and are supported by research findings.

**Practical Applications.** Information security management has developed into being a part of the organization's overall comprehensive framework (Saleh &



Alfantookh, 2011). Raising awareness concerning information security issues faced by academic institutions is important because the majority of reported breaches in 2011 have occurred in an educational environment (Ayyagari & Tyks, 2012). Managers have faced various information security challenges due to uncertainties in new technologies, obsolescence of their security processes, and overall needs for changes in security requirements (Abbas, Magnusson, Yngstrom, & Hemani, 2011). Information technology (IT) security management encompasses a blend of expectation, discovery, and reaction type processes along with a chain of actions that necessitate continual monitoring and control activities used to lessen the chance of information security attacks (Issa-Salwe & Ahmed, 2011; Sehgal et al., 2011). Technological controls and solutions are effective after users are familiar and skilled at using them; therefore, computer and information security awareness can be more significant than the technology itself in certain circumstances and situations (Chen et al., 2008). Becoming too reliant on one security element, such as security technologies, can place the organization at risk due to the large percentage of security breaches that are results of other areas or weakness such as error in human behaviors (Fielden, 2011).

The results of this study can be used by management and IT department personnel in colleges and universities, along with other organizations who are involved in the field of information technology and security. The results of this study are relevant and applicable to faculty, staff, students, researchers, and others who are in any relation to an institution of higher education who seek to understand how their personal information and identity is protected and secured. The findings of this study will help management of

colleges and universities assess and align policies, procedures, and objectives to better align with computer and information security requirements. The findings will also help to better align a culture that is aware of computer and information security and make it part of the organization's overall strategic objective.

Recommendations based upon this study along with earlier research have provided that there is not one particular or specific strategy when it comes to computer and information security. What this study has shown is that there are many different and necessary parts to an overall computer and information security strategy for an institution of higher education. Many technological tools such as the use of certain hardware and software was provided by the participants in order to reduce or eliminate computer and information security attacks, breaches, and threats, but there were also many other aspects provided as well to help meet the same objective. Other areas such as holding users responsible for computer and information security on their machines, having and updating written information security policies and adhering to them, having documented information security plans, disaster recovery plans, and business continuity plans, providing training for users on a periodical basis and implementing a campus-wide computer and information security awareness campaign.

**Future Research.** Additional research should be conducted to add to or complement the findings of this study. Several possible recommendations for future research have emerged from this study and include additional studies designed to determine the extent to which these findings can be generalized to other academic institutions, other institutions in other states, and other educational institutions in other

geographical areas. Additionally, the current study could be replicated for just community colleges, for just private colleges and universities, or for just public colleges and universities. In addition, quantitative studies should be conducted in order to determine the degree to which findings from this study can be generalized to a greater number of colleges and universities and to include different states and geographical areas.

Further research should be conducted on the very popular trend of bring-your-own-device (BYOD). Much attention is being given to the many portable devices such as smartphones, tablets, and laptops that are being used to access the academic institution's networks. One reason for the increase in threats and vulnerabilities was the evolution of wireless networking found on many college campuses and gave rise to many serious security issues (Likhari, Yadav, & Keshava, 2011).

In addition, the 10 thematic categories identified in this study could have additional research conducted on them and be compared to previous studies of computer and information security to find any similarities or dissimilarities. Additional research designed to build upon the findings of this study can assist scholars, researchers, and practitioners in the field to determine the extent to which the findings from this study can be applied to other educational institutions or any other type of organization.

### **Conclusions**

Information security is a foremost concern for IT management since hackers are directing their targets toward colleges and universities to steal and compromise computing resources, property, and data (Perkel, 2010). The problem addressed in this study is the increase in information security breaches impacting institutions of higher

education (Ayyagari & Tyks, 2012; Collins et al., 2011; Perkel, 2010; Susanto, Almunawar, Tuan, Aksoy, & Syam, 2011). The purpose of this qualitative holistic multiple case study was to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. Using Complexity Leadership Theory, Fielden's holistic view framework theory, and the duality of technology model theory as the theoretical framework and foundation of this study, the specific problem was addressed and the purpose of the study was achieved.

The data generated in this study provided a deeper understanding of the computer and information security implementations recommended by professionals working in these institutions in an effort to share the findings of this study and help develop guidelines and/or a road map for information technology and security professionals to use at their colleges and universities or other educational related organizations. The findings of this study provide insight into the area computer and information security in that the participants all believed that dealing with computer and information security is a major challenge at their college or university. All the participants believed that user responsibility, written policies, documented plans, training, and implementing security awareness programs across campus is as important if not more important than the technical pieces such as firewalls, anti-virus software programs, or intrusion detection and prevention tools. An additional key finding in this study was the number of institutions that do not have a comprehensive IT security plan, a disaster recovery plan, or a business continuity plan. This current research agrees with past research in that having

these three different types of plans is an important part of the overall computer and information security strategy. Participants disagreed with whether or not there could be an all-inclusive one-size-fits-all comprehensive information security plan, but they all did agree some type of plan was needed and it is possible to have separate plans for the separate needs of the institution. Participants realized training users just in the basics of what to look out for in dealing with computer and information security, that benefits will arise and may help reduce security attacks, breaches, and threats.

The findings in this study support the Complexity Leadership Theory in that the IT personnel along with management at these colleges and universities must be able to quickly adapt to rapidly changing technological environments in order to better maintain confidential data and improve computer and information security. The findings of this study were in alignment with Fielden holistic model of information security. The following thematic categories are representative of Fielden's research and theory in regards to having a holistic view of computer and information security: users' responsibilities, written policies, types and benefits of having plans, training, best information security practices/tools, and implementation. Each of these thematic categories represent a different tactic in approaching to deal with computer and information security and management of the academic institutions do not just rely on one tactic alone. The results of this study were consistent with this research and the links well with the duality of technology theory. Technology is always changing, always updating, always improving, and at a rapid pace. Strategic choice is a major attribute of the duality of technology theory and in each of the colleges and universities, the IT

department personnel, along with management; choose which piece of computer and information security technology they will implement.

There was not a one-size-fits-all approach for implementing computer and information security technologies. Each institution's IT department and management must assess their needs and their computer and information security requirements and implement from this data. Information technology managers at institutions of higher education and any organization may benefit from this study and may be of interest to faculty, staff, students, researchers, and other practitioners. Overall, this study has extended the body of knowledge on computer and information security at colleges and universities within North Carolina and could be used to assess current computer and information security strategy in order to implement or improve upon this strategy.

## References

- Abbas, H., Magnusson, C., Yngstrom, L., & Hemani, A. (2011). Addressing dynamic issues in information security management. *Information Management & Computer Security*, 19(1), 5-24. doi:10.1108/09685221111115836
- Ahamed, S. (2010). The influence of scope and integrated experimental approaches to safe electronic commerce. *International Journal of Engineering Science and Technology*, 2, 448-456. Retrieved from <http://www.ijest.info/>
- Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, 25(2), 357-370. doi:10.1007/s10845-012-0683-0
- Almeida, F. (2012). Web 2.0 technologies and social networking security fears in enterprises. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 3(2), 152-156. Retrieved from <http://thesai.org/Publication/IJACSA/Default.aspx>
- Alwi, N., & Fan, I. (2010). E-learning and information security management. *International Journal of Digital Society (IJDS)*, 1(2), 148-156. Retrieved from <http://www.infonomics-society.org/IJDS/>
- Amancei, C. (2011). Practical methods for information security risk management. *Informatica Economica*, 15(1), 151-159. Retrieved from <http://revistaie.ase.ro/>
- Anand, V., Saniie, J., & Oruklu, E. (2012). Security policy management process within six sigma framework. *Journal of Information Security*, 3, 49-58. doi:10.4236/jis.2012.31006
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34, 613-A15. Retrieved from <http://www.misq.org/>
- Anonymous. (2010). Security first. *Nature*, 464, 1246-1246. doi:10.1038/4641246a
- Ayyagari, R., & Tyks, J. (2012). Disaster at a university: A case study in information security. *Journal of Information Technology Education: Innovations in Practice*, 11, 85-96. Retrieved from <http://www.informingscience.us/icarus/journals/jiteiip>
- Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for the novice researchers. *The Qualitative Report*, 13, 544-559. Retrieved from <http://www.nova.edu/ssss/QR/index.html>

- Bazeley, P. (2007). *Qualitative data analysis with NVivo*. Thousand Oaks, CA: SAGE Publications.
- Beebe, N., & Rao, V. (2010). Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process. *Communications of AIS*, 26, 329-358. Retrieved from <http://aisel.aisnet.org/cais/>
- Benson, K., & Rahman, S. M. (2011). Security risks in mechanical engineering industries. *International Journal of Computer Science & Engineering Survey*, 2(3), 75-92. doi:10.5121/ijcses.2011.2306
- Bernard, H. R., & Ryan, G. W. (2010). *Analyzing qualitative data: Systematic approaches*. Thousand Oaks, CA: SAGE Publications.
- Bloomberg, L. D., & Volpe, M. (2012). *Completing your qualitative dissertation: A road map from beginning to end* (2nd ed.). Thousand Oaks, CA: SAGE Publications.
- Boyatzis, R. (1998). *Transforming qualitative information: Thematic analysis and code development*. Thousand Oaks, CA: SAGE Publications.
- Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548. Retrieved from <http://www.misq.org/>
- Chander, S., & Kush, A. (2011). Security metrics and information systems in e-governance. *International Journal of Computing and Business Research*, 2(2), 1-13. Retrieved from <http://www.researchmanuscripts.com/>
- Chang, K., & Wang, C. (2011). Information systems resources and information security. *Information Systems Frontiers*, 13(4), 579-593. doi:10.1007/s10796-010-9232-6
- Chen, C., Medlin, D., & Shaw, R. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, 16, 360-376. Retrieved from <http://www.emeraldinsight.com/products/journals/journals.htm?id=imcs>
- Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, 35, 397-A3. Retrieved from <http://www.misq.org/>
- Cline, M., Guynes, C. S., & Nyanoga, A. (2010). The impact of organizational change on



- information systems security. *Journal of Business & Economics Research*, 8(1), 59-64. Retrieved from <http://journals.cluteonline.com/index.php/JBER>
- Collins, J., Sainato, V., & Khey, D. (2011). Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors. *International Journal of Cyber Criminology*, 5, 794-810. Retrieved from <http://www.cybercrimejournal.com/index.html>
- Computer Security Institute (CSI). (2010). *2010/2011 Computer crime and security survey*. Retrieved from <https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf>
- Corbin, J., & Strauss, A. (2007). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (3rd ed.). Thousand Oaks, CA: SAGE Publications.
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: SAGE Publications.
- Davis, G., Garcia, A., & Zhang, W. (2009). Empirical analysis of the effects of cyber security incidents. *Risk Analysis: An International Journal*, 29, 1304-1316. doi:10.1111/j.1539-6924.2009.01245.x
- Denzin, N. K. (1970). *The research act: A theoretical introduction to sociological methods*. Chicago, IL: Aldine.
- Denzin, N. K., & Lincoln, Y. S. (2008). *Collecting and interpreting qualitative materials* (3rd ed.). Los Angeles, CA: SAGE Publications.
- Dey, I. (1993). *Qualitative data analysis: A user-friendly guide for social scientists*. London, England: Routledge.
- Donlevy, J. (2011). Teachers, technology and training: Shrinking schools and hard choices. *International Journal of Instructional Media*, 38(2), 111-112. Retrieved from <http://www.adprima.com/ijim.htm>
- Eisenhardt, K.M. (1989). Building theories from case study research. *The Academy of Management Review*, 14, 532-550. Retrieved from <http://www.aom.pace.edu/amr/>
- Enescu, M., Enescu, M., & Sperdea, N. M. (2011). The specifics of security management: The functions of information security required by organizations. *Economics, Management and Financial Markets*, 6, 200-205. Retrieved from <http://addletonacademicpublishers.com/economics-management-and-financial-markets/journals/emfm/about-the-journal.html>

- Fadel, K. J. (2012). User adaptation and infusion of information systems. *The Journal of Computer Information Systems*, 52(3), 1-10. Retrieved from <http://iacis.org/jcis/jcis.php>
- Farrell, R. (2010). Securing the cloud—Governance, risk, and compliance issues reign supreme. *Information Security Journal: A Global Perspective*, 19, 310-319. doi:10.1080/19393555.2010.514655
- Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *Communications of AIS*, 28, 329-356. Retrieved from <http://aisel.aisnet.org/cais/>
- Fielden, K. (2011). An holistic view of information security: A proposed framework. *International Journal for Infonomics*, 4, 427-434. Retrieved from <http://www.infonomics-society.org/IJI/>
- Figg, W. (2008). Computer security breaches: A threat to credit sales. *Review of Business Information Systems*, 12(4), 7-12. Retrieved from <http://www.cluteinstitute.com/journals/RBIS.html>
- Fisher, K., & Shorter, J. (2013). Emerging ethical issues: universities and information warfare. *Journal Of Academic & Business Ethics*, 71-10. Retrieved from <http://www.aabri.com/jabe.html>
- Fisher, W. P., & Stenner, A. (2011). Integrating qualitative and quantitative research approaches via the phenomenological method. *International Journal of Multiple Research Approaches*, 5(1), 89-103. doi:10.5172/mra.2011.5.1.89
- Folorunso, O., Akinwale, A., & Ikuomola, A. (2010). Using visual analytics to develop situation awareness in network intrusion detection system. *Computer and Information Science*, 3, 240-251. doi:10.5539/cis.v3n4p240
- Ganeshkumar, K., Arivazhagan, D., & Sundaram, S. (2013). Strategies of cybercrime: Viruses and security sphere. *Journal of Academia and Industrial Research (JAIR)*, 2(7), 397-401. Retrieved from <http://jairjp.com/>
- Garrison, C., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216-230. doi:10.1108/09685221111173049
- Gibbs, G. (2007). *Analyzing qualitative data*. Thousand Oaks, CA: SAGE Publications.
- Gillon, K., Branz, L., Culnan, M., Dhillon, G., Hodgkinson, R., & MacWillson, A.

- (2011). Information security and privacy-Rethinking governance models. *Communications of AIS, 2011*, 561-570. Retrieved from <http://aisel.aisnet.org/cais/>
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33-56. doi:10.3233/JCS-2009-0398
- Goyal, S. (2012). A survey on the applications of cryptography. *International Journal of Engineering and Technology, 2*, 352-355. Retrieved from <http://www.ijetch.org/index.htm>
- Groenewald, T. (2004). A phenomenological research design illustrated. *International Journal of Qualitative Methods, 3*(1), 1-26. Retrieved from <http://ejournals.library.ualberta.ca/index.php/IJQM/index>
- Grummon, P. T. H., (2010). Trends in higher education. *Planning for Higher Education, 38*(3), 51-59. Retrieved from [https://www.scup.org/page/SCUP\\_PHE](https://www.scup.org/page/SCUP_PHE)
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*, 203-236. Retrieved from <http://www.jmis-web.org/>
- Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management & Computer Security, 17*(3), 276-289. doi:<http://dx.doi.org/10.1108/09685220910978112>
- Guynes, C. S., Wu, Y., & Windsor, J. (2011). E-Commerce/Network security considerations. *International Journal of Management and Information Systems, 15*(2), 1-7. Retrieved from <http://journals.cluteonline.com/index.php/IJMIS>
- Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security, 17*, 388-407. doi:10.1108/09685220911006687
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:10.1016/j.dss.2009.02.005
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6

- Hoadley, E. D., Deibel, J., Kistner, C., Rice, P., & Sokhey, S. (2012). Seeking best practices in the balancing act between data security and operational effectiveness. *International Journal of Management & Information Systems*, 16, 183-188. Retrieved from <http://journals.cluteonline.com/index.php/IJMIS/index>
- Hurley-Hanson, A., & Giannantonio, C. (2009). Crisis response plans post 9/11: current status and future directions. *Academy of Strategic Management Journal*, 8, 23-37. Retrieved from <http://www.alliedacademies.org/public/AffiliateAcademies/asm.aspx>
- Issa-Salwe, A. M., & Ahmed, M. (2011). Risk management of an information system by assessing threat, vulnerability and countermeasure. *International Journal of Research and Reviews in Computer Science (IJRRCS)*, 2(1), 111-114. Retrieved from <http://scholarlyexchange.org/ojs/index.php/IJRRCS>
- Jo, H., Kim, S., & Won, D. (2011). Advanced information security management evaluation system. *KSII Transactions on Internet and Information Systems (TIIS)*, 5, 1192-1213. doi:10.3837/tiis.2011.06.006
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34, 549-A4. Retrieved from <http://www.misq.org/>
- Jones, M. (2008). An evaluation of privacy and security issues at a small university. *Technology Interface Journal*, 10(2), 1-7. Retrieved from <http://et.nmsu.edu/~etti/>
- Jonnalagadda, S. K., & Mallela, S. S. (2011). An expeditious intelligent framework for detecting anomalies. *International Journal of Research and Reviews in Information Security and Privacy (IJRRISP)*, 1(2), 25-32. Retrieved from <http://www.sciacademypublisher.com/journals/index.php/IJRRISP>
- Jose, A., & Lakshuni, S. V. (2014). Web security using visual cryptography against phishing. *Middle-East Journal of Scientific Research*, 20 (12), 2626-2632. DOI: 10.5829/idosi.mejsr.2014.20.12.21145
- Jourdan, Z., Rainer, R., Marshall, T., & Ford, F. (2010). An investigation of organizational information security risk analysis. *Journal of Service Science*, 3(2), 33-42. Retrieved from <http://journals.cluteonline.com/index.php/JSS>
- Kadlec, C., & Shropshire, J. (2010). Best practices in IT disaster recovery planning among US banks. *Journal of Internet Banking and Commerce*, 15(1), 1-11. Retrieved from <http://www.arraydev.com/commerce/jibc/>

- Katzan, H. (2010). On the privacy of cloud computing. *International Journal of Management and Information Systems*, 14(2), 1-12. Retrieved from <http://journals.cluteonline.com/index.php/IJMIS>
- Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technical factors. *MIS Quarterly Executive*, 9(3), 163-175. Retrieved from <http://misqe.org/ojs2/index.php/misqe/index>
- Khodarahmi, E. (2009). Crisis management. *Disaster Prevention and Management*, 18, 523-528. doi:10.1108/09653560911003714
- Kim, Y. G., & Cha, S. (2012). Threat scenario-based security risk analysis using use case modeling in information systems. *Security Communication Networks*, 5, 293–300. doi:10.1002/sec.321
- Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). *International Journal of Computer Science and Security (IJCSS)*, 5(1), 39-53. Retrieved from <http://www.cscjournals.org/csc/journals/IJCSS/description.php?JCode=IJCSS>
- King, N. (1998). *Qualitative methods and analysis in organizational research*. London, England: SAGE Publications.
- King, N., & Horrocks, C. (2010). *Interviews in qualitative research*. Los Angeles, CA: SAGE Publications.
- Klenke, K. (2008). *Qualitative research in the study of leadership*. Bingley, UK: Emerald Publishing Group.
- Kolb, N., & Abdullah, F. (2009). Developing an information security awareness program for a non-profit organization. *International Management Review*, 5(2), 105-110. Retrieved from [http://www.usimr.org/abstracts/abstract12\\_v5\\_n2\\_09.html](http://www.usimr.org/abstracts/abstract12_v5_n2_09.html)
- Koskosas, I. (2011). The performance pyramid framework to information systems security management process. *ARNP Journal of Systems and Software*, 1(5), 164-171. Retrieved from <http://www.scientific-journals.org/index.php>
- Koskosas, I., Kakoulidis, K., & Siomos, C. (2011). A model performance to information security management. *International Journal of Business and Social Science*, 2(4), 47-54. Retrieved from <http://www.ijbssnet.com/update/>
- Koskosas, I., Kakoulidis, K., & Siomos, C. (2011). Information security: Corporate

- culture and organizational commitment. *International Journal of Humanities and Social Science*, 1(3), 192-198. Retrieved from <http://www.ijhssnet.com/update/>
- Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18, 316-327. doi:10.1108/09685221011095236
- Kumari, L., Debbarma, S., & Shyam, R. (2011). Security problems in campus networks and its solutions. *International Journal of Advanced Engineering & Application*, 1(23), 1-4. Retrieved from <http://www.steps-india.com/ijaea/index.html>
- Kuzma, J. (2011). An examination of privacy policies of global university web sites. *Journal of Emerging Trends in Computing and Information Sciences*, 2(10), 485-491. Retrieved from [http://www.cisjournal.org/journalofcomputing/archive/vol2no10/vol2no10\\_3.pdf](http://www.cisjournal.org/journalofcomputing/archive/vol2no10/vol2no10_3.pdf)
- Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, 18(1), 4-13. doi:10.1108/09685221011035223
- Landsman, K. (2009). College IT leaders confident about network security. *Community College Journal*, 80(1), 8. Retrieved from <http://www.aacc.nche.edu/Publications/CCJ/Pages/default.aspx>
- Lazovic, M., & Simic, D. (2011). Botnets: the evolution and the possible solution. *TTEM- Technics Technologies Education Management*, 6, 829-835. Retrieved from <http://www.ttem-bih.org/>
- Leech, N. L., & Onwuegbuzie, A. J. (2011). Beyond constant comparison qualitative data analysis: Using NVivo. *School Psychology Quarterly*, 26(1), 70-84. Retrieved from <http://www.apa.org/pubs/journals/spq/>
- Likhar, P., Yadav, R. S., & Keshava, R. M. (2011). Securing IEEE 802.11g WLAN using open VPN and its impact analysis. *International Journal of Network Security & Its Applications (IJNSA)*, 3(6), 97-113. doi:10.5121/ijnsa.2011.3607
- Liu, S., & Ormaner, J. (2009). From ancient fortress to modern cyberdefense. *IT Professional Magazine*, 11(3), 22-29. doi:10.1109/MITP.2009.48
- Luftman, J., & Zadeh, H. S. (2011). Key information technology and management issues 2010–11: an international study. *Journal of Information Technology* 26, 193–204. doi:10.1057/jit.2011.3
- Lungu, I., & Tabusca, A. (2010). Optimizing anti-phishing solutions based on user

- awareness, education and the use of the latest web security solutions. *Informatica Economica*, 14(2), 27-36. Retrieved from <http://revistaie.ase.ro/>
- Ma, Q., Schmidt, M., & Pearson, J. (2009). An integrated framework for information security management. *Review of Business*, 30(1), 58-69. Retrieved from <http://www.stjohns.edu/academics/graduate/tobin/research/review>
- Ma, X., Zou, H., & Li, Y. (2011). Research and application of contingency plan based on hospital network and information system security. *Computer and Information Science*, 4(6), 105-110. doi:10.5539/cis.v4n6p105
- Maskari, S., Saini, D., Raut, S., & Hadimani, L. (2011). Security and vulnerability issues in university networks. *Proceedings of the World Congress on Engineering*, 1, 1-5. Retrieved from <http://www.iaeng.org/WCE2011/>
- Meade, M. (2009). Data security and privacy at colleges and universities. *The Computer & Internet Lawyer*, 26(10), 26-31. Retrieved from <http://search.proquest.com.proxy1.ncu.edu/docview/222874647/fulltext/833F59ABEE824478PQ/1?accountid=28180>
- Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy Of Information & Management Sciences Journal*, 14(2), 91-116. Retrieved from <http://alliedacademies.org/public/AffiliateAcademies/aims.aspx>
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook* (2nd ed.). Thousand Oaks, CA: SAGE Publications.
- Mohamed, H. A. R. (2014). A proposed model for IT disaster recovery plan. *International Journal of Modern Education and Computer Science*, 4, 57-67. doi:10.5815/ijmecs.2014.04.08
- Monfelt, Y., Pilemalm, S., Hallberg, J., & Yngström, L. (2011). The 14-layered framework for including social and organizational aspects in security management. *Information Management & Computer Security*, 19(2), 124-133. doi:10.1108/09685221111143060
- Morgan, D. L. (1998). *Focus groups as qualitative research*. London, England: SAGE Publications.
- Morris, S., Tuttle, J., & Essic, J. (2009). A partnership framework for geospatial data preservation in North Carolina. *Library Trends*, 57, 516-540. Retrieved from [http://www.press.jhu.edu/journals/library\\_trends/](http://www.press.jhu.edu/journals/library_trends/)

- Murray, M. (2010). Database security: What students need to know. *Journal of Information Technology Education: Innovations in Practice*, 9, 61-77. Retrieved from <http://www.informingscience.us/icarus/journals/jiteiip>
- Nan, N. (2011). Capturing bottom-up information technology use processes: A complex adaptive systems model. *MIS Quarterly*, 35, 505-A7. Retrieved from <http://www.misq.org/>
- Neuendorf, K. A. (2002). *The content analysis guidebook*. Thousand Oaks, CA: SAGE Publications.
- Nollau, B. (2009). Disaster recovery and business continuity. *Journal of GXP Compliance*, 13(3), 51-58. Retrieved from <http://www.gxpandjvt.com/>
- Ologunde, A. O., & Akinlolu, A. A. (2012). Business strategy as a measure of organizational performance. *International Journal of Business and Management*, 7(1), 241-253. doi:10.5539/ijbm.v7n1p241
- Omar, A., Alijani, D., & Mason, R. (2011). Information technology disaster recovery plan: Case study. *Academy of Strategic Management Journal*, 10(2), 127-141. Retrieved from <http://www.alliedacademies.org/public/AffiliateAcademies/asm.aspx>
- Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, 3, 398-427. Retrieved from <http://orgsci.journal.informs.org/>
- Ou, C. (2013). Multiagent-based computer virus detection systems: Abstraction from dendritic cell algorithm with danger theory. *Telecommunication Systems*, 52(2), 681-691. doi:<http://dx.doi.org/10.1007/s11235-011-9512-6>
- Patten, K. P., & Harris, M. A. (2013). The need to address mobile device security in the higher education IT curriculum. *Journal of Information Systems Education*, 24(1), 41-52. Retrieved from <http://jise.org/Volume24/24-1/PDF/Vol24-1pg41.pdf>
- Patton, M. Q. (2002). *Qualitative research & evaluation methods*. Thousand Oaks, CA: SAGE Publications.
- Pearce, M., Zeadally, S., & Hunt, R. (2010). Assessing and improving authentication confidence management. *Information Management & Computer Security*, 18(2), 124-139. doi:10.1108/09685221011048355
- Perkel, J. (2010). How safe are your data? *Nature*, 464, 1260-1261. Retrieved from <http://www.nature.com/nature/index.html>



- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778. Retrieved from <http://www.misq.org/>
- Ramachandran, A., & Ramachandran, S. (2012). Rapid and proactive approach on exploration of database vulnerabilities. *International Journal on Computer Science and Engineering (IJCSE)*, 4, 224-234. Retrieved from <http://www.enggjournals.com/ijcse/>
- Randolph, J. J. (2009). A guide to writing the dissertation literature review. *Practical Assessment, Research & Evaluation*, 14(13), 1-13. Retrieved from <http://pareonline.net/>
- Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, 20(1), 121-139, 156. Retrieved from <http://isr.journal.informs.org/>
- Ransbotham, S., & Mitra, S., & Ramsey, J. (2011). Are markets for vulnerabilities effective? *MIS Quarterly*, 36(1), 43-64. Retrieved from <http://www.misq.org/>
- Reddy, S. S., & Prasad, S. T. (2012). Robust IP spoof control mechanism through packet filters. *International Journal of Computer Trends and Technology*, 3(1), 1-6. Retrieved from <http://www.ijettjournal.org/index.html>
- Rice, M. (2011). The institutional review board is an impediment to human research: the result is more animal based research. *Philosophy, Ethics, and Humanities in Medicine*, 6(12), 1-10. doi:10.1186/1747-5341-6-12
- Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). Thousand Oaks, CA. SAGE Publications.
- Rudman, R. J. (2014). The influence of knowing web 2.0 risks and controls on web 2.0 usage and security practices of online users. *Journal of Applied Business Research*, 30(1), 105-n/a. Retrieved from <http://journals.cluteonline.com/index.php/JABR>
- Ryan, J. H., Mazzuchi, T. A., Ryan, D. J., Lopez de la Cruz, J., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, 39, 774-784. doi:10.1016/j.cor.2010.11.013
- Saleh, M. F. (2011). Information security maturity model. *International Journal of Computer Science and Security (IJCSS)*, 5, 316-337. Retrieved from <http://www.cscjournals.org/csc/journals/IJCSS/description.php?JCode=IJCSS>

- Saleh, M., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, 9, 107-118. doi:10.1016/j.aci.2011.05.002
- Saleh, Z. I., Refai, H., & Mashhour, A. (2011). Proposed framework for security risk assessment. *Journal of Information Security*, 2(2), 85-90. Retrieved from <http://www.scirp.org/journal/jis/>
- Sehgal, N., Sohoni, S., Xiong, Y., Fritz, D., Mulia, W., & Acken, J. (2011). A cross section of the issues and research activities related to both information security and cloud computing. *IETE Technical Review*, 28, 279-291. doi:10.4103/0256-4602.83549
- Seidman, I. (2013). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (4<sup>th</sup> ed.). New York, NY: Teachers College Press.
- Shank, G. D. (2006). *Qualitative research. A personal skills approach* (2nd ed.). Upper Saddle River, NJ: Pearson Merrill Prentice Hall.
- Shim, W. (2012). An analysis of information security management strategies in the presence of interdependent security risk. *Asia Pacific Journal of Information System*, 22(1), 79-101. Retrieved from <http://apjis.or.kr/>
- Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security*, 19(2), 95-112. doi:10.1108/09685221111143042
- Shropshire, J. D., Warkentin, M., & Johnston, A. C. (2010). Impact of negative message framing on security adoption. *The Journal of Computer Information Systems*, 51(1), 41-51. Retrieved from <http://www.iacis.org/jcis/jcis.php>
- Singh, N., Chauhan, P., & Chandra, N. (2013). Applicability of network logs for securing computer systems. *ACEEE International Journal Of Network Security*, 4(1), 54-60. doi: 01.IJNS.4.1.18
- Smith, R. (2009). Information security-A critical business function. *Journal of GXP Compliance*, 13(4), 62-68. Retrieved from <http://www.gxpandjvt.com/>
- Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly*, 34(3), 463-486. Retrieved from <http://www.misq.org/>

- Smith, T., Koohang, A., & Behling, R. (2010). Understanding and prioritizing technology management challenges. *The Journal of Computer Information Systems*, 51(1), 91-98. Retrieved from <http://www.iacis.org/jcis/jcis.php>
- Sobel, P. (2009). Plan for the worst. *Internal Auditor*, 66(6), 61-65. Retrieved from <http://www.theiia.org/intauditor/>
- Spanier, G. (2010). Creating adaptable universities. *Innovative Higher Education*, 35(2), 91-99. doi:10.1007/s10755-009-9134-z
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34, 503-522. Retrieved from <http://www.misq.org/>
- Stake, R. E. (1995). *The art of case study research*. Thousand Oaks, CA: SAGE Publications.
- Stake, R. E. (2006). *Multiple case study analysis*. New York, NY: The Guilford Press.
- Steffee, S. (2010). Employees ignoring IT security. *Internal Auditor*, 67(5), 14-16. Retrieved from <http://www.theiia.org/intauditor/>
- Stiawan, D., Idris, M. Y., Salam, M. S., & Abdullah, A. H. (2012). Intrusion threat detection from insider attack using learning behavior-based. *International Journal of the Physical Sciences*, 7, 624 – 637. doi:10.5897/IJPS11.1381
- Styles, M., & Tryfonas, T. (2009). Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users. *Information Management & Computer Security*, 17(1), 44-52. doi:10.1108/09685220910944759
- Surisetty, S., & Kumar, S. (2011). McAfee Security Center evaluation under DDoS attack traffic. *Journal of Information Security*, 2(3), 113-121. Retrieved from <http://www.scirp.org/journal/jis/>
- Susanto, H., & Almunawar, M. N. (2012). Information security awareness: A marketing tool for corporate's business process. *Computer Science Journal*, 1-12. Retrieved from <http://comsj.org/>
- Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information security challenge and breaches: Novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology*, 2(1), 67-75. Retrieved from <http://www.ijest.info/>
- Susanto, H., Almunawar, M. N., Tuan, Y. C., Aksoy, M. S., & Syam, W. P. (2011).

- Integrated solution modeling software: New paradigm on information security review and assessment. *International Journal of Science and Advanced Technology*, 1(10), 90-99. Retrieved from <http://www.ijstat.com/>
- Taluja, S., & Dua, R. L. (2012). Survey on network security, threats & firewalls. *International Journal of Advanced Research in Computer Engineering & Technology*, 1(7), 53-58. Retrieved from <http://ijarcet.org/index.php/ijarcet/index>
- Tan, Y., & Takakuwa, S. (2011). Use of simulation in a factory for business continuity planning. *International Journal of Simulation Modelling*, 10(1), 17-26. doi:10.2507/IJSIMM10(1)2.17
- Tarn, J., Raymond, H., Razi, M., & Han, B. T. (2009). Exploring information security compliance in corporate IT governance. *Human Systems Management*, 28(3), 131-140. doi:10.3233/HSM-2009-0698
- Teijlingen van, E., & Hundley, V. (2001). The importance of pilot studies. *Social Research Update*, 35, 1-4. Retrieved from <http://sru.soc.surrey.ac.uk/SRU35.pdf>
- Tyagi, N. K., & Srinivasan, S. (2011). Ten-stage security management strategy model for the impacts of 'Security Threats on E-Business'. *International Journal of Computer Applications*, 21(5), 1-4. Retrieved from <http://www.ijcaonline.org/>
- Uhl-Bien, M., & Marion, R. (2009). Meso-Modeling of leadership: Integrating micro- and macro-perspectives of leadership. *The Leadership Quarterly*, 20, 631-650. doi: 10.1016/j.leaqua.2009.04.007
- Veiga, A. D., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207. doi.org/10.1016/j.cose.2009.09.002
- Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information security and Sarbanes-Oxley compliance: An exploratory study. *Journal of Information Systems*, 25(1), 185-211. doi:10.2308/jis.2011.25.1.185
- Walters, L. (2007). A draft of an information systems security and control course. *Journal of Information Systems*, 21(1), 123-148. Retrieved from <http://www.jisonline.com/>
- Wang, P. (2010). Chasing the hottest IT: Effects of information technology fashion on organizations. *MIS Quarterly*, 34(1), 63-85. Retrieved from <http://www.misq.org/>
- Warren, M., & Leitch, S. (2010). Hacker taggers: A new type of hackers. *Information*

*Systems Frontiers*, 12(4), 425-431. doi:<http://dx.doi.org/10.1007/s10796-009-9203-y>

- Wengraf, T. (2001). *Qualitative research interviewing: biographic narratives and semi-structured methods*. Thousand Oaks, CA. SAGE Publications.
- Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4-19. doi:10.1108/09685220910944722
- Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management & Computer Security*, 18(1), 26-42. doi:10.1108/09685221011035241
- Whitman, M. E., & Mattord, H. J. (2010). *Management of information security* (3rd ed.) Boston, MA: Course Technology, Cengage Learning.
- Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.) Boston, MA: Course Technology, Cengage Learning.
- Wolcott, H. F. (2009). *Writing up qualitative research* (3rd ed.). Thousand Oaks, CA: SAGE Publications.
- Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *The Review of Business Information Systems*, 15(3), 9-21. Retrieved from <http://journals.cluteonline.com/index.php/RBIS/index>
- Xing, S., Xue, H., & Li, G. (2010). Honeypot protection detection response recovery model for information security management policy. *Asian Social Science*, 6(12), 50-53. Retrieved from <http://www.ccsenet.org/journal/index.php/ass>
- Yin, R. K. (2009). *Case study research. Design and methods* (4th ed.). Thousand Oaks, CA: SAGE Publications.
- Yin, R. K. (2012). *Applications of case study research* (3rd ed.). Thousand Oaks, CA: SAGE Publications.
- Young, R. (2010). Evaluating the perceived impact of collaborative exchange and formalization on information security. *Journal of International Technology & Information Management*, 19(3), 19-37. Retrieved from [http://www.iima.org/index.php?option=com\\_content&view=article&id=49&Itemid=54](http://www.iima.org/index.php?option=com_content&view=article&id=49&Itemid=54)

- Young, R., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of AIS, 2010*, 245-266. Retrieved from <http://aisel.aisnet.org/cais/>
- Zafar, H., Ko, M., & Osei-Bryson, K. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal, 25*(1), 21-37. doi:10.4018/irmj.2012010102
- Zhou, S., Zhang, Q., Wei, X., & Zhou, C. (2010). A summarization on image encryption. *IETE Technical Review, 27*, 503-510. doi:10.4103/0256-4602.72583
- Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*, 583–592. doi:10.1016/j.future.2010.12.006

## Appendices

## **Appendix A: Interview Questions Guide**

The purpose of this qualitative holistic multiple case study is to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. There will be a total of 12 participants as holistic units of analysis selected from 12 distinct and separate colleges and universities within the state of North Carolina. The institutions will be derived from a population of more than 220 institutions of higher education in the state of North Carolina and the IT personnel selected from these institutions. The interview participants will be IT professionals working in and having responsibility over IT security.

The goal of this study is to explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education. Information technology (IT) management and university administrators could use the detailed information gathered from this study to help and aid in designing, implementing, or verifying appropriate and required IT security tools, processes, procedures, systems and strategies.

---

The following questions are to be answered based on your understanding and experiences as an IT professional working at a college/university within the State of North Carolina.

---

Interviewer: Kevin J. Misenheimer, NCU Ph.D. Candidate

---

Each interview should take 45-60 minutes.

---

### **Section One—Computer and Information Security Attacks, Breaches, Threats**

1. How does your institution define computer and information security attacks?
2. How does your institution define computer and information security breaches?
3. How does your institution define computer and information security threats?
4. What types of computer and information security attacks are most common for your institution?
5. What types of computer and information security breaches are most common for your institution?



6. What types of computer and information security threats are most common for your institution?

### **Section Two—Computer and Information Security Responsibility and Planning**

7. How should users (faculty/staff/students) be held responsible for information security procedures on institution owned computers at your institution?
8. Describe how your college or university trains users to be aware of computer and information security? How does your institution train users to be proactive in implementing computer and information security defense procedures?
9. What should be included in a written policy concerning computer and information security for your institution? Describe the main points that should be addressed.
10. What would be the benefits of having an all-inclusive comprehensive IT security plan at your institution? A disaster recovery plan? A business continuity plan? Are there any disadvantages? Explain.

### **Section Three—Computer and Information Security Implementations (Base answers on recommendations to achieve best results in information security)**

11. What are some of the best information security practices relating to hardware tools you would recommend for colleges and universities to implement?
12. What are some of the best information security practices relating to software tools you would recommend for colleges and universities to implement?
13. What are some of the best information security practices relating to methods, processes, and procedures you would recommend colleges and universities to implement?
14. What are some of the best information security practices relating to education, training, and awareness programs you would recommend for colleges and universities to implement?

### **Section Four—Computer and Information Security Related Issues**

15. What are the top three major risks a college or university could experience if a successful information security attack, breach, or threat would occur?

16. How often do you evaluate and update IT security procedures and policies at your institution? Do you feel those procedures and policies should be updated more often? Less often? Please explain.
17. How should the information security awareness program be implemented at a college or university? Explain what the process should involve and differentiate between employees and students.

## Appendix B: Dissertation Participation Permission Request Letter

Hello, my name is Kevin J. Misenheimer and I am a Ph.D. Doctoral Candidate with Northcentral University (NCU). I request your permission to contact a member of your IT Department in which to ask if they would like to be included in my study. My dissertation title is: Exploring Information Technology Security Requirements for Academic Institutions to Reduce Information Security Attacks, Breaches, and Threats.

The name of the member will not be disclosed or presented in any of the published documents or within the dissertation. Nothing proprietary or confidential will be asked of your IT member. Nothing will be identified specifically about your college or university or what you have done or will do pertaining to information technology security.

The interview questions are attached if you would like to view them. There is a Consent Form and Information Letter also attached for more information. This part of the process will be conducted later.

NCU requires your permission in order to contact a member of your IT Department and to make sure you are aware of the potential interview. If you can just reply to this email stating that I have your college/university's permission, this will suffice and allow me to further my research.

I will then contact a member of your IT Department and ask if they would be willing to be interviewed and then obtain the consent form.

I am a faculty member of Stanly Community College, Albemarle, NC.

Thank you so much and have a wonderful day.

### Appendix C: Dissertation Participation Introduction Letter

Hello,

You are invited to participate in an interview for my doctoral research study titled “Exploring Information Technology Security Requirements for Academic Institutions to Reduce Information Security Attacks, Breaches, and Threats”.

If you agree to participate in this study, you will be asked semi-structured questions during the interview. Interviews should last approximately 45-60 minutes.

The general purpose of this research study is to understand what management at colleges and universities can do to maximize their protection of the institutions’ information, computers, network, and other assets through the implementations of information security concepts, procedures, tools, software, hardware, in order to reduce or eliminate information security attacks, breaches, and threats.

Your in-depth responses to the interview questions can contribute significantly to my research findings. Once this study is finalized and approved by Northcentral University, you will be provided an electronic copy of my dissertation manuscript.

The interview sessions will be recorded and you will have a chance to review transcriptions from the interview sessions to provide comments regarding accuracy. Information collected from the interview sessions will only be used for the purpose of this study. Your and your institution’s identity will be kept confidential and anonymous.

If you are willing to participate in this study, please read and sign the attached Informed Consent Form and return it to me via email at [kevin.misenheimer@gmail.com](mailto:kevin.misenheimer@gmail.com). Once I receive the signed form, I will contact you to schedule an interview session. Please contact me if you have any questions via email or call me at 704-984-3326.

Thank you.

Sincerely,

Kevin J. Misenheimer, Ph.D. Candidate  
Northcentral University

### **Appendix D: Informed Consent Form**

Dissertation Title: Exploring Information Technology Security Requirements for Academic Institutions to Reduce Information Security Attacks, Breaches, and Threats

My name is Kevin J. Misenheimer and I am a Ph.D. candidate at the Northcentral University working on a doctoral degree. I am conducting a research study entitled “Exploring Information Technology Security Requirements for Academic Institutions to Reduce Information Security Attacks, Breaches, and Threats”. The purpose of this qualitative holistic multiple case study is explore factors potentially contributing to improved information security and reduced attacks, breaches, and threats among institutions of higher education.

Your participation will involve a face-to-face or telephone interview discussion. The questions relate to your knowledge and experiences as a member of an IT Department but not as a member of your academic institution. This means nothing will be asked of you in regards to what your college/university has implemented.

Your participation in this study is voluntary. If you choose not to participate or to withdraw from the study at any time, you can do so without penalty or loss of benefit to yourself. The results of the research study may be published but your identity will remain confidential and your name will not be disclosed to any outside party.

**As a participant in this study, you should understand the following:**

1. You may decline to participate or withdraw from participation at any time without consequences.
2. Your identity will be kept confidential.
3. Kevin J. Misenheimer, the researcher, has thoroughly explained the parameters of the research study and all of your questions and concerns have been addressed.
4. If the interviews are recorded, you must grant permission for the researcher, Kevin J. Misenheimer, to digitally record the interview. You understand that the information from the recorded interviews may be transcribed. The researcher will structure a coding process to assure that anonymity of your name is protected.
5. Data will be stored in a secure and locked area. The data will be coded such that your name is not associated with the data collected.
6. The research results will be used for publication.

7. The benefit for your participation in this study includes access to the final dissertation manuscript. No incentives are offered.

8. There are no known risks in this study. You will not be asked to disclose proprietary or confidential information about your employer. You may choose to not answer a question and may withdraw at any time.

9. You will be asked to provide in-depth verbal responses to interview questions asked by the researcher. Based on your preference and availability, the researcher will conduct the interview session with you over the phone or by face-to-face. The interview session will be recorded and should last around 45-60 minutes.

10. There is no deception in this study.

“By signing this form you acknowledge that you understand the nature of the study, the potential risks to you as a participant, and the means by which your identity will be kept confidential. Your signature on this form also indicates that you are 18 years old or older and that you give your permission to voluntarily serve as a participant in the study described.”

If you have any questions concerning the research study, please call me at 704-984-3326 or email me at [kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu) or you may contact my academic advisor Mr. Seth Hardesty at 1-888-327-2877 ext: 8146 [shardesty@ncu.edu](mailto:shardesty@ncu.edu) or my dissertation chair Dr. Michael Shriner at 1- 928-771-6856 [mshriner@ncu.edu](mailto:mshriner@ncu.edu) or NCU’s IRB office at 1-888-327-2877.

You will receive a copy of this authorized document.

Participant’s Name: \_\_\_\_\_

Participant’s Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Researcher’s Name: \_\_\_\_\_

Researcher’s Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## **Appendix E: Information Technology Security Requirements Recommended**

The need for risk assessments. Risks must be understood and acknowledged and the IT security measures that are taken must be commensurate with these risks.

The need for an IT security organizational culture.

The need to create, communicate, implement, endorse, monitor, and enforce security policies across an organization.

The need to make every member of the organization aware of the importance of IT security and to train them in good IT security practices.

The need for access controls to make certain only identified and authorized users with a legitimate need access information and system resources.

The need to monitor, audit, and review IT security measures regularly.

The need for business continuity plans that are tested regularly.

## Appendix F: Permission to Use Computer and Information Security Threats Table

**From:** Fan, Ip-Shing [mailto:I.S.Fan@cranfield.ac.uk]  
**Sent:** Wednesday, August 22, 2012 9:54 PM  
**To:** Kevin Misenheimer  
**Cc:** ijdspapers@infonomics-society.org; Najwa Hayaati Mohd Alwi  
**Subject:** RE: Request Permission to Use Table in Dissertation Please

Dear Kevin,

As the paper author, I am very happy for you to use the table provided you fully acknowledge the source and follow all the academic convention on citation and referencing.

Best regards,

Fan.

**From:** Kevin Misenheimer [mailto:kmisenheimer7517@stanly.edu]  
**Sent:** 22 August 2012 20:49  
**To:** Fan, Ip-Shing  
**Cc:** [ijdspapers@infonomics-society.org](mailto:ijdspapers@infonomics-society.org)  
**Subject:** Request Permission to Use Table in Dissertation Please

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the table titled:

Computer and Information Security Threats

It is from the following source:

Alwi, N., & Fan, I. (2010). E-learning and information security management. *International Journal of Digital Society (IJDS)*, 1(2), 148-156. Retrieved from <http://www.infonomics-society.org/IJDS/>

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.



## Appendix G: Permission to Use Security Incidents and End –Effects Table

---

**From:** Dov Shirtz [dovshirtz@gmail.com]  
**Sent:** Wednesday, August 15, 2012 3:38 PM  
**To:** Kevin Misenheimer  
**Subject:** Re: Request Permission to use Table in Dissertation Please

You have my permission. Just include the proper reference.

Good luck.

Dov shirtz

2012 8 15 20:26, תאמ "Kevin Misenheimer" <[kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)>:

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the table titled:

Security Incidents and End-Effects

It is from the following source:

“Optimizing Investment Decisions in Selecting Information Security Remedies,” by D. Shirtz and Y. Elovici, 2011, *Information Management & Computer Security*, 19, p. 105. Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

---

**From:** Laura Jenkins [LJenkins@emeraldinsight.com]  
**Sent:** Wednesday, August 15, 2012 4:03 AM  
**To:** Kevin Misenheimer  
**Subject:** RE: Request Permission to use Table  
 Dear Kevin,

Please allow me to introduce myself, my name is Laura Jenkins and I am the Rights Manager here at Emerald Group Publishing- please accept my sincere apologies for the delay in responding to your email.

I am pleased to say that subject to full referencing I can grant you free permission to include the material detailed below within your dissertation;

- Table 5 from Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security*, 19(2), 95-112. doi:10.1108/0968522111143042

Please note however that if in the future you publish your dissertation you will need to clear permission again.

Good luck with your dissertation,

Kind Regards,

Laura Jenkins  
Rights Manager

[www.emeraldinsight.com](http://www.emeraldinsight.com)

*Emerald is a leading independent publisher of global research with impact in business, society, public policy and education.*

---

**From:** Kevin Misenheimer [mailto:kmisenheimer7517@stanly.edu]

**Sent:** 06 August 2012 19:39

**To:** Permissions

**Subject:** Request Permission to use Table

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the table titled Security Incidents and End-effects in my dissertation. It is from the following source:

Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security*, 19(2), 95-112. doi:10.1108/0968522111143042

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

Emerald Group Publishing Limited, Registered Office: Howard House, Wagon Lane,  
Bingley, BD16 1WA United Kingdom. Registered in England No. 3080506, VAT No.  
GB 665 3593 06

## Appendix H: Permission to Use Traditional Risk Management Process Table

---

From: Nicole Beebe [Nicole.Beebe@utsa.edu]  
Sent: Wednesday, August 15, 2012 1:58 PM  
To: Kevin Misenheimer  
Cc: Chino Rao  
Subject: RE: Request to use Table in Dissertation Please

Hi, Kevin.

Certainly. Just please cite the article when presenting the table.

Take care.  
-Nicole

NICOLE L. BEEBE, Ph.D., CISSP  
Assistant Professor

The University of Texas at San Antonio  
Department of Information Systems & Cyber Security  
College of Business  
One UTSA Circle  
San Antonio, Texas 78249  
Cell: 210.269.5647  
Fax: 210.458.6305  
[nicole.beebe@utsa.edu](mailto:nicole.beebe@utsa.edu)  
<http://faculty.business.utsa.edu/nbeebe>

From: Kevin Misenheimer [mailto:kmisenheimer7517@stanly.edu]  
Sent: Wednesday, August 15, 2012 12:33 PM  
To: Nicole Beebe  
Subject: Request to use Table in Dissertation Please

Hello,  
My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the table titled:

Traditional Risk Management Process

It is from the following source:

“Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process,” by N. Beebe and V. Rao, 2010, *Communications of the Association for Information Systems*, 26, p. 332.

Thanks for considering my request.

I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix I: Permission to Use The Goal Setting Process Table

---

From: ikoskosas@uowm.gr [ikoskosas@uowm.gr]  
Sent: Thursday, August 16, 2012 3:23 AM  
To: Kevin Misenheimer  
Subject: Re: Request to use Table in Dissertation Please

Hello Kevin

As before, you can use the table only if you refer to the source (e.g., author's name - my name).

Kind Regards  
Ioannis

Quoting Kevin Misenheimer <kmisenheimer7517@stanly.edu>:

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the table titled:

The Goal Setting Process

It is from the following source:

"A Model Performance to Information Security Management," by I. Koskoasa, K. Kakoulidis, and C. Siomos, 2011, International Journal of Business and Social Science, 2, p. 49.

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix J: Permission to Use Risk Factors by Percentages Table

---

From: Clute Institute Staff [staff@cluteinstitute.com]  
 Sent: Wednesday, August 08, 2012 12:59 PM  
 To: Kevin Misenheimer  
 Subject: FW: Request Permission to use Table

Hi-

I am forwarding the response from Professor Jourdan.

Have a great day!

Ann

Please add our email address (staff@CluteInstitute.com) to your address book and please add our domain name (CluteInstitute.com) to your "safe senders" list.

~~~~~  
 The Clute Institute  
 www.CluteInstitute.com  
 Staff@CluteInstitute.com  
 Tel: 303-904-4750; Fax: 720-259-2420

-----Original Message-----  
 From: Zack Jourdan [mailto:sjourdan@aum.edu]  
 Sent: Wednesday, August 08, 2012 10:54 AM  
 To: Clute Institute Staff  
 Subject: RE: Request Permission to use Table

All of the authors approve of the use of the table as long as it is cited.

Thanks,

Zack Jourdan  
 Auburn University at Montgomery  
 Office 310H: 334-244-3122  
 IS & DS Department: 334-244-3479

---

From: Clute Institute Staff [staff@cluteinstitute.com]  
 Sent: Wednesday, August 08, 2012 11:00 AM  
 To: Kevin Misenheimer

Subject: RE: Request Permission to use Table

Hi-

We retain the copyright only for our use online and in hard copy. I am forwarding your email to the most recent email addresses that we have for the authors' permission. (We did not have a correct email address for Professor Marshall).

Have a great day!

Ann

Please add our email address  
([staff@CluteInstitute.com](mailto:staff@CluteInstitute.com)<<mailto:staff@CluteInstitute.com>>) to your address book and please add our domain name (CluteInstitute.com) to your "safe senders" list.

~~~~~  
The Clute Institute  
[www.CluteInstitute.com](http://www.CluteInstitute.com)  
[Staff@CluteInstitute.com](mailto:Staff@CluteInstitute.com)  
Tel: 303-904-4750; Fax: 720-259-2420

From: Kevin Misenheimer [<mailto:kmisenheimer7517@stanly.edu>]  
Sent: Wednesday, August 08, 2012 9:38 AM  
To: Clute Institute Staff  
Subject: Request Permission to use Table

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the table titled:

Risk Factors by Percentages

It is from the following source:

Jourdan, Z., Rainer, R., Marshall, T., & Ford, F. (2010). An investigation of organizational information security risk analysis. *Journal of Service Science*, 3(2), 33-42. Retrieved from <http://journals.cluteonline.com/index.php/JSS>

Thanks for considering my request. I look forward to your reply.



E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix K: Permission to Use Top 10 Computer and Information Security Threats for 2010 Table

**From:** Minh Jo [mailto:minhojo@gmail.com]  
**Sent:** Thursday, August 23, 2012 11:59 AM  
**To:** Kevin Misenheimer  
**Subject:** Re: Request Permission to use Table

Dear Kemin,

I am sorry to be late for my reply to your request.  
 I am happy for you to use the title of the referenced paper.

Best,

--

Minho Jo  
 Founder and Editor-in-Chief,  
 KSII Transactions on Internet and Information Systems, indexed in SCIE (Thomson Reuters) and SCOPUS (Elsevier).  
[WWW.ITIIS.ORG](http://WWW.ITIIS.ORG)

On Fri, Aug 10, 2012 at 5:28 PM, "TIIS Admin" <[tiis@ksii.or.kr](mailto:tiis@ksii.or.kr)> wrote:

----- Forwarded Message Infomation -----

From: Kevin Misenheimer <[kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)>  
 To: "[tiis@ksii.or.kr](mailto:tiis@ksii.or.kr)" <[tiis@ksii.or.kr](mailto:tiis@ksii.or.kr)>  
 Sent: 12-08-09 00:43:05  
 Subject: Request Permission to use Table

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the table titled:

Top 10 Computer and Information Security Threats for 2010

It is from the following source:

Jo, H., Kim, S., & Won, D. (2011). Advanced information security management evaluation system. *KSII Transactions on Internet and Information Systems (TIIS)*, 5(6), 1192-1213. doi:10.3837/tiis.2011.06.006

Thanks for considering my request. I look forward to your reply.

---

**From:** Dongho WON [dhwon@security.re.kr]  
**Sent:** Sunday, August 19, 2012 7:59 PM  
**To:** Kevin Misenheimer  
**Subject:** Re: Request Permission to use Table in Dissertation Please  
Dear Kevin Misenheimer

Thank you for your mail.  
We allow you to cite our table titled.

Dongho Won

**From:** [Kevin Misenheimer](#)  
**Sent:** Thursday, August 16, 2012 3:16 AM  
**To:** [dhwon@security.re.kr](mailto:dhwon@security.re.kr)  
**Subject:** Request Permission to use Table in Dissertation Please

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the table titled:

Top 10 Computer and Information Security Threats for 2010

It is from the following source:

“Advanced Information Security Management Evaluation System,” by H. Jo, S. Kim and D. Won, 2011, *KSII Transactions on Internet and Information Systems (TIIS)*, 5, p. 1203. Published by Perimeter E-Security.

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix L: Permission to Use Four Security Actions Table

---

From: alex.koohang@gmail.com [alex.koohang@gmail.com] on behalf of JCIS Editor-in-Chief [jcis@iacis.org]  
Sent: Wednesday, August 08, 2012 6:26 PM  
To: Kevin Misenheimer  
Subject: Re: Request Permission to use Table

Kevin,

As long as proper credit is given, no permission is required to cite the text or use the table. Good luck on your dissertation.

Alex

On Wed, Aug 8, 2012 at 11:51 AM, Kevin Misenheimer <[kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)> wrote:

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the table titled:

Four Security Actions

It is from the following source:

Shropshire, J. D., Warkentin, M., & Johnston, A. C. (2010). Impact of negative message framing on security adoption. *The Journal of Computer Information Systems*, 51(1), 41-51. Retrieved from <http://www.iacis.org/jcis/jcis.php>

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix M: Permission to Use Types of Attacks Experienced from 2006-2010 Table

---

From: Robert Richardson [rrichardson@techweb.com]  
Sent: Wednesday, August 15, 2012 2:37 PM  
To: Kevin Misenheimer  
Subject: RE: Request Permission to use Table in Dissertation Please

You're welcome to use the table as you describe.

Best,

Robert

---

From: Kevin Misenheimer [kmisenheimer7517@stanly.edu]  
Sent: Wednesday, August 15, 2012 2:22 PM  
To: Robert Richardson  
Cc: CSI  
Subject: Request Permission to use Table in Dissertation Please  
To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the table titled Types of Attacks Experienced from 2006-2010 in my dissertation.

It is from the following source:

2010 CSI Computer Crime and Security Survey: 149 Respondents. Where (---) is listed, this type of attack was not asked in that year. Adapted from "2010 CSI Computer Crime and Security Survey" by Computer Security Institute, 2011, p. 17.

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.



## Appendix N: Permission to Use Cognitive Skills of Users as Relating to Information Security Table

**From:** Hennie Kruger [mailto:Hennie.Kruger@nwu.ac.za]  
**Sent:** Sunday, August 26, 2012 10:08 AM  
**To:** Kevin Misenheimer  
**Subject:** Re: Request Permission to use Table in Dissertation Please

Hi Kevin

I spoke to my co-authors and you can use the table with the necessary references. All the best with your studies.

Regards  
 Hennie Kruger

Sent from my iPad

On 20 Aug 2012, at 5:26 PM, "Kevin Misenheimer <[kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)>" <[kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)> wrote:

Okay thank you very much!

---

**From:** Hennie Kruger [[Hennie.Kruger@nwu.ac.za](mailto:Hennie.Kruger@nwu.ac.za)]  
**Sent:** Monday, August 20, 2012 6:12 AM  
**To:** Kevin Misenheimer  
**Subject:** Re: Request Permission to use Table in Dissertation Please

Hi Kevin

Thank you for your e-mail. I am at a conference at the moment and will attend to the matter as soon as I am back at the office

Regards  
 Hennie Kruger

Prof HA Kruger  
 School of Computer, Statistical and Mathematical Sciences  
 North-West University  
 Private Bag X6001  
 Potchefstroom  
 2520 South Africa

Tel +27 18 2992539  
[Hennie.Kruger@nwu.ac.za](mailto:Hennie.Kruger@nwu.ac.za)

Vrywaringsklousule / Disclaimer: <http://www.nwu.ac.za/it/gov-man/disclaimer.html>

>>> Kevin Misenheimer <[kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)> 08/15/12 20:29 >>>

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the table titled Cognitive Skills of Users as Relating to Information Security in my dissertation. It is from the following source:

"A Vocabulary Test to Assess Information Security Awareness" by H. Kruger, L. Drevin, and T. Steyn, 2010, *Information Management & Computer Security*, 18, p. 320.

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.



## Appendix O: Permission to Use Information / Computer Security and Privacy Concerns Table

From: Nyaboga, Andrew [mailto:NyabogaA@wpunj.edu]  
 Sent: Wednesday, September 05, 2012 9:25 AM  
 To: Clute Institute Staff; Kevin Misenheimer  
 Subject: RE: Request Permission to use Table

Yes- with reference and acknowledgement

Andrew B. Nyaboga Ph.D  
 Associate professor  
 William Paterson University  
 Department of Accounting and Law  
 Wayne, New Jersey 07470  
 Tel. (973) 720-2403

---

From: Melinda Cline [mailto:mcline@ggc.edu]  
 Sent: Wednesday, August 08, 2012 11:31 AM  
 To: Clute Institute Staff  
 Subject: Re: Request Permission to use Table

Hi! Thank you for your request. You are welcome to use the publication.

Melinda Cline, Ph.D.

Sent from my iPhone

From: Guynes, Steve [Steve.Guynes@unt.edu]  
 Sent: Wednesday, August 08, 2012 1:28 PM  
 To: Clute Institute Staff  
 Cc: Kevin Misenheimer  
 Subject: Re: Request Permission to use Table

You may use it.

C. S. Guynes

Sent from my iPhone

On Aug 8, 2012, at 10:11 AM, "Clute Institute Staff" <staff@cluteinstitute.com> wrote:

Hi-

We retain the copyright only for our use online and in hard copy. I am forwarding your email to the most recent email addresses that we have for the authors' permission.

Have a great day!

Ann

Please add our email address (staff@CluteInstitute.com) to your address book and please add our domain name (CluteInstitute.com) to your "safe senders" list.

~~~~~  
 The Clute Institute  
 www.CluteInstitute.com  
 Staff@CluteInstitute.com  
 Tel: 303-904-4750; Fax: 720-259-2420

From: Kevin Misenheimer [mailto:kmisenheimer7517@stanly.edu]  
 Sent: Wednesday, August 08, 2012 10:42 AM  
 To: Clute Institute Staff  
 Subject: Request Permission to use Table

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the table titled:

Information / Computer Security and Privacy Concerns

It is from the following source:

Cline, M., Guynes, C. S., & Nyaboga, A. (2010). The impact of organizational change on information systems security. *Journal of Business & Economics Research*, 8(1), 59-64.

Retrieved from <http://journals.cluteonline.com/index.php/JBER>

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix P: Permission to Use Distribution of Information Security Policy Use Table

---

From: Pascal Ravesteijn [pascal.ravesteijn@hu.nl]  
 Sent: Tuesday, August 14, 2012 8:05 AM  
 To: Kevin Misenheimer  
 Subject: Fwd: Request Permission to use Table

Dear Kevin,

As long as you apply the appropriate referencing you can use the table in your dissertation.

With kind regards,

Pascal Ravesteijn  
 editor JITIM

-----Oorspronkelijk bericht-----

Van: system@iima.org [mailto:system@iima.org]  
 Verzonden: woensdag 8 augustus 2012 18:54  
 Aan: Jos van Reenen  
 Onderwerp: Request Permission to use Table

From: Kevin Misenheimer at kmisenheimer7517@stanly.edu What is the reason of your mail to the webmaster?: I would like to receive more information Please place your message in this box:: To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the table titled:

Distribution of Information Security Policy Use

It is from the following source:

Young, R. (2010). Evaluating the perceived impact of collaborative exchange and formalization on information security. *Journal of International Technology & Information Management*, 19(3), 19-37.

Thanks for considering my request. I look forward to your reply.

## Appendix Q: Permission to Use Ten Stage Security Management Strategy Model Figure

Authors were contacted to inform them they would be referenced and cited.

**From:** narendra tyagi [mailto:narendratyagi\_21@yahoo.com]  
**Sent:** Thursday, August 09, 2012 4:14 AM  
**To:** Kevin Misenheimer  
**Subject:** Re: FW: Request Permission to use Figure

Dear K.M.Sir  
 Season's Greetings  
 I am ready to permit you for using the figure, from my published work "Ten-Stage security management strategy model for the impacts of 'Security Threats on E-Business" International Journal of Computer Applications, on your request with condition that you will have to Include our names as 2nd authors in your publication and duly inform us as well as in time. If you agree this proposal I will grant my permission for the affirmation of the same.  
 Thanks and Regards  
 You Truly  
 Prof.N.K.Tyagi

--- On **Wed, 8/8/12, Kevin Misenheimer** <[kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)> wrote:

From: Kevin Misenheimer <[kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)>  
 Subject: FW: Request Permission to use Figure  
 To: "[narendratyagi\\_21@yahoo.com](mailto:narendratyagi_21@yahoo.com)" <[narendratyagi\\_21@yahoo.com](mailto:narendratyagi_21@yahoo.com)>, "[dss\\_dce@yahoo.com](mailto:dss_dce@yahoo.com)" <[dss\\_dce@yahoo.com](mailto:dss_dce@yahoo.com)>  
 Date: Wednesday, 8 August, 2012, 10:35 PM  
 My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the figure titled Ten Stage Security Management Strategy Model in my dissertation.

It is from the following source: Tyagi, N. K., & Srinivasan, S. (2011). Ten-Stage security management strategy model for the impacts of 'Security Threats on E-Business'. International Journal of Computer Applications, 21(5), 1-4

Thanks for considering my request. I look forward to your reply.

**From:** [editor.ijca4@gmail.com](mailto:editor.ijca4@gmail.com) [mailto:[editor.ijca4@gmail.com](mailto:editor.ijca4@gmail.com)] **On Behalf Of** Editor IJCA  
**Sent:** Wednesday, August 08, 2012 1:24 AM  
**To:** Kevin Misenheimer  
**Subject:** Re: Request Permission to use Figure

Dear Kevin Misenheimer,

Thank you for the inquiry. We recommend you to convey your request to the authors Prof. N.K.Tyagi ([narendratyagi\\_21@yahoo.com](mailto:narendratyagi_21@yahoo.com)) and Prof. S.Srinivasan ([dss\\_dce@yahoo.com](mailto:dss_dce@yahoo.com)). Once you receive the consent, the figure can be used in your dissertation.

Feel free to contact us for any inquiry.

Regards,  
Editorial Support Team,  
International Journal of  
Computer Applications,  
Foundation of Computer Science,  
New York, USA.

[www.ijcaonline.org](http://www.ijcaonline.org)

On Mon, Aug 6, 2012 at 11:50 PM, ijcaonline <[editor@ijcaonline.org](mailto:editor@ijcaonline.org)> wrote:  
From Kevin Misenheimer at [kmisenheimer7517@stanly.edu](mailto:kmisenheimer7517@stanly.edu)

To whom it may concern, My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the figure titled Ten Stage Security Management Strategy Model in my dissertation. It is from the following source: Tyagi, N. K., & Srinivasan, S. (2011). Ten-Stage security management strategy model for the impacts of 'Security Threats on E-Business'. International Journal of Computer Applications, 21(5), 1-4 Thanks for considering my request. I look forward to your reply.

--

Call for Paper (Open): <http://www.ijcaonline.org/calls->

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix R: Permission to Use Information Security Awareness Program Lifecycle Figure

---

From: R. David [cscpress@cscjournals.org]  
Sent: Thursday, August 09, 2012 12:38 PM  
To: Kevin Misenheimer  
Subject: Re: Request Permission to use Figure

Dear Kevin,

There is no problem in using any part of the published paper as long as you mention a clear reference/citation in your paper to support the content.

Papers using many references/citations actually represent the level of research carried out to support the publication work.

Thank you.

R. David  
CSC Press, Computer Science Journals (CSC Journals)

B-5-8 Plaza Mont Kiara, Mont Kiara  
50480, Kuala Lumpur, Malaysia

Tel: + 603 6207 1607, + 603 2782 6991

Fax:+ 603 6207 1697

Url: <http://www.cscjournals.org>

----- Original Message -----

From: [Kevin Misenheimer](mailto:Kevin.Misenheimer)  
To: [cscpress@cscjournals.org](mailto:cscpress@cscjournals.org)  
Sent: Wednesday, August 08, 2012 8:07 AM  
Subject: Request Permission to use Figure

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the figure titled:

Information Security Awareness Program Lifecycle

It is from the following source:

Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). *International Journal of Computer Science and Security (IJCSS)*, 5(1), 39-53. Retrieved from <http://www.cscjournals.org/csc/journals/IJCSS/description.php?JCode=IJCSS>

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

No virus found in this message.

Checked by AVG - [www.avg.com](http://www.avg.com)

Version: 2012.0.2197 / Virus Database: 2437/5185 - Release Date: 08/07/12



## Appendix S: Permission to Use Information Security Planning Involves Planning at Various Levels Figure

**From:** Tmitri A. Owens [mailto:towens@cis.gsu.edu]  
**Sent:** Wednesday, August 22, 2012 3:52 PM  
**To:** Kevin Misenheimer  
**Subject:** FW: reprint authorization approval

Good Day,

Attached is the reprint authorization.

Thanks for your patience,

Tmitri Owens, MPA  
Program Director  
Association for Information Systems  
404-413-7444  
404-413-7443 (fax)

AIS is hosted and located in the Computer Information Systems Department  
Georgia State University, 35 Broad Street, Suite 917, Atlanta, GA 30303  
Phone: +1 404 413 7445 Fax: +1 404 413 7443 E-mail: [onestop@aisnet.org](mailto:onestop@aisnet.org) Internet:  
<http://www.aisnet.org>

*It is our pleasure to serve you. Click [here](#) to tell us how we did.*

Good Day Kevin,

Please complete the attached reprint form & return to me for processing. There is no fee associated.

Thanks,

Tmitri Owens, MPA  
Program Director  
Association for Information Systems  
404-413-7444  
404-413-7443 (fax)

AIS is hosted and located in the Computer Information Systems Department  
Georgia State University, 35 Broad Street, Suite 917, Atlanta, GA 30303  
Phone: +1 404 413 7445 Fax: +1 404 413 7443 E-mail: [onestop@aisnet.org](mailto:onestop@aisnet.org) Internet:  
<http://www.aisnet.org>

*It is our pleasure to serve you. Click [here](#) to tell us how we did.*

**From:** Kevin Misenheimer [<mailto:kmisenheimer7517@stanly.edu>]

**Sent:** Wednesday, August 08, 2012 12:01 PM

**To:** [eLibrary@aisnet.org](mailto:eLibrary@aisnet.org)

**Subject:** Request Permission to use Figure

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the figure titled:

Information Security Planning Involves Planning at Various Levels

It is from the following source:

Young, R., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of AIS*, 2010(26), 245-266. Retrieved from <http://aisel.aisnet.org/cais/>

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix T: Permission to Use Performance Pyramid Framework Figure

---

From: ikoskosas@uowm.gr [ikoskosas@uowm.gr]  
Sent: Thursday, August 16, 2012 3:21 AM  
To: Kevin Misenheimer  
Subject: Re: Request Permission to use Figure

Dear Kevin

You can use my pyramid framework if you refer to the source of course.

Best Regards  
Ioannis

Quoting Kevin Misenheimer <kmisenheimer7517@stanly.edu>:

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use the Figure titled Performance Pyramid Framework in my dissertation. It is from the following source:

Performance Pyramid Framework. Adapted from "A Model Performance to Information Security Management," by I. Koskosas, K. Kakoulidid, and C. Siomos, 2011, International Journal of Business and Social Science, 2, p. 50.

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix U: Permission to Use A Strategic Framework for Effective Information Security Figure

---

From: MISQE [misqe@indiana.edu]  
 Sent: Tuesday, August 14, 2012 3:49 PM  
 To: Kevin Misenheimer  
 Subject: RE: Request Permission to use Figure

Hi Kevin,

As long as you provide a proper citation to the article you are free to use the figure for not-for-profit purposes. If the dissertation becomes part of any for-profit publication (i.e. - textbook), we require a \$50 royalty payment.

Thank you,  
 Randy Minas  
 Managing Editor, MIS Quarterly Executive

From: Kevin Misenheimer [mailto:kmisenheimer7517@stanly.edu]  
 Sent: Wednesday, August 08, 2012 12:16 PM  
 To: MISQE  
 Subject: Request Permission to use Figure

To whom it may concern,

My name is Kevin Misenheimer and I'm a Doctoral candidate at Northcentral University, AZ. I'm seeking your permission to use in my dissertation the figure titled:

A Strategic Framework for Effective Information Security

It is from the following source:

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technical factors. *MIS Quarterly Executive*, 9(3), 163-175. Retrieved from <http://misqe.org/ojs2/index.php/misqe/index>

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

## Appendix V: Permission to Use Information Security Framework Figure

**From:** Kay Fielden [mailto:kayafielden@gmail.com]  
**Sent:** Thursday, August 23, 2012 10:38 PM  
**To:** Kevin Misenheimer  
**Subject:** permission to use the Information Security Framework

**From:** Kevin Misenheimer [mailto:kmisenheimer7517@stanly.edu]  
**Sent:** Thursday, August 23, 2012 1:02 PM  
**To:** [Publisher@InformingScience.org](mailto:Publisher@InformingScience.org)  
**Subject:** Request Permission to Use Figure in Dissertation

Hi Kevin,

You have my permission to use this figure - please cite when you use it

regards

Kay

Hello, my name is Kevin Misenheimer and I am a doctoral student at Northcentral University, AZ. I am working on my dissertation and am trying to contact:

**Kay Fielden**  
 Unitec Institute of Technology  
 Auckland, New Zealand

The email I have for Kay Fielden at Unitec is not working.

I'm seeking your permission to use in my dissertation the figure titled:

Information Security Framework

It is from the following source:

Fielden, K. (2011). An holistic view of information security: A proposed framework.  
*International Journal for Infonomics*, 4(1/2), 427-434. Retrieved from

I have been unsuccessful in contacting the author.

Thanks for considering my request. I look forward to your reply.

E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties.