A QUANTITATIVE STUDY ON THE RELATIONSHIP OF INFORMATION SECURITY POLICY AWARENESS, ENFORCEMENT, AND MAINTENANCE TO INFORMATION SECURITY PROGRAM EFFECTIVENESS

by

Michael T. François

STEVEN BROWN, Ph.D., Faculty Mentor and Chair

JOHN POIRIER, Ph.D., Committee Member

JANE ALLEN PETRICK, Ph.D., Committee Member

Rhonda Capron, Ed. D., Dean of Technology

School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

December 2016

Abstract

Today's organizations rely heavily on information technology to conduct their daily activities. Therefore, their information security systems are an area of heightened security concern. As a result, organizations implement information security programs to address and mitigate that concern. However, even with the emphasis on information security, there has been a steady increase in information security violations. Therefore, the purpose of this quantitative survey study is to assess the factors that lead to an ineffective information program by investigating the relationship of an organization's awareness, enforcement, and maintenance of its information security policy program to its program's effectiveness. The study used a 5-point Likert scale survey instrument, which was administered through SurveyMonkey's online web portal using the SurveyMonkey Audience. The sample size for this study was 119 volunteers. These volunteers were asked question on their organization's information security program effectiveness, policy awareness, policy enforcement, and policy maintenance. This study employed multiple regression to predict values on the dependent or criterion variable level of information security program effectiveness from a set of independent predictor variables for the levels of information security policy awareness, enforcement, and maintenance. The independent variables total policy awareness, total policy enforcement, and total policy maintenance were found to be statistically significant predictors of the level of total program effectiveness.

Dedication

This dissertation is dedicated to my wife Elen Benjamin-Francois, Children Simba, Malika, and Grand Children Jeremih and Meliana Francois. Thanks for your patients and support throughout this journey. I would also like to thank my many other supporters throughout this Journey to include but not limited to Grandmother Fenola François, my mother Erica Schaper, Yvonne Toussaint, and Sweeny Toussaint Jr., and Lisa Wiltshire.

Acknowledgments

I wish to thank Dr. Steven A. Brown, Dr. Jane Petrick, and Dr. John Poirier for their assistance with this dissertation study. Special thanks to Dr. Dino Fontaine, Dr. Denis Griffith, and Dr. Anastasie Jackson for their support.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Introduction to the Problem

Today's organizations rely on information technology (IT) to conduct their business activities (Chang & Wang, 2011; Doherty, Anastasakis, & Fulford, 2011; Ifinedo, 2012; Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Mbowe, Zlotnikova, Msanjila, & Oreku, 2014). These systems store and manage sensitive information that, if handled inappropriately, can have devastating consequences for organizations. Consequently, this is an area of heightened security concern because of the highly confidential information stored in these information systems (Chang & Wang, 2011; Ifinedo, 2014). IT managers consider information security as a primary concern (Drtil, 2013; Jalal-Karim, 2013; Willison & Warkentin, 2013). As a result, organizations implement information security programs to address and mitigate their security concerns. Although organizations have placed emphasis on information security, there has been a steady increase in information security breaches (Ifinedo, 2014; Paulsen & Coulson, 2011). These security violations can be extremely expensive to an organization (Wilson & Warkentin, 2013; Paulsen & Coulson, 2011). Accordingly, scholars are interested in the effectiveness of information security programs (Ifinedo, 2012; Knapp & Ferrante, 2012; Paulsen & Coulson, 2011). The three key components to achieving this are the inclusion of formal policies, the active maintenance of these policies, and employee awareness of information security policies (Knapp & Ferrante, 2012).

Background of the Study

An effective information security program incorporates technical and non-technical methods (Ifinedo, 2012). The traditional methods encompass the technical means of protection, such as firewalls, anti-virus, and anti-spyware software; whereas, the non-technical approaches

address the human concerns that incorporate policies and procedures. Scholars agree that an effective information security program should take processes, technology, and people into consideration (Paulsen & Coulson, 2011). These findings suggest that organizations' information security programs need to recognize and incorporate the human component. This component is recognized as the weakest link in an information security program (Cavallari, 2011; Chen, Ramamurthy, & Wen, 2013; D'Arcy & Devaraj, 2012; Guo, Yuan, Archer, & Connelly, 2011; Harnesk & Lindström, 2011; Hu, Xu, Dinev, & Ling, 2011; Ifinedo, 2012; Lowry, Posey, Roberts, & Bennett, 2014; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Vance, Anderson, Kirwan, & Eargle, 2014). Researchers agree that a considerable amount of information security violations are due to employees' policy noncompliance (Cheng, Li, Li, Holm, & Zhai, 2013).

However, an employee's primary excuse for policy infraction is a lack of awareness and understanding of policies (Markovitz, 2012). This justification corroborates why an awareness and maintenance program is essential for an effective information security program. Furthermore, research findings indicate that an effective awareness program increases the effectiveness of an institution's information security program (Harnesk & Lindström, 2011; Padayachee, 2012; Wolf, Haworth, & Pietron, 2011). However, numerous organizations view awareness programs as being inefficient and expensive (Paulsen & Coulson, 2011). In addition, researchers argue that previous findings on awareness effectiveness are inconclusive (Wolf et al., 2011).

For that reason, the theory of organizational learning will be utilized in this study to explore the link between policy awareness, enforcement, and maintenance and an effective information security program. Knapp and Ferrante (2012) used the theory of organizational

learning to explore awareness and maintenance influence on an effective information security program. Similarly, Hedström, Kolkowska, Karlsson, and Allen (2011) used the theory to investigate factors that influence employees' noncompliance. The theory of organizational learning addresses security concerns through a double-loop concept, which allows managers to address security concerns immediately and make changes to the underlying philosophy (Kerman, Freundlich, Lee, & Brenner, 2012; Kim, MacDonald, & Andersen, 2013; Mohanty & Kar, 2012). The double-loop approach encourages the study of employees' behavior and applies that knowledge to guide the development of security policy. This theory implies that security policies are only observed through employee action (Kerman et al., 2012; Kim et al., 2013; Mohanty & Kar, 2012).

Statement of the Problem

Currently, data breaches are frequent occurrences that affect businesses, the economy, and national security. According to Privacy Rights Clearinghouse (2015), 303,135,385 breaches were reported between January 2011 and March 2015. It is estimated that data breaches cost United States (U.S.) companies $6.75 million in 2010 (Paulsen & Coulson, 2011). Moreover, research reveals that, on average, U.S. organizations expend 2.1% of their daily profit on information security (Fenz, Ekelhart, & Neubauer, 2011). Findings conclude that employee noncompliance is a principal reason for information security breaches (Guo et al., 2011; Paulsen & Coulson, 2011; Willison & Warkentin, 2013). In most cases, an employee's noncompliance is due to ignorance, oversight, and conflicting values (Hedström et al., 2011).

Moreover, there are three key components to an effective information security program: the inclusion of formal policies, the active maintenance of these policies, and employee awareness of information security policies (Knapp & Ferrante, 2012). Researchers have pointed

out that the awareness of policies influences employees' willingness to comply (Cheng et al., 2013). However, security risk areas and work environments are constantly changing, which can make the awareness of policies obsolete (Allam, Flowerday, & Flowerday, 2014). Hence, this study will examine the ineffectiveness of information security programs when organizations fail to implement policy awareness, enforcement, and maintenance programs as a component of their information security program (Knapp & Ferrante, 2012; Rashid, Zakaria, & Zulhemay, 2013). Information security program effectiveness is a measure of performance that determines whether a program is achieving its objective of protecting the organization's information (Knapp & Ferrante, 2012). Therefore, ineffectiveness indicates the program's inability to achieve its objective.

Purpose of the Study

The purpose of this quantitative survey study, with a correlational research design, is to assess the factors that lead to an ineffective information program by investigating the relationship of an organization's awareness, enforcement, and maintenance of an information security policy program to its program's effectiveness. For this study, program effectiveness is a measure of performance that determines whether the program is achieving its objective of protecting the organization's information (Knapp & Ferrante, 2012). Additionally, the study will address limitations found in Knapp and Ferrante's (2012) study, adding to that body of knowledge. First, their responses were not drawn from a sample of general employees but professionals in the information security field. Second, their study was not generalizable to other

populations of employees because the sample was drawn from a population of information security professionals.

This study's independent variables are information security policy awareness, information security policy enforcement, and information security policy maintenance. Information security policy awareness represents an employee's knowledge and comprehension of an organization's information security policy (Knapp & Ferrante, 2012), information security policy enforcement is described as the method used to impose an organization's rules, and information security policy maintenance is described as an organization's ability to adapt and develop new strategies to adjust to changes in their environment and improve performance and effectiveness. The dependent variable, information security effectiveness, is a measurement of how effectively an organization's information security program accomplishes its goal of protecting the organization's information (Knapp & Ferrante, 2012).

Rationale

The proposed study addresses a gap in the body of knowledge, as determined by Knapp and Ferrante (2012). Since Knapp and Ferrante's (2012) study sample was from a population of information security professionals, the results are not generalizable to other populations of employees (Knapp & Ferrante, 2012). The researchers recommended that future research survey workers whose knowledge is external to information security. The literature indicates that these conventional users are a major source of vulnerability to an organization's information security (Guo et al., 2011). The proposed study focuses on employees with knowledge external to

information security because they are an organization's weakest link for information security (Shahraki & Nikmaram, 2013).

Surveying organizations' average computer users will provide, from those most familiar with information security effects, a more enhanced comprehension of the factors needed for an effective information security program. Accordingly, the findings should yield valid and reliable results needed for a positive effect on employees' attitudes and behaviors towards information security. Moreover, the study will provide information to help reduce employee noncompliance, thereby reducing the number of security breaches encountered by organizations (Ifinedo, 2012; Padayachee, 2012). Such an outcome may contribute to the reduction of organizations' overall expenditures due to information security breaches (Fenz et al., 2011; Paulsen & Coulson, 2011).

Research Questions

Researchers suggest that there is a relationship between the awareness, enforcement, and maintenance of an information security policy program and the effectiveness of this program (Ifinedo, 2014; Paulsen & Coulson, 2011). Numerous research findings indicate that an effective information security awareness program increases the effectiveness of an institution's information security program (Harnesk & Lindström, 2011; Padayachee, 2012; Wolf et al., 2011). These findings support the idea that awareness training and education have a positive influence on employees' compliance. However, opponents argue that previous studies on information security awareness are inconclusive (Wolf et al., 2011). These opposing perspectives indicate inconclusiveness in the literature regarding the predictive relationship between

information security policy awareness, enforcement, and maintenance and the effectiveness of an organization's information security program. As such, a gap remains in the body of knowledge.

Furthermore, research has shown that some organizations view information security awareness programs as being inefficient and expensive (Paulsen & Coulson, 2011). As a result, these organizations are reluctant about investing in an awareness program. Studies indicate that 43% of surveyed individuals stated that less than 1% of their organization's information security budget was designated for awareness training (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2012). Accordingly, researchers agree that there is a need for further research on information security awareness (Wolf et al., 2011).

Similarly, some researchers stress the importance of information security policy enforcement in achieving an effective information security program (Chang & Wang, 2011; Hedström et al., 2011; Ifinedo, 2012; Ifinedo, 2014). Information security policy enforcement can be sorted into two popular categories, including control-based compliance and value-based compliance. Control-based compliance models stipulate that human behavior must be restricted and controlled (Hedström et al., 2011). These models use bureaucratic rules to encourage employees' compliance with organization information security policy. In addition, this approach uses fear of punishment as a deterrent (Lowry et al., 2014). Another method within this approach is reward or a combination of punishment and reward. However, empirical findings regarding the influence of reward and punishment on compliance are inconclusive (Chen et al., 2013). On the other hand, value-based compliance models consider the inclusion of employees' values and beliefs in the development of information security policies (Hedström et al., 2011). This approach encourages information security managers to focus on employees' needs and habits

when developing policies. However, there is a dearth of research on value-based compliance, as it relates to information security.

Equally important, researchers argue that security risk areas and work environments are constantly changing, leading to policies and policy awareness becoming obsolete (Allam et al., 2014). The objective of an information security maintenance program is to ensure that information security policies and programs are still meeting the security needs of the organization (Knapp & Ferrante, 2012). Thus, an effective information security program should have continuous education and training for employees (Bower, 2011). This continuous update of policies and training requires a maintenance plan. These concerns helped develop this study's research question.

Research Question: Are information security policy awareness, enforcement, and maintenance significant predictors of information security program effectiveness?

H_0: Information security policy awareness, enforcement, and maintenance are not statistically significant predictors of information security program effectiveness.

H_A: Information security policy awareness, enforcement, and maintenance are statistically significant predictors of information security program effectiveness.

Significance of the Study

The significance of this study will be to expand on previous knowledge of information security. The study explores information security policy awareness, enforcement, and maintenance in relation to information security program effectiveness. Understanding this relationship will provide knowledge that may allow practitioners to develop more effective information security programs. As a result, this study will assist in mitigating employee noncompliance and potentially reduce the percentage of breaches encountered by organizations.

Moreover, reducing the percentage of breaches will eventually minimize the financial burden of organizations due to information security breaches.

The results of this study will add to the body of information on information security. Furthermore, the findings should contribute further information on the relationship between information security policy awareness, enforcement, maintenance and information security program effectiveness. This added information will provide scholars and practitioners with a profound understanding of the effects that information security policy awareness, enforcement, and maintenance have on information security program effectiveness. The study is especially relevant in the mitigation of employee noncompliance to information security policy because data gathered is from the employee's perspective. Therefore, it addresses the relationships between IVs and DVs from the employee's point of view. With employees being the weakest link in security programs, this study may provide information that can enhance information security program effectiveness (Knapp & Ferrante, 2012).

Definitions of Terms

Information security program effectiveness (SPE). This is a measure of performance that determines whether the program is achieving its objective of protecting the organization's information (Knapp & Ferrante, 2012).

Information security policy awareness (ISPA). This is the organization's effort to educate employees about security policies (Knapp & Ferrante, 2012).

Information security policy enforcement (ISPE). This is the organization's effort to correct an employee's policy violation (Knapp & Ferrante, 2012).

Information security maintenance (ISPM). This is the organization's effort to update policies periodically (Knapp & Ferrante, 2012).

Assumptions and Limitations

Several assumptions are used in guiding this study. The first assumption in this study is that the theory of organizational learning explains the association between independent variables (Allam et al., 2014; Hedström et al., 2011; Knapp & Ferrante, 2012). The theory uses a double-loop approach, which encourages the study of employees' behavior and applies that knowledge to guide the development of security policy. The second assumption is the ontology that medium to large organizations with information security programs include information security management programs that contain policy awareness, enforcement, and maintenance. The third assumption is the axiology that independent and dependent variables can be measured through employees' perceived knowledge and understanding of an organization's information security program. A fourth assumption is that participants selected from SurveyMonkey's panel of volunteers are a true representation of the population. Finally, there is an assumption that findings will assist in developing effective information security programs.

One limitation of this study is internal validity due to research design. The research approach is quantitative survey with a correlational research design, thereby limiting the findings and discussion to relationships (and not causal). Another limitation is that respondents may not be representative of the population. The survey response rate is limited by cost and time to only two waves of responses. Dillman (2014) states that, other than online surveys, there is no method of collecting survey data that offers so much potential for so little cost.

Nature of the Study

The theory of organizational learning, which was developed by Argyris and Schön (1996), will be used in this study (Hedström et al., 2011; Knapp and Ferrante, 2012). This theory was used in Hedström et al. (2011) to develop their value-based model for information security

(IS) policy compliance. In addition, the theory of Organizational Learning was also used in Knapp and Ferrante's (2012) study on IS effectiveness in organizations. Argyris and Schön's (1996) theory of organizational learning addresses security concerns through a double-loop concept, which allows managers to address security concerns immediately and make changes to the underlying philosophy (Kerman et al., 2012; Kim et al., 2013; Mohanty & Kar, 2012). The double-loop approach encourages the study of employees' behavior and applies that knowledge to guide the development of security policy. This theory implies that security policies are only observed through employee action. (Kerman et al., 2012; Kim et al., 2013; Mohanty & Kar, 2012). In contrast, single-loop learning concentrates on revising policy inaccuracies (Kerman et al., 2012; Kim et al., 2013; Mohanty & Kar, 2012). As applied to this study, this theory indicates that the independent variables policy awareness, enforcement, and maintenance should have a positive influence on the dependent variable IS program effectiveness. Certainly, this positive influence is predicted because, by implementing the theory of organizational learning, organizations are continuously learning and amending their fundamental philosophy.

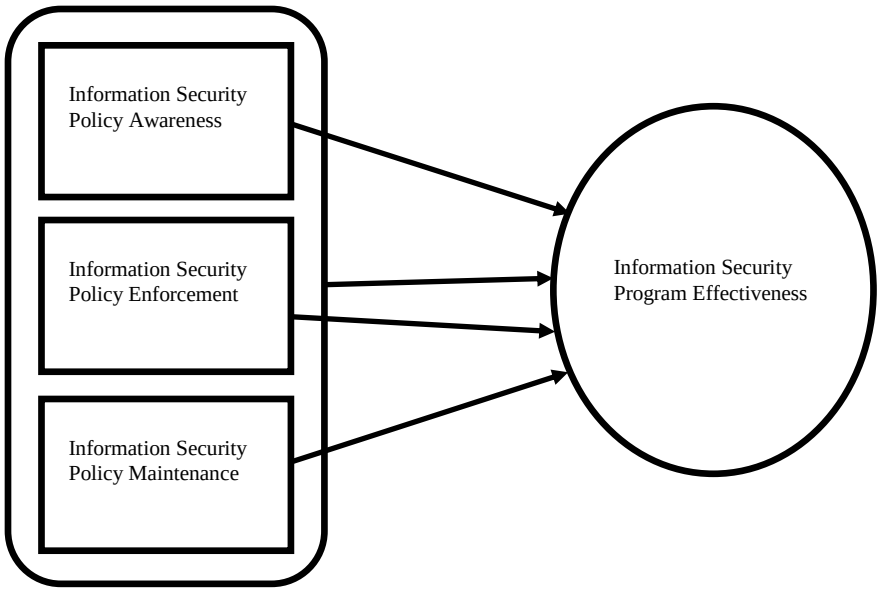

Figure 1. Theoretical model of information security policy and program effectiveness

Organization of the Remainder of the Study

Chapter 2 examines the existing agglomeration of knowledge associated with this research study and provides a background on information security programs, policy awareness, policy maintenance, and policy enforcement. Chapter 3 explains and justifies the research methodology, data collection, analysis, and steps employed to ensure that the research was conducted in an ethical manner. Chapter 4 presents the statistical analysis of the data collected. Chapter 5 discusses the study's results, implications, and limitations and provides recommendations for future research.

CHAPTER 2. LITERATURE REVIEW

Information technology serves as an organization's information backbone (Chang & Wang, 2011; Doherty et al., 2011; Hedström, Karlsson, & Kolkowska, 2013; Ifinedo, 2012; Jalal-Karim, 2013; Lebek et al., 2014; Mbowe et al., 2014). According to Al-Mukahal and Alshare (2014), information technology is not only a vital element to organizations but also required if they intend on competing in the market. These information systems are used to store and maintain confidential information, thereby increasing information security apprehension (Chang & Wang, 2011; Ifinedo, 2014; Sommestad, Hallbeg, Lundholm, & Bengtsson, 2014; Yoon & Kim, 2013). Additionally, with advancements in technology, the value of information continues to increase in many companies. As a result, the challenges and risks confronting information systems have increased (Mbowe et al., 2014; Mukundan & Sai, 2013; Soomro, Shah, & Ahmed, 2015).

Moreover, considering the abundance of breaches reported, these concerns are not outlandish. Privacy Right Clearinghouse (2015) revealed that, between 2011 and 2015, organizations reported 2,228 breaches. A recent survey indicated that 45.6% of respondents reported that their organization encounters at least one information security attack every year (Silic & Back, 2013). Vance, Siponen, and Pahnila (2012) also acknowledge that companies average at least one breach per year. However, reported incidents constitute only those that were made public, and most organizations hesitate on reporting information security incidents to avoid potential repercussion (Steinbart, Raschke, Gal, & Dilla, 2016). Therefore, the number reported by Privacy Right Clearinghouse may just be the pinnacle.

These breaches can have a negative repercussion on an organization's operations and assets by interfering with information confidentiality, availability, and integrity (CAI) (Steinbart

et al., 2016; Jalal-Karim, 2013). The cost of information security violations can be exorbitant to an organization. Additionally, the expenses are generally both implicit and explicit to afflicted organizations (Gordon, Loeb, & Zhou, 2011), and indirect deprivations are often more severe than direct ones (Bojanc & Jerman-Blažič, 2013).

Researchers have indicated that information security breaches could have an adverse impact on a company's earnings and reputation (Safa, Von Solms, & Furnell, 2016; Steinbart et al., 2016). One information security breach cost a USA company $61 million in one year as it tried to recover from damages (Soomro et al., 2016). The organization also encountered a profit loss of 46% in one quarter of the same year. Soomro et al. (2016) mentioned that, in 2013, the average cost of information security breaches in the USA was between $4.4 million and $9.4 million. Moreover, information security breaches cost taxes payers trillions of dollars (Khey & Sainato, 2013). Furthermore, although organizations have placed emphasis on information security, breaches have continued to increase (Ifinedo, 2014; Paulsen & Coulson, 2011). This dilemma has propelled information security as a preeminent concern for IT administrators and senior management (Dahbur, Isleem, & Ismail, 2012; Drtil, 2013; Hedström et al., 2013; Montesdioca & Maçada, 2015; Mukundan & Sai, 2014; Willison & Warkentin, 2013). The 2012 Global Risk Report listed information security breaches in the top five hazards the world will encounter in this decade (Fenz, Heurix, Neubauer & Pechstein, 2013).

The continuous upsurge in information security breaches has led scholars to the realization that traditional techniques of information security may not be applicable (Bojanc & Jerman-Blažič, 2013; Cavallari, 2011; da Veiga & Martins, 2015; Paulsen & Coulson, 2011; Safa et al., 2016; Safa, Sookhak, Von Solms, Furnell, Ghani, & Herawan, 2015; Singh, Gupta, & Ojha, 2013; Skorodumov, Skorodumova, & Matronina, 2015; Yoon & Kim, 2013; Wall, Palvia,

& Lowry, 2013). Conventional approaches, including the use of software such as anti-viruses, anti-spyware, and firewalls, lack the necessary components to obtain the required information security (Chen et al., 2013; Safa et al., 2016). These approaches ordinarily alert users of threats and depend on users to make educated decisions on the most appropriate method of mitigating the risk. Unfortunately, research indicates that most users ignore the alerts or circumvent the technology (Paulsen & Coulson, 2011; Vance et al., 2014).

The research findings also indicate that 38% of data breaches were due to lost paper files, 27% to misplaced portable equipment, and 11% to hackers (Soomro et al., 2016). Equally important, Soomro et al. (2016) noted that a large threat to information security was malicious insiders. Furthermore, rather than targeting technology to infiltrate information systems, hackers often gain access through human error (Safa et al., 2016). This dilemma indicates that information security is not only an IT issue but also a human resource concern. Therefore, companies that fail to consider the human aspect of information security are apt to fail at protecting their information systems. Information security managers consider employees as the biggest risk to their information security network (Shahraki & Nikmaram, 2013). Hence, proper employee behavior mitigates security breaches (Safa et al., 2016).

Furthermore, employees' risky behavior may expose sensitive information and interfere with technological security. To support this, the findings of a survey indicated that 49% of respondents admitted to occasionally engaging in risky behavior and 28% said they did so frequently (Cox, 2012). Also, a significant amount of information security incidents transpires in the workplace because of employee infringements (Ifinedo, 2012). These occurrences can be intentional or accidental violations by employees. A survey conducted on a security management company indicated that approximately 40% of respondents acknowledged that their primary

security concern is employees accidentally endangering security (Al-Mukahal & Alshare, 2014). Additionally, this survey revealed that 49% of security incidents were because of accidental disclosures through the Internet. Because of these results, researchers have indicated that employees are the biggest threat to information security (Al-Mukahal & Alshare, 2014; Arachchilage & Love, 2014; Aydin & Chouseinoglou, 2013; Cavallari, 2011; Chen et al., 2013; D'Arcy & Devaraj, 2012; Doherty et al., 2011; Guo et al., 2011; Harnesk & Lindström, 2011; Hu, Dinev, Hart, & Cooke, 2011; Hu et al., 2011; Ifinedo, 2012; Lowry et al., 2014; Montesdioca & Maçada, 2015; Parsons et al., 2013; Shropshire, Warkentin, & Sharma, 2015; Skorodumov et al., 2015; Thomson & Van Niekerk, 2012; Tsohou, Karyda, & Kokolakis, 2015; Tsohou et al., 2012; Vance et al., 2014; Wall et al., 2013). Statistics show that employees being an organization's weakest link is a common opinion in the information security field. Alternatively, these findings also confirm that employees are the key to mitigating data breaches (Vance et al., 2012; Wall et al., 2013).

A recent information security survey indicated that 91% of its participants were concerned about employees as a security vulnerability (Padayachee, 2012). Additionally, the same survey indicated that 79% of participants alleged employee error as the primary reason for security breaches. Another survey conducted by the Japan Network Association revealed that out of the 1,032 security failures that occurred in 2005, 42% were due to human blunder (Komatsu, Takagi, & Takemura, 2013). Komatsu et al. also revealed that, in 2009, information security incidents increased, with user errors declining by 7.9% and administrative errors increasing by 5.9% to 50.9%.

Likewise, research shows that managers are just as likely to engage in information security violations as ordinary employees (D'Arcy & Devaraj, 2012). According to recent

studies, the Verizon 2010 Data Breach Investigations Report concluded that 48% of breaches were due to employee mismanagement (Vance, Lowry, & Eggett, 2013). The same research explained that, in 2010 and 2011, 29% of surveyed individuals expressed knowledge of violations due to insiders. The study also revealed that, although information security traditional countermeasures are designed to mitigate external intrusion (not malicious insiders), 33% of breaches were due to malicious employees. (Vance et al., 2013). Therefore, the traditional approaches are rendered particularly useless.

Information Security

Depending on who you ask, information security has several definitions. For instance, it has been defined as the ability to protect information and information systems' confidentiality, integrity, and availability (CIA) (Mukundan & Sai, 2014; Singh et al., 2013; Yildirim, Akalp, Aytac, & Bayram, 2011). Confidentiality is defined as the ability to prevent unauthorized entities from gaining access to information (Mukundan & Sai, 2014). Moreover, integrity involves ensuring the accuracy and fullness of the data (Mukundan & Sai, 2014). Equally important, availability refers to making information accessible to authorized individuals (Mukundan & Sai, 2014). Thus, a violation of CIA is considered a failure of information security.

Similarly, information security is also defined as users' perceptions of importance, responsibility, and level of security (Safa et al., 2015). Accordingly, with new advancements in technology comes greater opportunities for security violations (Skorodumov et al., 2015). Therefore, despite users' continuous increase in computer literacy, security issues are expected to multiply (Aydin & Chouseinoglou, 2013). These increased security concerns substantiate the importance of information security (Wall et al., 2013). Therefore, success in such an environment demands the implementation of an effective information security program (Hall,

Sarkani, & Mazzuchi, 2011). Most information security programs combine information security policy, awareness, enforcement, and maintenance programs. However, there is little encyclopedic research on the indispensable components that signify an effective information security program (Steinbart et al., 2016). Conversely, the enormous amount of breaches being reported is an indication that most information security programs are not effective (Steinbart et al., 2016).

Information Security Program

Information security strategy is a primary challenge for organizations (Hall et al., 2011). Thus, organizations are spending significant amounts of money on technology and information systems in an attempt to mitigate data breaches (Jalal-Karim, 2013). In recent years, many software and hardware protection techniques have been constructed to safeguard information and information systems (Öğütçü, Testik & Chouseinoglou, 2016). Accordingly, advancement in software and hardware safeguards have reduced their inconsistency, thereby mitigating breaches caused by software and hardware deficiencies. However, these improvements barely crack the surface of the violations that are encountered every year.

According to Öğütçü et al. (2016), information security is only as strong as its weakest link. These authors emphasized that hackers usually employ social engineering to target employees who are considered the weakest link in the information security chain, further stressing that breaches are not a technology problem but a human problem. Therefore, organizations that depend on technology to defend their information assets from violations will soon come to realize that their programs are insufficient (Montesdioca & Maçada, 2015). An effective information security program incorporates technical and non-technical methods (Ifinedo, 2012). The traditional methods encompass the technical means of protection; whereas,

the non-technical approaches address human concerns. Scholars agree that an effective information security program should take processes, technology, and people into consideration (Paulsen & Coulson, 2011). Traditional approaches to information security make allowance for processes and technology. However, organizations' information security programs need to recognize and incorporate the human component.

Accordingly, researchers suggest two dominant approaches to a comprehensive information security program: a business-centered approach and a people-centered approach (Aydin & Chouseinoglou, 2013; Paulsen & Coulson, 2011). The business-centered approach views the program from a risk-analysis cost-effective method; whereas, the people-centered approach focuses on encouraging employees to be better information security citizens. Organizations develop security programs to provide the elements needed to govern information security citizens. These information security programs often address technology, processes, and users (Semer, 2012). An information security program includes guidelines, legislation, specifications, best practices, and policies used to guide employees in their daily routines. Thus, plans that only consider technology are not sufficient in mitigating violations (Montesdioca & Maçada, 2015).

For instance, recent research indicates that, despite the implementation of technical solutions in 2008, both the United Kingdom and United States saw a momentous increase in reported data breaches due to employee behavior (Renaud & Goucher, 2012). These results indicate the need for comprehensive information security programs. These programs, which are often considered the key component in mitigating information security risks, are managed at three levels, including policies, guidelines, and measures (Singh et al., 2013). Furthermore, security compliance indicates conformance with policies and procedures within the

organization's security program (Cavallari, 2011). Equally important, information security policy is the foundation of an organization's information security program (Chang & Wang, 2011). However, efforts to maintain an information security program are often only recognized after security fails.

Most standard definitions of information security include concerns pertaining to information and data management, encompassing confidentiality, integrity, and availability (Laybats & Tredinnick, 2016; Rhee, Ryu, & Kim, 2012). Additionally, information security threats can be divided into three categories, including intentional consequences of intentional actions, unintentional consequences of intentional actions, and unintentional consequences of unintentional actions (Laybats & Tredinnick, 2016). Intentional consequences of intentional actions involve deliberate attacks on information systems with calculated results; whereas, unintentional consequences of intentional actions relate to employees' accidental actions resulting in data breaches. Moreover, unintentional consequences of unintentional actions can be described as an accidental loss or destruction of data. As the authors noted, intentional consequences of intentional actions are the easiest to predict and negate. Included in this category of threats are hacking, denial of service attacks, malicious software, industrial espionage, deliberate data theft, exposure, and breaches (Laybats & Tredinnick, 2016). Therefore, these threats can be mitigated through technical solutions, such as software or hardware. On the other hand, the other two classes of threats are much harder to predict and counteract. Therefore, information security and information security programs are at the center of the solution in addressing these threats.

Information Security Policy

There are five fundamental components to implementing an organization's information security program, including formal policies, risk analysis, objectives, technology, execution plan, compliance, and team (Paulsen & Coulson, 2011). Additionally, the literature review proposes information security policies, education, training, and awareness as non-technical measures used to achieve information security (Lebek et al., 2014). Furthermore, Liu (2015) acknowledges information security policy as the most critical component of an effective information security program. Hence, if employees are not cognizant of information security policies, then the information security program will be ineffective.

Security policy is often recommended for mitigating employees' information security violations (Guo et al., 2011). For example, Lowry et al. (2014) suggested using policy and technology to reduce information security risk, specifically using technology to detect or block information security violations and policy to enforce procedures. Research findings have illustrated that policies can act as a behavioral guideline to employees, allowing them to conduct themselves properly (Chang & Wang, 2011). However, employees often violate information security policy.

An information security policy violation is the act of an employee intentionally or unintentionally utilizing a computer in a way that contravenes company policy (Hu et al., 2011). A widespread information security violation entails excess violations by employees (Vance et al., 2013). This type of abuse can manifest itself as employees' illegally gaining access to company information. Researchers agree that a considerable amount of information security violations are due to employees' policy noncompliance (Cheng et al., 2013). Policies often dictate certain procedures that must be followed by employees. However, insiders have given several excuses

as to why they fail to follow these procedures, including (1) they were not aware of the procedure, (2) they were not trained on the procedure, (3) they did not comprehend the procedure, (4) the policy or procedure was too long, and (4) the procedure was not accessible (Markovitz, 2012). These justifications for violating policy demonstrate why an awareness and maintenance program is essential to an effective information security program. However, the first step should be the creation of a clear and comprehensive information security policy. Researchers have recognized that information policies are often developed and implemented in a provisional fashion (Renaud & Goucher, 2012). These researchers argued that this ad hoc development and implementation could be credited to a lack of empirical support for guidelines on formulating and executing policies.

There are three key components to an effective information security plan, including formal policies, active maintenance of these policies, and employee awareness of these policies (Knapp & Ferrante, 2012). The principal threat to an organization's information security is employees' noncompliance to policy (Cheng et al., 2013; Siponen, Mahmood, & Pahnila, 2014). There is increasing evidence that a large proportion of organizations' information security complications are the result of employees' information security policy violations (Doherty et al., 2011; Robertson, 2012; Skorodumov et al., 2015). Therefore, it is important that policy address the technical and non-technical characteristics of information security. An information policy is essentially a list of guidelines targeting a particular group of people and aimed at accomplishing expected rational outcomes (Al-Mukahal & Alshare, 2014; Yildirim et al., 2011).

In other words, a policy should serve as an instrument that provides guidance to manage and protect information (Doherty et al., 2011; Mbowe et al., 2014). An effective policy should include acceptable uses of information systems, users' information security responsibilities,

required training for all users, and consequences for policy violation (Sommestad, Karlzén, & Hallberg, 2015). Overall, the policy should provide users with all the necessary information needed to operate in a secure environment. An effective information policy can also mitigate security breaches (Soomro et al., 2015). According to researchers, an effective information security policy is the most important requirement for planning, implementing, and preserving information security in an organization (Chang & Wang, 2011; Pathari & Sonar, 2012; Singh et al., 2013). This policy provides the guidance needed to ensure the proper handling of information and information systems by users.

Moreover, an effective information policy should modify and improve users' information security behavior towards compliance (Safa et al., 2016). Information security policies emerge in a variety of formats and magnitudes, sometimes enforced by laws and regulations (Basin, Jugé, Klaedtke, & Zălinescu, 2013). However, the effectiveness of policies, guidelines, and awareness programs depends on employees' ability and willingness to comply (Doherty et al., 2011; Hedström et al., 2013; Montesdioca & Maçada, 2015). Nevertheless, more than half of all information security breaches are due to employee policy violations (Sommestad et al., 2015). Therefore, understanding the factors that influence this behavior should assist in reducing violations. It is logical, then, to presume that employee awareness of information security policy is the first step towards that objective.

Policy Awareness

Researchers have pointed out that the awareness of policy influences employees' willingness to comply (Cheng et al., 2013). Policy is implemented not only to simplify tasks but also to guide and influence safe information system behaviors (Han & Lei, 2011; Montesdioca & Maçada, 2015; Yoon & Kim, 2013). However, employees cannot adhere to an unknown policy.

Research indicates that the leading disincentive to a successful information security program is a lack of awareness by managers and employees (Rhee et al., 2012). Therefore, it is imperative that they are made aware of information security policies. Without awareness, an effective policy is rendered ineffective (Soomro et al., 2016).

According to Renaud and Goucher (2012), employees frequently read policies impetuously. However, researchers acknowledge that all employees should be educated on information security awareness (da Veiga & Martins, 2015; Ifinedo, 2014; Paulsen & Coulson, 2011; Rashid et al., 2013). According to Tsohou et al. (2015), an information security awareness program is essential to an effective information security program. These researchers went on to point out that information security awareness positively influences employees' information security policy behavior. Renaud and Goucher (2012) also acknowledged that policies could affect change in employees' behavior when accompanied by an effective awareness and education program. Additionally, Tsohou et al. (2015) stated that awareness is also linked to an employee's perception of sanctions, which increases policy compliance. Safa et al. (2015) disclosed similar assertions for employing information security awareness programs. Likewise, Soomro et al. (2016) acknowledged that awareness is the most effective measure for an information security program, and Cox (2012) argued that employee awareness is imperative.

Moreover, information security awareness is a process that intends to influence an organization's culture and its users' perspectives, principles, and attitudes by focusing on information security (Doherty et al., 2011; Tsohou et al., 2015). Thus, involving employees in this process mitigates a potential information security risk. However, a generic education has limited results on employees' behavior. Therefore, employees should be trained on the actual risk that may be inflicted on them. In other words, awareness education should be tailored to the

organization's security concerns. Furthermore, employees should be trained on the intention and objectives of security controls. Employees often have a distorted perception of risk due to insufficient knowledge (Rhee et al., 2012).

Therefore, information security officers must understand employees' awareness of a policy in order to determine its effectiveness (Al-Mukahal & Alshare, 2014). Furthermore, Renaud and Goucher (2012) implied that employees should be involved in the development and implementation of security policies. This involvement should reduce their need to circumvent controls in order to complete a task efficiently. Also, employees will be aware of policies as they are developed and implemented. Al-Mukahal and Alshare (2014) noted that employees who are not aware of a policy are most likely to violate the policy.

Additionally, trained employees influence other insiders to comply with information security policy. Researchers acknowledged that social influence is a positive factor for employee compliance (Ifinedo, 2014). Furthermore, the sharing of knowledge among employees is an effective method of increasing information security awareness (Safa et al., 2016). Thus, awareness training helps develop an organization's information security culture, establish an effective information security program, and improve employees' security behavior (da Veiga & Martins, 2015; Paulsen & Coulson, 2011; Rashid et al., 2013). Moreover, knowledgeable employees are more confident in their information security decisions. An awareness program helps to improve employees' unethical and ethical perceptions regarding information security (Cox, 2012). In a recent survey, 54% of respondents indicated that employee awareness training was their most important security practice (Phillips, 2014). In addition, 64% of organizations in North America have inaugurated awareness programs (da Veiga & Martins, 2015).

Nevertheless, many security breaches are due to employees' unawareness of policies and security risks (Cavallari, 2011; Tsohou et al., 2012). Rhee et al. (2012) argued that a significant portion of information security violations are the result of a lack of managers' and employees' awareness. These researchers associated optimistic bias to administrators' low levels of awareness and commitment regarding information security threats. They defined optimistic bias as a person's underestimation of the probability of negative occurrences. Additionally, their findings indicate that managers believed external networks propose a greater risk to their information security. Rhee et al. (2012) also noted that companies should increase security awareness training to negate optimistic bias. They believed that security awareness training and the systematic treatment of security threats are better remedies for resolving security violations than ad hoc approaches. Liu (2015) endorsed similar conclusions by emphasizing that employees' perceptions of security dictate their behavior.

Moreover, employees' information security behavior determines the number of security violations encountered by an organization. Consequently, researchers acknowledge that the majority of security violations by insiders are done unintentionally due to employee ignorance. Again, researchers insist on employee awareness training as a means of reducing information security risks across a broad spectrum (Allam et al., 2014; da Veiga & Martins, 2015; Parsons et al., 2013). In addition, an effective awareness program increases the effectiveness of an organization's information security program (Bower, 2011; da Veiga & Martins, 2015; Harnesk & Lindström, 2011; Padayachee, 2012; Wolf et al., 2011). According to Wolf et al. (2011), education and awareness training may be the most noticeable security measures, as these efforts attempt to change employee behavior and establish best practice.

However, numerous organizations view awareness programs as inefficient and expensive (Paulsen & Coulson, 2011). Organizations question their effectiveness because, regardless of training, most employees do not comply with policy (Cox, 2012). Furthermore, many awareness programs are not functioning as well as they should (Tsohou et al., 2012). Consequently, organizations question the return on investment (Cox, 2012). Research findings indicate that 43% of surveyed individuals stated that less than 1% of their information security budget was designated for awareness training (Tsohou et al., 2012). In addition, 55% felt that the investment in awareness training was insufficient.

However, there is research that supports organizations' disinclination to invest in an awareness program. For instance, researchers argue that previous research on awareness effectiveness is inconclusive (Aydin & Chouseinoglou, 2013; Wolf et al., 2011). Furthermore, researchers highlight numerous challenges of information security awareness programs, including direct benefits and justifying return on investment (Singh et al., 2013). Additionally, researchers argue that security awareness does not have a consistent definition and requires clarity (Wolf et al., 2011). In other words, scholars cannot agree on a precise definition of information security awareness.

Moreover, these same researchers emphasize the need for further research on information security awareness. Öğütçü et al. (2016) highlighted a lack of empirical research on the effectiveness of information security program design on employees' behavior. These findings can be interpreted by organizations to mean that awareness programs are ineffective. Thus, there are areas that an awareness program should address in order to be effective, including employee security knowledge, attitude, and behavior (Allam et al., 2014; Rashid et al., 2013). The program

should ensure that employees not only comprehend the organizations' security risks and policies but also align their attitudes according to company policy and procedure.

An awareness program should be designed as a fundamental step towards cultivating organizational learning (Wu, Guynes, & Windsor, 2012). Wu et al. (2012) believed that awareness training should reside in each employee's organizational memory. Moreover, these authors acknowledged that security awareness could benefit from organizational learning. Employees could glean on past information security incidents stored in their organizational memory, allowing them to make timely and effective decisions in safeguarding information. Equally important, the awareness program should influence behavior towards policy compliance.

Recent research indicates that 63% of user security breaches are due to ignorance and obscurity of policy (Pathari & Sonar, 2012). Therefore, it is important that information security policies are clear in order to foster effective awareness programs and policy compliance (Safa et al., 2015; Soomro et al., 2016). Additionally, information security awareness programs should place focus on the weakest link of information security – employees (Semer, 2012). Equally important, information security programs should be regularly updated in order to keep up with changes in policy and organizational environment (Safa et al., 2015). Maintaining a modernized information security program is critical in mitigating security violations. Finally, an organization's awareness program, combined with an enforcement program, will decrease security breaches (Safa et al., 2015). Therefore, organizations should include an enforcement program in their overall information security program.

Policy Enforcement

Policy enforcement procedures should focus on activities where users neglect to execute information security policy, including administration escalation processes (Semer, 2012).

Research findings show that 28% of information security professionals admitted that they fail to enforce internal enforcement policy (Pathari & Sonar, 2012). Furthermore, a recent survey indicates that 42% of respondents acknowledged information security policy enforcement as a considerable challenge to their information security program (Phillips, 2014). According to Steinbart et al. (2016), survey respondents revealed that increasing deterrent and preventive intentions, when combined with an elevated perceived severity of sanctions, enhances information security effectiveness. Policy enforcement may be sorted into two popular categories, including control-based compliance and value-based compliance. Control-based compliance models stipulate that human behavior must be restricted and controlled (Hedström et al., 2011). Scholars adopt a broad array of theories to support their research on control-based compliance, including the theory of reasoned action, the theory of protection motivation, the deterrence theory, the accountability theory, the rational choice theory, the social control theory, the integrated control theory, the regulatory focus theory, and the theory of planned behavior (Chen, Ramamurthy, & Wen, 2015; Hu et al., 2011; Ifinedo, 2012; Padayachee, 2012; Tsohou et al., 2015; Vance et al., 2014; Vance et al., 2012; Vance et al., 2013).

However, the most commonly used theory in control-based research is the general deterrence theory. This theory, which has been used by itself or in combination with one of the previously mentioned methods, was employed in Straub and Welke's (1998) study, in which they recommended that companies use theory-based security programs (Chen et al., 2015). Lee, Lee, and Yoo (2004) also used it in their study which identified the deterrence factors that influenced information security abuse by both internal users and external intruders (Chen et al., 2015). Chen et al. (2015) also pointed out Herath and Rao's (2009) use of the general deterrence

theory, in combination with the protection motivation theory, in identifying factors that had an impact on policy attitudes.

The general deterrence theory was employed by D'Arcy, Hovav, and Galletta (2009) in their investigation on the perceived severity of sanctions (Chen et al., 2015). Chen et al. (2013) also used this theory, combined with the compliance theory, in their research on enforcement and employees' intentions to comply with security policies (Chen et al., 2015). The deterrence theory, which is said to have originated with Hobbes, Beccaria (1748–1832), and Bentham (1738–1794), presupposes that an individual considers the pros and cons when determining whether to perpetrate a violation (Al-Mukahal & Alshare, 2014; Siponen & Vance, 2010). According to Al-Mukahal and Alshare (2014), this theory assumes that people are only fundamentally rational in their actions and choice transgressions when there is profit. Therefore, humans are less likely to commit infractions when the perceived certainty, severity, and expeditiousness of sanctions are greater (Al-Mukahal & Alshare, 2014). These researchers went on to further state that sanctions could be formal or informal. Formal sanctions, which are the backbone of the theory, are strict punishments enforced for specific infractions; whereas, informal sanctions use social ramification to quail undesired behavior (Al-Mukahal & Alshare, 2014).

Therefore, control-based models typically use formal sanctions to mitigate noncompliance. These models use bureaucratic rules to compel employees to obey organization information security policy. This approach neglects the consideration of human behavior and culture in the development of policy. As a result, control-based compliance models utilize reward and punishment to influence employees' behavior. This philosophical belief is supported by studies which show that forceful policies make potential offenders understand the negative

consequences of their behavior (Chang & Wang, 2011). Consequently, scholars supporting control-based compliance believe that strong policy will influence malicious users into curtailing their negative behaviors. The policies promote fear of punishment as a deterrent (Lowry et al., 2014). Individual scholars seem to agree that penalties have a significant effect on users' security behaviors (Safa et al., 2015). Another approach is to use rewards to influence positive behavior. However, empirical findings pertaining to the influence of reward and punishment on compliance are inconclusive (Chen et al., 2013).

According to Yoon and Kim (2013), enforcement policies based on reward and punishment did not have a significant effect (or even an adverse effect) on employees' compliance with information security policy. In fact, convenience, habit, organizational culture, and social influence seemed to have a greater impact on employee compliance. Further, findings show that employees' intention to comply was significantly influenced by normative beliefs, self-efficacy, and attitude (Yoon & Kim, 2013). Information security is often not part of the end user's assignment or performance evaluation (Guo et al., 2011). Additionally, information security policy can often be inconvenient or in conflict with employees' performance goals (Guo et al., 2011; Parsons et al., 2013; Vince et al., 2012). As a result, employees often violate policy with performance goals in mind.

Furthermore, research findings suggest that employees use neutralization techniques to justify noncompliance (Chen et al., 2013; Willison & Warkentin, 2013). Neutralization is a technique used by employees to justify a policy violation. The neutralization theory was first introduced in an effort to explain how adolescents justify participation in criminal activities (Li & Cheng, 2013). Researchers argue that employees' neutralization techniques have more influence on policy compliance than sanctions (Barlow, Warkentin, Ormond, & Dennis, 2013; Li

& Cheng, 2013; Siponen & Vance, 2010). Additionally, scholars seem to be more attracted to neutralization techniques as a more superior explanation for employees' noncompliance (Barlow et al., 2013; Li & Cheng, 2013; Siponen & Vance, 2010).

Most studies about information security utilize the first five techniques of neutralization, as proposed by Sykes and Matza's (1957) seminal work (Li & Cheng, 2013; Siponen & Vance, 2010). The five techniques most commonly utilized are denial of responsibility, denial of injury, denial of victim, condemnation of condemners, and appeal to higher loyalties. Denial of responsibility refers to an employee denying any responsibility for committing a deviant action (Li & Cheng, 2013; Siponen & Vance, 2010). Denial of injury entails an employee justifying an action by its minimal damage to an organization and its employees (Li & Cheng, 2013; Siponen & Vance, 2010). Denial of victim is used when the perpetrator's actions affect a victim that is not physically visible or is unknown (Li & Cheng, 2013; Siponen & Vance, 2010). Condemnation of condemners refers to the employee neutralizing the action by blaming the victim of the action. Finally, appeal to higher loyalties is employed when employees believe that they are in a predicament that must be solved at the expense of violating policy.

In addition to Sykes and Matza's five neutralization techniques, Minor (1981) added the technique defense of necessity (Siponen & Vance, 2010). This technique is used when employees justify an action by convincing themselves that it was necessary. However, researchers have endorsed awareness and education as countermeasures for neutralization (Al-Mukahal & Alshare, 2014). Al-Mukahal and Alshare also asserted that a clear policy scope would invalidate the effects of neutralization. Another factor that influences employee behavior is habit. Vince et al. (2012) noted that habit plays a substantial role in employees' compliance with information security policy. Habit can assist in determining how an employee views the

severity of a threat. Additionally, researchers should pay particular attention to the influence of trust over employees' behavior. Al-Mukahal and Alshare (2014) defined trust as the level of faith that employees have in each other which allows them to share sensitive information. These researchers suggested that trust can often promote risky behavior. Employees may share passwords to sensitive data or engage in gossip that leads to divulging confidential information.

Similarly, organizational culture and social influence can guide employees' behaviors (Alhogail & Mirza, 2014; Harnesk & Lindström, 2011; Hu et al., 2012; Ifinedo, 2014; Siponen et al., 2012; Willison & Warkentin, 2013). These factors employ peer pressure to change behavior. Researchers seem to agree that these factors have a stronger influence on employee compliance than reward and punishment. Nevertheless, supporters of control-based compliance models emphasize the use of reward and punishment in conjunction with each other (Chen et al., 2013). The combination counteracts the negative consequences of using them individually.

Value-based Compliance

Researchers admitted that, as information security systems become more secure, users are finding ways to bypass the security to ease usability (Dhillon, Oliveira, Susarapu, & Caldeira, 2016). These authors noted that users value usability over security, which results in security being compromised. Additionally, these authors implied that users are more disposed to integrated solutions that advocate both usability and security. According to Flores, Antonsen, and Ekstedt (2014), the holistic approach to information security takes human components, such as values, norms, beliefs, and behavioral patterns, into consideration. Therefore, it is in the best interest of security to consider users' values and beliefs. Value-based compliance models consider the inclusion of employees' values and beliefs in the development of information

security policies (Hedström et al., 2011). These models encourage security managers to focus more on the needs of employees.

In other words, information security managers can develop policy that would assist employees in accomplishing their goals while promoting positive behavior towards security (Guo et al., 2011). Organizations must develop policies that employees can accept as a function of their job and not an annoyance. Unfortunately, there is minimum research on value-based compliance, as it relates to information security. However, value-based compliance has been studied in other areas to address noncompliance. The seminal work of Hedström et al. (2011) was the first study to propose a solution to noncompliance in information security. The researchers drew their support from two theories: Argyris and Schön's (1996) theory of organizational learning and Weber's (1978) social action theory. Argyris and Schön's theory of organizational learning handles security concerns through a double-loop concept, which allows managers to address concerns immediately and make changes to the underlying philosophy (Kerman, et al., 2012; Kim et al., 2013; Mohanty & Kar, 2012). The double-loop approach encourages the study of employees' behavior and applies that knowledge to guide the development of security policy. Additionally, it should reduce the gap between theory and practice. Similarly, Weber's social action theory (SAT) concentrates on employee behavior. Hedström et al. (2011) and others that support value-based compliance contend that, if organizations do not consider human behavior when developing security policies, there will continue to be a gap between theory and practice.

Program Maintenance

Regardless of the enforcement method, a maintenance program is required for an effective security program. Security risk areas and work environments are constantly changing,

which can render policies and awareness programs obsolete (Allam et al., 2014; Pathari & Sonar, 2012). Tsohou, Karyda, Kokolakis, and Kiountouzis (2015) argued that changes in awareness are associated with modifications on the organizational, technological, and individual levels. According to these authors, the organizational level includes changes to information security strategies, power relations, and distribution of responsibilities. They explained the technological level as changes in existing infrastructure and implementation of tools to support awareness behaviors. Further, Tsohou et al. (2015) defined the individual level as consisting of employee attitude, work habits, and consciousness of their role in security. Random changes in these levels may occur, affecting the effectiveness of an awareness program.

Therefore, it is significant that information security managers implement a maintenance program to review and measure the effectiveness of their security programs. The objective of an information security maintenance program is to ensure that information security policies and programs still meet the security needs of the organization (Knapp & Ferrante, 2012). The maintenance program should analyze policy violations to determine the root cause of infractions. Identifying the fundamental cause of violations will allow measures to be implemented that discourage employees' noncompliance (Guo et al., 2011). These measures can be in the form of improved policies, enforcement sanctions, and awareness and education programs.

Additionally, an effective program should offer continuous education and training for employees (Bower, 2011). Notwithstanding, research indicates that awareness of risk does not guarantee compliance and only provides temporary relief from risk (Allam et al., 2014). However, for the maintenance program to be temporally effective, awareness training and education must be continuous. To ensure compliance training and education is productive, two concerns must be addressed, including (1) a comprehensive training program and (2) methods of

measuring how well the lessons were assimilated (Bower, 2011). In other words, the training program should be a component of the overall security plan.

Moreover, the training program should include quizzes and tests as a way of measuring its effectiveness. However, measuring awareness and the information security program's overall effectiveness requires measuring long-term changes in employees' attitudes and behaviors (Tsohou et al., 2012). Equally important, performing a cost-benefit analysis is just as difficult due to the unclear return on investment (Tsohou et al., 2012). As a result, the short-term approach of determining information security program effectiveness is through employees self-reporting. However, the reliability of this self-reporting is questionable, as employees may provide responses that they presume are expected of them. Finally, the maintenance program should ensure that policies are continuously updated to address changes in organizational environment, information systems, and risks. These conditions are constantly changing due to internal and external circumstances.

Program Effectiveness

Information security program effectiveness is a circumstance of program denouement (Bower, 2011). It is a measure of performance that decides whether the program objective of protecting organizational information is being accomplished (Knapp & Ferrante, 2012). In other words, organizations should know if their information security program is averting information security violations. The literature seems to indicate that an effective information security program should incorporate effective information security policy, awareness, and maintenance programs. Technology such as strong encryption and robust firewalls are worthless without comprehensive policies to guide users on the proper use of those tools (Robertson, 2012). Thus,

organizations should use a combination of technical and non-technical approaches, such as policies, awareness, and training, to combat breaches.

The literature review seems to indicate that awareness is one of the most effective ways of mitigating information security violations. Similarly, awareness programs raise employees' knowledge and alertness of information security concerns. Furthermore, fear influences employees' security compliance intentions based on aspects such as anticipated threat severity (Tsohou et al., 2015). Therefore, ensuring that employees are aware of potential threats is significant in reducing violations. However, it is important to note that empirical support is insignificant to the relationship between employee intentions and actual behavior (Shropshire et al., 2015). In other words, due to awareness, employees' intentions may not necessarily translate to actual behavior. Nevertheless, researchers seem to imply that a comprehensive information security program encompasses information security policies, an awareness program, an enforcement program, and a maintenance program (Chen et al., 2015). The goal of an information security program is to reduce or mitigate security breaches.

Therefore, it is important that these organizations focus on strengthening the weakest link in their information security chain. In other words, organizations should revolutionize information security's weakest link to be its cardinal defense (Aydin & Chouseinoglou, 2013). Additionally, the future of organizations depends on the level of information and information technology (Jo, Kim, & Won, 2011). Therefore, it is important that an information security program protects both internal and external information and information systems. However, research on organizational breaches is infrequent in the academy (Khey & Sainato, 2013; Lee & Lee, 2012). Consequently, information security violations continue to be a serious challenge for

organizations (Singh et al., 2013). This challenge continues to cost organizations millions, if not billions, of dollars annually.

Theoretical Framework

The ideology of the theory of organizational learning will be used in this study. According to Wang and Huang (2013), the concept of organizational learning was first expressed by March and Simons in 1958. These researchers pointed out that organizational learning saw rapid growth during the 1990s due to increase in technology and corporate competition. However, Argyris and Schön (1996) developed the first model for organizational learning (Hedström et al., 2011; Knapp and Ferrante, 2012). Organizational learning is a term used by most scholars to describe heterogeneous general organizational experiences. Therefore, the term has several conflicting definitions.

For instance, Argyris and Schön (1996) defined it as a process where employees identify and solve errors through change in their organizational doctrine (Popescu, Bunea & Radu, 2014). Lyles (1985) defined organizational learning as the process of reconstructing actions, with the support of new knowledge that allows a comprehensive understanding of the organization (Popescu et al., 2014). Alternatively, Wang and Huang (2013) defined organizational learning as a convoluted construct with numerous definitions that incorporates extensive concepts to explain the phenomenon. Moreover, Muehlfeld, Sahib, and Witteloostuijn (2012) defined organizational learning as experienced-based learning that advances performance through its effects, knowledge development, and transfer by causing changes in the organization's core philosophy. As a result, researchers have advanced the theory in three principal directions (Muehlfeld et al., 2012). First, scholars have concentrated on the aspect of experience features rather than the quantity of amassed experience (Muehlfeld et al., 2012). Second, they have analyzed possibilities that

control the way experience affects learning (Muehlfeld et al., 2012). Third, researchers have moved past a conventional assessment of learning based on financial performance (Muehlfeld et al., 2012).

However, Argyris and Schön's (1996) organizational learning model is used in this study. This theory was used in Hedström et al. (2011) to develop their value-based model for information security policy compliance. In addition, the theory of organizational learning was also used in Knapp and Ferrante's (2012) study on information security effectiveness in organizations. Argyris and Schön's (1996) theory of organizational learning addresses security concerns through a double-loop concept, which involves changing the action theories and challenging the core system ideologies (Popescu et al., 2014).

In contrast, single-loop learning involves changing the learning action theories without calling the underlying assumptions into question (Popescu et al., 2014). In other words, small changes are made to specific rules based on past failures (Baskerville, Spagnoletti, & Kim, 2014). Single-loop learning focuses on the specific actions of employees instead of the managing theory of the action. This approach often has a quick fix for procedures but fails to address the governing principles. On the other hand, double-loop learning allows managers to address security concerns immediately and make changes to the underlying philosophy (Kerman, Freundlich, Lee, & Brenner, 2012; Kim et al., 2013; Mohanty & Kar, 2012). Double-loop learning presumes that organizations should analyze the primary concepts and alter those principles to resolve the problem (Baskerville et al., 2014). The double-loop approach encourages the study of employees' behavior and applies that knowledge to guide the development of security policy. This theory implies that security policies are only observed through employee action and allows managers to address the immediate problem and make

changes to the underlying ideology (Kerman, et al., 2012; Kim et al., 2013; Mohanty & Kar, 2012). In contrast, single-loop learning concentrates on revising inaccuracies in policies (Kerman et al., 2012; Kim et al., 2013; Mohanty & Kar, 2012). The theory of organizational learning promotes change in the organization by employing an exploitation of previous certainties and an exploration of new possibilities (Iarossi, Miller, O'Connor, & Keil, 2013). As applied to this study, this theory indicates that the independent variables policy awareness, policy enforcement, and policy maintenance should have a positive influence on the dependent variable information security program effectiveness. A positive influence is predicted because, by implementing the theory of organizational learning, organizations are continuously learning and amending their fundamental philosophy.

Contributions to the Field

The results of this study will add to the body of knowledge on information security. Furthermore, the findings should contribute to the understanding of the relationship between information security policy awareness, enforcement, maintenance and information security program effectiveness. This added information will provide scholars and practitioners with a profound understanding of the effects that information security policy awareness, enforcement, and maintenance have on information security program effectiveness. This study is especially relevant in the mitigation of employee noncompliance to information security policy because data gathered is from employees' perspectives. Therefore, it addresses the relationships of IVs and DV from their point of view. As employees are the weakest link of security programs, this study may provide information that can enhance information security program effectiveness (Knapp & Ferrante, 2012). As a result, policy writers may gain the knowledge necessary to transform users from information security's weakest link to its greatest strength. Equally

important, these improved policies should enhance the reduction of information security breaches.

Summary

Information technology serves as the backbone of modern organizations (Mbowe et al., 2014), allowing them to make accurate and timely decisions. However, due to the increased amount of information security breaches encountered by organizations in recent years, a closer review of the effectiveness of information security programs is needed. Information security's fundamental objective is to protect information in terms of confidentiality, integrity, and availability (Mukundan & Sai, 2014). A comprehensive information security program should address both technical and non-technical peculiarities (Ifinedo, 2012). Technical characteristics include anti-virus software, spyware, firewalls, and similar security software and hardware devices. Likewise, information security programs should also address non-technical aspects, such as human behavior and values.

Therefore, an effective information security program should incorporate information security policy, information security employee awareness, policy enforcement, and program maintenance. Information security policy is considered the foundation for an optimum information security program (Singh et al., 2013). Information security policies provide guidelines and best practices to users. Additionally, policy dictates employee behavior expected by the organization. Likewise, information security awareness programs educate employees on information security policies and threats (Wolf et al., 2011). Hopefully, awareness of these policies and threats influences employee behavior, thereby causing policy conformity.

Similarly, enforcement programs provide the necessary procedures required to enforce information security policy. These enforcement policies include the actual punishment and

escalation methods vital for the imposed policy. Enforcement may be categorized into two areas of interest, including control-based compliance and value-based compliance (Ifinedo, 2014). Control-based compliance uses reward and punishment to enforce policy. In addition, control-based compliance does not consider user values. Some scholars insist that the control-based approach fails to address the human conditions of information security.

Therefore, these scholars argue that control-based compliance may not be the best enforcement method (Yoon & Kim, 2013). In contrast, value-based compliance takes employee values into consideration (Hedström et al., 2011). Value-based is the most current approach and uses organizational learning as its theoretical framework. Value-based compliance depends on individual learning to influence the organization's core philosophy and, in return, organizational learning to influence employees. Maintenance programs are required to ensure policy, awareness, and enforcement, and information security programs are modernized to meet the organization's security needs. Finally, an effective information security program should address information security's weakest link. An effective information security program should transform users into assets.

CHAPTER 3. METHODOLOGY

The purpose of this quantitative survey study, with a correlational research design, is to determine the relationship of an organization's information security policy awareness, enforcement, and maintenance to its effectiveness. Researchers seem to suggest that there is a relationship between information security policy awareness, enforcement, and maintenance and the effectiveness of an organization's information security program (Ifinedo, 2014; Paulsen & Coulson, 2011). Hence, the research question and hypotheses are restated as follows:

ResQ: Are information security policy awareness, enforcement, and maintenance significant predictors of information security program effectiveness?

H_0: Information security policy awareness, enforcement, and maintenance are not statistically significant predictors of information security program effectiveness.

H_A: Information security policy awareness, enforcement, and maintenance are statistically significant predictors of information security program effectiveness.

Research Design

This study uses a correlational survey research design. The purpose of a correlational research design is to determine the extent to which two or more variables are statistically related or used in prediction. However, correlational design does not imply causation (Creswell, 2014). The design is nonexperimental since no variables are manipulated. Likewise, multivariate correlation is used to identify relationships between multiple independent variables and a single dependent variable (Lomax & Li, 2013). George Udny Yule first introduced multivariate correlation in 1897 (Lomax & Li, 2013). Conversely, one disadvantage of multivariate correlation research is that it does not indicate causal inference (Connelly, 2012; Ingham-Broomfield, 2014; Lomax & Li, 2012; Patten, 2014; Swanson & Holton, 2005). The approach

was used in this study to investigate the relationships between information security policy awareness, enforcement, and maintenance and information security program effectiveness. To achieve this purpose, the research was guided by the question: what is the relationship between information security policy awareness, enforcement, and maintenance and information security program effectiveness?

Methodological Approach

The study was investigated using a non-experimental approach. Quantitative studies can be accomplished using three primary approaches, including experimental, quasi-experimental, and non-experimental (Delost & Nadder, 2014; Sánchez-Algarra & Anguera, 2012). The best approach depends on the level of control and manipulation the researcher wants to exert on the study variables (Sánchez-Algarra & Anguera, 2012). In other words, a non-experimental approach is used with research that does not include an intervention or the manipulation of variables (Delost & Nadder, 2014; Sánchez-Algarra & Anguera, 2012; Spector & Meier, 2014).

This approach has been used in similar studies by Knapp and Ferrante (2012) and Siponen, Mahmood, and Pahnila (2014). Knapp and Ferrante investigated the relationship between information security awareness, enforcement, maintenance, and program effectiveness using a population of certified information security managers. Moreover, Siponen et al. (2014) researched the relationship between employees' self-efficacy, response efficacy, and compliance to information security policy. Therefore, the approach is appropriate in addressing the research questions presented in this study.

Methodological Model

This study used multiple linear regression to determine which independent variables are significant predictors of the dependent variable. Multiple regression can establish that the three

independent variables explain a proportion of the variance in the dependent variable at a significant level (through a significance test of R^2), as well as the relative predictive importance of the dependent variables (by comparing beta β weights) (Field, 2013). The model for a multiple linear regression with n observations is given by the equation $y=b_0 + b_1x_1 + b_2x_2 + b_nx_n + \varepsilon_i$, where y is the dependent variable, b_0 is the constant (intercept), b_1, b_2, and b_n are the unstandardized regression coefficients of each independent variable included in the regression model, and ε_i is the random error term usually described as residual.

Research Design Rationale

This study investigates three fundamental elements of security policy management and their relationship to the comprehensive security effectiveness of organizations. Security policies are often recommended as an organizational measure to combat internal security threats resulting from end user misconduct (Guo et al., 2011). However, employees must be aware of the policy for it to have any effect on their behavior (Rashid et al., 2013). In addition, awareness of policy without enforcement reduces policy effectiveness. Therefore, policy awareness and enforcement seem to be associated. Furthermore, security risk areas and environments are in a state of constant transformation. As a result, these constant changes can reduce policy effectiveness or make policy obsolete (Allam et al., 2014). Therefore, policy maintenance is necessary for maintaining effective policy. Accordingly, it would be difficult to isolate the relationship between one of these variables and information security program effectiveness. Therefore, a multivariate correlation allowed the investigation to look at all three variables and their relationships to the dependent variable.

Sample

Population selection is an essential part of the research design and was used as a guide for the researcher (Marshall & Rossman, 2011). The target population for this study is full-time employees of medium to large organizations that use a computer for their daily work activities. The population size was based on the United States Department of Labor Bureau of Labor Statistics. According to the Bureau, in May 2014, the estimated population for computer and mathematics occupations was 3,834,180.

Sample Frame

The sample frame was prequalified respondents from SurveyMonkey's online database. This database consists of approximately three million volunteers recruited from the United States population. SurveyMonkey conducts regular benchmarking surveys to ensure their volunteers are representative of the United States population. The sample was randomly selected individuals from SurveyMonkey's online database that met the criteria for this study. The volunteers were computer users from medium to large organizations with established information security programs within the United States. A precondition for participants is that more than 50% of their daily tasks are completed on a company computer. Additionally, participants must be between the ages of 18 and 75.

Sampling Procedures

Participants for the study were solicited through SurveyMonkey Audience, an online professional panel of volunteers (Lowry et al., 2014). The participants were required to answer a series of questions to ensure that they qualify based on the sample criteria. Utilizing SurveyMonkey ensured that all participants remain anonymous and confidential (Lowry et al., 2014). Additionally, all participants were required to acknowledge having read and understood

the study's informed consent. Participants for the study were randomly selected using the sample frame provided through SurveyMonkey's professional panel of volunteers (Creswell, 2014).

SurveyMonkey allows researchers to select their audience in a simple four step process. After completing the design (the online survey), the researcher selects "buy responses." Next, the researcher enters the number of responses needed. The researcher then selects the criteria for the volunteers. Once that is complete, SurveyMonkey distributes the survey to the target sample. In addition, SurveyMonkey regularly benchmarks surveys to ensure that volunteers are representative of the population. Moreover, SurveyMonkey provides volunteers with rewards for participating.

Sample Size

The GPower model 3.0.10 was used to determine the sample size for this study. This approach required a confidence interval, a confidence level for margin of error, and an estimated percentage of given response (Creswell, 2014). The population size was based on the United States Department of Labor Bureau of Labor Statistics. According to the Bureau, in May 2014, the estimated population for computer and mathematics occupations was 3,834,180. Similar research by Knapp and Ferrante (2012) used a sample size of 9,600 Certified Information System Security Professionals (CISSPs). Employing the GPower Model to determine the sample size, the F-test Multiple Regression: Omnibus model was used. The inputs for the model include an effect size $f^2 = 0.15$, $\alpha=0.05$, $\beta=0.95$, noncentrality parameter $\lambda=17.85$, and critical $F=2.684$, with a required sample size of 119.

Sample Rationale

The research question for this study addresses a multivariate problem that intends to identify the relationships between three independent variables and information security program

effectiveness. Previous research on the problem was achieved using certified information system security professionals (CISSPs) (Knapp & Ferrante, 2012). However, researchers have indicated that common employees in organizations are the weakest link in an organization's security program (Cavallari, 2011; Chen et al., 2013; D'Arcy & Devaraj, 2012; Guo et al., 2011; Harnesk & Lindström, 2011; Hu et al., 2011; Ifinedo, 2012; Lowry et al., Posey, 2014; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Vance et al., 2014). Therefore, to determine the effectiveness of an information security program, the study approaches the problem from the perspective of general employees. Additionally, random sampling is used to ensure that all members of the population have an equal opportunity to be represented (Vogt, 2007). Moreover, SurveyMonkey is utilized to gain access to the target population and sample. SurveyMonkey allows a task that is ostensibly impossible to be achieved at haste through technology.

Units of Analysis and Constructs

The units of analysis for this study are individual employees. The study collected data from employees on the effectiveness of the organization's information security program. Information was also gathered from these employees on the organization's information security policy awareness program. Further, data was collected from the employees on the organization's information security policy enforcement program. Finally, data was gathered from employees on the organization's information security policy maintenance program. Hence, this study consists of four constructs in the form of information security policy awareness, enforcement, and maintenance and information security program effectiveness. Information security policy awareness is the perceived knowledge of information security policy and threats (Knapp & Ferrante, 2012). Awareness of policy is believed to affect employees' enthusiasm to comply with policy (Cheng et al., 2013). Additionally, awareness is considered critical in the development of

security policy conformity (Harnesk & Lindström, 2011). Two closely related constructs are information security policy enforcement and information security policy maintenance (Knapp & Ferrante, 2012). Information security policy enforcement is used as a deterrent measure to enforce users' compliance with policy (Guo et al., 2011). Research has shown that even though employees are aware of policy, they do not necessarily comply (Guo et al., 2011). Accordingly, policy enforcement measures are implemented to encourage user accountability (Vance et al., 2013). Deterrence theory, the theory of planned behavior, and protection motivation theory have been applied to the research in an attempt to understand enforcement measures on employees' noncompliance (Guo et al., 2011; Ifinedo, 2012). The third construct is information security policy maintenance. The purpose of this construct is to make sure that policies are still accomplishing their intent (Knapp & Ferrante, 2012). Maintenance ensures that policies and their enforcement procedures are current. Finally, information security program effectiveness is a measure of performance that determines whether the program is achieving its objective of protecting the organization's information (Knapp & Ferrante, 2012).

Instrumentation/Measures

The measure used in this study is a 5-point Likert scale survey instrument developed by Knapp, Marshall, Rainer, and Ford (2005). The researchers originally used this instrument in their study "Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness." It was utilized again in Knapp and Ferrante's (2012) study "Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations." In the second study, the researchers completed a factor loading matrix using principal components factoring with varimax rotation (Knapp & Ferrante, 2012). The results indicated that each article loaded on its theoretical construct more than any other,

supporting convergent and discriminant validity. The instrument addresses four constructs, including information security program effectiveness, policy awareness, policy enforcement, and policy maintenance. Previously, the instrument was used to collect data from a population of CISSPs (Knapp & Ferrante, 2012). However, in this study, the instrument was used to collect similar data from a population of general computer users. Furthermore, because the instrument has not been previously used on this population and does not have any published psychometric information, a field test was conducted.

This test was conducted on the instrument for this study, which is required because the instrument is being used on the study population for the first time (Creswell, 2014). A panel of five (5) experts evaluated the overall procedure of data collection, preparation, and use. Two of the five panelists were concerned that participants may have difficulty with the definitions of some of the variables because these volunteers are not security experts. Additionally, one panelist felt that participants might not be able to answer two questions in the instrument because they were not security experts. Likewise, two panelists identified two items in the instrument that they felt could be considered redundant. However, all panelists agreed that the data collection process was nonintrusive. Furthermore, two panelists questioned the use of ordinal data for regression analysis. Nevertheless, they agreed it could be and has been done.

Data Collection

The survey was administered through SurveyMonkey's online web portal using the SurveyMonkey Audience. SurveyMonkey contacted volunteers and provided them with a link to the survey. Prior to participating in the survey, volunteers had to demonstrate that they met the research population criteria by answering a few questions. Next, all volunteers that fulfill the criteria were required to read and acknowledge that they understood the information consent

form (Flicker, Haans, & Skinner, 2004). Once volunteers acknowledged consent, they were then exposed to the survey. The survey was divided into six segments, including direction and definitions, demographics, information security program effectiveness, policy awareness, policy enforcement, policy maintenance, and conclusion (Creswell, 2014). The direction and definitions section explained the basic structure of the survey, the method used to answer questions, the definitions of any technical phrases, and the reminder that participants could stop at any time. The conclusion thanked participants and provided the researcher's contact information. At the completion of the survey, all that was required of participants to submit the survey was to click on the "submit" button. This approach allows participants to engage in the survey at their convenience and choice of location. However, participants were required to have access to a device that can connect to the Internet.

Data Analysis

This study used multiple linear regression to determine which independent variables are significant predictors of the dependent variable. Multiple regression can establish that the three independent variables explain a proportion of the variance in the dependent variable at a significant level (through a significance test of R^2), as well as the relative predictive importance of the dependent variables (by comparing beta β weights) (Field, 2013). Using multiple regression, the researcher can test theories about which set of variables is influencing the dependent variable. ANOVA and multiple regression seek to account for the variance in the score that is observed. Multiple regression shares all the assumptions of correlation, including linearity of relationships, the same level of relationship throughout the range of the independent variable ("homoscedasticity"), interval or near-interval data, absence of outliers, and data whose range is not truncated (Field, 2013). In addition, it is important that the model being tested is

correctly specified. The exclusion of important causal variables or the inclusion of extraneous variables can change the beta weights and, hence, the interpretation of the importance of the independent variables markedly.

The model for a multiple linear regression with n observations is given by the equation $y=b_0 + b_1x_1 + b_2x_2 + b_nx_n + \varepsilon_i$, where y is the dependent variable, b_0 is the constant (intercept), b_1, b_2, and b_n are the unstandardized regression coefficients of each independent variable included in the regression model, and ε_i is the random error term usually described as residual (Field, 2013). The random error is the difference between the observed and predicted values of the dependent variable (Field, 2013). The best-fitting line for the observed data is calculated by minimizing the sum of the squares of the vertical deviations from each data point to the regression line. If sig(F) < .05, then the regression model is considered significantly better than would be expected by chance, and we reject the null hypothesis of no linear relationship of y to the independents.

Using multiple regression, we can test theories (or models) about precisely which set of variables is influencing our dependent variable. What we are doing in both ANOVA and multiple regression is seeking to account for the variance in the score we observe (Field, 2013). Multiple regression shares all the assumptions of correlation: linearity of relationships, the same level of relationship throughout the range of the independent variable ("homoscedasticity"), interval or near-interval data, absence of outliers, and data whose range is not truncated. In addition, it is important that the model being tested is correctly specified. The exclusion of important causal variables or inclusion of extraneous variables can change the beta weights and, hence, the interpretation of the importance of the independent variables markedly (Garson, 2014; Williams, Garajales, & Kurkiewicz, 2013).

Regression coefficient b is the average amount the dependent increases when the independent increases one unit and other independents are held constant. To recapitulate, the b coefficient is the slope of the regression line: the larger the b, the steeper the slope, the more the dependent changes for each unit change in the independent. The b coefficient is the unstandardized simple regression coefficient for the case of one dependent. When there are two or more independents, the b coefficient is a partial regression coefficient, though it is common to simply call it a "regression coefficient." The beta value, which is a measure of how strongly each predictor variable influences the dependent variable, will become the path coefficient from the independent variables to the dependent variables. The beta is measured in units of standard deviation. For example, a beta value of 2.5 indicates that a change of one standard deviation in the predictor variable will result in a change of 2.5 standard deviations in the dependent variable. Thus, the higher the beta value, the greater the effect of the predictor independent variable on the dependent variable. The t-tests are used to assess the significance of individual b coefficients, specifically testing the null hypothesis that the regression coefficient is zero. Normally, variables not significant at the .05 level or better are dropped from the equation one at a time, starting with the most insignificant (Field, 2013; Garson, 2014).

R is a measure of the correlation between the observed and predicted values of the dependent variable. R squared (R^2) is the square of this measure of correlation and indicates the proportion of the variance in the dependent variable which is accounted for by the model. R^2 is called the coefficient of determination, and it represents the percentage of variance in the dependent variable that is explained by the independent variables. Additionally, it represents the proportionate reduction in the estimation error of the dependent variable when the independent variables are known (Garson, 2014; Myers, 2010).

Multicollinearity occurs when a high correlation is found between two or more predictor variables, and it causes problems when drawing statistical inferences concerning any contribution made by each predictor variable to the overall regression model (Field, 2013). Tolerance and variance inflation factor (VIF) values are used because they test for multivariate multicollinearity. They regress each independent variable on all the other independent variables in the equation simultaneously. When the tolerance value is less than 0.20, there is a problem with multicollinearity. When the value of tolerance is near 0, there is high multicollinearity of that variable, and the b and beta coefficients will be unstable. The more the multicollinearity, the lower the tolerance, the higher the standard error of the regression coefficients. The value VIF is the variance inflation factor, which is simply the reciprocal of tolerance. Therefore, when VIF is high, there is high multicollinearity and instability of the b and β coefficients. As a rule of thumb, VIF greater than 4.0 indicates multicollinearity (Garson, 2014).

Residuals are the difference between the observed values and those predicted by the regression equation. Thus, they represent error, as in most statistical procedures. Residual analysis is used for three primary purposes: (1) to spot heteroscedasticity (e.g., increasing error as the observed Y value increases), (2) to detect outliers (influential cases), and (3) to identify other patterns of error (e.g., error associated with certain ranges of X variables) (Argyrous, 2011). Frequency tables and descriptive statistics will be performed for each variable. Graphics will include histograms with normal curves, superimposed curves, boxplots, and scatterplots.

Researchers indicate that the best approach for handling missing data is research design. According to Vogt (2007), a survey must ensure that the questions are clearly written to mitigate participants skipping questions. Additionally, the author suggested another method of reducing the effects of missing data by using a large sample size. This research will be designed using

both suggestions. Moreover, the study will screen the data for outliers using boxplots (Vogt, 2007). The IBM SPSS® (Statistical Package for the Social Sciences) software will be used to provide all statistical analyses and tests.

Validity and Reliability

A panel of five (5) experts evaluated the items in the instrument for construct validity and intrusiveness. Similar guidelines to those used in Knapp and Ferrante's (2012) study were used to judge the instrument for intrusiveness. The instrument is considered acceptable if the individual items pass two conditions. First, items must be rated slightly intrusive (3) or not intrusive (4) by at least 3/5 of the expert panelists (Knapp & Ferrante, 2012). Second, items must receive a mean score of at least 2.75 from all panelists (Knapp & Ferrante, 2012).

Additionally, the mean of the overall items on the instrument must exceed 3.50. None of the items were found to be intrusive, with a minimum mean score of 3.80 for all individual items and an overall mean of 3.91. The readability scale used similar guidelines, whereby the instrument is considered acceptable if the individual items pass two conditions. First, items must be rated moderate (2) or easy (3) by at least 3/5 of the panelists. Second, items must receive a mean of at least 2.07 percent from all panelists. In addition, the mean of the overall items on the instrument must exceed 2.63. All items were found to be at the appropriate reading level for respondents, with an overall instrument mean of 3.0.

The constructed scale used the same guidelines as the readability, including that the item must be rated semi-appropriate (2) or appropriate (3) by at least 3/5 of the panelists. Next, the item must receive a mean of at least 2.07 percent from all panelists. All items received a mean of at least 2.40 or greater. Furthermore, the instrument received an overall mean of 2.87. Finally, the knowledge level scale used a similar guideline to judge knowledge level. Therefore,

knowledge level is acceptable if the individual items pass two conditions. First, items must be rated semi-appropriate (2) or appropriate (3) by at least 3/5 of the panelists. Second, items must receive a mean of at least 2.07 percent from all panelists. Two of the experts found items E1 and E2 in the instrument to be inappropriate to the knowledge level and sophistication of the respondents. Also, item E5 was found to be inappropriate to the knowledge level and sophistication of the respondents by one expert.

However, that same item was considered appropriate by the other four. Moreover, one of those experts felt that E5 was an excellent question. Two other items were found to be inappropriate to the knowledge level and sophistication of the respondents by only one expert. However, all items were considered acceptable by the guidelines, with the lowest mean of 2.2 for item E1 and an instrument overall mean of 2.79. Additionally, two experts found that items E1 and E2 were not significantly different. Moreover, one expert found that items PM1 and PM4 were not significantly different.

Ethical Considerations

A few basic ethical considerations must be addressed when working with human participants, including respect, beneficence, justice, and equity (Creswell, 2014; Patten, 2014; Salmons, 2010). Respect for a person includes ensuring that participants' privacy and confidentiality are not intruded (Creswell, 2014). Using SurveyMonkey allows participants to remain anonymous to the researcher. This method reduces the chance of violating participants' privacy rights and confidentiality. Additionally, there is nowhere on the survey that requires

participants to give their names or any other identifying characteristics. Furthermore, the researcher does not have access to volunteers' Internet protocol address.

Therefore, identifying individual participants will be onerous. Next, participants' risk is another ethical concern that the research needs to take into consideration (Creswell, 2014; Patten, 2014). There is always a certain amount of risk when dealing with human participants. However, the goal of an ethical researcher is to minimize that risk as much as possible. For this study, the researcher will look at the sensitivity of the items in the survey. This was focused on during the field test to ensure that no item is intrusive to participants. Additionally, the researcher has reviewed the instrument to verify that no jargon is used. However, if terminology is suspected as being technical or uncommon, then a definition will be given.

In addition, using SurveyMonkey to administer surveys and collect data reduces participants' exposure to physical harm and psychological anxiety. The survey will be distributed to all participants equally. Moreover, incentives will be handled by SurveyMonkey in the form of charitable donations and sweepstake entries for every survey completed. Participants will be rewarded with non-cash incentives to discourage participants from hurrying through the survey items.

CHAPTER 4. RESULTS

The purpose of this quantitative survey study, with a correlation research design, is to determine the relationship of an organization's information security policy awareness, enforcement, and maintenance programs to its information security program effectiveness. Researchers seem to imply that there is a relationship between information security policy awareness, enforcement, and maintenance and the effectiveness of an organization's information security program (Ifinedo, 2014; Paulsen & Coulson, 2011). The research question and hypotheses are restated as follows:

ResQ: Are information security policy awareness, enforcement, and maintenance significant predictors of information security program effectiveness?

H_0: Information security policy awareness, enforcement, and maintenance are not statistically significant predictors of information security program effectiveness.

H_a: Information security policy awareness, enforcement, and maintenance are statistically significant predictors of information security program effectiveness.

Multiple Regression Analysis

A multiple regression was performed to predict values of the dependent or criterion variable at the level of information security program effectiveness from a set of independent predictor variables for the levels of information security policy awareness, enforcement, and maintenance. Multiple regression is an evolution of simple regression (Field, 2013), the outcome of which is predicted by the linear combination of more than one predictor variable. There were 105 organizations responding to all the variables used for this multiple regression analysis. Table 1 illustrates the results of the descriptive statistics.

Table 1.
Descriptive Statistics

	Mean	Std. Deviation	N
Total Program Effectiveness	20.1238	3.81972	105
Total Policy Maintenance	15.7905	3.65244	105
Total Policy Enforcement	14.8667	3.82569	105
Total Policy Awareness	19.5619	4.48700	105

Descriptive statistics for the dependent criterion variable show that the average program effectiveness for these organizations was 20.12, with a standard deviation of 3.82. In addition, descriptive statistics for the independent variables exhibit that the average policy maintenance for these organizations was 15.79, with a standard deviation of 3.65. The descriptive statistics for the independent variables display that the average policy enforcement for these organizations was 14.86, with a standard deviation of 3.82. Moreover, the descriptive statistics for the independent variables illustrate that the average policy awareness for these organizations was 19.56, with a standard deviation of 4.48. Additionally, Figure 2 displays the histogram for the dependent variable. A histogram is used to show frequency distributions (Field, 2013). The distribution of data for the level of program effectiveness was not normal but skewed to the left. In other words, this histogram is positively skewed.

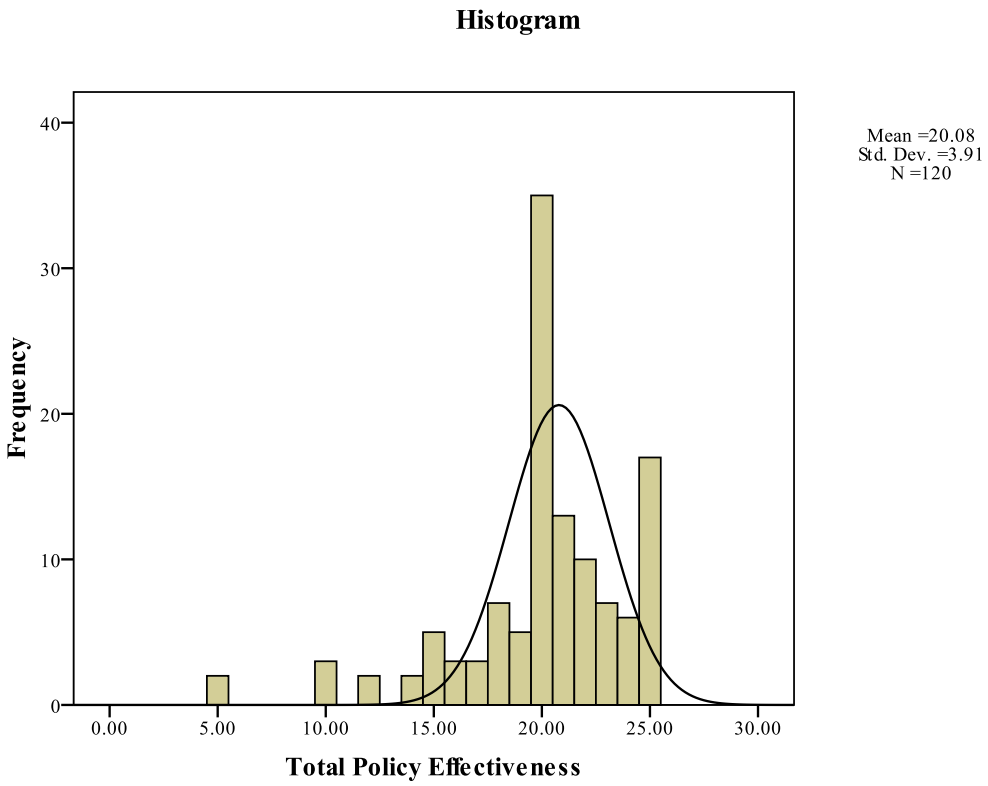

Figure 2. Histogram for Total Program Effectiveness

A correlation matrix is part of the multiple regression output so that the researcher can determine preliminary issues with multicollinearity between independent predictor variables. Pearson r Correlation is a standard measure that indicates the strength of the relationship between variables (Field, 2013). The results of this measurement can run from -1 to 0, suggesting that when one variable changes, the other variable changes in the opposite direction by the same amount. On the other hand, if the result is between +1 and 0, then when one variable changes, the other changes in the same direction by the same amount. Moreover, when the result is 0, when one variable changes, there is no change in the other variable. Table 2 exhibits the results of the Pearson r Correlation.

Table 2.

Pearson r Correlation

	Total Policy Maintenance	Total Policy Enforcement	Total Policy Awareness
Total Program Effectiveness Pearson Correlation	0.627	0.603	0.677
Sig. (1-tailed)	0.000	0.000	0.000
Total Policy Maintenance Pearson Correlation		0.577	0.747
Sig. (1-tailed)		0.000	0.000
Total Policy Enforcement Pearson Correlation			0.669
Sig. (1-tailed)			0.000

According to the results illustrated in Table 2, it does appear that there were significant correlations between the independent predictor variables. However, only the evaluation in tolerance values or variance inflation factor (VIF) values can determine the multicollinearity concerns in the final model. The multiple regression model was built using the *Enter* method for entering and removing variables from the equation. This method allows the researcher to enter all the independent variables into the equation simultaneously. This method is employed when the researcher is handling a small set of predictors and has not ascertained which independent variable will generate the best prediction equation. The results of this method are displayed in Table 3 (below).

Table 3.
Variables Entered/Removed[a] in the Multiple Regression Analysis

Model	Variables Entered	Variables Removed	Method
1	Total Policy Awareness	no	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).
2	Total Policy Enforcement	no	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).
3	Total Policy Maintenance	no	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).

a. Dependent Variable: Total Program Effectiveness

Next, a table of the multiple regression model summary is presented. Again, multiple regression is a distension of simple regression, whereby the result is predicted by a linear combination of two or more predictor variables (Field, 2013). The formula for such a model is expressed as $Y_i = (b_0 + b_1X_{1i} + b_2X_{2i} + \ldots + b_nX_{ni}) + \varepsilon_i$. This formula is explained, where Y is the outcome and X is each predictor. Additionally, each predictor has a regression coefficient b, which is associated with it. Moreover, b_0 represents the value of the result when all predictors equal zero (Fields, 2009). Table 4 illustrates the results of the multiple regression model summary for this study. Additionally, the ANOVA table can be found in Appendix B.

Table 4.

Multiple Regression Model Summary[d]

Model	*R*	*R* Square	Adjusted *R* Square	*Std.* Error of the Estimate	Change Statistics				
					R Square Change	*F* Change	*df*1	*df*2	*Sig. F* Change
1	0.677[a]	0.458	0.453	2.82493	0.458	87.143	1	103	0.000
2	0.706[b]	0.499	0.489	2.73027	0.041	8.266	1	102	0.005
3	0.723[c]	0.522	0.508	2.67902	0.023	4.940	1	101	0.028

a. Predictors: (Constant), Total Policy Awareness

b. Predictors: (Constant), Total Policy Awareness, Total Policy Enforcement

c. Predictors: (Constant), Total Policy Awareness, Total Policy Enforcement, Total Policy Maintenance

d. Dependent Variable: Total Program Effectiveness

The coefficient of determination R^2 demonstrated that 52.2% of the change in the variance of the level of total program effectiveness was explained by the levels of total policy awareness, total policy enforcement, and total policy maintenance. Table 4 indicates that the regression model is statistically significant. Thus, the null hypothesis was rejected, and the alternate hypothesis that the independent variables total policy awareness, total policy enforcement, and total policy maintenance were statistically significant predictors of the level of total program effectiveness [$F(3,101)=36.807$, $p<0.001$] was accepted.

Moreover, this multiple regression model included a table of regression coefficients, which indicate the strength of the relationship between the predictor and dependent variable (Field, 2013). In other words, it is the rate of change in the dependent variable based on a standard deviation of change in the predictor. The results of this table are displayed below in Table 5. Additionally, an explanation of the table follows. Further, the variables excluded at each

step of the multiple regression model development are illustrated in Appendix C. Furthermore, the multicollinearity evaluation of variables in multiple regression is shown in Appendix D.

Table 5.

Multiple Regression: Table of Regression Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	*t*	*Sig.*	Collinearity Statistics	
		B	*Std.* Error	Beta (β)			Tolerance	VIF
1	(Constant)	8.850	1.239		7.145	0.000		
	Total Policy Awareness	0.576	0.062	0.677	9.335	0.000	1.000	1.000
2	(Constant)	7.845	1.247		6.290	0.000		
	Total Policy Awareness	0.422	0.080	0.496	5.259	0.000	0.553	1.809
	Total Policy Enforcement	0.271	0.094	0.271	2.875	0.005	0.553	1.809
3	(Constant)	7.018	1.279		5.486	0.000		
	Total Policy Awareness	0.293	0.098	0.344	2.993	0.003	0.358	2.794
	Total Policy Enforcement	0.238	0.094	0.238	2.542	0.013	0.539	1.855
	Total Policy Maintenance	0.243	0.109	0.233	2.223	0.028	0.432	2.317

a. Dependent Variable: Total Program Effectiveness

The model coefficients and significance level for each of the independent variables are displayed in Table 5. Significant independent predictor variables ($p<0.05$) were total policy awareness [$t(104) = 2.993$, $p=0.003$], total policy enforcement [$t(104)= 2.542$, $p=0.013$], and total policy maintenance [$t(104)= 2.223$, $p=0.028$]. The model constant was also significant [$t(104) = 5.486$, $p <0.001$]. Additionally, the table showed that, from the tolerance values, there was no significant multicollinearity. Thus, the multiple regression model is:

Total Level of Program Effectiveness = 0.293 *Total Level of Policy Awareness* + 0.238 *Total Level of Policy Enforcement* + 0.243 *Total Level of Policy Maintenance* + 7.018

The standardized regression coefficients (β) are used to express the relationship between each significant predictor variable and the dependent variable. The β value for *total level of policy awareness* was 0.344, indicating that a one unit change in the level of policy awareness resulted in an increase in total program effectiveness by 0.344 units. Likewise, a β = 0.238 for the level of policy enforcement demonstrated that a one unit change in *total level of policy enforcement* resulted in an increase of 0.238 units in the level of total program effectiveness. The level of total program effectiveness increased by 0.233 units for every one unit increase in the *total level of policy maintenance*.

A residual statistic is the difference between the value that is predicted by the model and the observed value of the data. Residuals are used to verify if the theorized model is functional. In other words, if the residuals are consistently distant from the model prediction that might be an indication that the model's underlying theory is weak. A summary of the residuals that result from the predictor model is found in Table 6.

Table 6

Multiple Regression: Table of Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	*N*
Predicted Value	10.4064	23.9613	20.1238	2.76047	105
Residual	-16.07028	4.20983	0.00000	2.64010	105
Std. Predicted Value	-3.520	1.390	0.000	1.000	105
Std. Residual	-5.999	1.571	0.000	0.985	105

a. Dependent Variable: Total Program Effectiveness

The value for the residuals (*M*=20.12, *SD*=2.76) is related to the good R^2 value and good predictability of the level of total program effectiveness from the independent variable chosen. In fact, the range of values predicted by the model was fair (minimum predicted value=10.41, maximum=23.96). However, a simple way to use residuals to check the model is by plotting the residuals. The residual results are shown in the figures below. These include a plot of normality, a scatterplot of the predicted and standardized residuals, and a histogram of the standardized residuals. Figure 3 shows that the assumption of normality was met, as the points are close to the diagonal line. Each of the standardized residual plots show a random scatter of points with constant variability (see Figure 4).

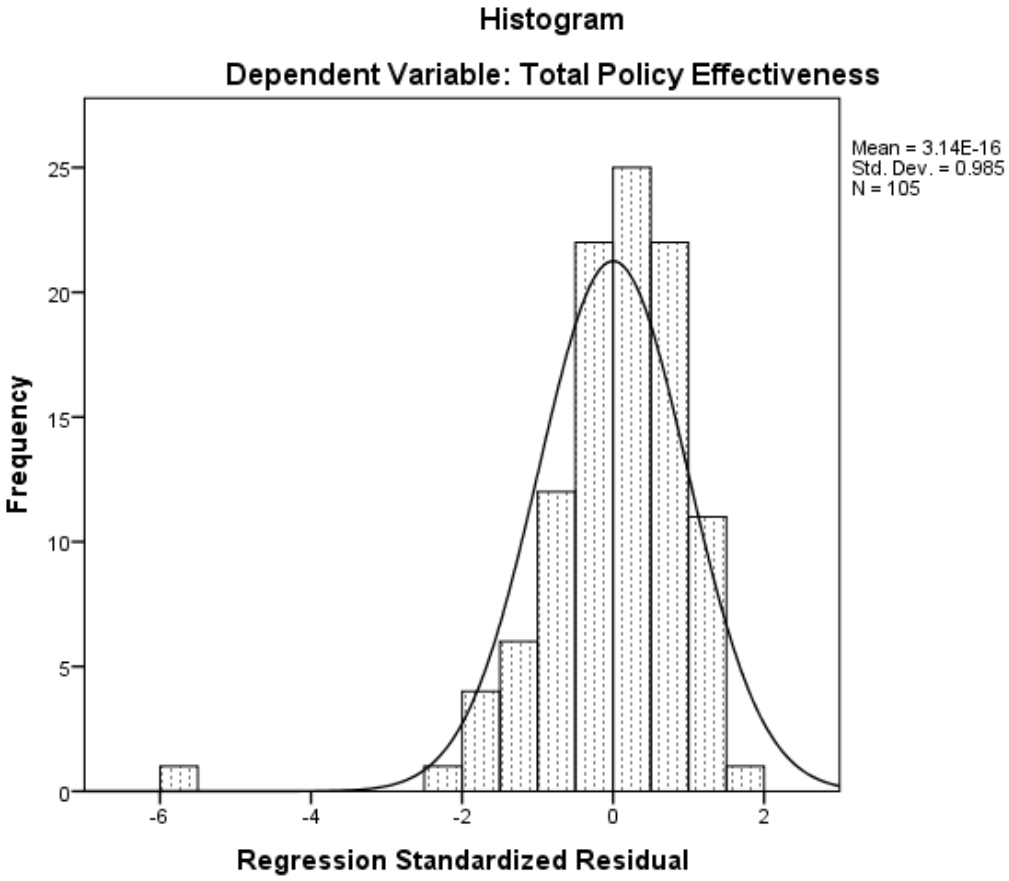

Figure 3. Histogram of Residuals for Total Program Effectiveness

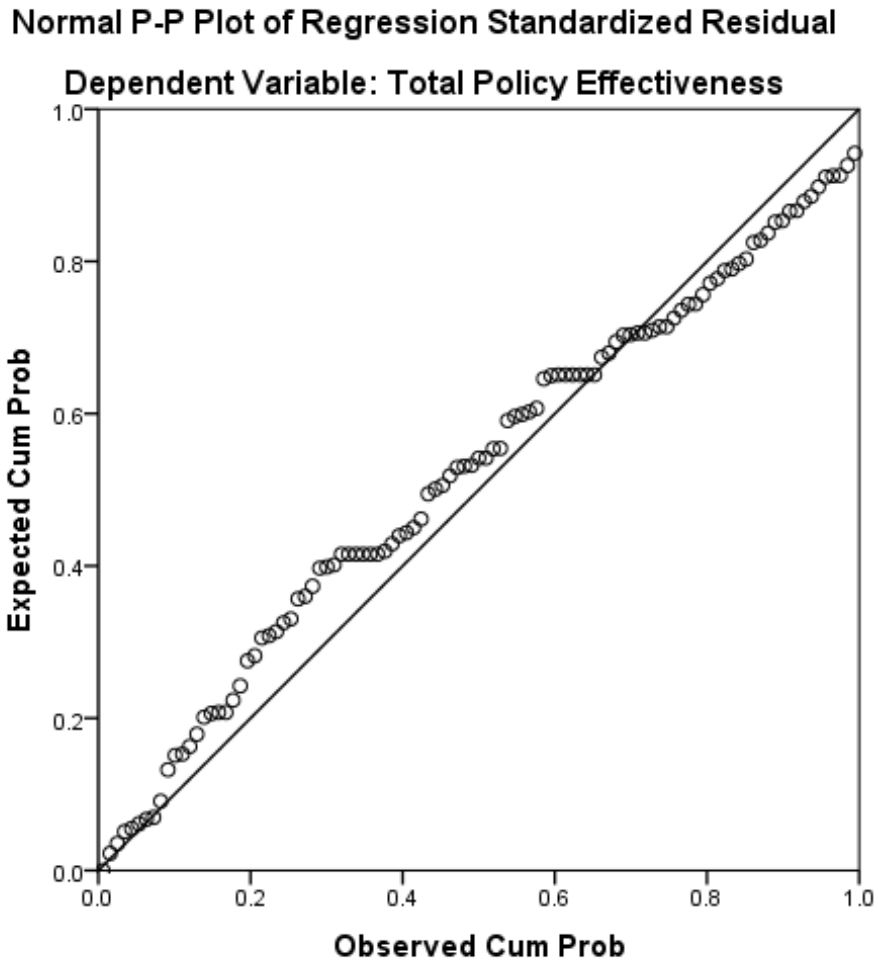

Figure 4. Normality Plot of Residuals for Total Program Effectiveness

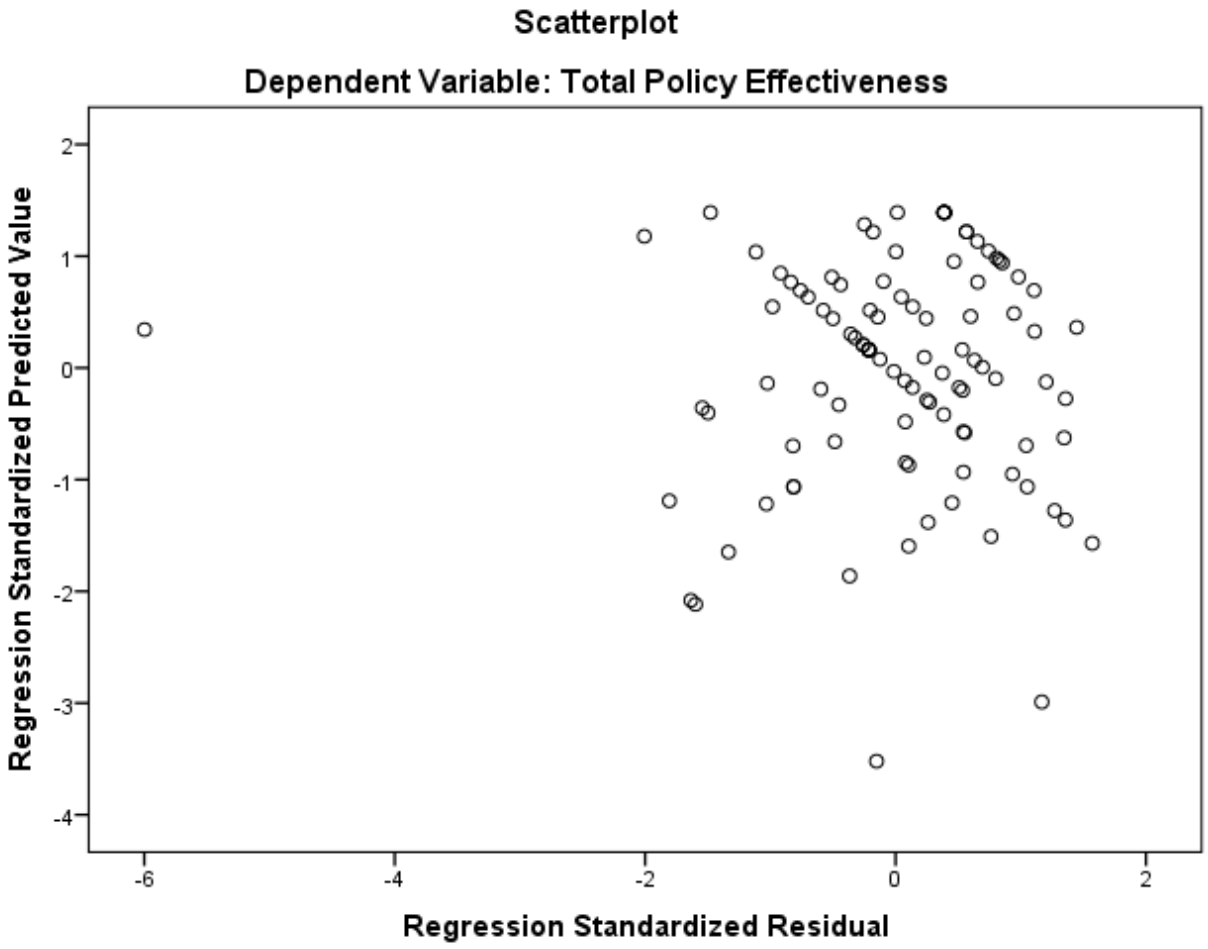

Figure 5. Scatterplot of Predicted Value for Total Program Effectiveness by Standardized Residuals

Tests of Mean Differences in Total Program Effectiveness Levels

Total Program Effectiveness by Gender

Further analyses were performed to determine whether there was a statistically significant difference in the total program effectiveness levels between male and female respondents based on the number of employees in the firm, whether the organization has a security office, and the level that approves the organization's security policy. Figure 6 displays an error bar plot of Total Program Effectiveness by Gender. An error bar plot is used prior to the independent t-test as a preliminary determination of whether there is no difference in the means and variances between the two groups. The x-axis represents the two groups from the independent variable (no/yes), and the y-axis represents the mean value of the dependent variable. In each error bar, the dot represents the mean of the group, which is read by placing a horizontal line to the left of the y-axis and reading the value for that group. The vertical distance between the two horizontal lines in each error bar is the variance. The closer in value the means are, the more likely the assumption of equal means will prove true when conducting the t-test. The more similar the vertical distance between the horizontal bars for each group, the more likely Levene's test of homogeneity of variance holds true. From the error bar plot, it appears the means were slightly different. It also appears that the variances in both the male and female groups were similar. Thus, we expect that the independent t-test will show no significant difference in means and variances.

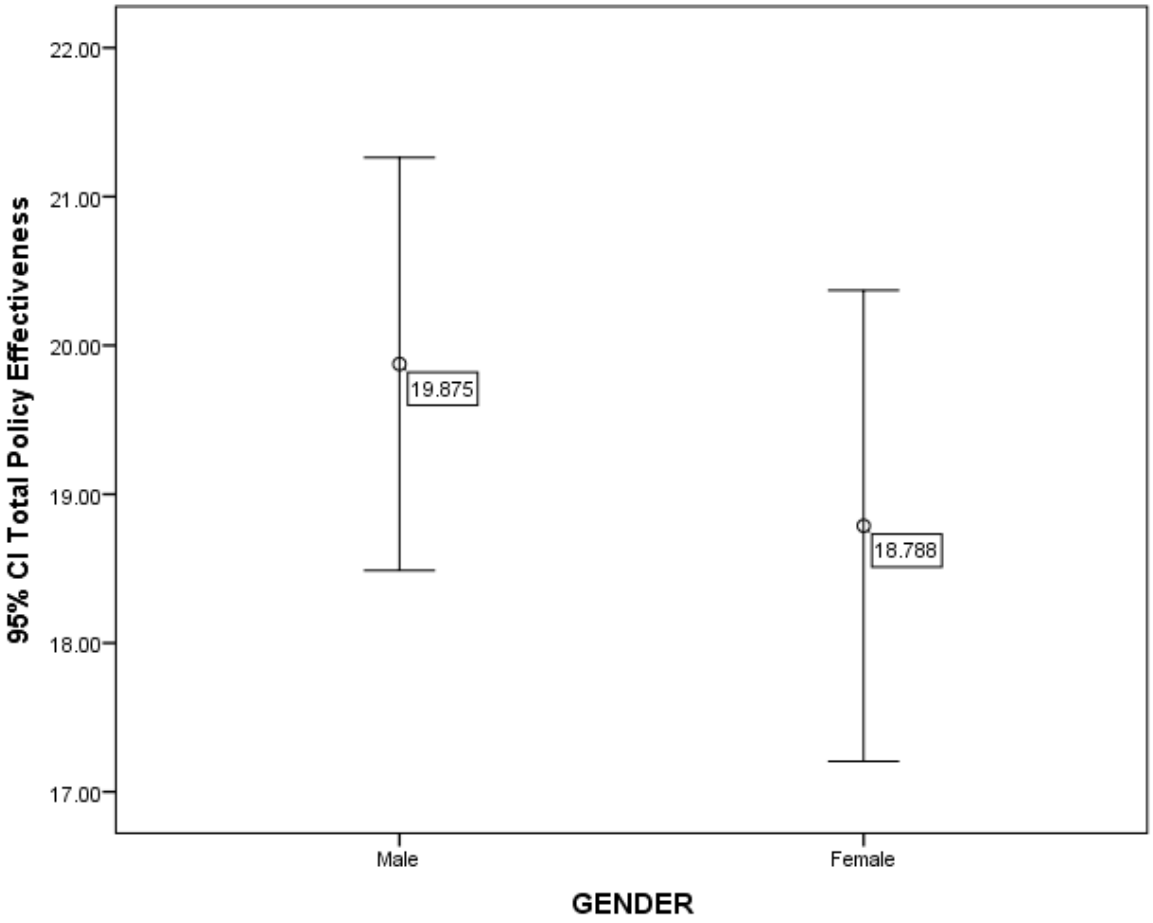

Figure 6. Error Bar for Total Program Effectiveness by Gender

The data was an analysis based on the perspective of gender. A t-test was performed on the independent samples to verify whether the means of the two groups were statistically different from each other. This evaluation is useful in comparing the means between the two groups. The t-test judges the difference between these means relative to the variability spread of the data (Field, 2013). Below, Table 7 shows the results of the t-test. Additionally, the group descriptive statistics for Total Program Effectiveness by Gender is illustrated in Appendix E.

Table 7.

Results of Independent Samples t-Test: Total Program Effectiveness by Gender

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Total Program Effectiveness	Equal variances assumed	3.600	0.064	0.900	47	0.373	1.0871	1.2082	-1.3434	3.5177
	Equal variances not assumed			1.072	45.186	0.289	1.0871	1.0137	-0.9544	3.1287

From Levene's homogeneity test of variances, there was no significant difference in the variances of total program effectiveness levels between males and females [$F(47)=3.600$, p=0.064]. In addition, the independent samples' t-test showed no significant difference in the mean levels of total program effectiveness between males and females [t (47) =0.900, p=0.373]. Overall, there was no significant difference between male and female users. The results eliminate the idea of differences based on gender.

Total Program Effectiveness by Number of Employees

From the error bar plot below, it appears that the mean levels of program effectiveness were different for some pairs of employee groups. It also appears that the variances for these group pairs were different. We might expect that the One-Way ANOVA and Levene's test will show significant differences in the means and variances of program effectiveness levels between some pairs of employee groups.

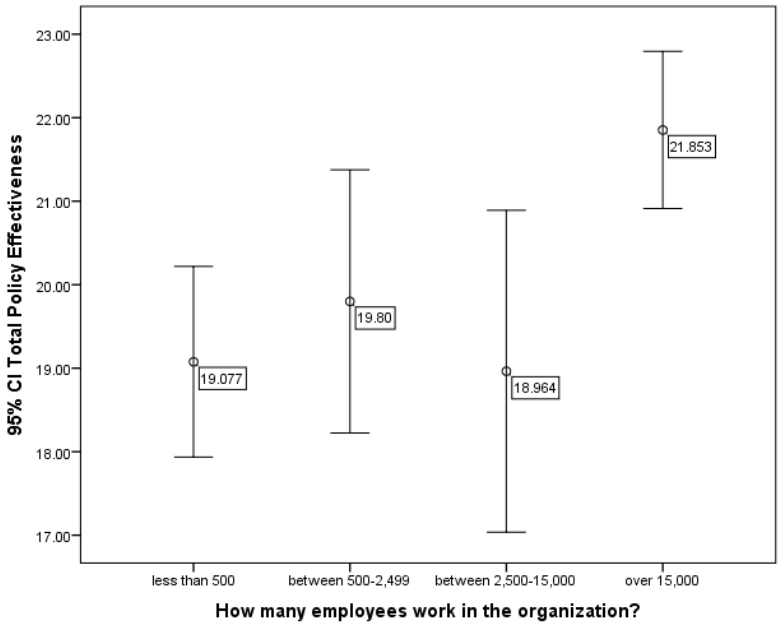

Figure 7. Error Bar for Total Program Effectiveness by Number of Employees

Levene's test of equal variances was completed on the total program effectiveness by number of employees. Equal variances across samples is also called homogeneity of variance (Field, 2013). The test was used to determine if there was a significant difference in variances between employee groups of different numbers. The first step in this analysis was to find the absolute values of deviations around the median of each group. These differences are compared between groups for variabilities. Table 8 displays the results of the test. Moreover, the group descriptive statistic Total Program Effectiveness by Number of Employees is located in Appendix F.

Table 8.

Levene's Test of Equal Variances: Total Program Effectiveness by Number of Employees

Levene Statistic	*df*1	*df*2	*Sig.*
2.537	3	114	0.060

Levene's test of equal variances showed no significant difference in variances between employee groups of different numbers. Therefore, a more robust F-test for ANOVA (Brown-Forsythe F-test) was not necessary. An F-test would be required if the results showed a wide spread between group medians. Next, a one-way ANOVA on the total program effectiveness by number of employees was completed. One-way ANOVA is used to compare more than two groups based on a single independent variable. Table 9 shows the results of the one-way ANOVA of the total program effectiveness by number of employees.

Table 9.

Results of One-Way ANOVA: Total Program Effectiveness by Number of Employees

	Sum of Squares	*df*	Mean Square	*F*	*Sig.*
Between Groups	169.989	3	56.663	3.978	0.010
Within Groups	1623.875	114	14.245		
Total	1793.864	117			

From the ANOVA results in the table above, there was a statistically significant difference in the mean levels of program effectiveness between employee groups of different numbers [F(3, 114)=3.978, p=0.010]. However, the test did not show where the groups were different. Therefore, further testing had to be employed to determine the exact location of the significant difference. Table 10 gives the results of one-way ANOVA post hoc tests.

Table 10.

Results of One-Way ANOVA Post Hoc Tests: Total Program Effectiveness by Number of Employees

	(I) How many employees work in the organization?	(J) How many employees work in the organization?	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Bonferroni	less than 500	between 500–2,499	-0.72308	1.01128	1.000	-3.4384	1.9923
		between 2,500–15,000	0.11264	1.02791	1.000	-2.6474	2.8727
		over 15,000	-2.77602*	0.98327	0.034	-5.4162	-0.1359
	between 500–2,499	less than 500	0.72308	1.01128	1.000	-1.9923	3.4384
		between 2,500–15,000	0.83571	0.99174	1.000	-1.8272	3.4986
		over 15,000	-2.05294	0.94540	0.192	-4.5914	0.4855
	between 2,500–15,000	less than 500	-0.11264	1.02791	1.000	-2.8727	2.6474
		between 500–2,499	-0.83571	0.99174	1.000	-3.4986	1.8272
		over 15,000	-2.88866*	0.96317	0.020	-5.4748	-0.3025
	over 15,000	less than 500	2.77602*	0.98327	0.034	0.1359	5.4162
		between 500–2,499	2.05294	0.94540	0.192	-0.4855	4.5914
		between 2,500–15,000	2.88866*	0.96317	0.020	0.3025	5.4748

*. The mean difference is significant at the 0.05 level.

Post hoc tests were performed to learn where the significant difference could be found. The mean difference in program effectiveness levels was greater for larger organizations, with over 15,000 employees (M =21.8529, SD = 2.69829, p=0.034), than the smallest organization, with less than 500 employees (M =19.0769, SD = 2.82734, p=0.034), and between the over 15,000 employees group (M =21.8529, SD = 2.69829, p= 0.020) and the 2,500 to 15,000 employees group (M =18.9643, SD = 4.970159, p= 0.020). This post hoc test is doable only when the omnibus ANOVA finds a significant effect.

Total Program Effectiveness by Dedicated Security Office

From the error bar plot in Figure 8 (below), it appears that the mean levels of program effectiveness were different for organizations with a dedicated security office than those without such an office. It also appears that the variances for these groups were different. Thus, we expect that the independent samples t-test and Levene's test will show significant differences in the means and variances of program effectiveness levels between organizations with a dedicated security office and those without such an office. However, there were differences in group sizes, which can affect the mean and variance tests.

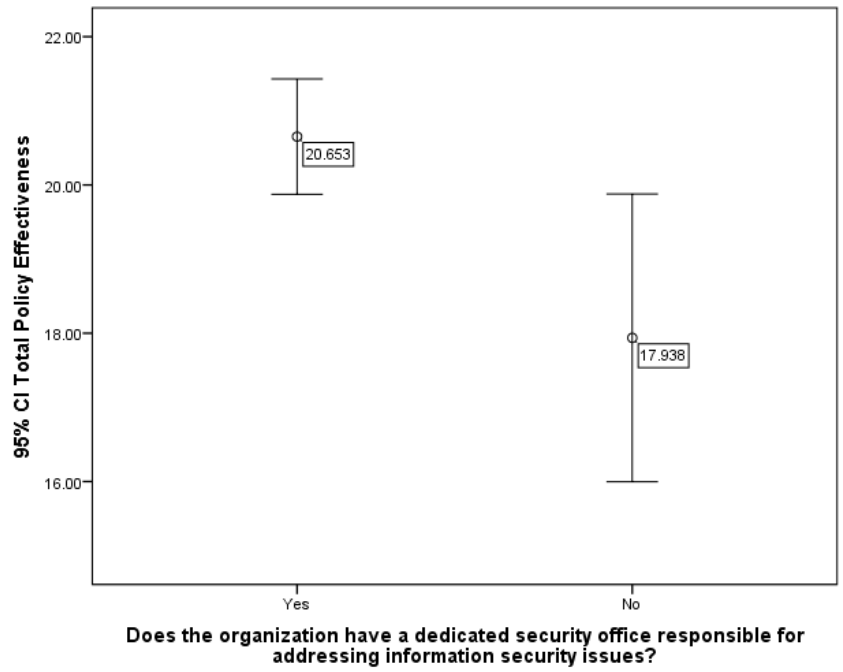

Figure 8. Error Bar for Total Program Effectiveness by Dedicated Security Officer

This study analyzed the data based on organizations with dedicated security offices and those without a dedicated security office. To summarize the data in a meaningful way, descriptive statistics were used. Descriptive statistics allow the research to describe the data, but they do not permit any conclusions regarding hypotheses. Table 11 provides the results of the group descriptive statistics. Additionally, Table 12 shows the results of the independent samples t-test. Again, the t-test allows the researcher to compare the two groups' total program effectiveness.

Table 11.

Group Descriptive Statistics: Total Program Effectiveness by Dedicated Security Office

	Does the organization have a dedicated security office responsible for addressing information security issues?	*N*	Mean	*Std*. Deviation	*Std*. Error Mean
Total Program Effectiveness	Yes	95	20.6526	3.81979	0.39190
	No	16	17.9375	3.64177	0.91044

Table 12.

Results of Independent Samples t-Test: Total Program Effectiveness by Dedicated Security Office

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Total Program Effectiveness	Equal variances assumed	0.381	0.538	2.647	109	0.009	2.71513	1.02575	0.68213	4.74814
	Equal variances not assumed			2.739	20.959	0.012	2.71513	0.99121	0.65355	4.77671

There was no significant difference in the variance levels of program effectiveness between the two groups [$F(109)=0.381$, $p=0.538$]. However, a significant difference was found in the mean levels of program effectiveness between organizations with a dedicated security office and those with no such office [$t(109)=2.647$, $p=0.009$]. The level of program effectiveness was greater for organizations with a dedicated security office ($M=20.6526$, $SD=3.81979$) than those with no such office ($M=17.9375$, $SD=3.64177$).

Total Program Effectiveness by Level Security Policy is Approved

Figure 9 (below) displays an error bar plot of total program effectiveness by the organization level that approves security policy. It appears that the mean levels of program effectiveness were different for organizations with executive level approval of security policy than those with middle management approval. It also appears that the variances for these groups were different. Thus, we expect that the independent samples t-test and Levene's test will show significant differences in the means and variances of program effectiveness levels between organizations with executive level approval of security policy and those with middle manager approval. However, there were differences in group sizes, which can affect the mean and variance tests.

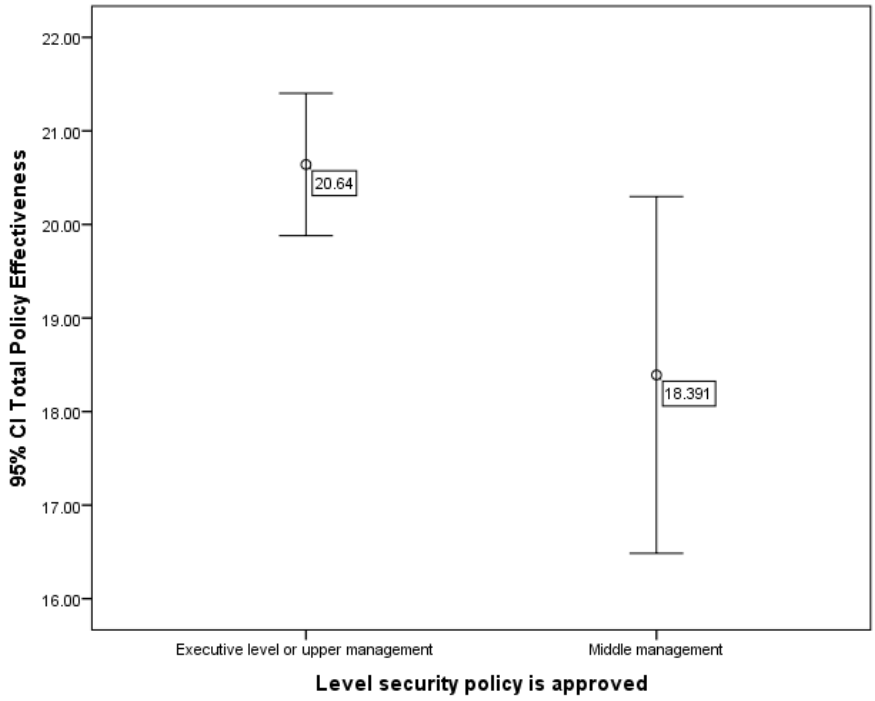

Figure 9. Error Bar for Total Program Effectiveness by Level Security Policy is Approved

Additionally, the data were analyzed on the premises of the level of security policy approval. A descriptive statistics table was used to analyze the data. Table 13 shows the results of descriptive statistics analysis. Furthermore, a t-test was employed to compare the results of the two groups. The results of the t-test can be seen in Table 14.

Table 13.

Group Descriptive Statistics: Total Program Effectiveness by Level Security Policy is Approved

	Level security policy is approved	N	Mean	Std. Deviation	Std. Error Mean
Total Program Effectiveness	Executive level or upper management	89	20.6404	3.60948	0.38260
	Middle management	23	18.3913	4.40804	0.91914

Table 14.

Results of Independent Samples t-Test: Total Program Effectiveness by Level Security Policy is Approved

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Total Program Effectiveness	Equal variances assumed	1.260	0.264	2.542	110	0.012	2.24915	0.88481	0.49565	4.00264
	Equal variances not assumed			2.259	30.059	0.031	2.24915	0.99559	0.21604	4.28225

From the table above, there was no significant difference in the variance levels of total program effectiveness between organizations with security policy approvals at the executive level and those with approvals at the middle management level [$F(110)=1.260$, $p=0.264$]. However, a statistically significant difference was discovered in the mean program effectiveness levels between these two approval groups [$t(110)=2.542$, $p=0.012$]. Organizations whose security policies were approved at the executive level had significantly higher levels of total program effectiveness ($M=20.6404$, $SD=3.60948$) than similar organizations with approval at the middle management level ($M=18.3913$, $SD=4.40804$).

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

Introduction

The purpose of this quantitative survey study, with a correlation research design, was to explore the factors that encourage an ineffective information program by investigating the relationship of an organization's information security policy awareness, enforcement, and maintenance to its information security program effectiveness. This study addressed a gap in the body of knowledge identified by Knapp and Ferrante (2012). These researchers' sample was from a population of information security professionals; therefore, the results are not generalizable to other populations of employees (Knapp & Ferrante, 2012). Knapp and Ferrante (2012) suggested that future research should be conducted on the subject with a sample population whose knowledge or expertise are external to information security. A study on the topic using this population is significant since literature indicates that these typical users are the primary source of vulnerability in an organization's information security program (Guo et al., 2011). Therefore, this study focused on employees with knowledge external to information security, being that they are the weakest link in the information security chain (Shahraki & Nikmaram, 2013).

As a result, this study used a non-experimental approach with a sample size of 119. The G*Power model 3.0.10 was used to determine the sample size. G*Power is an analysis program that may be utilized for many statistical tests (Faul, Erdfelder, Buchner, & Lang, 2009). G*Power can run most statistical tests used by social, behavioral, and biomedical sciences. The software provides the option of both graphical and numeric outputs. Additionally, the population size was based on the United States Department of Labor Bureau of Labor Statistics. The sample frame was prequalified respondents from SurveyMonkey's online database, the sample was

randomly selected individuals that met the criteria for this study, and the volunteers were computers users from medium to large organizations with established information security programs within the United States.

Discussion

This study employed multiple regression to predict values on the dependent or criterion variable level of information security program effectiveness from a set of independent predictor variables for the levels of information security policy awareness, enforcement, and maintenance. A total of 105 organizations responded to all the variables used for this multiple regression analysis. Descriptive statistics for the dependent criterion variable show that the average program effectiveness for these organizations was 20.12, with a standard deviation of 3.82. The regression model was found to be statistically significant. As a result, the null hypothesis was rejected, and the alternate hypothesis that the independent variables total policy awareness, total policy enforcement, and total policy maintenance were statistically significant predictors of the level of total program effectiveness [$F(3,101)=36.807$, $p<0.001$] was accepted.

Table 4.

Multiple Regression Model Summary[d]

Model	*R*	*R* Square	Adjusted *R* Square	*Std*. Error of the Estimate	Change Statistics				
					R Square Change	*F* Change	*df*1	*df*2	*Sig. F* Change
1	0.677[a]	0.458	0.453	2.82493	0.458	87.143	1	103	0.000
2	0.706[b]	0.499	0.489	2.73027	0.041	8.266	1	102	0.005
3	0.723[c]	0.522	0.508	2.67902	0.023	4.940	1	101	0.028

a. Predictors: (Constant), Total Policy Awareness

b. Predictors: (Constant), Total Policy Awareness, Total Policy Enforcement

c. Predictors: (Constant), Total Policy Awareness, Total Policy Enforcement, Total Policy Maintenance

d. Dependent Variable: Total Program Effectiveness

Accordingly, the results of this study indicate that information security awareness, enforcement, and maintenance have a direct impact on information security programs. Additionally, the findings reveal that information security awareness has the largest direct impact on information security program effectiveness. Moreover, information security maintenance has the smallest impact on information security program effectiveness. These findings are supported by similar results found in Knapp and Ferrante's (2012) study and other studies mentioned in the literature review. As depicted in the literature, numerous scholars acknowledge that an efficient information security awareness program enhances the effectiveness of the overall information security program (Bower, 2011; da Veiga & Martins, 2015; Harnesk & Lindström, 2011; Padayachee, 2012; Wolf et al., 2011).

Further, information security policy enforcement has a lesser direct impact on information security program effectiveness. However, the effect should be considered when

developing an effective information security program. According to findings in the literature review, enforcement is necessary for an organization's information security program effectiveness (Steinbart et al., 2016). Equally important, artisans must remember that there are two primary approaches to security enforcement, including control-based compliance and value-based compliance. The antecedent focuses on using reward and punishment to achieve implementation; whereas, the latter focuses on human values and beliefs to obtain obedience (Hedström et al., 2011). Additionally, scholars admit that if human behavior is not considered in the development of security programs, the gap between theory and practice will remain (Hedström et al., 2011).

Likewise, information security maintenance has the least impact on an effective program. However, considering information security fluidity, a program can quickly become obsolete without a maintenance segment (Allam et al., 2014; Pathari & Sonar, 2012). According to Tsohou et al. (2016), changes in the environment may occur due to modifications on the organizational, technological, and individual levels. Therefore, it is significant that security officers ensure information security programs address transformations in their environment (Knapp & Ferrante, 2012). For this purpose, an information security maintenance program is considered essential for an effective information security program.

First, results divulged that there was a statistically significant difference in the mean levels of program effectiveness based on employee size. In other words, the larger the organization, the more significant the difference. Second, results showed that organizations with a dedicated security office had a greater effect on the effectiveness of their information security program. Finally, this study's findings also revealed that organizations whose information

security policies are approved on the executive level contribute to a more efficient overall information security program.

Implications

This study contributes several implications for scholars and practitioners. First, security managers should incorporate information security awareness, enforcement, and maintenance in the development of their information security management programs. This result is supported by several studies that imply similar results (Knapp & Ferrante, 2012; Wolf et al., 2011).

Furthermore, security officers should encourage their organizations to invest in awareness education and training for all employees. According to the study findings, security awareness has the most significant impact on program effectiveness. Numerous other studies indicate that information security awareness has a significant positive effect on the overall information security program (Bower, 2011; da Veiga & Martins, 2015; Harnesk & Lindström, 2011; Padayachee, 2012; Wolf et al., 2011). Therefore, educating employees, the weakest link in information security chain (Shahraki & Nikmaram, 2013), should ultimately increase security.

Second, this study revealed that information security enforcement has a statistically significant impact on the efficiency of an information security program. Therefore, scholars and technicians should incorporate enforcement in their development of information security management schemes. A security strategy without a definite enforcement plan is an ineffectual program (Safa et al., 2015). However, when incorporating their enforcement plan, they should consider their organization's culture and their employees' culture, habits, and beliefs (Yoon & Kim, 2013), hence addressing the human factor in the security chain.

Third, although information security maintenance illustrated the least amount of impact on program performance, it is still a necessary factor in program effectiveness. A maintenance

program is necessary to ensure that policies, awareness, and enforcement programs are modernized to address changes in the corporate environment (Knapp & Ferrante, 2012). Without a dynamic maintenance program, an organization's security policies, awareness program, and enforcement program can instantaneously become ineffective (Allam et al., 2014; Pathari & Sonar, 2012). As a result, the entire information security program is rendered unsuccessful. Again, although information security maintenance has the smallest impact of the three predictors investigated in this study, the effectiveness of the other two may depend on it.

Fourth, the findings of this study indicate that the implementation of a dedicated information security office has a statistically significant impact on the effectiveness of an organization's information security program. This finding is supported by other studies which inferred that the implementation of an information security office or officer has a positive effect on security program effectiveness (Khey & Sainato, 2013; Renaud & Goucher, 2012). These studies acknowledged that an information security office reduces security risk. For that reason, organizations should seriously consider having an information security office (or at least an information security officer). These individuals are capable of providing particular attention to the needs of the organization's information security management (Khey & Sainato, 2013). Their primary endeavor should be to ensure that the organization's information security program is productive. The application of a security office should be compulsory for all medium- to large-scale organizations.

Finally, this study's findings determined that organizations whose security policies were approved at the executive level had significantly higher levels of total program effectiveness. This finding supports the ideology that information security should start from the top (Hu et al., 2012). Executives should be involved in all aspects of the information security process, including

policy development and approval (Alhogail & Mirza, 2014). Policies approved by senior management display the organization's obligation to information security. Accordingly, employees are more acceptable of policies that upper management support. Thus, the top management has an impact on employees' attitudes, organizational culture, and values (Hu et al., 2012).

Limitations

One limitation of this study is the internal validity of the research design. The research approach is a quantitative survey study with a correlational research design, thereby limiting the findings and discussion to one of relationships (and not causal) (Connelly, 2012; Ingham-Broomfield, 2014; Lomax & Li, 2012; Patten, 2014). Another limitation is that respondents may not be representative of the population. The survey response rate is limited by cost and time to only two waves of responses. However, Dillman (2014) states that, other than online surveys, there is no other method of collecting survey data that offers so much potential for so little cost. Additionally, the outlook of this study was restricted to the three components of information security policy. Notwithstanding, information security programs include much more than just those three elements (Knapp & Ferrante, 2012). Further, this study required self-reporting by participants (Vance et al., 2014). However, the reliability of participants self-reporting is questionable. That is, there is a concern that participants may provide answers that they infer are expected of them.

Recommendations

The subsequent recommendations are derived from the study findings, limitations, and literature review. As mentioned in the study limitations, it is proposed that the results of this study be investigated in an observational study. This would reduce the adverse effects of self-

reporting. Another suggestion to investigate would be to compare control-based enforcement to value-based enforcement in terms of their significance on the effectiveness of an information security program. Lastly, the other components that may affect the effectiveness of an information program, such as employee monitoring, security risk assessment, policy development, and senior management approval, should be explored.

Conclusion

In today's global market, information is one of the primary assets of most organizations (Al-Mukahal & Alshare, 2014). In most cases, access to that information allows executives to make split second decisions, which can increase profit or bankrupt an organization. Therefore, it is important that the information is accessible, accurate, and complete. This information also has to be protected from unauthorized malicious individuals. For that reason, information security performs an important role in an organization's business success. Information security's primary objective is to safeguard a company's information. However, statistics seem to indicate that there is a high rate of information violations (Sommestad et al., 2012; Vance et al., 2012). Moreover, based on the considerable number of breaches reported every year, it can be deduced that most information security programs are ineffective (Steinbart et al., 2016).

For this purpose, this study explored the predictors of an effective information security program. Although many components may contribute to an effective program, information security policy awareness, enforcement, and maintenance were chosen as the independent variables. The results of this study indicate that all three independent variables were statistically significant. In consequence, these independent variables are positive predictors of an effective information security program. Moreover, the results support what the majority of the literature review seems to imply.

Additionally, the study expands on Knapp and Ferrante's (2012) study and adds to the body of knowledge in the field of information security. Equally important, it provides technicians and scholars with additional information that may assist in developing a more robust information security model. Moreover, the improved models will help in mitigating information security violations and reducing the number of breaches that corporations encounter, thereby saving corporate funds.

REFERENCES

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology*, *64*(2), 540–549. Retrieved from www.jatit.org

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, *42*, 56–65. Retrieved from http://dx.doi.org/10.1016/j.cose.2014.01.005

Al-Mukahal, H. M., & Alshare, K. (2014). An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information and Computer Security*, *23*(1), 102–118. doi: 10.1108/ICS-03-2014-0018

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312. Retrieved from http://dx.doi.org/10.1016/j.chb.2014.05.046

Argyrous, G. (2011). *Statistics for research*. Thousand Oaks, CA: SAGE.

Aydin, Ö. M., & Chouseinoglou, O. (2013). Fuzzy assessment of health information system users' security awareness. *Journal Medical Systems, 37*, 1–13. doi: 10.1007/s10916-013-9984-x

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*(2013), 145–159. Retrieved from http://dx.doi.org/10.1016/j.cose.2013.05.006

Basin, D., Jugé, V., Klaedtke, F., & Zălinescu, E. (2013). Enforceable security policies revisited. *ACM Transaction on Information and System Security, 16*(1), 3, 3–26. doi: http://dx.doi.org/10.1145/2487222.2487225

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management, 51*(2014), 138–151. Retrieved from http://dx.doi.org/10.1016/j.im.2013.11.004

Bojanc, R., & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal*, *25*(2), 25–37. Retrieved from http://www.asem.org/asemweb-emj.html

Bower, J. (2011). How effective is your compliance training. *Journal of Health Care Compliance*, 37–40. Retrieved from https://www.complianceresource.com/publications/how-effective-is-your-compliance-training/

Cavallari, M. (2011). The organizational relationship between compliance and information security. *International Journal of Academic Business World, 5*(1), 63–76. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=plh&AN=82855805&site=ehost-live

Chang, K., & Wang, C. (2011). Information systems resources and information security. *Information System Frontiers, 13,* 579–593. doi: 10.1007/s10796-010-9232-6

Chen, Y., Ramamurthy, K., & Wen, K. (2013). Organizations' information security policy compliance: Stick or carrot approach. *Journal of Management Information Systems, 29*(3), 157–188. doi: 10.2753/MIS0742-1222290305

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11–19. doi: 10.1080/08874417.2015.11645767

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computer and Security, 39,* 447–459. doi: 10.1016/j.cose.2013.09.009

Connelly, L. M. (2012). Correlations. *Medsurg Nursing, 21*(3). Retrieved from https://amsn.org/professional-development/periodicals/medsurg-nursing-journal

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computer in Human Behavior, 28*(2012), 1849–1858. Retrieved from http://dx.doi.org/10.1016/j.chb.2012.05.003

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: SAGE.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091–1124. doi: 10.1111/j.1540-5915.2012.00383.x

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49,* 162–176. Retrieved from http://dx.doi.org/10.1016/j.cose.2014.12.006

Dahbur, K., Isleem, M. R., & Ismail, S. (2012). A study of information security issues and measures in Jordan. *International Management Review*, 8(2), 71–82. Retrieved from http://search.proquest.com/openview/3e5084bc2c853e217dddfb969e4cbe13/1?pq-origsite=gscholar

Delost, M. E., & Nadder, T. S. (2014). Guidelines for initiating a research agenda: Research design and dissemination of results. *Clinical Laboratory Science, 27*(4), 237–244. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/26084153

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior*, 61, 656-666. Retrieved from http://dx.doi.org/10.1016/j.ch.2016.03.068

Dillman, D. A. (2014). *Mail and Internet surveys: The tailored design method* (4th ed.). Hoboken, NJ: John Wiley and Sons.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*, 201–209. doi: 10.1016/j.ijinfomgt.2010.06.001

Drtil, J. (2013). Impact of information security incidents-Theory and reality. *Journal of Systems Integration*, *1*, 44–52. Retrieved from http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=85344146&site=ehost-live&scope=site

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: in which security solutions is it worth investing. *Communications of the Association for Information Systems, 28*(22), 329–356. Retrieved from http://aisel.aisnet.org/cais/vol28/iss1/22

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2013). Current challenges in information security risk management. *Information Management & Computer Security*, *22*(5), 410–430. doi: 10.1108/IMCS-07-2013-0053

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). Thousand Oaks, CA: SAGE.

Flicker, S., Haans, D., & Skinner, H. (2004). Ethical dilemmas in research on internet communities. *Qualitative Health Research*, *14*, 123–124. doi: 10.1177/1049732303259842

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers and Security*, 43(2014), 90–110. Retrieved from http://dx.doi.org/10.1016/j.cose.2014.03.004

Garson, D. (2014). *Multiple regression*. Raleigh, NC: Statistical Associates Publishing.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in cost. *Journal of Computer Security, 19*(2011), 33–56. doi: 10.3233/JCS-2009-0398

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*(2), 203–236. doi: 10.2753/MIS0742-1222280208

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155–176. doi: 10.1108/09685221111153346

Han, W., & Lei, C. (2011). A survey on policy languages in network and security management. *Computer Networks*, *56*, 477–489. doi: 10.1016/j.comnet.2011. 09.0149

Harnesk, D., & Lindström, J. (2011). Shaping security behaviour through discipline and agility implications for information security management. *Information Management and Computer Security, 19*(4), 262–276. doi:10.1108/0968522111 1173076

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security, 21*(4), 266–287. doi: 10.1108/IMCS-082012-0043

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J.P. (2011). Value conflict for information security management. *Journal of Strategic Information Systems, 20*, 373–384. doi: 10.1016/j.jsis.2011.06.001

Hu, Q., Dinev, T., Hart, P., Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–660. doi:10.1111/j.1540-5915.2012.00361.x

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Methods for evaluating and effectively managing the security behavior of employees. *Communications of the ACM, 54*(6), 54–60. doi: 10.1145/1953122.1953142

Iarossi, J., Miller, J., O'Connor, J., & Keil, M. (2013). Addressing the sustainability challenge: Insights from institutional theory and organizational learning. *Journal of Leadership, Accountability and Ethics, 10*(1), 76–91. Retrieved from http://dx.doi.org/10.2139/ssrn.1839802

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computer and Security, 31,* 83–95. doi: 10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management, 51,* 69–79. Retrieved from http://dx.doi.org/10.1016/j.im.2013.10.001

Ingham-Broomfield, R. (Dec 2014-Feb 2015). A nurses' guide to quantitative research. *Australian Journal of Advanced Nursing, 32*(2), 32–38. Retrieved from http://www.ajan.com.au/Vol32/Issue2/4Broomfield.pdf

Jalal-Karim, A. (2013). Evaluating the impact of information security on enhancing the business decision-making process. *World Journal of Entrepreneurship, Management and Sustainable Development, 9*(1), 55–64. doi: 10.1108/20425961311315719

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

Kerman, B., Freundlich, M., Lee, J. M., & Brenner, E. (2012). Learning while doing in the human services: Becoming a learning organization through organization change. *Administration in social work, 36,* 234–257. doi: 10.1080/03643107. 2011.573061

Khey, D. N., & Sainato, V. A. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal, 26,* 367–382. doi: 10.1057/sj.2013.24

Kim, H., MacDonald, R. H., & Andersen, D. F. (2013). Simulation and managerial decision making: A double-loop learning framework. *Public Administration Review, 73*(2), 291–300. doi: 10.111/j.1540-6210.2012.02656.x

Knapp, K. J. & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice, 13*(5), 66–80. Retrieved from http://www.na-businesspress.com/JMPP/ KnappKJ_Web13_5_.pdf

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security: An empirical study of intentional versus actual behavior. *Information Management & Computer Security, 21*(1), 5–15. doi: 10.1108/09685221311314383

Laybats, C. & Tredinnick, L. (2016). Information Security. *Business Information Review, 33*(2), 76–80. doi: 10.1177/0266382116653061

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review, 37*(12), 1049–1092. doi: 10.1108/MRR-04-2013-0085

Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information System Front, 14*, 375–393. doi: 10.1007/s10796-010-9253-1

Li, W. & Cheng, L. (2013). *Effects of neutralization techniques and rational choice theory on Internet abuse in the workplace*. Conference paper, Pacific Asia Conference on Information Systems, PACIS2013 at Jeju.

Liu, C. (2015). Types of employee perceptions of information security using Q methodology: An empirical study. *International Journal of Business and Information, 10*(4), 557–575. Retrieved from http://knowledgetaiwan.org/ijbi/

Lomax, R., & Li, J. (2013, July). Definitions of quantitative methods of research. *Correlational Research.* Retrieved from http://www.education.com/pdf/correlational-research/

Lowry, P. B., Posey, C., Roberts, T. L., & Bennett, R. J. (2014). Is your banker leaking your personal information: The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics, 121,* 385–401. doi: 10.1007/s10551-013-1705-3

Markovitz, D. (2012). Good written procedures equals compliance. *Journal of GPX Compliance, 16*(3), 39–42. Retrieved from http://search.proquest.com/openview/439fb580297542 6d40decc1b87f8ded6/1?pq-origsite=gscholar

Marshall, C. & Rossman, G. B., (2011). Designing qualitative research (5th ed.). Thousand Oaks, CA: SAGE

Mbowe, J. E., Zlotnikova, I., Msanjila, S. S., & Oreku, G. S. (2014). A conceptual framework for threat assessment based on organization's information security policy. *Journal of Information Security, 5*, 166–177. Retrieved from http://dx.doi.org/10.4236/jis.2014.54016

Mohanty K., & Kar, S. (2012). Achieving innovation and success: Organizational learning. *SCMS Journal of Indian Management,* 36–42. Retrieved from https://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=07d94bdd-d44c-4931-9df4-b6cc2c607d25%40sessionmgr1

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computer and Security, 48,* 267–280. Retrieved from http://dx.doi.org/10.1016/j.cose.2014.10.015

Muehfeld, K., Sahib, P. R., & Van Witteloostuijn, A. (2012). A contextual theory of organizational learning from failures and successes: A study of acquisition completion in the global newspaper industry, 1981–2008. *Strategic Management Journal, 33,* 938-964. doi: 10.1002/smj.1954

Mukundan, N. R., & Sai, L. P. (2014). Perceived information security of internal users in Indian IT services industry. *Information Technology Management, 15*, 1–8. doi: 10.1007/s10799-013-0156-y

Myers, J. L., Well, A. D., & Lorch, R. F. Jr. (2010). *Research design and statistical analysis* (3rd ed.) New York, NY: Routledge.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*(2016), 83–93. Retrieved from http://dx.doi.org/10.1016/j.cose.2015.10.002

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers and Security, 31*, 673–680. doi:10.1016/j.cose.2012.04.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security, 4*(2), 165–176. Retrieved from ww.sciencedirect.com/science/article/pii/S016740481300179X

Parsons, K. McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). A study of information security awareness in Australian government organisations. *Information Management & Computer Security, 2*(4), 334–345. doi: 10.1108/IMCS-10-20130078

Pathari, V., & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security, 20*(4), 264–280. doi: 10.1108/09685221211267648

Patten, M. L. (2014). *Understanding Research Methods* (9th Ed.). Glendale, CA: Pyrczak Publishing

Paulsen, C., & Coulson, T. (2011). Beyond awareness: Using business intelligence to create a culture of information security. *Communications of the IIMA, 11*(3), 35–54. Retrieved from http://scholarworks.lib.csusb.edu/ciima/vol11/iss3/4

Phillips, J. T. (2014). Plug internal data leaks with an effective IG program. *Information Management, 48*(3), 20–22, 24, 47. Retrieved from http://go.galegroup.com/ps/anonymous?id=GALE%7CA371969299&sid=googleScholar&v=2.1&it=r&linkaccess=fulltext&issn=15352897&p=AONE&sw=w&authCount=1&isAnonymousEntry=true

Popescu, D. M., Bunea, A., & Radu, M. (2014). The duality of the concept of

organizational learning. *Valahian Journal of Economic Studies, 5*(3), 63–68. Retrieved from http://search.proquest.com/openview/84689446a31d3474f4a403171ec628cc/1?pq-origsite=gscholar

Privacy Rights Clearinghouse (PRC). (2015) Chronology of data breaches: Security breaches 2011–present. [Dataset], http://www.privacyrights.org/data-breach, accessed 15 April 2015.

Rashid, R. M., Zakaria, O., & Zulhemay, M. N. (2013). The relationship of information security knowledge (ISK) and human factors: Challenges and solution. *Journal of Theoretical and Applied Information Technology, 57*(1), 67–75. Retrieved from http://www.jatit.org/ volumes/ Vol57No1/9Vol57No1.pdf

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: An uneasy partnership. *Information Management & Computer Security*, *20*(4), 296–311. doi: 10.1108/09685221211267666

Rhee, H., Ryu, Y. U., & Kim, C. (2012). Unrealistic optimism on information security management. *Computer & Security*, *31*(2012), 221–232. doi: 10.1016/j.cose.2011. 12.001

Robertson, R. A. (2012). Security auditing: The need for policies and practices. *Journal of Information Privacy & Security*, *8*(1), 30–37. Retrieved from http://www.tandfonline.com /doi/abs/10.1080/15536548.2012.11082760

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*(2015), 65–78. Retrieved from http://dx.doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*(2016), 70–82. Retrieved from http://dx.doi.org/10.1016/j.cose.2015.10.006

Salmons, J. (2010). *Online interviews: in real time.* Thousand Oaks, CA: SAGE.

Sánchez-Algarra, P., & Anguera, M. T. (2012). Qualitative/quantitative integration in the inductive observational study of interactive behaviour: impact of recording and coding among predominating perspectives. *Qual Quant, 47*, 1237–1257. doi:10.1007/s11135-012-9764-6

Semer, L. J. (2012). Evaluating the employee security awareness program. *Internal Auditor, 69*(6), 53–56. Retrieved from http://go.galegroup.com/ps/anonymous?p=AONE &sw=w&issn=00205745&v=2.1&it=r&id=GALE%7CA313439257&sid=googleScholar &linkaccess=fulltext&authCount=1&isAnonymousEntry=true

Shahraki, A. S., & Nikmaram, M. (2013). Human errors in computer related abuses. *Journal of Theoretical and Applied Information Technology, 47*(1), 93–97. Retrieved from www.jatit.org

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computer & Security, 49*, 177-191. Retrieved from http://dx.doi.org/ 10.1016/j.cose.2015.01.002

Silic, M., & Back, A. (2013). Information Security critical review and future directions for research. *Information Management & Computer Security*, *22*(3), 279–308. doi: 10.1108/IMCS-05-2013-0041

Singh, A. N., Gupta, M. P., & Ojha, A. (2013). Identifying factors of organizational information security management. *Journal of Enterprise Information Management, 27*(5), 644–667. doi: 10.1108/JEIM-07-2013-0052

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management, 51*, 217–224. Retrieved from http://dx.doi.org/10.1016/j.im.2013. 08.006

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–A12. Retrieved from https://pdfs.semanticscholar.org/c1e6/07f7f60251a51ff236f153 23a60760722dad.pdf

Skorodumov, B. I., Skorodummova, O. B., & Matronina, L. F. (2015). Research of human factors in information security. *Modern Applied Science*, *9*(5), 287–294. doi: 10.5539/mas.v9n5p287

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security, 22*(1), 42–75. doi:http://dx.doi.org/10.1108/IMCS-08-2012-0045

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, *23*(2), 200–217. Retrieved from https://pdfs.semanticscholar.org/ d425/3a891fdb3e1d7a85f7cd65d0b601f72b77fa.pdf

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2015). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2016), 215–225. Retrieved from http://dx.doi.org/10.1016/j.ijinfomgt.2015.11.009

Spector, P. E., & Meier, L. L. (2014). Methodologies for the study of organizational

behavior processes: How to find your keys in the dark. *Journal of Organizational Behavior, 35*, 1109–1119. doi:10.1002/job.1966

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems, 30*(1), 71–92. doi: 10.2308/isys-51257

Swanson, R. A., & Holton III., E. F. (2005). Research in organizations: Foundations and methods of inquiry. San Francisco, CA: Berrett Koehler Publications.

Thomson, K., & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security, 20*(1), 39–46. doi:http://dx.doi.org.10.1108/09685221211219191

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization for information security awareness programs. *Computers & Security, 52*(2015), 128–141. Retrieved from http://dx.doi.org/10.1016/j.cose.2015.04.006

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People, 25*(3), 327–352. doi: 10.1108/09593841211254358

Tsohou, A. Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38–58. Retrieved from www.palgrave-journals.com/ejis/

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insight from electroencephalography (EEG). *Journal for the Association for Information Systems, 15*, 679–722. Retrieved from http://aisel.aisnet.org/jais/vol15/iss10/2/

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information System, 29*(4), 263–289. doi: 10.2753/MIS0742-1222290410

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(2012), 190–198. Retrieved from http://dx.doi.org/10.1016/j.im.2012.04.002

Vogt, W. P. (2007). Quantitative research methods for professionals. Boston, MA: Pearson Education, Inc.

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information*

Privacy & Security, 9(4), 52–79. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1103&context=amcis2013

Wang, Y., & Huang, S. (2013). Organizational learning and human resource: A review of the theory and literatures. *International Proceedings of Economics Development and Research, 61* 56–59. doi: 10.7763/IPEDR.2013.V61.12

Williams, M. N., Garajales, C. A. G., & Kurkiewicz, D. (2013). Assumption of multiple regression: Correcting two misconceptions. *Practical Assessment, Research & Evaluation, 18*(11), 1–14. Retrieved from http:pareonline.net/getvn.asp?v=18&n=11

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1–20. Retrieved from https://pdfs.semanticscholar.org/04ac/6e2357ee3a45272199d6cc65fa3762490324.pdf

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://search.proquest.com/openview/a0ec10a0a419f1575dcd769b5a0b3656/1?pq-origsite=gscholar

Wu, Y., Guynes, C. S., & Windsor, J. (2012). Security awareness programs. *The Review of Business Information Systems (Online), 16*(4), 165. Retrieved from http://www.cluteinstitute.com/

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management, 31*(2011), 360–365. doi: 10.1016/j.ijinfomgt.2010.10.006

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People, 26*(4), 401–419. doi: 10.1108/ITP-12-2012-0147

APPENDIX A. STATEMENT OF ORIGINAL WORK

Academic Honesty Policy

Capella University's Academic Honesty Policy (3.01.01) holds learners accountable for the integrity of work they submit, which includes but is not limited to discussion postings, assignments, comprehensive exams, and the dissertation or capstone project.

Established in the Policy are the expectations for original work, rationale for the policy, definition of terms that pertain to academic honesty and original work, and disciplinary consequences of academic dishonesty. Also stated in the Policy is the expectation that learners will follow APA rules for citing another person's ideas or works.

The following standards for original work and definition of *plagiarism* are discussed in the Policy:

> Learners are expected to be the sole authors of their work and to acknowledge the authorship of others' work through proper citation and reference. Use of another person's ideas, including another learner's, without proper reference or citation constitutes plagiarism and academic dishonesty and is prohibited conduct. (p. 1)
>
> Plagiarism is one example of academic dishonesty. Plagiarism is presenting someone else's ideas or work as your own. Plagiarism also includes copying verbatim or rephrasing ideas without properly acknowledging the source by author, date, and publication medium. (p. 2)

Capella University's Research Misconduct Policy (3.03.06) holds learners accountable for research integrity. What constitutes research misconduct is discussed in the Policy:

> Research misconduct includes but is not limited to falsification, fabrication, plagiarism, misappropriation, or other practices that seriously deviate from those that are commonly accepted within the academic community for proposing, conducting, or reviewing research, or in reporting research results. (p. 1)

Learners failing to abide by these policies are subject to consequences, including but not limited to dismissal or revocation of the degree.

Statement of Original Work and Signature

I have read, understood, and abided by Capella University's Academic Honesty Policy (3.01.01) and Research Misconduct Policy (3.03.06), including Policy Statements, Rationale, and Definitions.

I attest that this dissertation or capstone project is my own work. Where I have used the ideas or words of others, I have paraphrased, summarized, or used direct quotes following the guidelines set forth in the APA *Publication Manual*.

Type	
Learner name and date	Michael Talibah François, November 2, 2016
Mentor name and school	Steven A. Brown, School of Business and Technology

APPENDIX B. Multiple Regression: ANOVA Table

Multiple Regression: ANOVA Table[a]

Model		Sum of Squares	*df*	Mean Square	*F*	*Sig.*
1	Regression	695.425	1	695.425	87.143	0.000[b]
	Residual	821.966	103	7.980		
	Total	1517.390	104			
2	Regression	757.045	2	378.522	50.779	0.000[c]
	Residual	760.346	102	7.454		
	Total	1517.390	104			
3	Regression	792.499	3	264.166	36.807	0.000[d]
	Residual	724.892	101	7.177		
	Total	1517.390	104			

a. Dependent Variable: Total Program Effectiveness

b. Predictors: (Constant), Total Policy Awareness

c. Predictors: (Constant), Total Policy Awareness, Total Policy Enforcement

d. Predictors: (Constant), Total Policy Awareness, Total Policy Enforcement, Total Policy Maintenance

APPENDIX C. Variables Excluded at Each Step in Multiple Regression Model Development[a]

Variables Excluded at Each Step in Multiple Regression Model Development[a]

Model		Beta In	t	*Sig.*	Partial Correlation	Collinearity Statistics		
						Tolerance	VIF	Minimum Tolerance
1	Total Policy Maintenance	0.275[b]	2.589	0.011	0.248	0.443	2.259	0.443
	Total Policy Enforcement	0.271[b]	2.875	0.005	0.274	0.553	1.809	0.553
2	Total Policy Maintenance	0.233[c]	2.223	0.028	0.216	0.432	2.317	0.358

a. Dependent Variable: Total Program Effectiveness

b. Predictors in the Model: (Constant), Total Policy Awareness

c. Predictors in the Model: (Constant), Total Policy Awareness, Total Policy Enforcement

APPENDIX D. Evaluation of Multicollinearity of Variables in Multiple Regression[a]

Evaluation of Multicollinearity of Variables in Multiple Regression[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions			
				(Constant)	Total Policy Awareness	Total Policy Enforcement	Total Policy Maintenance
1	1	1.975	1.000	0.01	0.01		
	2	0.025	8.874	0.99	0.99		
2	1	2.950	1.000	0.01	0.00	0.00	
	2	0.032	9.560	0.88	0.04	0.35	
	3	0.018	12.911	0.11	0.96	0.65	
3	1	3.932	1.000	0.00	0.00	0.00	0.00
	2	0.032	11.009	0.88	0.03	0.26	0.01
	3	0.024	12.775	0.11	0.07	0.63	0.35
	4	0.012	18.165	0.00	0.90	0.11	0.64

a. Dependent Variable: Total Program Effectiveness

APPENDIX E. Group Descriptive Statistics: Total Program Effectiveness by Gender

Group Descriptive Statistics: Total Program Effectiveness by Gender

	GENDER	N	Mean	*Std*. Deviation	*Std*. Error Mean
Total Program Effectiveness	Male	16	19.8750	2.60448	0.65112
	Female	33	18.7879	4.46345	0.77699

APPENDIX F. Group Descriptive Statistics: Total Program Effectiveness by Number of Employees

Group Descriptive Statistics: Total Program Effectiveness by Number of Employees

	N	Mean	*Std.* Deviation	*Std.* Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Less than 500 Employees	26	19.0769	2.82734	0.55449	17.9349	20.2189	12.00	25.00
Between 500–2,499	30	19.8000	4.22146	0.77073	18.2237	21.3763	5.00	25.00
Between 2,500–15,000	28	18.9643	4.97015	0.93927	17.0371	20.8915	5.00	25.00
Over 15,000	34	21.8529	2.69829	0.46275	20.9115	22.7944	15.00	25.00
Total	118	20.0339	3.91563	0.36046	19.3200	20.7478	5.00	25.00