

2015

Designing an effective information security policy for exceptional situations in an organization: An experimental study

George S. Antoniou

Nova Southeastern University, antoniou@nova.edu

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

 Part of the [Business Administration, Management, and Operations Commons](#), [Business Law, Public Responsibility, and Ethics Commons](#), [Databases and Information Systems Commons](#), [Information Security Commons](#), [Management Information Systems Commons](#), and the [Strategic Management Policy Commons](#)

Share Feedback About This Item

NSUWorks Citation

George S. Antoniou. 2015. *Designing an effective information security policy for exceptional situations in an organization: An experimental study*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (949) https://nsuworks.nova.edu/gscis_etd/949.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Designing an effective information security policy for exceptional situations in an organization: An experimental study

By

George S. Antoniou

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2015

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

Gurvirender P. Tejay, Ph.D.
Chairperson of Dissertation Committee

Date

Steven R. Terrell, Ph.D.
Dissertation Committee Member

Date

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

Date

Approved:

Amon B. Seagull, Ph.D.
Interim Dean, College of Engineering and Computing

Date

College of Engineering and Computing
Nova Southeastern University

2015

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

Designing an effective information security policy for exceptional situations in an organization: An experimental study

By
George S. Antoniou

November, 2015

An increasing number of researchers are recognizing the importance of the role played by employees in maintaining the effectiveness of an information security policy. Currently, little research exists to validate the relationship between the actions (behaviors) taken by employees in response to exceptional situations (antecedents) regarding an organization's information security policy, the impact (consequences) those actions have on an organization, and the motives that prompt those actions. When these exceptional situations occur, employees may feel compelled to engage in behaviors that violate the terms of an information security policy because strict compliance with the policy could cause the organization to lose revenue, reputability or some other business advantage. To address this issue, this research study investigated how to design an effective information security policy for exceptional situations in an organization. In order to achieve this goal, this study explored how an information security policy should be designed with the critical components of clarity, comprehensiveness, ease of use and flexibility, in addition to including provisions for the work contingencies of employees. The aim of this proposed study was to demonstrate how the application principles of the prima-facie, utilitarian and universalizability design theories can aid in designing an information security policy that includes these essential elements. The research study explored the effectiveness of the policy's design and the effect it had on employee compliance with the policy in exceptional situations. A survey questionnaire was administered to a control group and an experimental group consisting of full-time and part-time employees who worked in various departments of a single organization. The survey employed a five-point Likert-type scale. The data gathered from the questionnaire was analyzed. Inferential statistics used the general linear model (GLM), including the *t*-test, analysis of covariance (ANCOVA), regression analysis, and factor analysis with the latest SPSS version computer statistical analysis program. This study built to develop a model for designing an effective information security policy for exceptional situations in an organization. Based on the analysis of fit the model for designing an effective information security policy for exceptional situations in an organization was determine to be a success model. This study should provide many opportunities for future research, as well as providing information security practitioners and academics a solid roadmap for designing effective information security policies within an organization to apply during exceptional situations.

Acknowledgements

I would like to express my gratitude to my advisor and dissertation committee chair, Dr. Tejay, for his guidance and encouragement from inception to completion of this dissertation.

In addition, I'm extremely thankful to Dr. Terrell and Dr. Littman, my dissertation committee members, for their feedback, suggestions and tough questions, which helped increase the quality of my research work.

I am grateful to my management, co-workers and friends for their continuous support and friendship, which has given me the confidence to complete the dissertation report.

Further, I express my gratitude to the participants of my study. With their input I was able to collect data for my dissertation report.

Throughout my doctoral program, my family has been a constant source of support. Special thanks to my wife Laura and to my three daughters, Talia, Ariana and Alexi, for the patience and understanding while I was studying until the wee hours or reading during their cheerleading, football, hockey practices and games. Thank you for your understanding, unconditional love and support.

Although not with us today, I give special thanks to my younger sister Nicki, my father Stasi and my parents-in-law, Ken and Pat, for believing in me.

Special thanks goes to my sister-in-law Lisa. You acted as my sounding board and provided valuable advice, help, and laughs as the "grammar-police."

Table of Contents

Table of Contents	3
List of Tables	5
List of Figures.....	6
Chapter 1	7
Introduction.....	7
1.1 Background.....	7
1.2 Research problem and argument	11
1.3 Importance of research problem	15
1.4 Definitions of Key Terms.....	19
Chapter 2	21
Review of the Literature.....	21
2.1 Introduction	21
2.2 Challenges faced by organizations.....	23
2.3 Information security policy approaches.....	25
2.4 Information Security Standards, Policies, and Guidelines.....	28
2.5 Developing and implementing an information security policy	30
Chapter 3	34
Research Methodology	34
3.1 Introduction	34
3.2 Theoretical Basis	36

3.3	Hypotheses	38
3.4	Research Design.....	43
3.5	Phases 1 and 2 – Awareness of Problem and Suggestion.....	51
3.6	Phase 3 – Artifact Development.....	52
3.7	Phase 4 – Evaluation	58
3.7.1	Sample population.....	59
3.7.2	Study instrument.....	61
3.7.3	Data Analysis	63
3.7.4	Analysis Procedures	64
3.7.5	Methods of Analysis.....	66
3.7.6	Internal and External Validity.....	68
3.7.7	Results	70
3.8	Phase 5 – Conclusion.....	71
3.9	Miscellaneous.....	71
3.9.1	Limitations	71
3.9.2	Delimitations.....	73
	Chapter 4	74
	Results of repeated measures ANOVA Analysis.....	74
4.1	Introduction	74
4.2	Data Preparation	74
4.3	Demographic Findings.....	75
4.4	Findings.....	77

4.5	Summary	81
	Chapter 5	82
	Conclusion	82
5.1	Introduction	82
5.2	Findings - Contributions.....	82
5.3	Implications.....	84
5.4	Limitations	85
5.5	Recommendations for future research.....	86
5.6	Conclusion.....	86
	Reference	89
	Appendix A.....	100
	Appendix B.....	101
	Appendix C.....	104

List of Tables

Table 1. Design-science research guidelines (Hevner et al., 2004, p. 83)	47
Table 2. Two groups, A & B, pre-test, post-test.....	60
Table 3. Likert scale with a five-point range (reverse order descriptor).....	63
Table 4. Threats to Internal Validity (Campbell & Stanley, 1963)	69
Table 5. Threats to External Validity (Campbell & Stanley, 1963)	70
Table 6. Gender Distribution.....	75
Table 7. Age Distribution	76
Table 8. Education Level Distribution	76

Table 9. Security Certification Distribution.....	77
Table 10. Cronbach’s alpha	78
Table 11. Paired Samples Test.....	79
Table 12. H1 Prima Facie.....	79
Table 13. H2 Utilitarian.....	80
Table 14. H3 Universalizability	80
Table 15. Hypotheses Results.....	81

List of Figures

Figure 1. Research model.....	42
Figure 2. The general methodology of design research Kuechler and Vaishnavi (2008). 50	
Figure 3: Prototyping (based on Sommerville 2007, p. 411).....	53
Figure 4. Design science research framework (Adapted from Hevner et al. 2004 p. 80). 55	

Chapter 1

Introduction

1.1 Background

As the electronic storage of information grows increasingly prevalent because of advancements in technology, the need for organizations to develop and utilize modernized methods and systems to protect the confidentiality, integrity and availability (CIA) of their information assets also continues to escalate. Electronically stored information is susceptible to a host of new cyber threats from both insiders and outsiders (Dunkerley & Tejay, 2009). However, information security specialists generally agree that the establishment and implementation of an information security policy is one of the most essential factors in safeguarding an organization's information assets (Da Veiga, & Eloff, 2010; Dzazali, Sulaiman, & Zolait, 2009; Eloff, J., & Eloff, M., 2005; Parker, 1997; Straub, 1990; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; Warman, 1992). Increasingly, researchers (Siponen, & Vance, 2010; Siponen, Pahlila, & Mahmood, 2010; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; Knapp, Morris, Marshall, & Anthony, 2009; Bulgurcu, Cavusoglu, & Benbasat, 2010) recognize the importance of the role played by employees in maintaining the integrity and effectiveness of information systems (IS) security policies (Puhakainen & Siponen, 2010; Karjalainen & Siponen, 2011), particularly in the case of exceptional situations (Siponen & Iivari, 2006).

The issue of employee noncompliance with an information security policy is strongly related to the sociability of human nature (Bulgurcu, Cavusoglu, & Benbasat, 2009; Mitnick & Simon, 2002; Renaud, 2012). As determined by Scott, Laurie, Angermeier, Raymond, and Boss, (2009) as well as Bosworth and Kabay (2002), an information security policy induces employees to contemplate their views about their obligation to follow the terms of the policy in order to secure and safeguard the information assets of an organization. Organizations that try to compel reluctant employees to accept and obey an inflexible information security policy are likely to be met with opposition. The reasons for this opposition are because a rigorous policy tends to complicate an employee's tasks and because it is human nature for an individual to rebel when he or she feels coerced or pressured. Consequently, employees should be able to easily understand and follow a clear, flexible and comprehensive information security policy. Depending on the factors related to clarity, comprehensiveness and ease of use that an organization takes into account during the policy's development, employees may regard the policy as either a meaningless show of authority or a manifestation of their personal ideals and beliefs (Cavallari, 2011; D'Arcy, & Hovav, 2007; Smith, Winchester, Bunker, & Jaimeson, 2010; Workman, & Gathegi, 2007).

Although some information security policies may prove reliable in maintaining the integrity of sensitive data under a routine state of affairs in the work environment, many organizations face the challenge of designing and enforcing an information security policy that employees can follow during exceptional situations. An exceptional situation is defined as an unforeseen business proposition or prospect that arises in organizations

with a fluctuant and variable outlook and that may entail employees to violate an information security policy in order to promote the welfare of the organization (Siponen & Iivari, 2006).

Because of the rapidly evolving nature of today's corporate world, it is growing more and more common for organizations to operate in a continual state of flux as new technological and social concerns and circumstances steadily arise (Tidd & Bessant, 2011; Alaa, 2009; Patel, Eldabi, & Khan, 2010). According to Houry, (2012), these emergent organizations are more likely to encounter exceptional situations than businesses whose future outlook is generally stable (Alatalo, Oinas-Kukkonen, Kurkela & Siponen, 2002; Baskerville & Siponen, 2002; Kingsford, 2008; Truex, Baskerville & Klein, 2001). When these exceptional situations occur, employees may feel compelled to engage in behaviors that violate the terms of an information security policy because strict compliance with the policy could cause the organization to lose revenue, reputability or some other business advantage (Siponen & Iivari, 2006). However, despite an employee's favorable intentions, the outcome of his or her decisions may not always be advantageous for the organization.

An organization can be defined as a business of any type and may range in size from small to large. Although some organizations are more likely to encounter unpredictable occurrences than others, the information assets of a sole proprietorship or a conglomerate are both exposed to the same risks based on the actions of the employees in regard to an information security policy when an exceptional situation does occur. For this reason, an information security policy that accounts for the possibility of exceptional

situations is important for all organizations (Hedström, Kolkowska, Karlsson, & Allen, 2011; Siponen, Willison, Baskerville, 2008; Willison, & Warkentin, 2013).

In essence, an information security policy is a product of how both people and systems are organized and managed (Warkentin & Willison, 2009; Baskerville & Siponen, 2002). As such, organizations need to carefully consider the design process of the information security policy and to thoroughly evaluate the policy's clarity, comprehensiveness, flexibility and ease of use to aid employees in following its terms when they are presented with exceptional situations. Therefore, it is crucial for organizations to understand the behaviors and motives of employees who intentionally ignore or disregard the information security policy in exceptional situations, potentially placing personal and organizational information at risk.

The design and provisions of an information security policy may vary depending upon the nature of a particular organization or department. For instance according to Doherty, Anastasakis and Fulford, (2009), governments, large corporations, small businesses and universities are each likely to produce distinct information security policies that are suitable for their particular business requirements. Similarly, unique policies may be required by an organization's various departments, such as human resources, sales, communications, marketing, accounting, customer, and information technology. In addition, the stipulations in an information security policy can range from highly detailed to loosely structured. One rule may explicitly inform an employee of the various steps to take or to avoid in order to prevent a breach of security while another rule provides only a broad observation of the risks and penalties of noncompliance.

These penalties or sanctions have the ability to influence the decisions that employees make about complying with the terms of an information security policy. When faced with an exceptional situation, some employees may choose to strictly comply with an information security policy if they feel that their job security is at risk, even if they believe that violating the information security policy is in the best interests of the organization.

1.2 Research problem and argument

The research problem was to investigate how to design effective information security policies for exceptional situations in an organization. Employees need guidance to make a decision to follow or violate an information security policy when faced with exceptional situations. An effective information security policy should be clear, comprehensive, usable, and flexible enough to accommodate a wide range of data, activities, and resources. It should also be designed to provide employees with guidance on how to handle unexpected or uncommon situations or incidents that may occur in the workplace. A poorly designed information security policy may provide inadequate protection for sensitive data or cause employees to take actions that are detrimental to the organization (Herath & Rao, 2009). As stated by Herath and Rao, various factors play a role in determining an employee's willingness to observe or abuse the terms of an information security policy, including intrinsic and extrinsic incentives and penalties, the social acceptability of a given behavior, and personal beliefs. Employees are far less likely to comply with an information security policy that is not clear, comprehensive,

flexible, and easy to understand and use. Besnard and Arief (2004) asserted that the interaction between employees and computers should play a more significant role in the design of an information security policy. Additionally, Workman, Bommer, and Straub (2008) argued that IS specialists still struggle with the issue of how to effectively apply an information security policy. Based on the research results of Workman, Bommer, and Straub, the primary reason for this struggle was because of the flaws in the methodologies used in the majority of studies that have analyzed and examined the issue of employee compliance. An information security policy should allow employees to easily comprehend, follow and observe its terms in order to assist them in making the appropriate decisions, regardless of their experience, intelligence or skill level.

An information security policy should be effective and sustainable in an organization. As indicated by Siponen, Baskerville, & Heikka, 2006, an organization can help to increase the soundness of its information security program through the design and development of an information security policy that is clear, comprehensive, flexible and usable. After implementing such a policy, an organization should regularly examine, appraise and address any differences that subsequently occur in the security of its information assets (Milicevic, & Goeken, 2010). Milicevic and Goeken stated that these periodic assessments and revisions can help an organization to ascertain if stages of rapid adjustments in its structure or proceedings impact the effectiveness of its information security policy.

The research argument was that an effective information security policy should be clear, comprehensive, flexible and usable and should take into account the work

contingencies of the employees of an organization. An information security policy requires a design process and application principles that focus on clarity, comprehensiveness, flexibility and usability, particularly in regard to guidelines for handling exceptional situations. This type of policy is more effective in maintaining the confidentiality, integrity and availability of an organization's information assets (Siponen & Iivari, 2006).

An information security policy should be flexible. The security of an organization's information assets is jeopardized to varying degrees whenever an employee fails to comply with an information security policy. The reasons that employees violate the terms of an information security policy are complex and varied (Herath & Rao, 2009). According to Herath and Rao, a combination of social, economic and psychological factors affect an employee's decision-making process when contemplating whether to comply with or ignore the terms of an information security policy. In addition, employees may unintentionally violate the policy because they are not aware of its terms. However, of greater concern to practitioners are those instances in which an employee knowingly violates an information security policy, even if it is not done with malicious intent (Warkentin & Willison, 2009). An employee may feel that complying with the policy is too time-consuming, pointless or complex. These security breaches are especially liable to occur when an employee encounters an exceptional situation that necessitates a swift response (Siponen & Iivari, 2006). A degree of flexibility in a policy gives employees the opportunity to make choices based on response

time, client satisfaction, data security and other factors that are in the best interests of the organization.

An information security policy should take into account the work contingencies of the employees of an organization. A classic professional in the field of information systems security, Desman (2001) argued that the effectiveness of information security relies more on human factors than on technological factors. Similarly, other long-standing industry authorities such as Gaunt (2000), as well as more contemporary experts (Puhakainen & Siponen, 2010), agree that the issue of employee compliance is one of the greatest risks to the safety of an organization's information assets. Furthermore, the failure of an information security policy to take into account the risks presented by exceptional situations or the dynamics that influence an employee's behavior under these circumstances increases the probability of insider threats. Without any guidelines to follow when exceptional situations arise, an employee is liable to take actions that compromise the CIA of an organization's data or cause the organization to miss out on lucrative business prospects (Siponen & Iivari, 2006). As stated by Hadasch, Maedche and Mueller (2011), an employee can compromise the CIA of an organization's information assets with even one careless misstep while carrying out his or her daily job functions. However, an information security policy must also enable employees to perform their prescribed duties in a methodical, efficient and timely manner in order to remain cost efficient (Bulgurcu, Cavusoglu, & Benbasat, 2010; Pahnla, Siponen, & Mahmood, 2007).

An information security policy should be usable. If employees do not comply with an information security policy, the safety of the organization's information assets may be compromised. Oftentimes, employees feel that certain procedures in an information security policy hinder their ability to complete daily work tasks in a timely manner (Siponen & Iivari, 2006; Siponen & Vance, 2010). This mindset or belief is due in large part to the fact that an information security policy is too complex, rigid, unsound or time-consuming to obey. The issue of employee noncompliance with an information security policy is of fundamental importance to organizations and their information security experts. According to Desman (2001), the behaviors and attitudes of people are more closely intertwined with the field of information security than are technological or procedural matters (Desman, 2001; Shin, 2010). Consequently, an organization's workforce poses the greatest threat to its information security (Gaunt, 1998; Warkentin, & Willison, 2009).

1.3 Importance of research problem

Currently, little research exists to validate the relationship between the actions (behaviors) taken by employees in response to exceptional situations (antecedents) regarding an organization's information security policy, the impact (consequences) those actions have on an organization, and the motives that prompt those actions. As stated by Siponen and Iivari (2006), current studies overlook these important relationships. One of the most crucial links to examine in this chain was the connection between employees'

actions and the justifications that caused the employees to behave in such a manner. Once understood, the correlation between these factors may assist an organization in designing and implementing an information security policy that is more conducive to effectively resolving exceptional situations, resulting in more favorable consequences for the well-being of an organization's information assets. As stated by Dunkerley and Tejay (2009), if an organization is aware of its risk factors and takes appropriate measures to alleviate them, it can expedite the handling of its business transactions and affairs.

Bostrom, Gupta and Thomas (2009) argue that it is ill-advised for any organization to adopt an IS theory that disregards or underestimates the importance of the human element in regard to the security of the organization's information assets. Employees are far less likely to comply with an information security policy that is complicated and unyielding.

However, in order for an information security policy to gain general approval from management and staff, an organization needs to consider the opinions, suggestions and ideas of its employees during the policy's design process (Gaunt, 2000). This enables the organization to create an information security policy with content that is clear, comprehensive and understandable. Employees can also provide valuable recommendations on how to develop information security procedures that can prove beneficial in handling exceptional situations. Numerous researchers support the belief that employee participation is essential, claiming that human behavior is among the top three concerns of an organization for enhancing the security of its information security

policy (Dhillon & Backhouse, 2000; Dutta & McCrohan, 2002; Hitchings, 1995) by providing employees with a sense of ownership for their input.

Information security breaches caused directly by the failure of employees to comply with an information security policy represent a growing concern for organizations (Stanton, Stam, Mastrangelo, & Jolton, 2005). As the demand for confidentiality and discretion in business matters continues to increase along with the pace of technological advancements, so too does the competitiveness among organizations to develop reliable information security policies. Therefore, an organization that gains a trustworthy reputation for consumer privacy also gains a distinct strategic advantage over its competitors, thereby amplifying the significance of an effective information security policy and making it a necessary foundation for the success of an organization.

As noted by D'Arcy, Hovav, & Galletta, (2009), between 50 to 75 percent of information security problems in an organization are associated with the factor of human involvement. However, this recognition gives researchers and practitioners no insight into the dynamics that cause or motivate employees to breach an information security policy. It is not clear whether the breaches are accidental, intentional or caused by information security policies that are inflexible and unclear, failing to provide employees with guidelines on how to handle exceptional situations. To address this lack of knowledge, Dutta and Roy (2008); Gonzalez and Sawicka (2002); Mishra and Dhillon (2006, June); Sawicka and Kopainsky, (2008, July); Stanton (2007); Van Niekerk and von Solms (2005) advocate the need for empirically based research studies that investigate the relationship

between the culture or milieu of an organization and its information system (IS), including the employees.

An information security policy is the underpinning that protects an organization's privileged data and secures the confidentiality of its employees' and clients' information. By inviting employees from various departments to participate in the design process of an information security policy, organizations can increase the likelihood of creating a policy that is easier for personnel to understand and follow and that helps to ensure employee compliance. Additionally, if organizations incorporate the flexibility and application principles of design theories into their information security policies, they can improve their probability of achieving a positive outcome in exceptional situations (Siponen & Iivari, 2006).

A widely held conviction is that the safety of an organization's information assets is dependent upon the implementation of an information security policy. However, developing a successful information security policy is a difficult undertaking that requires the consideration of many elements and dynamics (Karyda, Kiountouzis, & Kokolakis, 2005). Employees may occasionally violate an information security policy because they regard it as an impediment that obstructs their workflow. In fact, many organizations fail to achieve the objectives they have set with the execution of their information security policy (Karyda et. al, 2005). It is essential for an organization's information security experts to appreciate the significance of human involvement in relation to the success or failure of an information security policy and to consider design principles when developing information security policies for exceptional situations. More specifically,

these specialists need to comprehend how societal factors, such as the differences between cultures and generations, can impact the viewpoints, feelings and opinions that employees have toward complying with an organization's information security policy (Al-Awadi, 2010).

Despite the fact that organizations regard an information security policy as a necessity, the implementation of an information security policy cannot guarantee that an employee is going to obey it. Consequently, the purpose of this study was to address the impact that the information-security design process had on the employees' voluntariness (behavior) and the relationship between the policy's clarity, comprehensiveness, flexibility, usability and its effectiveness in exceptional situations.

1.4 Definitions of Key Terms

The terms that were used in this study are defined as follows.

Information systems are defined as the deployment of information technology to collect, process and disseminate information in organizations and society. Employees using information technology are an important aspect of an information system. Information systems include both technological components and the humans who use them to store, process and distribute electronic data (Avison & Fitzgerald, 1995).

Information Security is defined as “a well-informed sense of assurance that information risks and controls are in balance” (Anderson, 2003 p. 310). The goal of information

security is to protect business assets and reduce costs by avoiding security violations and reducing the negative effects they have on an organization.

Corporate business policy is defined as a set of diverse documents regarding an organization's business objectives and intent to address business-related issues and to provide guidelines to ensure that all decisions and activities are aligned with the defined strategies as part of corporate governance (Wheelen & Hunger, 2008). Policies dictate acceptable and unacceptable behaviors within an organization, including penalties for violation of the policy's terms (Knapp, Marshall, Anthony, 2009).

Information security policy is a written, living document outlining the actions and procedures that employees should follow in order to protect an organization's information security assets (Siponen & Iivari, 2006). According to Bulgurcu et al. (2010), an information security policy outlines the function and tasks of employees in order to protect an organization's information assets. Hone and Eloff (2002) suggest the information security policy should be short and easy to read.

Exceptional situations are defined as atypical circumstances that may arise in an emergent organization and cause employees to take actions that conflict with an information security policy (Siponen & Iivari, 2006).

Chapter 2

Review of the Literature

2.1 Introduction

One of the primary goals of an information security policy is to provide guidance to employees in an organization by decreasing its risk, safeguarding its critical information assets and lowering its expenditures for information security management (Shoraka, 2011). In addition to complying with all internal and external regulations and protocols, the policy should help to advance the structure and functionality of an organization's information system (Nigam & Siponen, 2011).

When stripped to its basic framework, an information security policy consists of the rules and procedures that employees are requested to follow in order to protect the private information of an organization and its clients. This framework is lent substance by comprehensiveness, clarity, a degree of autonomy, and adaptability to various situations. Ideally, the policy's construction is completed by an awareness of how human behavior can affect the manner in which that underlying structure is supported and vice versa. As argued by Dunkerley and Tejay (2009), it is critical to apprehend the behaviors of the people who utilize the information assets of an organization in order to create a successful information security policy. Conversely, a poorly designed document provides limited usability and voluntariness and may negatively affect the employees' willingness to comply with it. Consequently, the information security policy itself may pose an inside

threat to an organization if it is not well-designed because employees are more apt to misconstrue it or bypass its requirements, resulting in a state of noncompliance, which may subject confidential information to a breach of security (Sipior & Ward, 2008).

As concluded by many recent studies, the human element was the cause of many information security breaches (Herath & Rao, 2009; Lineberry, 2007; West, Mayhorn, Hardee, & Mendel, 2009). Therefore, information security professionals must realize that the success of an information security policy relies upon an understanding of the multifaceted nature of human beings as much as it does upon technological expertise (Soo Hoo, 2000). In addition, practitioners must identify how an employee's motives and level of freedom in making decisions about obeying or disregarding an information security policy are influenced by the circumstances surrounding an exceptional situation (Siponen & Iivari, 2006).

Although the use of an information security policy is widely advocated for protecting confidential data, few experimental studies investigated how the structure, phrasing and execution of a policy affect an organization (Verendel, 2009). Despite this lack of empirical research, indications strongly suggest that a versatile, functional and straightforward information security policy most effectively safeguards the confidential data of an organization (Bahtiyar, & Ufuk, 2012; Sun, Han, & Liu, 2008). Any type of breach or violation in an information security policy can be very costly and detrimental to an organization. Therefore, it is vital for any organization to invest its time and resources into designing an information security policy that diminishes this potential risk factor.

2.2 Challenges faced by organizations

In a study conducted by Cisco (2008), over 50 percent of employees acknowledged that they had knowingly violated the terms of their organization's information security policy and an average of nearly half of the employees at the various companies taking part in the study said that the reason they chose to violate the policy was based on the assumption that the risks associated with their transgressions were negligible. However, many organizations reported that employee abuse of information security policies resulted in negative consequences that cost them a significant amount of time and money to repair and led to the eradication or misappropriation of confidential data (Cisco).

Although a considerable number of studies focused on the issue of employee noncompliance, many organizations still face distinct challenges when developing an information security policy. According to Long (2002), some of these challenges include the level of satisfactory risk acceptance; variations in procedures among different departments as a result of the unique threats faced by each; the legal constraints placed on various business units according to their geographical location; personal viewpoints; and the values, philosophies and politics of different cultures. When the risk-management department of an organization implements an information security policy that covers all of the organization's branches and divisions (Soo Hoo, 2000; Spears, 2006; Wang,

Chaudhury, & Rao, 2008), it can decrease the possibility of jeopardizing the organization's information assets by positively influencing the actions of employees (Hadasch et al., 2011).

Baskerville and Siponen (2002) concluded that when an organization is experiencing rapid internal changes in its structure, it may enforce stringent safety measures that can restrict an employee's ability to retrieve or view sensitive data, essentially acting as an impediment that can pose a serious threat to the successful continuation of an organization. This dilemma impedes an organization's ability to grow and pressures organizations to produce information security policies that are contradictory and stringent. Oftentimes, the organizational changes made by a company are due to profitable business ventures that were unanticipated, possibly causing an organization to temporarily enforce procedures that are in opposition to the terms of its information security policy.

One of the most consequential problems faced by organizations, however, is that the view of reality held by the majority of people opposes some of the practices defined by an information security policy (Bosworth & Kabay, 2002). An employee might allow a colleague without the same level of credentials to view confidential documents simply because the two of them are working together on an assignment or might share a password based only on the fact that a co-worker is someone he or she trusts or likes. However, most information security policies are still effective to some degree in discouraging employee noncompliance (Straub & Nance, 1990), making them a necessary component of an organization's information security management system.

According to Siponen and Iivari (2006), organizations that deal with variable conditions on a regular basis are in particular need of employing an information security policy that is developed according to application principles. The use of application principles are effective in helping an organization to develop an information security policy that defines not only the actions and behaviors that employees are mandated or forbidden to perform during times of stability but also those that are considered reasonable and unreasonable in exceptional situations. In addition, they grant employees a measure of autonomy to use their own judgment in making a decision.

An information security policy needs to provide employees with a precise awareness of its objectives. It should also include well-defined explanations, examples and descriptions, in addition to specific details of an employee's expectations and obligations (Gaunt, 1998). An information security policy that is designed appropriately encourages and inspires an employee to contribute to an organization's aim of maintaining the security of its confidential information.

2.3 Information security policy approaches

Many researchers have published studies on different approaches to implementing an information security policy, including checklists and industry standards (BSI, 2012; GASSP, 1999), a virtual methodology (Hitchings, 1995) and a security-planning system (Straub & Welke, 1998). However, these studies largely failed to offer organizations any

pragmatic assistance on how to design the information security policy (Baskerville & Siponen, 2002).

Hone and Eloff (2002) agreed that an information security policy plays a role of central importance in any organization's information security division. Because an information security policy is oftentimes difficult to prepare and design, organizations may obtain ready-made policies or templates from a variety of sources, such as textbooks and the Internet. However, these policies are usually not industry-specific and may require modification in order to meet the needs of a particular organization. Baskerville and Siponen (2002) asserted that ready-made policies offer organizations little guidance with preparing a policy, which is a matter of greater importance than simply providing employees with a catalog of acceptable or unacceptable actions. Although some organizations have consultants or IS specialists to make these revisions, Bjorck (2004) stated that this does not necessarily solve the problem of properly implementing the information security policy, which employees and management may ignore, even if they are making an important business decision regarding information security. In addition, Von Solms (1999) asserted that some organizations may not proffer the funds to effectively employ an information security policy unless management believes that the value is worth the cost.

Recent ISO/IEC directives (2011) defined a normative element of an information security policy as one that states the boundaries of the policy or specifies its conditions. More specifically, these ISO/EIC procedures postulate terms and acceptable equivalents that an organization is required to use when denoting normative elements in an

information security policy that are not mandatory in exceptional cases. The terms indicated in Part 2 of the ISO/IEC Directives, which include “may,” “need not” and “can,” are intended to give employees a degree of independence and direction when making choices on the actions to take in exceptional situations.

However, the effectiveness of these procedures is criticized for a number of reasons. Some of these reasons are that the procedures are too broad and hypothetical for a particular organization or marketplace, require managers to dedicate ample time to scrutinizing and enhancing their effectiveness, and do not place emphasis on increasing customer satisfaction. In addition, it is argued that ISO 9001 focuses more on the regulations and guidelines of an information security policy than on providing employees with insight on how to interpret those procedures (Seddon, 2000). Both ISO 9000 and 9001 are criticized for presenting organizations with a registration process that is both laborious and costly (Clifford, 2005). Consequently, the need to design an information security policy that takes into account an employee’s motivations and provides guidance for an employee on how to construe the terms of the policy, particularly in exceptional situations, remains a relevant issue for organizations.

Many current researchers also advocate executing information security policies that prohibit improper use of IS data, equipment and processes in order to decrease the risks presented by employees (Hadasch et al., 2011). These studies helped to clarify some of the factors that can influence employee compliance with an information security policy, including an understanding of the risks of noncompliance with protective technologies (Dinev & Hu, 2007; Herath & Rao, 2009; Liang & Xue, 2010), the real or

perceived intrinsic and extrinsic benefits and motivations of compliance versus noncompliance, such as self-efficacy, ease of use, organizational support, deterrents and social stimuli (Bulgurcu et al., 2010; Liang & Xue; Pahnla et al., 2007; Siponen & Vance, 2010) and the reluctance to make inappropriate use of an organization's information security assets (D'Arcy, Hovav, & Galletta, 2008; Johnston & Warkentin, 2010). However, these studies largely failed to provide information security specialists with specific advice on how to design an information security policy, especially one that was effective in helping employees to resolve exceptional situations (Siponen & Iivari, 2006).

2.4 Information Security Standards, Policies, and Guidelines

According to Vroom and von Solms (2004), not all employees' violations of information security policies are carried out with intentional or malicious intents. The violations can be the result of negligence, a lack of understanding, clarity or comprehensiveness, or ignorance of the security policies of the organization. Some standards exist to address such violations and to specify how they can be avoided in organizations.

In order to help universalize technology-based regulations, some organizations regularly publish updated standards and guidelines in order to help universalize the methods of maintaining and promoting information security management systems (ISMS), in addition to other technologies. The SANS Institute (Smith, 2004) and the International Organization for Standardization (ISO) ISO/IEC 27000 recommended the

application of an information security policy that is adaptable and allows for exceptions to the rules based on unique circumstances.

Although interest in IS security has increased in recent years, very few empirical studies examined how designing information security policies for exceptional situations can benefit organizations. ISO 27000 suggests that an organization needs to continually update and revise its information security policy to ensure that it remains clear, comprehensive, easy to use and appropriate to the organization's specific business objectives and strategic goals. Again, this information failed to provide organization with assistance on how to develop and implement an information security policy that incorporates these elements and is easily understood by employees, especially regarding exceptional situations.

Existing literature agrees that employees who have malicious intent or who do not comply with an information security policy under normal conditions are the main threat to an organization's information assets. However, there are also many instances in which an employee violates an information security policy in the belief that his or her decision to do so is more advantageous to the organization than complying with the policy (Siponen & Iivari, 2006; Siponen & Vance, 2010). In today's swiftly advancing technological environment, it is not uncommon for clients to request last-minute changes or modifications to a product or service they are obtaining from an organization. With little time to prepare for these adjustments, employees may need to temporarily violate information security policies in order to accommodate a client's needs. Therefore, it is critical for organizations to analyze the reasons and justifications that motivate

employees to obey or ignore information security policies in exceptional situations and the effect of the employees' actions on all parties involved in the business transaction.

2.5 Developing and implementing an information security policy

An information security policy safeguards the confidentiality, integrity and availability of an organization's paper and electronic documents and the privacy of clients, personnel and the company in its entirety from various threats and hazards (Da Veiga, Martins, & Eloff, 2007). Consequently, information security policies are usually designed as "living documents." A living document is one that is revised and expanded over time. This type of document is particularly suited for an information security policy because of the rapid technological, procedural and business changes that are made in today's world (Von Solms & Von Solms, 2004).

Initially, surveys based on ad hoc theories or empirical analyses were the primary methods of gathering data from an organization's workforce by IS researchers evaluating the issue of employee compliance with an information security policy (Hu, Xu, Dinev, & Ling, 2011). As of late, however, IS researchers are recognizing the growing importance of examining this concern through the lens of more established theories (D'Arcy et al., 2008; Dinev & Hu, 2007; Siponen, 2000).

As previously stated, an organization may face the challenging issue of human involvement when developing and implementing an information security policy. The success of many of the procedures in an information security policy often relies upon the

compliance of an organization's employees. Analyzing and evaluating the effectiveness of such procedures is possible only if the actions taken by humans are assessable and subject to persuasion and if the organization encourages compliance by rewarding positive behaviors and penalizing negative behaviors (Siponen, Pahnla, & Mahmood, 2010).

According to Liang and Xue (2010), it is critical to understand the impact that an individual working in a socio-technical environment can have on the security of an information system. The socio-technical theory recognizes two distinct yet interrelated subsystems that operate in most organizations: a technical subsystem made up of equipment, techniques and processes and a social system made up of employees and their skills, expertise, viewpoints and principles (Bostrom et al., 2009). Recent IS security studies are placing increased focus on how individual employees can negatively or positively impact the security of an organization's information assets in a socio-technical work setting (Liang & Xue).

The design theories proposed by Siponen and Iivari (2006) offer an effective solution to this problem because their application principles are intended to account for the factor of human involvement. In addition, Siponen and Iivari offered pragmatic advice to researchers and scholars on how to gather empirical evidence to design a policy that can aid employees with taking the appropriate actions in exceptional situations, including those cases that present a conflict between achieving an organization's business objectives and strictly complying with the information security policy. When integrated into an information security policy, these design theories promote employee compliance

by informing employees of the circumstances, justifications and causes that are acceptable or unacceptable in regard to violating the policy's terms without fear of punishment or reprisal.

Depending on an employee's intrinsic motivations, achieving the goal of the application principle itself may prove rewarding. According to Beswick (2002), some individuals feel a sense of gratification or fulfillment if their actions or accomplishments endorse their sense of self-worth or support their ethical or moral beliefs. An employee may feel satisfaction if his or her violation of an information security policy based on the utilitarian design theory brings happiness to the greatest amount of people in an exceptional situation. In addition, information security policies that utilize the prima-facie, utilitarian and universalizability design theories can be tested empirically to evaluate their effectiveness (Siponen & Iivari, 2006). Therefore, these design theories are a practical alternative for organizations seeking to devise an effective information security policy.

According to Siponen and Iivari (2006), the two fundamental features that should be incorporated into an information security policy during its design process are adaptability and ease of use, in regard to both terminology and application. These elements help to increase the likelihood of employee compliance.

Although Siponen and Iivari (2006) do not address the process of meta-design, their theoretical models for the prima-facie, utilitarian and universalizability design theories contain all the standard elements of a meta-policy. According to Baskerville and Siponen (2002), a meta-policy focuses on the development of an information security policy as well as its flexibility, application and validity. In addition, it is created to

expedite revisions to procedures in an information security policy that contradict the business objectives of an organization as it continues to grow and evolve (Baskerville & Siponen). Baskerville and Siponen argue that information security policies based on traditional checklists and universal standards, such as those issued by the ISO, are less effective than meta-policies because they are too generalized to apply to the distinctive culture of individual organizations.

Information security policies that contain standard normative procedures cannot adequately stipulate actions or processes to resolve every conceivable circumstance that may arise in an exceptional situation (Siponen & Iivari, 2006). However, Siponen and Iivari argued that employees can effectively resolve a broad spectrum of exceptional situations if an information security policy is designed with the following three elements: a kernel theory basis; application principles from that kernel theory specifying how employees should manage exceptional situations; and hypotheses that can be tested. As defined by Siponen and Iivari, testable hypotheses denote an organization's intention to develop a research agenda to assist in advancing the continued analysis of information security policies.

Chapter 3

Research Methodology

3.1 Introduction

The research methodology was based on the framework proposed by Hevner, March, Park and Ram (2004), which emphasized the design-science aspect of IS research while recognizing that this approach is inextricably linked to the behavioral-science paradigm. The researcher followed the design science approach (Hevner et al.) to answer the following research question: "Does adopting the prima-facie, utilitarian, and universalizability normative theories help organizations to design an effective information security policy in exceptional situations?". The goal of design science is to offer innovative and applicable organizational solutions in the form of design artifacts to help resolve a problem domain's challenges and obstacles (Hevner et al.). As stated by Hevner et al, design science in the realm of information technology (IT) is ultimately intended to solve issues related to the development, application and execution of information systems by creating a unique and effective artifact that provides an organization with practical benefits.

An artifact is described as an instantiation, model, construct or method that is used to produce or employ one or more components of an information system other than those involving the constituents that make up a particular organization, including its

culture, employees, structure and commercial practices (Hevner et al., 2004). Although the paradigm of design science is an indispensable factor in the formation of an IT artifact, these distinctive characteristics of an organization still play an integral role in the crafting and executing of an operative information system (Hevner et al., 2004).

The artifact of this study was an information security policy. A method to design and implement an information security policy that it is effective in resolving exceptional situations in an organization was developed and evaluated to achieve this goal. According to Hevner et al. (2004), the success of a design science research project involving an IT artifact relies upon a thorough evaluation of the artifact's value, effectiveness, comprehensiveness and dependability in the context of the specific organization that it is designed to benefit. Hence, the utility and efficacy of IS design theories are established by evaluating their outputs: design artifacts.

Researchers must assess a design artifact to establish its usefulness, effectiveness and merit. The goal of the design artifact evaluation is to show that the proposed artifact provides value to the problem domain. If the artifact evaluation reveals that a design artifact meets the problem domain's requisites and restrictions, the researcher is able to confirm that the design theory is complete and effective. This study used an experimental method to evaluate the efficacy of an information security policy based on the prima-facie, utilitarian and universalizability design theories in resolving exceptional situations in an organization.

3.2 Theoretical Basis

The theoretical basis for the study followed Siponen and Iivari's (2006) prima-facie, utilitarian and universalizability design theories to achieve the goal of designing and implementing an information security policy that helps employees to effectively resolve exceptional situations in an organization. These are normative theories that account for the factor of human involvement by providing employees with guidance on the appropriate actions to take in exceptional situations, particularly those cases that present a conflict between achieving an organization's business objectives and strictly complying with the information security policy (Siponen & Iivari, 2006).

The prima-facie theory, developed by Ross (2003), purports that a person's actions are acceptable if the good that results from taking those actions is greater than the good that results from not taking them. From an IS security perspective, this means that if an employee violates the terms of an information security policy in an exceptional situation, those actions are acceptable as long as they prove more beneficial to an organization than if the employee had adhered to the terms of the policy.

The utilitarianism and other normative theories form the most suitable basis for the development and application of information security policies that account for the possibility of exceptional situations and the actions that people should take when adhering to the standard would have deleterious effects (Siponen & Iivari, 2006).

Conceived by Kant (2002) in 1785, the moral philosophy of universalizability states that an action or behavior is morally just if the maxim on which it is based could be

universally accepted. Although based on this premise, Siponen and Iivari's (2006) universalizability design theory recognized varying degrees of universality. Their theory consists of two sub-theses—impartial and security partial—that act as the application principles for an information security policy (Siponen & Iivari, 2006). The impartial universalizability thesis stipulates that an employee is permitted to take an action if any other worker in the organization is granted that privilege under comparable circumstances, and the security partial universalizability thesis requires an employee to contemplate if the organization's president or information security manager would permit any responsible employee to take the action in question (Siponen & Iivari, 2006). Based on these theories, this study intended to confirm that an information security policy can effectively resolve information security conflicts that arise in exceptional situations if the policy affords employees the possibility of taking actions that violate its terms on the condition that these actions are more universally acceptable than taking actions that comply with its terms.

As argued by Siponen and Iivari (2006), philosophical normative theories can provide organizations with some understanding of the conditions and motives that cause employees to violate normative information security policies in exceptional circumstances and aid practitioners in the design and implementation of an information security policy that helps employees to effectively resolve contingencies in the workplace. According to Warman (1992), normative standards of an information security policy specify how employees should or should not handle certain situations involving the CIA

of an organization's information assets. In contrast, non-normative standards are informational or explanatory in nature (Krupansky, 2005).

However, Siponen and Iivari (2006) pointed out that empirical research needs to be conducted in order to determine (a) if employees choose to violate or to observe an information security policy in exceptional situations; (b) how employees justify their decisions based on the application principles of the design theories; (c) the degree of influence those motivating factors have on the actions taken by employees. The results of these findings will contribute to the body of extant knowledge that endeavors to remedy the challenge of human involvement in the crafting and administering of an information security policy, particularly in organizations where exceptional situations regularly generate conflicts with an organization's business goals and objectives.

3.3 Hypotheses

The following hypotheses were adapted from Siponen and Iivari's (2006) testable design product hypotheses for designing application principles to cover exceptional situations in an organization's information security policy based on the prima-facie, utilitarian or universalizability design theory. The hypotheses for this study focused primarily on turbulent organizations with a rapidly changing business environment (Siponen & Iivari, 2006). According to Siponen and Iivari (2006), these organizations were much more likely to encounter exceptional situations that may require an employee

to violate the terms of an information security policy in order to support the organization's best interests.

Moore and Benbasat (1991) argued that an individual's perceived qualities of an information technology (IT) innovation (method, process, procedure, etc.) are a more reliable indicator of his or her subsequent behaviors than the actual characteristics of that innovation. Therefore, voluntariness refers to an employee's perception of his or her freedom of choice in complying with or violating an information security policy's terms. The voluntarism is a common construct in all three normative theories and included in all hypotheses to show the impact of voluntariness on the acceptance of policy.

Effectiveness indicates the success of an information security policy in persuading an employee to take the actions that provide the greatest intrinsic and extrinsic benefits to an organization, its employees and clients, and the individual performing the actions.

Net benefits denote the business advantages gained by an organization, not including any egocentric gains to the individual performing the actions. Net benefits are the application principle in the prima-facie design theory by Siponen and Iivari (2006), which was based on the prima-facie ethical theory of Ross (2003). Based on the premises of this theory, it is expected that the research experiment validated that an information security policy can effectively resolve information security conflicts that arise in exceptional situations if the policy grants employees the liberty of compromising its guidelines when the benefits of doing so are greater than the benefits of compliance.

The prima-facie design theory allows for violations of the terms of an information security policy in exceptional situations if the benefits expected to be gained by noncompliance outweigh those expected to be gained by compliance.

- H1: If the employees' voluntarism and the expected benefits of noncompliance increase, then an organization will experience fewer consequences in response to employee noncompliance in exceptional situations.

The philosophy of utilitarianism developed by Bentham (1907) is based on the moral foundation of behaving in a manner that provides the most utility, or happiness, and the least amount of pain to the greatest number of individuals. Siponen and Iivari (2006) adapted this philosophical theory to their utilitarian design theory, which promotes taking the actions that spread happiness to the greatest number of individuals involved in a business transaction. This approach provides employees with some latitude in taking actions that violate an information security policy if the anticipated effects of the actions are more advantageous to the organization than the anticipated effects of the actions produced by complying with the policy (Siponen & Iivari, 2006). Consequently, it is expected that the quasi-experimental study revealed that an information security policy can effectively resolve information security conflicts that arise in exceptional situations if the policy gives employees the option of contradicting its terms in order to adhere to security objectives that profit the greatest number of individuals involved in a business transaction.

- H2: If the employees' voluntarism and happiness of noncompliance increase, then an organization will experience fewer consequences in response to employee noncompliance in exceptional situations.

The utilitarian design theory states that employees should obey the terms of an information security policy under standard conditions but that the terms may be violated if the number of people who profit from overall adherence to security objectives by this action is greater than the number of people who do not profit.

The universalizability design theory states that employees should obey an information security policy in ordinary situations. In exceptional situations, however, they may follow one of the theory's two sub-theses.

- H3: If the employees' voluntarism and universalizability of noncompliance increase, then an organization will experience fewer consequences in response to employee noncompliance in exceptional situations.

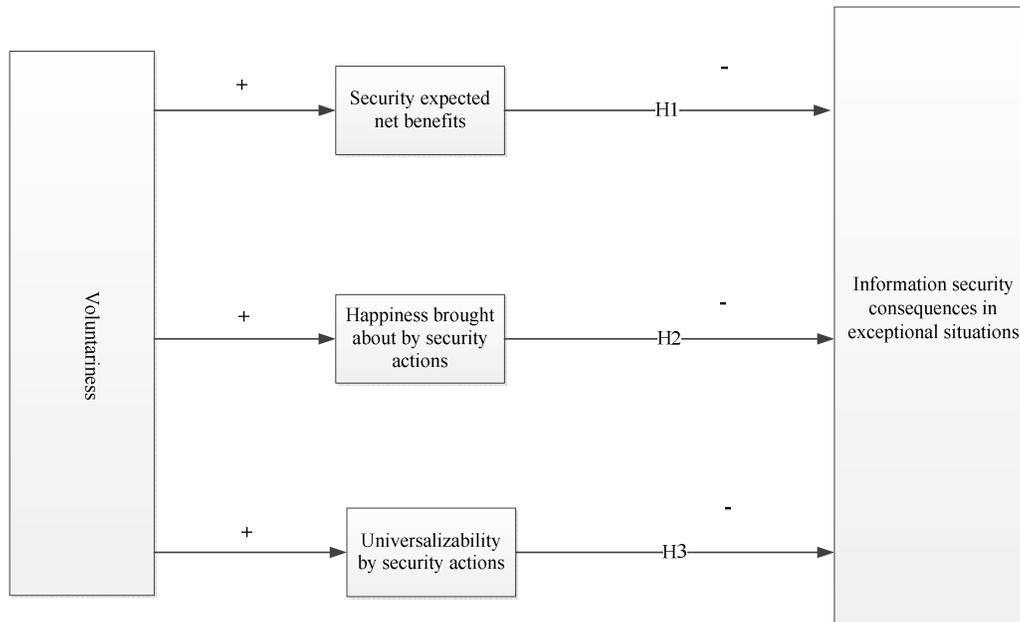


Figure 1. Research model.

Adapted from Siponen and Iivari's (2006) "Six Design Theories for IS Security," Figure 1 illustrates the dynamics that account for an information security policy that is successful in exceptional situations. According to Siponen and Iivari (2006), the "success" of a policy is defined in terms of the positive information-security consequences (dependent variable) that result from an employee's actions in exceptional situations based on the independent variables. The minus sign following a hypothesis indicates if this theorized association is expected to minimize the dependent variable. The plus signs following the independent variables in Figure 1 indicate if those variables have an interactive relationship with the dependent variable. For example, H1 illustrates that as the voluntariness and expected benefits of an action increase, there is a

corresponding rise in the probability that an organization will experience positive consequences in response to employee actions in exceptional situations.

The dependent variable in this study was the consequences of an employee's actions on the information security of an organization, and the independent variables were the unique application principles of the prima-facie, utilitarian and universalizability design methods, along with the degree of voluntariness an information security policy allowed an employee. The application principle (or kernel theory) for the prima-facie design theory aims to achieve the greatest net benefits for an organization. Likewise, the intentions of the application principles for the utilitarian and universalizability design theories strive to achieve the greatest degree of adherence to security objectives and universalizability, respectively. Although Siponen and Iivari (2006) investigated the potential effects of other design theories on the success or failure of an information security policy, this study focused on the three design theories mentioned above because of their flexibility and their recognition of and allowance for the fact that disobeying the terms of an information security policy sometimes resulted in a more positive outcome for an organization than the consequences of complying with the terms of a policy.

3.4 Research Design

This research study followed the design science research approach in IS. The purpose of design science is to contribute to the knowledge base for the design and construction of artifacts and to enhance the understanding of how to solve the social and organizational problem for which the artifact is designed. According to Walls, Widmeyer

and Sawy (1992), while the natural sciences are geared to find answers to questions about the way things actually are, design sciences seek to answer questions about how things should be. When design sciences are applied to the field of IS, the development of artifacts is used to reach established goals (Simon, 1996).

Design science research is defined by Hevner et al. (2004) as follows:

"Design science research is a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem. The fundamental principle of design science research is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact."

Design science is research that is intended to add to the body of knowledge in the academic field and to provide guidance to practitioners through the creation of information system artifacts using precise and meticulous methods (Hevner et al., 2004). When used as a tool to develop a product, design science can be thought of as "a plan of something to be done or produced" (March & Smith, 1995). In this regard, design science is a research method that relies on the establishment of unique artifacts to solve problems (Hevner et al.; Kuechler & Vaishnavi, 2008), contribute to human knowledge and awareness, and endow organizations with an increased ability to manage resources, including their employee base. Through the development and utilization of the artifact with the appropriate tools and techniques, the design-science research output solution is achieved (March & Smith). One of the primary goals of a design-science artifact is to augment and expand the knowledge base related to the resolution of complicated and challenging business problems (Hevner et al., 2004).

As observed by Hevner et al. (2004), the design artifact and IS design theory are alike in many ways. Meta-design is a framework that satisfies meta-requirements through the application of specific elements defined by a particular group of artifacts and guidelines (Markus, Majchrzak, & Gasser, 2002). The conceptual foundations of meta-designs and meta-requirements are cultivated from the alteration, expansion or application of kernel theories (Hevner et al., 2004). According to Markus et al., the method used to design an artifact is, in essence, the set of standards that ultimately leads to the formation of the artifact.

Design science research leads to a normative IS philosophy that benefits both scholars and practitioners (Markus et al., 2002). Hevner et al. (2004) asserted that rigor and relevance are essential elements of the results of any IS research, which is intended to supplement the body of existing knowledge and to prove effective when put into practice in the workplace. A key purpose of design science research, as a problem-solving concept (Hevner et al., 2004; March & Smith, 1995; Simon, 1996; Walls et al., 1992), is to assist organizations in achieving their business objectives. In order to achieve this goal, those who conduct design science research must acquire a thorough understanding of the theory and be able to formulate a precise description of the business problem they are striving to resolve.

According to Hevner et al. (2004), the assessment process that is chosen relies upon the consideration of the accessibility of needed materials and the careful evaluation of the characteristics of the problem and the artifact design. Hevner et al. (2004) also

suggested that it is advantageous to make use of existing assessment methods to assist in calculating the efficacy and rigorousness of potential IT artifacts.

Hevner et al. (2004) proposed that IS research falls into one of two categories: the behavioral paradigm or the design science paradigm. The former seeks to determine the truth and the latter seeks to create a utilizable artifact (Hevner et al., 2004). Hevner et al. (2004) also stated that the development of effective IS design theories and artifacts is improved by taking into account the needs of the business world and combining them with data drawn from the existing academic base to successfully satisfy the dual requirements of rigor and relevance that are essential to achieving the goal of constructing an effective design theory and IS artifact.

The results of this type of research are both relevant and rigorous because they are designed to solve a distinctive business problem and are generally reached by attempting to prove a design theory that can contribute to the academic knowledge base (Hevner et al., 2004). The seven guidelines suggested by Hevner et al. (2004) for research involving design science are summarized in Table 1 below and described in more detail in the following paragraphs.

The first design-science guideline proposed by Hevner et al. (2004) is that it is essential for an artifact to be devised as a model, construct, method or instantiation. According to Hevner et al. (2004), the foundation of IS research is the IS artifact, which incorporates into its design the features that are the essence of all phases of IS development, from examination to fabrication to implementation. The central focus of IS research is the problem relevance, which refers to the interest and significance the

problem has to the business world. By rigorously evaluating a design, researchers can improve and advance the process of developing an artifact by identifying and correcting any flaws or weaknesses.

This research study applied the seven design-science research guidelines introduced by Hevner et al. (2004) to all aspects of the design-science research process in order to foster results that meet the objectives of rigor and relevancy. The seven design-science research guidelines, as defined by Hevner et al. (2004), are presented in Table 1.

Table 1. Design-science research guidelines (Hevner et al., 2004, p. 83)

Guideline	Description
1. Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
2. Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
3. Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
4. Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
5. Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
6. Design as a Search	The search for an effective artifact requires utilizing available Process means to reach desired ends while satisfying laws in the problem environment.
7. Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

The guidelines applied to this research study are discussed in the order they are presented in Table 1.

Guideline 1: Design as an Artifact. Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation (Hevner et al., 2004, p. 83).

The design artifact of this research study is to develop an information security policy effective in exceptional situations.

Guideline 2: Problem Relevance. The objective of design-science research is to develop technology-based solutions to important and relevant business problems (Hevner et al., 2004, p. 83).

Siponen and Iivari (2006) stated that there is a lack of information about how to design information security policies intended to handle exceptional situations in an organization. One purpose of this research study was to address this deficiency of knowledge.

Guideline 3: Design Evaluation. The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods (Hevner et al., 2004, p. 83).

The evaluation of the design artifact was demonstrated and illustrations for applying the assessment methods in practice were presented in this research study.

Guideline 4: Research Contributions. Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies (Hevner et al., 2004, p. 83).

The contributions of this research study were the final results of the design of information security policies for the Information Systems domain.

Guideline 5: Research Rigor. Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact (Hevner et al., 2004, p. 83).

This study used design theories to develop and test different information security policies and to evaluate the policies through experiments.

Guideline 6: Design as a Search. The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment (Hevner et al., 2004, p. 83).

The design-science research was based on literature reviews of information security policy implementation and design in the IS domain.

Guideline 7: Communication of Research. Design-science research must be presented effectively to technology-oriented and management-oriented audiences (Hevner et al., 2004, p. 83).

This research study was intended for technology-oriented practitioners and academicians who are researching issues related to designing an effective information security policy. It also provided additional knowledge to managerial-oriented personnel seeking to evaluate, implement and design an effective information security policy in the information security field.

In summary, the Hevner et al. (2004) guidelines provided the following characteristics:

1. Rigorous development of an artifact that meets business needs
2. Implementation of quality standards
3. Contributions toward the body of knowledge
4. Suitable evaluation; ability to form the core of design science research

In addition, the research process of this research study used the general design research cycle explained by Kuechler and Vaishnavi (2008) and illustrated in Figure 2.

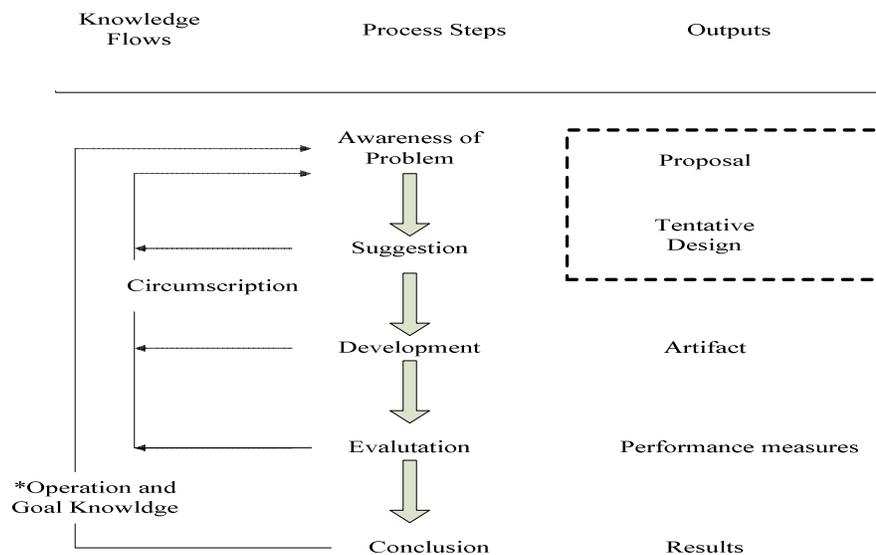


Figure 2. The general methodology of design research Kuechler and Vaishnavi (2008).

The design science research methodology proposed by Kuechler and Vaishnavi (2008) comprises five phases: (a) awareness of a problem, (b) suggestions, (c) development, (d) evaluation, and (e) conclusion. The following section explains how

these phases correlate with the design science framework and how the phases were used in this research study. The research study started with Phase 1 and Phase 2, which formulated a problem based on literature review. Phase 3 developed the artifact and the design concept model, and Phase 4 was the performance of a quasi-experiment for evaluation. Finally, Phase 5 consisted of completion of the data analysis results.

3.5 Phases 1 and 2 – Awareness of Problem and Suggestion

Siponen and Iivari (2006) indicated that there is a need to develop information security policies designed to deal with exceptional situations in organizations. Following the second guideline as stated by Hevner et al. (2004), Phases 1 and 2 of this study formulated a problem taken from literature review and examined and showed the importance and relevance of designing an information security policy in the IS domain, based on the prima-facie, utilitarian, and universalizability design theories. The design process of an information security policy in these phases was based on these three theories and was discussed and reviewed with a team of five information security practitioners in the organization. A lack of design information for security policies in the field of IS domain was addressed in this research study (D'Aubeterre, Iyer, & Singh, 2009; Kolkowska & Dhillon, 2012). The literature is lacking in empirical studies that closely examine how to design clear, flexible and comprehensive information security policies so employees can make positive decisions when faced with exceptional situations (Whitman, 2008). Designing an effective information security policy for

exceptional situations in an organization is valuable for at least three potential reasons. An information security policy needs to provide clarity and communicate potential risk to employees of an organization in exceptional situations, in addition to ensuring that risk mitigation methods are in place. The policy also needs to increase flexibility for employees when making decisions about "mandatory" rules and reporting identified violations in exceptional situations. Lastly, the design effectiveness of an information security policy can be increased if the policy is comprehensive and it is integrated with other business policies in the organization, making it a part of the organization's culture (Puhakaiken & Siponen, 2010). The end product of these phases was a proposal for new research and the results are an effective design of an information security policy in exceptional situations.

3.6 Phase 3 – Artifact Development

This research study focused on the prima-facie, utilitarian, and universalizability design theories in order to develop an information security policy artifact. During this phase, the artifact was developed based on literature review and the three aforementioned normative theories utilizing design application principles. The literature review, organizational strategies and processes, business needs, and the roles and behaviors of people were used to create an information security policy. An information security policy prototype was developed and implemented. Prototyping development was borrowed from the software engineering discipline, as shown in Figure 3.

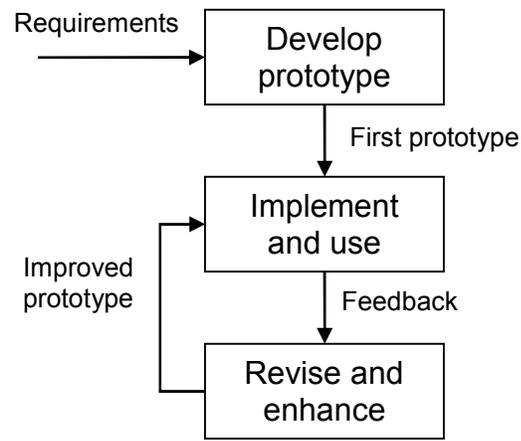


Figure 3: Prototyping (based on Sommerville 2007, p. 411)

After the development of the information security policy prototype, the overall concept was evaluated (Sommerville, 2007). The evaluation process was intended to determine if the design artifact meets the conditions of the problem domain, ensuring that it is functional and efficient. Design artifacts should be assessed according to five specific criteria: observational, analytical, experimental, testing, and descriptive (D'Aubeterre et al., 2009). An experiment based on empirical evidence is of assistance in validating the characteristics of the intended design artifact (Hevner et al., 2004) and producing broad-spectrum results (Creswell, 2008). Experimental evaluations examine the nature and performance of design artifacts through the application of simulation and controlled experiments. Baskerville, Pries-Heje, and Venable (2007) proposed that an evaluation process conducted using experiments or other "hard methods" can help to reduce errors and ensure the procedure is all-inclusive.

Combining the paradigms of behavioral science and design science, Hevner et al. (2004) established an information systems research framework. Hevner et al. (2004) asserted that the integration of these two sciences enhances information systems research. As described in Figure 3, the information systems research framework defines information systems research through the construction and assessment of theories and artifacts. This study used a quantitative research method to prove hypotheses by exploring how different variables influence and impact each other. The information security policy design process can impact employee behavior regarding information security policies in exceptional situations. The variables used in this research focused on the information security policy design developed for an organization. These variables explored an employee's voluntariness to comply with the terms of an existing information security policy during exceptional situations. The dependent variable was information-security consequences. The independent variables were as follows: (a) security expected benefits; (b) happiness brought about by security actions; (c) universalizability by security actions; and (e) voluntariness (Siponen & Iivari, 2006). The output of this phase was an information security policy artifact. Practitioners should assess a design artifact's value and efficiency to determine its benefits to an organization. According to Hevner et al. (2004), the knowledge base contains reliable approaches for the rigorous assessment of a design artifact. As suggested by Hevner et al. (2004), the primary factors guiding the evaluation process should be the basic characteristics of the problem and the artifact and resources accessible to the researcher.

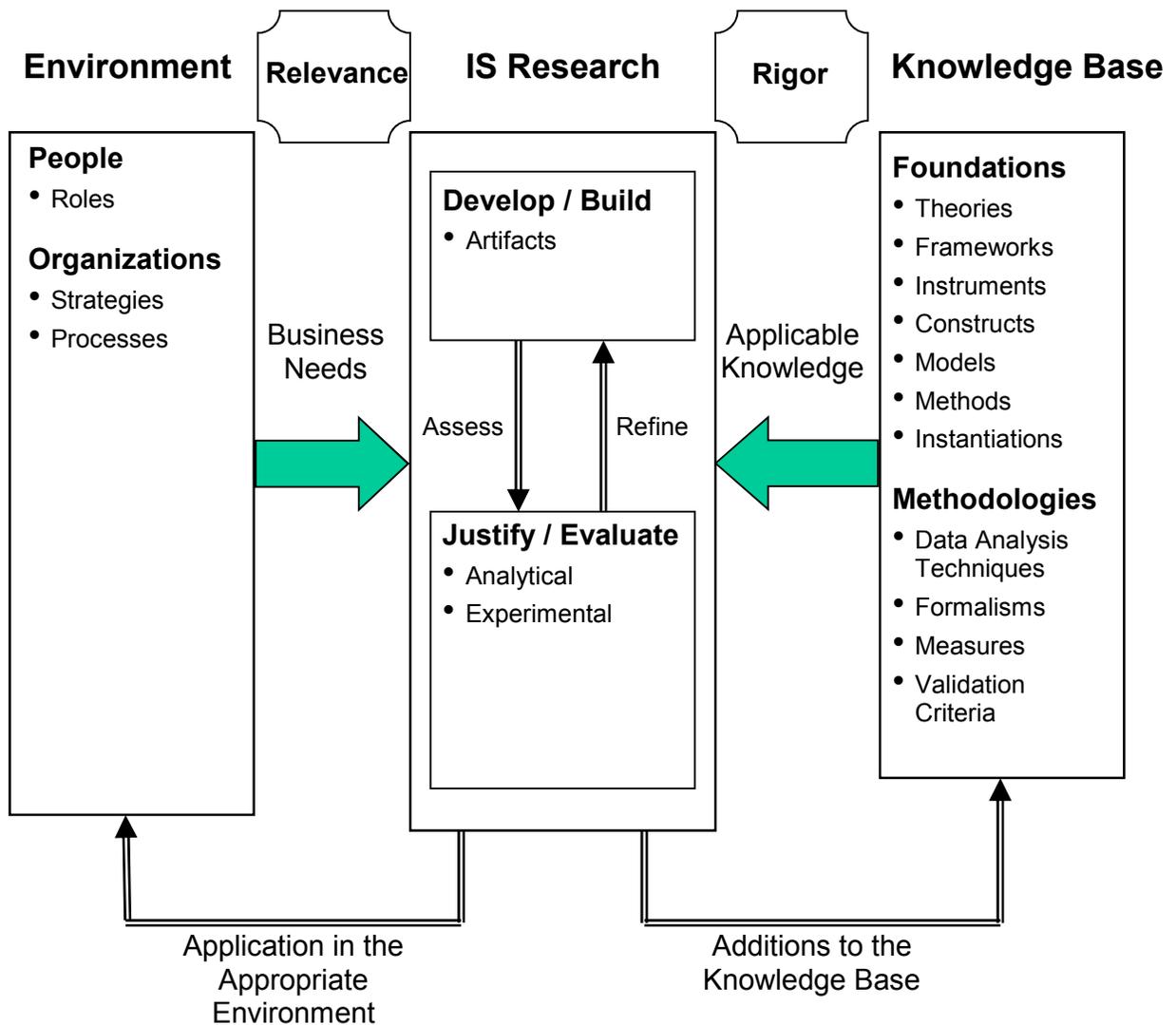


Figure 4. Design science research framework (Adapted from Hevner et al. 2004 p. 80).

The environment and the applicable knowledge base regulate research activity. The environment can be defined as the problem space where the relevant research criteria are found. The knowledge base can be defined as a combination of research methods and

information systems research foundations. At the hub of this framework is information systems research, where applicable research methods are selected from a knowledge base in an associated field and utilized according to an organization's requirements.

The IT artifact is at the center of design science research and is based on both theory and practice to ensure an efficient system. It is possible for artifacts to generate innovative theories, so the future should be considered during the design process. Design scientists need to contemplate the research questions that will have to be answered when the artifact is being evaluated. This normative approach is frequently motivated by a conventional outlook of design and the idea of "wicked" problems; for example, the production of a functional artifact can be considered a contribution to science in itself if the design space in which it was developed posed considerable enough difficulties for the design scientist (Hevner et al., 2004).

Artifacts are “intended to solve identified organizational problems. Such artifacts are represented in a structured form that may vary” (Hevner et al., 2004, p. 77). The artifact for this research project was how to design an information security policy that is effective in organizations in exceptional situations. The relevance of the problem is important because the research objective of the study was to address the lack of information about how to design information security policies intended to handle exceptional situations in an organization and to improve this deficiency of knowledge. The adopted research approach, therefore, followed the principle of “design theory hypothesizing the effectiveness of the artifact(s) to achieve the goal(s)” (Baskerville et al., 2011, p. 124).

Experiments and surveys are some of the common tools used in the evaluation and validation process in research methodologies in the paradigm of behavioral science. Researchers in the information systems industry have long been analyzing and identifying theories by using these traditional methodologies. On the contrary, design science attempts to appraise the usefulness and value of the design artifact in the field of information systems research. This assessment cannot be accurately made unless the effectiveness and quality of the system are well-defined. For instance, some of the characteristics that might describe the quality of the system are usability, practicality, comprehensiveness, stability, precision, dependability, and functionality (Hevner et al., 2004). The aim of the assessment is to evaluate the effectiveness of the system and to offer objectives for gradual enhancements to the artifact over time. The degree to which information systems research meets the needs of organizations determines the degree of relevance while the proper utilization of methodologies and foundation principles establishes the bearing of relevance. Although other systems artifacts are also of significance in the development of IS policies, March and Smith (1995) and Hevner et al. (2004) argued that models, methods, and constructs are the most legitimate artifacts. Constructs describe the theoretical terminology of a domain. Models express how constructs are associated. Methods explain how to complete an assignment. Theories are increasingly improved during the design-construction stage when concepts or methodologies of an experimental nature are utilized.

The proposed end products of design science are generally twofold: (a) a serviceable artifact that helps to resolve an explicit and demanding problem in a

practicable manner within a particular framework, and; (b) significant contributions to information security practitioners. The information security policy was developed with input from subject-matter experts based on organizational strategies and processes and business needs utilizing a prototype approach. Design science research involves a greater number of elements than social-science research, such as communication with subject-matter experts (SMEs), an understanding of the environment and conditions surrounding the design, and construction and analysis of the system. A design science research approach relies more heavily on theories in the decision-making process than a standard systems research approach and on the capacity to gain broad assumptions from the important act of developing the system.

3.7 Phase 4 – Evaluation

Design artifacts evaluated empirically through the use of experimentation help to establish the artifact's characteristics (Hevner et al., 2004) and offer a foundation for general conclusions. Walls et al. (1992) recommended an experimental design in which the results of a group using an IT artifact are compared to the results of a group that is not using an IT artifact. This study involved a pretest-posttest design that included a treatment group and a control group. The participants were not assigned to these groups by random assignment. Instead, a quasi-experiment, nonrandomized pretest-posttest design was conducted using an experimental group and a control group. The experimental group (Group A) underwent the treatment (X_1), while the control group

(Group B) received no treatment at all. The control group also served as the benchmarking point of comparison to evaluate the design effectiveness of an information security policy for exceptional situations in an organization (Campbell & Stanley, 1963; Creswell, 2008; Shadish, Cook, & Campbell, 2002).

3.7.1 Sample population

The population of this study was full-time and part-time employees who work in a single organization. There was a nonrandom sampling of participants and a nonrandom assignment of participants from the organization's administrative employee directory into the two groups. Also, the group that received the treatment and the group that acted as the control group were randomly selected (Creswell, 2008). According to Walls et al. (1992), one practical design concept is to conduct an experiment in which the IT artifact is provided to an experimental group while being withheld from a control group. The results of each group can then be compared and contrasted (Walls et al., 1992).

Thirty participants in the quasi-experiment for this research study were non-randomly assigned into a control group and an experimental group with 15 participants in each group. According to Gay (1996), a minimum of 15 participants per group for quasi-experimental studies is sufficient and valid.

The experimental group (Group A) was provided with an information security policy and hypothetical scenarios adapted from Siponen and Iivari (2006) and Siponen and Vance (2010) upon which to base their answers. The treatment group (Group A) was

given a pretest and posttest treatment to determine if violating the information security policy was attributable to policy design. The responses of the participants in the treatment group (Group A) were compared to those of the participants in the control group (Group B). Participants in Group B received an information security policy upon which to base their answers. The participants in Group A were presented with a hypothetical scenario describing an information security situation. They were asked to identify if the design elements in the scenario are related to following or violating the information security policy (treatment X). The participants in the control group (Group B) were presented with the information security policy design artifact conceptualization and evaluation method process, followed by questions that aimed at identifying the consequences of their actions on information security in exceptional situations. There was no treatment given to Group B. In summary, two observations were made for Group A and Group B, one prior to treatment X_1 (pretest, O_1 / pretest, O_3) and one after treatment (posttest, O_2 / posttest, O_4).

Table 2. Two groups, A & B, pre-test, post-test.

Group	Pre-test	Treatment	Post-test
<i>Treatment group = A</i>	O_1	(X_1)	O_2
<i>Control group = B</i>	O_3		O_4

Treatment “X” represents the exposure of a group to an experimental variable or treatment, the effect of which was measured. Post-test “O” represents “an observation or measurement recorded on an instrument” (Creswell, 2008 p. 171).

The results of the data collection were analyzed to predict the outcome of the experiment in regard to how information security policy design elements can increase the effectiveness of an information security policy in exceptional situations.

3.7.2 Study instrument

A survey was developed and tested for reliability and validity and was used for the data collection. As a validated instrument, a survey is useful in establishing accurate associations between any variables used in the experiment (Creswell, 2008). A survey is a term that includes all techniques of data collections in which an individual is asked to respond to questions in a particular order. Surveys are useful instruments for collecting data while providing anonymity to the respondent, promoting responses that are more accurate and trustworthy (Creswell, 2008).

The survey was divided into two parts. The first part focused on obtaining demographic information about the respondent and the organization. The following demographic information was collected: gender, age, years of experience, years with the organization, educational level, and security certifications.

The second part was composed of questions designed to assess the various aspects of information security policy design. An expert panel with ten participants who had information security certification, such as CISM, CISSP and CISA (Hevner & Chatterjee, 2010), verified the validity of the survey instrument and established if the participants of the survey were likely to have trouble responding to any of its components (Hevner & Chatterjee, 2010; Stewart, Shamdasan, & Rook, 2007). During instrument

survey development, questionnaire questions that may have appeared to be unclear, intrusive or confusing to the potential study participants were eliminated using a willingness-to-answer scale (Knapp, Marshall, Rainer, & Ford, 2006). An item-to-construct scale was also used to help eliminate double-barreled questions and to address content validity (Hinkin, 1998). The researcher employed the procedure for developing a measurement instrument provided by Hinkin (1998). The instrument is illustrated in appendix B. A five-point Likert-type scale was used. Scalar questions enable a respondent to give an opinion as an answer. Numeric scales grant the ability to give a positive or negative response to a statement (Dawes, 2008). The scale's granularity may vary, in general. For example, a coarse scale may range from one to three while a fine scale may range from one to ten. According to DeVellis, 2011, scales ranging between one to five or seven are generally adequate to give respondents sufficient differentiation. Scales that are odd-numbered give respondents the option to remain “neutral,” while scales that are even-numbered are given to respondents if a “neutral” response will detract from the study's validity (Dillman, Smyth & Christian, 2009). Scalar questions frequently employ Likert scales (Dix, Finlay, Abowd & Beale, 2004; Preece, Rogers & Sharp, 2007). The survey instrument was used to answer questions in regard to the clarity, comprehensiveness, flexibility and usability of the design of an information security policy, as illustrated in appendix B.

The hypothetical scenarios and questions were adopted from seminal papers of Siponen & Iivari, 2006 and Siponen & Vance, 2010 and were based on the hypotheses H1, H2 and H3 of the prima-facie, utilitarian and universalizability design theories,

respectively. The survey used a Likert scale with a five-point range. According to Dawes, 2008, the five-point Likert format is the most prevalent to ensure scale validity and reliability. The number 1 represented "strongly disagree," and the number 5 represented "strongly agree," granting every question a distinctive negative and positive descriptor.

Table 3. Likert scale with a five-point range (reverse order descriptor).

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
5	4	3	2	1

For every question, the number 1 signified the negative descriptor with the lowest value, the number 5 signified the positive descriptor with the highest value, and the number 3 signified a neutral value. If a respondent choose a low value, it signified that the individual felt a more powerful associative connection with the statement. If a respondent choose a high value, it signified that the individual felt a weak associative connection with the statement. Therefore, the stronger the respondent's associative connection, the more negative the individual's outlook, and the weaker the respondent's associative connection, the more positive the individual's outlook. The data were gathered using a questionnaire and were quantitative in nature, using the scale development theory proposed by DeVellis (2011).

3.7.3 Data Analysis

For the purposes of this research study, statistical regression analysis techniques were used to analyze the data to determine the dependability, validity and internal

stability of the instrument. Inferential statistics and factorial analysis strategies were employed, as suggested by Creswell (2008), which included an overall review of all information, data preparation, data reduction, organization and categorization. Inferential statistics used the general linear model (GLM) and included a repeated measure ANOVA (Nelder & Wedderburn, 1972).

This study employed a posttest and pretest non-equivalent control group design of the quasi-experimental research design. An inferential statistics quasi-experimental research approach was used because the study was conducted in only one organization. A posttest and pretest non-equivalent control group of quasi-experimental design was used. The experimental and control groups were not equated by randomization in the organization.

The data analysis employed repeated measures of ANOVA to determine if voluntariness in following the information security policy resulted in different consequences of actions taken by employees. If different consequences of actions taken by employees were detected, the analysis also ascertained the impact on overall design effectiveness.

3.7.4 Analysis Procedures

The following approach was used to prepare the data before analysis. The first step included examining and validating the results. During data analysis, data were

entered into Microsoft Excel and exported to SPSS for further analysis. Any missing data were added using the missing data function in SPSS.

According to Shadish, Cook, and Campbell (2002), quasi-experimental designs are effective for obtaining information on the relationships between cause and effect. However, this approach is not devoid of risks in regard to its validity. Shadish et al. (2002) proposed three principles to help overcome these threats when using a quasi-experimental design:

1. Identification and evaluation of plausible threats to internal validity.
2. Control by design. Multiple control groups, multiple baselines, and statistical control as a last resort.
3. Coherent pattern matching. This principle involves making a complex prediction about a particular causal hypothesis that would leave few viable alternative explanations. The logic behind this principle is that the more complex the prediction, the less likely that a given alternative could generate the same results (Terrell, 2012).

Identification and evaluation of plausible threats to internal validity were conducted during the reliability and validity testing of the survey instrument and quasi-experimental design phase.

Regression analysis was performed to examine how well the independent variables explained the dependent variable (Cohen, Cohen, West & Aiken, 2003). Regression models can be used to predict values on information security consequences (dependent variable) based on information from the (independent) variables security

expected benefits; happiness brought about by security actions; universalizability by security actions; and voluntariness.

Overall Model Fit (*F*-Test): Was employed to ascertain if it is more beneficial to use the regression model rather than only the mean of the dependent variable. Additionally, calculations of the overall sample level of mean scores for all Likert-scaled items were reported.

3.7.5 Methods of Analysis

Descriptive statistics, and repeated measures ANOVA were used as tools to test hypotheses. The three hypotheses in this study were tested using the *t*-test to determine the significant difference between the means scores of the pretest and posttest treatments of the participants in order to find out if the results were statistically significant at Cronbach's α 0.05 levels. The focus of the hypotheses was the difference between variables of interest. Hypotheses H1 through H3 were tested to determine the degree of significance and, specifically, whether this difference was greater than would be expected by chance. Given that hypotheses H1 through H3 compare two variables, inferential statistical methods were also applied (Creswell 2008). The hypothesis H1 through H3 were then analyzed using *t*-test. The *t*-test, *t*-value and standard error of the difference were used to assess whether the means of the two groups (A & B) were statistically different from each other (Terrell, 2012). A pretest was used in this study because the control group and treatment group needed to be examined for equality, as group selection

was not random and groups may have had preexisting differences (Campbell & Stanley, 1963). Results from the *t*-test were examined for significant and insignificant differences between the two groups on the pretest. In order to test the three hypothesis, H1, H2 and H3, an Cronbach's α level of $p < 0.05$ were used.

ANCOVA (analysis of covariance) is an extension of ANOVA and was used to examine whether group means (categorical independent variable) differed on the information security consequence (ISC) dependent variable after statistical control for another continuous variables (covariate). The analysis was accomplished through the selection of general linear model (GLM) procedures and repeated measures ANOVA (Nelder & Wedderburn, 1972).

The results of the survey from the pre-test and post-test groups were analyzed using the SPSS-computer-statistical analysis program. Both descriptive and inferential statistical analysis techniques were used to identify any relationships and group differences in scores on the survey items and Likert scale scores. In order to determine if a linear relationship existed between dependent variables for each group, a scatterplot was generated to confirm linearity assumptions. A Pearson's correlation was conducted to examine multicollinearity among the dependent variables (Cohen, Cohen, West & Aiken, 2003; Harrell, 2001; Myers, 1990). According to Cohen et al., statistics aid researchers in excluding the significant risk that the soundness of the results of an experiment could be attributable to probability instead of actual dissimilarities in the test group. Additional statistics were run to assess normality and univariate outliers, in which histograms and boxplots were examined to ensure that any that noted dissimilarities were

not the result of a recording error. The confidence level setup for the analysis was set to 0.5 to decrease the chances of making a type I error. Univariate analyses of variance for each dependent variable were conducted as follow-up tests, using the Bonferroni method for controlling Type I error rates for multiple comparisons and were tested at a significance level of 0.5.

3.7.6 Internal and External Validity

Internal validity refers to the degree to which the independent variables may impact the differences detected in the dependent variables. Another possible threat to internal validity is the extraneous variables. If these variables are not controlled, their results may mistakenly appear to be attributable to the effects of the experiment itself. External validity indicates how significantly the scope of a study's findings may accurately or inaccurately affect the generalizability (applicability) of those findings outside of the sample. Threats to external validity are helpful in determining how errors may be made in the generalizing of the findings of a study.

Campbell and Stanley's (1963) seminal paper served as the designated basis for the description of possible threats to the internal and external accuracy of the findings of this study, based on its research design. The following table provides a definition of each threat present and its manner of being controlled for internal validity.

Table 4. Threats to Internal Validity (Campbell & Stanley, 1963)

Threats to Internal Validity		Presence	Control of Threat
		Yes / No	
History	Events, other than the experimental treatments, influence results.		Keep a list of dropouts in both treatment and control groups
Maturation	During the study, psychological changes occur within participants		Control variables, nonrandom sampling
Testing	Exposure to a pretest or intervening assessment influences performance on a posttest.		Will use ANCOVA to adjust pretest scores
Instrumentation	Testing instruments or conditions are inconsistent; or pretest and posttest are not equivalent, creating an illusory change in performance.		Examination of data sources over study period
Statistical Regression	Scores of participants that are very high or very low tend to regress towards the mean during retesting.		Three or more observation points, nonrandom sampling
Selection	Systematic differences exist in participants' characteristics between treatment groups.		Evaluation of sampling criteria
Experimental Mortality	Participant attrition may bias the results.		Comparisons between retained and lost participants
Diffusion of Treatments	Implementation of one condition influences participants in another condition.		Participants in the control group will receive treatment at a different date
Interaction effect of selection biases and treatment	Sample not representative of the population i.e. not selected randomly		Non-random assignment will be used
Reactive experimental arrangements	Participants' knowledge of participating in experiment may affect their responses		Will not control

The following table provides a definition of each threat present and its manner of being controlled for external validity.

Table 5. Threats to External Validity (Campbell & Stanley, 1963)

Threats to External Validity		Presence	Control of Threat
		Yes / No	
Interaction of testing and treatment	The interaction of testing with treatment		A pretest is not used on the experimental group.
Interaction of selection and treatment	The interaction of treatments with treatment		The population is described in the research study. A statistical technique such as ANCOVA is used, in conjunction with quasi-experimental design.
Reactive arrangements	Tests of significance for this design		No lab setting is used. A control group and an experimental group are used.
Multiple-treatment interference	Multiple treatments are given to the same participants		No multiple treatments are given.

3.7.7 Results

Results from the data analysis and interpretation are described in Chapter Four.

Bivariate and multivariate analyses were performed on the data.

3.8 Phase 5 – Conclusion.

A design-science research methodology was applied in order to achieve the research study objective of designing an information security policy that is effective in exceptional situations. As the final process of the research study, this phase disclosed the results and contributions of the experiment, including the artifact design and all additional knowledge regarding the design process, such as construction and evaluation. The output of this phase was an acceptable research contribution. The conclusion phase indicated termination of the design project. The design-science research results were published and communicated to technical and management audiences (Hevner et al., 2004).

3.9 Miscellaneous

3.9.1 Limitations

This study was limited to full-time and part-time employees who worked in the following departments of a single organization: information systems and technology; human resources; finance; legal; and corporate communications. The priorities of the study were to determine if and why employees violated or complied with an information security policy in exceptional situations based on the application principles—net benefits, overall adherence to security objectives, and universality of actions— of the prima-facie, utilitarian and universalizability design theories. In terms of generalizability, the study

was limited to the adult population with the general exclusion of adults who were at or beyond retirement age. However, the study sample was represented a diverse range of ages in the adult population. All of the participants in the study were chosen on a volunteer basis and retained the right to withdraw at any point in time. Therefore, the participants who completed the study may not accurately represent the adult population (Creswell, 2008).

The participants in this experiment were asked to engage in an analysis-of-attitude survey using independent and dependent variables that were intended to gauge the participant's actions instead of the participant's opinions. Although it was anonymous, this study may have been limited by the participant's subjectivity or deceptive responses. In addition, the study was not intended to use a self-directed learning readiness scale or to determine the qualities or elements that promoted the participant's fulfillment in life. Rather, it determined how significant or valuable the participants considered certain assets and attributes in contributing to their happiness or satisfaction in life.

The study consisted of pre-test and post-test experimental exercises. However, because quantitative research is generally inflexible and employs brief dialog sessions, it is susceptible to inaccuracies if the study is not conducted accurately. In addition, the participant's moral principles or unwillingness to comply can interfere with the successful execution of the experiment. Finally, if the sampling and weighting of a quantitative experiment are mishandled, the accuracy and findings of the study may be jeopardized.

There is the possibility of bias in the data generated by the study because it was conducted at the researcher's place of employment and because participants may not respond accurately when they are aware that they are participating in an experiment. The participants may also have considered some of the terminology in the study to be ambiguous or obscure in meaning, making it difficult for them to accurately assess their responses to certain questions.

Additionally, even though employees may believe that an information security policy is important; their actions are not always reconciled with this belief. Therefore, it is possible that a participant may not behave as indicated in a response if he or she is faced with that situation in the actual workplace.

3.9.2 Delimitations

The effectiveness of design theories other than the prima-facie, utilitarian and universalizability design theories are beyond the scope of this study. Additionally, this study did not intend to examine employee compliance with an information security policy under normal or stable circumstances or determine the frequency with which employees or organizations encounter exceptional situations (Siponen, & Vance, 2010; Zafar, & Clark, 2009).

Chapter 4

Results of repeated measures ANOVA Analysis

4.1 Introduction

The previous chapters presented, outlined and discussed the research methodology, quasi experiment, data gathering techniques and the methods used to show and analyze the gathered data. This chapter details the results of those phases.

4.2 Data Preparation

Prior to analysis, the data were prepared to assure they would accurately execute within the SPSS software. First, the results gathered from the questionnaires were examined and validated. Second, the data were entered from the questionnaires into a Microsoft Excel spreadsheet and exported to an SPSS tool. The pretest and posttest data collected from group A and group B were coded and entered into SPSS version 23.0 for descriptive statistical analyses and interpretation. Participant responses to statements based on a Likert scale were considered as ordinal variables and assigned codes. Code 1 represented “strongly disagree” while code 5 represented “strongly agree.” Third, any missing data were added using the missing data function in the SPSS tool. This format was deemed closest to the data cleaning input in the SPSS tool. The data collected from the pre-intervention test and the post-intervention test were analyzed by descriptive

statistics. The results on the given questions in both the pretest and the posttest were analyzed.

4.3 Demographic Findings

Of the 32 participants' total responses utilized within this quasi-experimental study, 15 points of demographic data were collected. Participants were initially asked to identify their gender. Of the participants, 65.6% identified as male and 34.4% identified as female. Table 6 below presents the gender distribution of the questionnaire participants.

Table 6. Gender Distribution

Gender	Frequency	Percentage of Respondents
Male	21	65.6
Female	11	34.4

Next, participants were asked to identify their age group. None of the participants were in the 18-30 age group; 15.6% of participants identified themselves as members of the 30-39 age group; 34.4% of participants identified themselves as members of the 40-49 age group; and 50% of participants identified themselves as members of the 50-65 age group. Table 7 shows the age distribution of the questionnaire participants.

Table 7. Age Distribution

Age	Frequency	Percentage of Respondents
18-29	0	0.0
30-39	5	15.6
40-49	11	34.4
50-65	16	50.0

Participants were also asked to describe their highest completed level of education. Of the participants, 9.4% responded that they had completed high school; 18.8% responded that they had completed an Associate's degree; 53.1% responded with completion of a Bachelor's degree; 18.8% responded with completion of a Master's degree; and none of the participants responded that they had earned a Doctorate degree. Table 8 presents the education level distribution of the questionnaire participants.

Table 8. Education Level Distribution

Age	Frequency	Percentage of Respondents
High School	3	9.4
AA/AS	6	18.8
BA/BS	17	53.1
MA/MS	16	18.8
PhD	0	0

Participants were also asked to describe their highest completed level of education. Of the participants, 9.4% responded that they had completed high school; 18.8% responded that they had completed an Associate's degree; 53.1% responded with completion of a Bachelor's degree; 18.8% responded with completion of a Master's degree; and none of the participants responded that they had earned a Doctorate degree. Table 9 presents the security certification level distribution of the questionnaire participants.

Table 9. Security Certification Distribution

Age	Frequency	Percentage of Respondents
CISSP	0	0
CISM	0	0
CISA	2	6.3
OTHER	5	15.6
NONE	25	78.1

4.4 Findings

The effectiveness of design theories other than the prima-facie, utilitarian and universalizability design theories are beyond the scope of this study. Cronbach's α was calculated at 0.719, suggesting an acceptable reliability coefficient among the items

tested. The design model demonstrated internal consistency through Cronbach's α . The table 10 represents the Cronbach's α reliability coefficient.

Table 10. Cronbach's alpha

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.719	.656	18

The pre-test and post-test activity included concurrent administration of identical questionnaires to both Group A (treatment) and Group B (control group - no treatment). The goal of the pre-test questionnaire was to examine the participants' first reactions to the concepts of voluntariness; security-expected benefits; happiness brought about by security actions; universalizability by security actions; and attitudes. The results then served as a foundation upon which to base comparisons for the intervention's outcome and effects. The purpose of the post-test questionnaire was to examine the direct consequences of the intervention on participants' voluntariness; security expected benefits; happiness brought about by security actions; universalizability by security actions; and attitudes. The contents of the pretest and posttest questionnaires were identical. A paired-samples *t*-test was used to compare the mean scores of the pretest treatment group A and posttest control group B. The table 11 shows results at .000 Sig. (2-tailed) and the significant level is less than .05.

Table 11. Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
	Group - Participant	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	Group - Participant	-7.000	4.711	.833	-8.698	-5.302	-8.405	31	.000

The results show that at .000 Sig. (2-tailed), the significant level is less than .05, and the difference is significant.

For H1, a comparison of the mean of the six prima-facie questions of each treatment was completed. Using a paired *t*-test, the data support H1 with a *p* value \leq 0.000. The results from hypothesis H1 show that when participants used the design artifact treatment, they were able to answer all six questions pertaining to the prima-facie in contrast to those who did not receive the treatment.

Table 12. H1 Prima Facie

One-Sample Test						
Test Value = 0						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
H1	20.003	31	.000	13.37500	12.0113	14.7387

For H2, a comparison of the mean of the six utilitarian questions of each treatment was completed. Using a paired *t*-test, the data support H2 with a *p* value \leq

0.000. The results from hypothesis H2 show that when participants used the design artifact treatment, they were able to answer all six questions pertaining to utilitarian theory hypotheses in contrast to those who did not receive the treatment.

Table 13. H2 Utilitarian

One-Sample Test						
	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
H2	20.003	31	.000	13.37500	12.0113	14.7387

For H3, a comparison of the mean of the six universalizability questions of each treatment was completed. Using a paired *t*-test, the data support H3 with a *p* value \leq 0.000. The results from hypothesis H3 show that when participants used the design artifact treatment, they were able to answer all six questions pertaining to the universalizability theory in contrast to those who did not receive the treatment.

Table 14. H3 Universalizability

One-Sample Test						
	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
H3	20.003	31	.000	13.37500	12.0113	14.7387

4.5 Summary

The effectiveness of design theories other than the prima-facie, utilitarian and universalizability design theories are beyond the scope of this study.

Table 15. Hypotheses Results

Hypotheses	Results
H1: If the employees' voluntarism and the expected benefits of noncompliance increase, then an organization will experience fewer consequences in response to employee noncompliance in exceptional situations.	Supported
H2: If the employees' voluntarism and happiness of noncompliance increase, then an organization will experience fewer consequences in response to employee noncompliance in exceptional situations.	Supported
H3: If the employees' voluntarism and universalizability of noncompliance increase, then an organization will experience fewer consequences in response to employee noncompliance in exceptional situations.	Supported

Results show that all three hypotheses - H1, H2, and H3 - are supported.

Chapter 5

Conclusion

5.1 Introduction

This chapter provides the conclusion of the research study and includes a summary of the findings. It further outlines recommendations for future research studies. Limitations in this research study have been presented in a separate section.

5.2 Findings - Contributions

The contribution of this study is to use the design science research method and to provide a design science artifact to practitioners and scholars to design effective information security policies in exceptional situations in emergent organizations.

The scope of the methodologies, settings and goals of IS information security research is continually increasing. To increase its hypothetical, scholarly and scientific base, IS information security research also needs to expand to include participation and research developments from other fields of study. The difficulty faced by researchers is that attaining significant contributions from other disciplines is a complicated process. Researchers must be aware of changes that are occurring in all aspects of the IS information security research field and how these changes may affect the interaction between relevant disciplines.

Based on the analysis of fit the model for designing an effective information security policy for exceptional situations in an organization was determine to be a success model.

It was discovered in the posttest that there was an increase in the scores of the employees' voluntarism across the three design theories. This could be attributed to the use of the three design theories to develop an effective information security policy. These findings can be significant to practitioners who seek to develop an effective information security policy in exceptional situations. Indeed, the results of this study implied that the questionnaire, and the prima-facie, utilitarian and universalizability design theories used by the researcher were effective tools for designing an effective information security policy in exceptional situations in an organization. This finding agrees with the works of Siponen and Iivari (2006) and confirmed the recommendation of the use of the prima-facie, utilitarian and universalizability design theories in designing effective information security policies. Although all information security policies must contain some non-normative elements, the following analogy helps to clarify how a policy based primarily on normative standards can aid employees in making choices that are the most advantageous to an organization, particularly when those choices need to be made swiftly and decisively. Findings in the study show employees need a degree of voluntarism to violate information security policies for the greatest benefit of the organization in exceptional situations.

These findings also indicate that designing an information security policy with the three elements of a kernel theory basis; application principles from that kernel theory specifying how employees should manage exceptional situations; and hypotheses that can be tested can assist in advancing the continued effectiveness of information security policies that may arise in an exceptional situation (Siponen & Iivari, 2006).

In conclusion it could be strongly affirmed that the use of application and effectiveness of design science approach to information security of the prima-facie, utilitarian and universalizability design theories are key when developing an effective information security policy for exceptional situations in an organization. The method to apply these three design principles and develop security policy provided rigorous testing and empirical support to design theories for information security policy proposed by Siponen and Iivari (2006).

5.3 Implications

The information security policy design approach contributes to the IS knowledge base by shrinking the existing research gap in the design of information security policies in exceptional situations in emergent organizations. This approach provides a methodology that incorporates kernel-theory requirements and constraints into the analysis and design phases and considers meta-policies as functional security requirements. This approach also supplies practitioners with a method that can be used to develop and design an information security policy in exceptional situations in emergent

organizations. Organizations and practitioners would benefit from designing effective information security policies. The design instantiation artifact can help practitioners to design effective information security policies in exceptional situations in emergent organizations to improve the general state of information security. Hevner et al. (2004) suggest the use of a sequential research process that involves determining a pertinent business problem that the design of an IT artifact can resolve and evaluating the artifact with the proper methodologies so that it can be added to the IS knowledge base.

5.4 Limitations

The main limitations were that the study focus only on normative theories and only 32 participants from one organization participate in testing. The primary barrier in this research study was the difficulty in designing an information security policy that analyzed or accounted for the motivations that caused employees to comply with or violate the terms of the policy in exceptional situations. In order to determine if an information security policy design process and the application principles that focus on clarity, comprehensiveness, flexibility and usability regarding guidelines for handling exceptional situations were effective, a design science research approach needed to be followed (Hevner, 2004). Without any guidelines to follow when exceptional situations arise, an employee is liable to take actions that compromise the CIA of an organization's data or cause the organization to miss out on lucrative business prospects (Siponen &

Iivari, 2006). The issue of employee noncompliance with an information security policy is of fundamental importance to organizations and their information security experts.

5.5 Recommendations for future research

In designing future studies, the following suggestions may be considered.

- a. Future research should explore of other theories for design.
- b. Future research should study a much larger population size. Increasing the sample size would enhance the validity of the findings.
- c. Future research should examine the economics of employees' deliberate violations of information security policies in exceptional situations in emergent organizations.

The proposed future research studies will encourage further research that will offer valuable insights to practitioners and scholars in the area of designing effective information security policies in emergent organizations.

5.6 Conclusion

This study built upon Siponen & Iivari (2006) and Hevner, March, Park and Ram (2004) to develop a model for designing an effective information security policy for exceptional situations in an organization. The results significantly increase the understanding of the importance of designing an effective information security policy in

exceptional situations and provide empirical direction to practitioners on how to achieve this goal.

Many organizations fail to develop and administer an information security policy that analyzes or accounts for the motivations that cause employees to comply with or violate the terms of the policy in exceptional situations. As a result, employees may be left with a lack of direction or independence in taking the actions that are the most beneficial for an organization. This, in turn, can lead employees to make choices that endanger an organization's information assets. Employees may be faced with the conflict of having to violate the terms of an information security policy in order to satisfy a client's unanticipated request in a timely manner. Even if violating the policy provides advantages for the organization that outweigh those of adhering to it, an employee may decide that it is best to strictly comply with the information security policy if he or she is provided with no guidance or flexibility in determining how to handle exceptional situations. Therefore, it is in the best interests of an organization to develop and implement an information security policy that provides employees with guidelines on how to deal with exceptional situations and grants them a degree of voluntariness in adhering to those guidelines, particularly in cases where the terms of the policy contradict the organization's business goals and objectives.

Information security policies need to be designed to provide clarity, flexibility and usability to employees whether they violate the policy, intend to comply with it or do comply with it during exceptional situations that address the impact of the perceived benefits of non-compliance. The research study demonstrated how a design science

research approach can be useful not only for the design of IS information security policies but also for the design of a research instrument to study exceptional situations in the implementation of IS information security policies. This study uses a design science research (Hevner et al., 2004) approach that readily lends itself to the need for information security research that equally supports the critical elements of rigor and relevance. The caution and detail used in the methodologies and tools of design science research aid researchers in developing a more distinct and refined approach to the research problem and solution space prior to beginning substantive studies.

In order to develop additional processes and procedures for creating research instruments that aid in the design of information security policies in exceptional situations, it is necessary to evaluate, compare and contrast various research techniques. Information gleaned from the design science research field in IS is valuable in ascertaining the stringent development of research tools that provide highly effective results for determining research methods and practices to use in the design of information security policies in exceptional situations.

The results of this study suggest that design science research principles and kernel theory techniques provide clarity, comprehensiveness, ease of use and flexibility to influence practitioners when designing and implementing information security policies in exceptional situations in emergent organizations. Therefore an important factor to take into account is that the design, development and implementation of information security policies that allow deliberate violations of their terms by employees in emergent organizations decreases the information security consequences in exceptional situations.

Reference

- Anderson, J. (2003). Why we need a new definition of information security. *Computers and Security*, 22(4), 308-313.
- Alatalo, T., Oinas-Kukkonen, H., Kurkela, V., & Siponen, M. (2002). Information systems development in emergent organizations. In *Information Systems Development* (pp. 115-122). New York, NY: Springer.
- Al-Awadi, M. (2010). *A study of employees' attitudes towards organisational information security policies in the UK and Oman*. *Information Security*. University of Glasgow. Retrieved from <http://theses.gla.ac.uk/860/>
- Avison, D., & Fitzgerald, G. (1995). *Information systems development: Methodologies, techniques and tools* (2nd ed.). London: McGraw-Hill.
- Bahtiyar, S., & Ufuk Çaglayan, M. (2012). Extracting trust information from security system of a service. *Journal of Network and Computer Applications*, 35(1), 480–490.
- Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Journal of Logistics Information Management*, 15(5/6), 2-8, 337-346. doi:10.1108/09576050210447019
- Baskerville, R., Pries-Heje, J., & Venable, J. (2007). Soft design research: Extending the boundaries of evaluation in design research. *Proceedings of the 2nd DESRIST Conference, Pasadena, CA, May 13-15, 2007* (pp. 19-38). Ann Arbor, MI: UMI Dissertations Publishing.
- Bentham, J. (1907). *An Introduction to the principles of morals and legislation*. Oxford: Clarendon Press. Retrieved from <http://www.econlib.org/library/Bentham/bnthPML.html> (Original work published 1780)
- Besnard, D., & Arief, B. (2004). Computer security impaired by legal users. *Computers & Security*, 23(3), 253-26. doi:10.1016/j.cose.2003.09.002
- Beswick, D. (2002). Management implications of the interaction between intrinsic motivation and extrinsic rewards. Retrieved from <http://www.beswick.info/psychres/management.htm>
- Bjorck, F. (2004). Institutional theory: A new perspective for research into IS/IT security in organisations. *Proceedings of the 37th Hawaii International Conference on System Sciences*. Retrieved from <http://csdl.computer.org/dl/proceedings/hicss/2004/2056/07/205670186b.pdf>

- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164.
- Bostrom, R., Gupta, S., & Thomas, D. (2009). A meta-theory for understanding information systems within sociotechnical systems. *Journal of Management Information Systems*, 26(1), 17-47. doi:10.2753/MIS0742-1222260102
- Bosworth, S., & Kabay, M. E. (2002). *Computer Security Handbook* (4th ed.). New York, NY: John Wiley & Sons, Inc.
- British Standards Institution (BSI). (2012). Standards and Publications. Retrieved from <http://www.bsiamerica.com/Standards-and-Publications/>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548. MIS Quarterly & The Society for Information Management.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009, August). Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. *Computational Science and Engineering*. Paper presented at 12th IEEE International Conference on Computational Science and Engineering, Vancouver, Canada, 29-31 August (pp. 476-481). Los Alamitos, CA: IEEE Computer Society
- Cisco Systems. (2008, October 21). Data leakage worldwide: The effectiveness of security policies. Retrieved from http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.html
- Campbell, D. T., & Stanley, J. C. (1963). *Experimental and quasi experimental designs for research*. Chicago, IL: Rand McNally.
- Cohen, J. (1973). Eta-squared and partial eta-squared in fixed factor ANOVA designs. *Educational and Psychological Measurement*, 33, 107-112. DOI: 10.1177/001316447303300111
- Creswell, J. W. (2008). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage.
- Clifford, S. (2005, May 1). So many standards to follow, so little payoff. *Inc. Magazine*. Retrieved from <http://www.inc.com/magazine/20050501/management.html>

- Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences*, 3rd Ed. Mahwah, NJ: Lawrence Erlbaum Associates.
- Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Boston, MA: Houghton Mifflin Company.
- D'Arcy, J., Hovav, A., & Galletta, D. (2008). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98. INFORMS: Institute for Operations Research.
- D'Aubeterre, F., Iyer, L. S., & Singh, R. (2009). An empirical evaluation of information security awareness levels in designing secure business processes. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*.
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.
- Da Veiga, A., Martins, N., & Eloff, J.H.P. (2007). Information security culture - validation of an assessment instrument. *Southern African Business Review*, 11(1), 147-166.
- Dawes, J. (2008). Do data characteristics change according to the number of scale points used? *International Journal of Market Research*, 50(1), 61-77.
- Desman, M.B. (2001). *Building an information security awareness program*. Boca Raton, FL: Auerbach Publications. Retrieved from <http://www.crcnetbase.com/isbn/9781420000054>
- DeVellis, R. F. (2011). *Scale development: Theory and applications* (Vol. 26). Sage Publications, Incorporated.
- Dhillon, G., & Backhouse, J. (2000). Information systems security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.
- Dillman, D. A., Smyth, J. D., & Christian, L. M. (2009). *Internet, mail and mixed-mode surveys: The tailored design* (3rd ed.). Hoboken, New Jersey: John Wiley & Sons, Inc
- Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 386-408.

Dix, A., Finlay, J., Abowd, G. & Beale, R. (2004). Human-computer interaction (3rd ed.) Available from <http://www.pearsonhighered.com/educator/product/HumanComputer-Interaction/9780130461094.page>

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29(6), 449-457.

Dunkerley, K., & Tejay, G. (2009). Developing an information systems security success model for government context. *AMCIS 2009 Proceedings* (pp. 3-9). Retrieved from <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan040963.pdf>

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), 67-87.

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, 26(4), 584-593.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, 2005(11), 10-16.

GASSP (1999, June). Generally Accepted System Security Principles, version 2.0. *Information Systems Security*, 8(3). Retrieved from <http://all.net/books/gassp2/index.html>

Gaunt, N. (1998). Installing an appropriate information security policy. *International Journal of Medical Informatics*, 49(1), 131-134.

Gaunt, N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics*, 60(2), 151-157.

Gay, L. R. (1996). Educational research: Competencies for analysis and application (5th ed.). New York: Macmillan.

Gonzalez, J., & Sawicka, A. (2002). A framework for human factors in information security. *Methodology*. 02, 1-6. WSEAS International Conference on Information Security. World Scientific and Engineering Academy and Society (WSEAS). Retrieved from <http://www.wseas.com/wseas/books/brazil2002/papers/448-187.pdf>

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, 30(3), 611-642.

- Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, 8(5), 312-335.
- Hadasch, F., Mueller, B., & Maedche, A. (2011). Leaking confidential information by non-malicious user behavior in enterprise systems – design of an empirical study. *MCIS 2011 Proceedings*. Retrieved from <http://aisel.aisnet.org/mcis2011/126>
- Herath, T., & Rao, H. R. (2009, May). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165. doi:10.1016/j.dss.2009.02.005
- Hevner, A., March, S.T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75-105. doi:10.2307/249422
- Hevner, A., Chatterjee, S. (2010). Design research in information systems. *Theory and practice*. (22) Springer-Verlag.
- Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods*. 1(1)
- Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computer & Security*. 14(5), 377-383. doi:10.1016/0167-4048(95)97088-R
- Hone, K., & Eloff, J.H.P. (2002, October 1). Information security policy – what do international security standards say? *Computers & Security*, 21(5), 402-409. doi:10.1016/S0167-4048(02)00504-7
- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6), 54-60. doi:10.1145/1953122.1953142
- ISO/IEC Directives, Part 2. (2011, April). Rules for the structure and drafting of international standards (6th ed.). Retrieved from http://www.iec.ch/members_experts/refdocs/iec/isoiec-dir2%7Bed6.0%7Den.pdf
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly & The Society for Information Management*, 34(3), 549-566.
- Kant, I. (2002). *Groundwork for the metaphysics of morals*. New Haven and London: Yale University Press. (Original work published 1785)

Knapp, K.J., Marshall, T. E., Rainer, K. R., Jr., & Ford, F. N, (2006) Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36. doi: 10.1108/09685220610648355

Knapp, K. J., Morris, R. F., Marshall, T. E., & Anthony, T. (2009). Information security policy : An organizational-level process model. *Computers & Security*, 28(7), 493-508. doi:10.1016/j.cose.2009.07.001

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), 518-555.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers and Security*, 24(3), 246-260. doi:10.1016/j.cose.2004.08.011

Kingsford, R. (2008). Development and support of complex information systems in emergent organizations: Structures, processes and governance. Doctor of Philosophy thesis, School of Information Systems and Technology, University of Wollongong. <http://ro.uow.edu.au/theses/1999>

Kolkowska, E., & Dhillon, G. (2012). Organizational power and information security rule compliance. *Computers & Security*, 1-9.

Kuechler, W. L. and Vaishnavi, V. K. (2008). Theory development in design science research: Anatomy of a research project. In proceedings of the Third International Conference on Design Science Research in Information Systems and Technology (DESRIST 2008).

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, 11(7), 394-413. doi: 10.1.1.170.5816

Lineberry, S. (2007). The human element: The weakest link in information security. *Journal of Accountancy*, 204(5), 44-49.

Long, G. P. (2002). Security policies in a global organization. SANS Institute InfoSec Reading Room. Retrieved from http://www.sans.org/reading_room/whitepapers/policyissues/security-policies-global-organization_501

March, S. T., and Smith, G., (1995). Design and natural science research on information technology. *Decision Support Systems* 15(4), 251-266.

- Markus, M.L., A. Majchrzak, and L. Gasser (2002). A Design theory for systems that support emergent knowledge processes. *MIS Quarterly*, 26(3), 179-212.
- McFadzean, E., Ezingard, J. N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, 31(5), 622-660.
- Mitnick, K. D., & Simon, W. L. (2002, October). *The art of deception: Controlling the human element of security*. Indianapolis, Indiana: Wiley Publishing, 2002.
- Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, 2(3), 192-222.
- Nelder, J.A., & Wedderburn, R.W.M. (1972). Generalized linear models. *Journal of the Royal Statistical Society, Series A* 135(3), 370-384.
- Nigam, A., & Siponen, M. (2011). Designing information systems security policy methods: A meta-theoretical approach. *Proceedings of JAIS Theory Development Workshop. Sprouts: Working Papers on Information Systems*, 11(150). Retrieved from <http://sprouts.aisnet.org/11-150>
- Krupansky, J. (2005, December 16). Definition: Non-normative. Activity. Retrieved from http://activity.com/def/non_normative.htm
- Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *40th Hawaii International Conference on System Sciences* (pp. 1-10).
- Parker, D. B. (1997). Information Security in a Nutshell. *Information Security Journal: A Global Perspective*, 6(1), 14-19. doi:10.1080/10658989709342524
- Preece, J.R., Rogers, Y., & Sharp, H. (2007). *Interaction design: Beyond human-computer interaction*. 3rd ed. New York, NY: John Wiley & Sons.
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778.
- Renaud, K. (2012). Blaming noncompliance is too convenient: What really causes information breaches? *Security & Privacy, IEEE*, 10(3), 57-63. doi: 10.1109/MSP.2011.157

- Ross, D. (2003). *The Right and the Good*. Oxford: Clarendon Press. Retrieved from <http://www.oxfordscholarship.com/view/10.1093/0199252653.001.0001/acprof-9780199252657> (Original work published 1930)
- Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Boston, MA: Houghton Mifflin.
- Seddon, J. (2000, November 18). The 'quality' you can't feel. *The Guardian*. Retrieved from <http://www.guardian.co.uk/money/2000/nov/19/workandcareers.madeleinebunting>
- Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, 22(5), 428-438.
- Shoraka, B. (2011). An empirical investigation of the economic value of information security management system standards. Available from ProQuest Dissertations and Theses database. (UMI No. 3456209).
- Simon, H.A. (1996). *The Science of the Artificial*, (3rd ed.) MIT Press, Cambridge, Mass.
- Sipior, J., & Ward, B. (2008). A framework for information security management based on guiding standards: a United States perspective. *The Journal of Issues in Informing Science and Information Technology*, 5, 51-60.
- Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management Computer Security*, 8(1), 31-41.
- Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems*, 7(7), 445-472.
- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2), 64-71.
- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly & The Society for Information Management*, 34(3), 487-502.
- Smith, Peni D. (2004). Developing & implementing an information security policy and standard framework. SANS Institute InfoSec Reading Room. Retrieved from http://www.sans.org/reading_room/whitepapers/hipaa/developing-implementing-information-security-policy-standard-framework_1401
- Sommerville, I. (2007). *Software engineering* (8th ed.). New York: Addison-Wesley.

- Soo Hoo, K. J. (2000, June). How much is enough? A risk-management approach to computer security. *Workshop on Economics and Information Security* (pp. 1-99). doi:10.1.1.16.4127
- Spears, J. (2006). A holistic risk analysis method for identifying information security risks. In Dowland, P., Furnell, S., Thuraisingham, B., & Wang, X. (Eds.). *Security Management, Integrity, and Internal Control in Information Systems, 193*, 185-202. Boston: Springer.
- Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers Security, 24*(2), 124-133. doi:10.1016/j.cose.2004.07.001
- Stewart, D., Shamdasani, P.N., & D.W. Rook. (2007). *Focus groups: Theory and practice* (2nd ed., Vol. 20.). Newbury Park, CA: Sage Publications.
- Straub, D.W., & Nance, W.D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60. doi:10.2307/249307
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information System Research, 1*(2), 255-277. doi:10.1287/isre.1.3.255
- Straub, D.W., & Welke, R.J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly, 22*(4), 441-64. doi:10.2307/249551
- Sun, YL., Z Han, Liu. KJR., (2008). Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine, 46*, 112-9
- Surowiecki, J. (2008, April 28). Parsing Paulson. *The New Yorker*. Retrieved from http://www.newyorker.com/talk/financial/2008/04/28/080428ta_talk_surowiecki.
- Terrell, S. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York: Guilford Press.
- Theoharidou M., Kokolakis S., Karyda M., & Kiountouzis E., (2005). The insider threat to information systems and the effectiveness of ISO 17799. *Computers & Security, 24*(6), 472-484.
- Tidd, J., & Bessant, J. (2011). *Managing innovation: integrating technological, market and organizational change* (4th ed.). Chichester, England: Wiley.

- Verendel, V. (2009). Quantified security is a weak hypothesis. *Proceedings of the 2009 workshop on New security paradigms workshop - NSPW '09*, 37.
- Von Solms, R. (1999). Information Security Management: Why Standards are Important. *Information Management & Computer Security*, 7(1), 50-57. doi:10.1145/310930.310984
- Von Solms, R. and Von Solms, B. (2004). From policies to culture. *Computers & Security*, 23(6), 504-508. doi:10.1016/j.cose.2004.01.013
- Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computer & Security*, 23(6), 191-198.
- Walls, J.G., Widmeyer, G.R., and El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. *Information Systems Research*, 3(1) 36-59.
- Wang, J., Chaudhury, A., and Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research*, 19(1), 106 - 120. doi: 10.1287/isre.1070.0143
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101-105. doi:10.1057/ejis.2009.12
- Warman, A.R. (1992). Organizational computer security policy: the reality. *European Journal of Information Systems*, 1(5), 305-10. doi:10.1057/ejis.1992.2
- West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2009). The weakest link: A psychological perspective on why users make poor security decisions. In M. Gupta, & R. Sharman (Eds.), *Social and human elements of information security: Emerging trends and countermeasures* (pp. 43-60). Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-036-3.ch004
- Wheelen, T., and Hunger, J., (2008). *Strategic Management and Business Policy: Concepts and Cases*, New Jersey: Pearson Prentice and Hall Pub.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816. doi:10.1016/j.chb.2008.04.005
- Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, 58(2), 212-222.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, 24(1)

Appendix A

Hypothetical Scenario:

“Jack works in a software house, which has strict security rules laid down by a senior security specialist, who is regarded as the authority figure in security matters. The security policy includes a rule that states that passwords are personal and that one’s password cannot be given to anybody else. Any exception must be approved by the senior security specialist. During the summer, while the senior security specialist and most of the developers are on their holidays, Jack and a few of his co-workers receive additional requirements for feature changes from an important customer. Jack needs to make changes to the software quickly in order to keep to the deadline. To do this, Jack needs to access some files to which he currently does not have access (access can be granted by a developer, who is on his holiday at that time, and the security specialist or his subordinates). Jack cannot reach the senior security specialist at that time, and the developer who has control over the files is also on holiday. He is available, but cannot remember his password any more (he forgot it while on holiday). Jack contacts Matt, who is a subordinate of the senior security specialist, but Matt wonders if he dares to violate the IS security policy of the organization. If Matt does not grant access to Jack, the result is that the software company will miss the deadline, which further results in the software company having to compensate the client financially. This may further damage the reputation of the software company, which in turn may reduce future contracts, and lead to other consequences.”

Appendix B

Survey Questionnaire:

Please read each statement; then indicate the degree to which you agree/disagree with the statement as it relates to the hypothetical scenario by selecting the appropriate answer.

Gender:

Male: ___ Female: ___

Age:

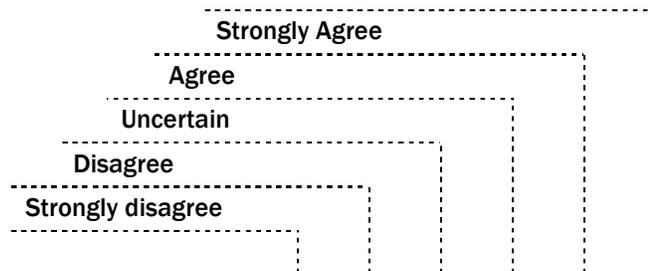
18 – 29 ___ 30 – 39 ___ 40 – 49 ___ 50 – 65 ___

Educational Level:

High School ___ AA/AS ___ BA/BS ___ MA/MS ___ Doctorate ___

Security Certification:

CISSP ___ CISM ___ CISA ___ Other ___



- | | | | | | |
|---|---|---|---|---|---|
| 1. If I was Matt I would dare to violate the information security policy in the described hypothetical scenario. | 1 | 2 | 3 | 4 | 5 |
| 2. If I were absolutely sure that the benefits of violating the IS security policy and guidelines in the example situation would exceed the costs, I would be ready to violate the policy and guidelines. | 1 | 2 | 3 | 4 | 5 |
| 3. It is okay to violate the company information security policy if no damage is done to the company. | 1 | 2 | 3 | 4 | 5 |

- | | | | | | |
|---|---|---|---|---|---|
| 4. It is acceptable to violate a company information security policy to get a job done. | 1 | 2 | 3 | 4 | 5 |
| 5. If you were the president of the organization, would you allow violation of the IS security policy by any trustworthy member of the project group in order to speed up software development? | 1 | 2 | 3 | 4 | 5 |
| 6. It would cause problems in my life if I jeopardized my future job promotion prospects for taking the actions that Jack did in the hypothetical scenario. | 1 | 2 | 3 | 4 | 5 |
| 7. It would cause problems in your life if you were formally sanctioned for taking the actions that Jack did in the hypothetical scenario. | 1 | 2 | 3 | 4 | 5 |
| 8. I feel that general adherence to my company's information security policy compensates for occasionally violating its terms. | 1 | 2 | 3 | 4 | 5 |
| 9. I feel my hard work in the company compensates for occasionally violating an information security policy. | 1 | 2 | 3 | 4 | 5 |
| 10. It is okay to violate the company information security policy when you are in a hurry. | 1 | 2 | 3 | 4 | 5 |
| 11. I would be unhappy if others knew that I had violated a company's information security policy. | 1 | 2 | 3 | 4 | 5 |
| 12. It would cause me problems if I felt unhappy that managers knew that I had violated the company information security policy. | 1 | 2 | 3 | 4 | 5 |
| 13. I would be unhappy if team members knew that I had violated a company's information security policy. | 1 | 2 | 3 | 4 | 5 |
| 14. It is acceptable to violate the company information security policy if circumstances seem to offer you little other choice. | 1 | 2 | 3 | 4 | 5 |
| 15. It is okay to violate the company information security policy if no harm is done to me or to another colleague. | 1 | 2 | 3 | 4 | 5 |

- | | | | | | |
|--|----------|----------|----------|----------|----------|
| 16. If I knew that violation of IS security policy and guidelines in the example situation represented just and honest action, I would be ready to violate the policy and guidelines. | 1 | 2 | 3 | 4 | 5 |
| 17. If the proposed action does not comply with Company policy, but lead to business success, would you violate the IS security policy? | 1 | 2 | 3 | 4 | 5 |
| 18. It is not as wrong to violate a company information security policy that is not reasonable. | 1 | 2 | 3 | 4 | 5 |

Appendix C

The following table depicts the how each question is linked to hypotheses and research model.

Question Number	Hypotheses	Design Theory
1	H1	Prima-Facie
2	H1	
3	H1	
4	H1	
5	H1	
6	H1	
7	H2	Utilitarian
8	H2	
9	H2	
10	H2	
11	H2	
12	H2	
13	H3	Universalizability
14	H3	
15	H3	
16	H3	
17	H3	
18	H3	