

2021

Orientation and Social Influences Matter: Revisiting Neutralization Tendencies in Information Systems Security Violation

Frank Curtis King

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



Part of the [Computer Engineering Commons](#), [Computer Sciences Commons](#), and the [Library and Information Science Commons](#)

Share Feedback About This Item

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

Orientation and Social Influences Matter: Revisiting Neutralization Tendencies in
Information Systems Security Violation

by
Frank King Jr.

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

College of Computing and Engineering
Nova Southeastern University

2021

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

Souren Paul

Souren Paul, Ph.D
Chairperson of Dissertation Committee

4/26/21

Date

[Signature]

Prasad Rudramuniyaiah, Ph.D.
Dissertation Committee Member

4/26/21

Date

[Signature]

Ling Wang, Ph.D.
Dissertation Committee Member

4/26/21

Date

Approved:

Meline Kevorkian

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

4/26/21

Date

College of Computing and Engineering
Nova Southeastern University

2021

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

Orientation and Social Influences Matter: Revisiting Neutralization Tendencies in Information Systems Security Violation

By

Frank C King Jr.
April 2021

It is estimated that over half of all information systems security breaches are due directly or indirectly to the poor security practices of an organization's employees. Previous research has shown neutralization techniques as having influence on the intent to violate information security policy. In this study, we proposed an expansion of the neutralization model by including the effects of business and ethical orientation of individuals on their tendencies to neutralize and compromise with information security policy. Additionally, constructs from social influences and pressures have been integrated into this model to measure the impact on the intent to violate information security policy from social perspectives.

This study is a quantitative study that used a survey methodology for data collection. A stratified sampling method was used to ensure equal representation in the population. A sample of members was collected using a random sampling procedure from each stratum. All data were collected by sending a survey link via email through SurveyMonkey's participant outreach program to the aforementioned groups. Partial least squares were used for data analysis.

Findings showed business and ethical orientation had a negative impact on accepting neutralization techniques which ultimately result in the intent to violate information security policy. Furthermore, this research found neutralization, social influences, and social pressures as having 24 percent of influence to violate information security policy. Business orientation and ethical orientation contributed to 15 percent of influence in variance on employees accepting neutralization techniques.

Implications of this research suggest information security policies can be compromised by employees and additional measures are needed. Behavioral analytics may provide an understanding of how employees act and why. Routine training is necessary to help minimize risks, and a healthy security culture will promote information security as a focal point to the organization.

Acknowledgements

First, I would like to thank God for seeing me through this journey, for with Him, all things are possible. I would like to dedicate this degree to my late father, Frank C. King, Sr., who passed shortly after I began this program. Accomplishing such academic success would have made him proud. I love and miss him very much.

This degree would have not been possible without a great team. To my committee chair, Dr. Paul, I express my sincere gratitude and appreciation for your guidance as my dissertation chair. I truly appreciate your commitment, even after you departed ways with Nova Southeastern University. You remained resolute in the quest for my successful completion of this degree, and for that I am grateful.

To Dr. Wang, I thank you for agreeing to be a part of my committee. Your feedback through all facets of this process was invaluable. Thank you for your guidance and encouragement, both of which helped me remain focused throughout this process. To Dr. Rudramuniyaiah, thank you for agreeing to be on my committee and for providing excellent feedback and support. It is truly because of all of you that I can complete this journey and focus on the next phase of my career.

To my family, I thank all of you for your understanding, words of wisdom, and unwavering support. There were times I needed to realign priorities to complete this process, and you graciously gave me the space and time I needed. While you often took a “back seat” on this journey, your love and support did not go unnoticed. I appreciate you more than you know.

To all of you, I sincerely thank you, and I appreciate your support and contributions to the accomplishment of this momentous milestone. THANK YOU, THANK YOU
THANK YOU!

Table of Contents

Abstract	ii
Acknowledgements	iii
List of Tables	vii
List of Figures	viii

Chapters

1. Introduction	1
Problem Statement	3
Goal	5
Research Questions	6
Relevance and Significance of the Study	6
Barriers and Issues	8
Limitations	8
Delimitations	9
Definitions of Terms	9
Summary	11
2. Literature Review	13
Theoretical Foundation	14
Business Orientation	16
Ethical Orientation	21
Neutralization Theory	25
Neutralization Techniques	30
Social Influences	33
Social Pressures	38
Summary	43
Contributions of the Research Study	44
3. Methodology	46
Research Method	46
Instruments and Measures	47
Validity and Reliability	52
Data Collection	54

Population and Sample	56
Data Analysis Strategy	58
Resources Requirements	60
Summary	61

4. Results 63

Pre-Analysis Data Screening	63
Data Analysis	66
Hypotheses Testing	75
Summary	778

5. Conclusions 79

Discussion	80
Limitations and Future Studies	84
Conclusion	86

Appendices

A. Summary of Prior Research on Employees IS Security Violations	88
B. Summary of Prior Research on Business Orientation	90
C. Summary of Prior Research on Ethical Orientation	95
D. Summary of Prior Research on Neutralization	99
E. Summary of Prior Research on Social Influences	102
F. Summary of Prior Research on Social Pressures	105
G. NSU Consent to be in a Research Study	107
H. Survey Questionnaire	109
I. IRB Approval	116
J. Collected Data (n=206)	117
K. Stem & Leaf, Q-Q Plots, Histogram	120
L. PLS Analysis, Model Fit, Reliability, Validity, Coefficient and Outer loading	136
M. PLS Analysis After Deleting N7, N10, and SI4	138
N. PLS Analysis with Bootstrapping	141
O. Organizational Statistical Information	142
P. Reliability and Validity	144
Q. Discriminant Validity of Constructs	146

References 156

List of Tables

Tables

1. Definitions of Six Techniques from the Neutralization Theory 30
2. Constructs and Instrument Source 49
3. Distribution of Organizational Samples 58
4. Model Fit and Accepted Values 66
5. Outer Model Loadings 68
6. Construct Reliability and Validity 69
7. Discriminant Validity: Indicator and Item Cross Loadings 70
8. Discriminant Validity (Fornell and Larcker Criterion) 71
9. Discriminant Validity Heterotrait-Monotrait Ratio (HTMT) 71
10. Descriptive Statistics for Organizational Groups 73
11. Descriptive Statistics for Gender 73
12. Descriptive Statistics for Organizational Size 74
13. Descriptive Statistics for Model Constructs 74
14. Summary of Hypothesis Tests 775

List of Figures

Figures

1. Research Model: Expansion of Neutralization Model 16
2. PLS Analysis Results for Intent to Violate Information Security Policy 77

Chapter 1

Introduction

Studies in violation of information security policy have historically been reviewed from the perspective of deterrence theory, by both practitioners and IS scholars (Kankanhalli et al., 2003; Straub, 1990; Teo et al., 2003). Siponen and Vance (2010) recognized that all IS violations cannot be best explained through the lens of deterrence theory by fear of sanctions because employees typically fall into neutralization techniques (Sykes & Matza, 1957). Deterrence theory claims that both law-abiding citizens and those that commit rule breaking believe the norms and values of the community in general (Sykes & Matza, 1957). Siponen and Vance (2010) built on the previous research model that identified the constructs shame, informal sanctions, and formal sanctions as independent variables that influence the intention to violate IS security policy. Siponen and Vance (2010) created a multidimensional second-order construct with several distinct dimensions that exist within the construct neutralization. The research model illustrated the causal effect the first order constructs—denial of responsibility, denial of injury, defense of necessity, metaphor of the ledger, condemnation of the condemners, and appeal to higher loyalties—have on neutralization. In turn, the research model of Siponen and Vance demonstrates the effect neutralization has on the intention to violate IS security policy. Neutralization theory initially was used

in the study of criminology and sociology and soon was applied in the field of information systems security.

Because of the gap in the inability to explain dismissal of normative behavior, neutralization theory provides a method of understanding how an individual can engage in delinquency without damaging one's self-image. The findings of Siponen and Vance (2010) suggest that neutralization techniques influence employee's intentions to violate IS security policies. However, their research did not explain why employees drift into a neutralization state in the first place. This research filled that gap and evaluated business and ethical orientation perspectives of employees prior to accepting neutralization techniques. Moreover, the examination of cognitive thought processes from both a business and ethical orientation provided more insight into why employees ultimately violate information system security policy. Human factors, for instance, have always been predominantly seen as the number one threat to an organization's risk management. Therefore, business and ethical orientation factors are now in question as to why certain incidents occur more than others. Likewise, the theory of neutralization has become useful in aiding in a better explanation of how users are able to rationalize certain actions prior to committing intention to violate IS policy. Notwithstanding, business and ethical orientation, neutralization theory, and social influences and pressures are important factors to take into account prior to writing IS policies for organizations. Previous research from Siponen and Vance (2010) showed that neutralization played a role in employees' intent to violate IS policy; however, it did not show or explain why employees drift into such a state in accepting these techniques.

The main goal of this research study is to contribute to the body of knowledge in exploring new insights into why employees drift into a state of neutralization and violate IS policies. The need for this work was suggested by the work of Siponen and Vance (2010) in their article, “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations.” The term “drift” can be defined as “a temporary period of irresponsibility or an episodic relief from moral constraint” (Maruna & Copes, 2005, p. 231). Siponen and Vance illustrated a perspective in which employees may drift into neutralization techniques unknowingly because they are subconsciously making business and ethical decisions based on their own business and ethical orientation. Cognitive frames may make employees blind when confronting decisions to violate IS policy. Employees may be limited due to the fact they may not see the ethical big picture. Consequently, employees may not consider business decisions as ethical decisions, thus, different decisions are made. Further research was needed to examine the way in which a decision is framed that enables employees to drift into a state of neutralization and ultimately commit the intent to violate IS policy. Furthermore, the research model incorporated a holistic view of the various perspectives that either directly or indirectly affect the overall influences on the intent to violate IS policy through the lens of social influences and pressures (Siponen & Vance, 2010).

Problem Statement

This study addressed the research problem of why employees drift into a state in which they begin using neutralization techniques and violate employee information system (IS) security policy. In this context, I responded to the need to better understand why employees ultimately violate IS policy after consciously or subconsciously accepting

one of six neutralization techniques. Maruna and Copes (2005) defined neutralization as a theory of delinquency that illustrates the excuses and justifications which deviants use to rationalize behaviors that might themselves be implicated in the etiology of deviant behavior.

Although advances in hardware and software technologies have made great strides, human beings are still the weakest link in the defense against internal security attacks. More importantly, employees are considered the biggest threat to an organization because they are trusted with the knowledge and privilege of the organization's resources and therefore pose the biggest danger given their intimate knowledge about the organizational systems and the permissions they receive. In 2008, a survey from CSI Computer Crime and Security Survey reported that 44% of survey respondents reported that insider abuse was the second most frequent form of security breach (Richardson et al., p. 2). D'Arcy et al. (2009) investigated insider misuse and found that insider misuse is a significant threat to organizations. Siponen and Vance (2014) conducted a study that showed knowledgeable college students, who were well abreast of safe practices, failed to comply with safe computing. In their empirical study using a rational choice model, students continued to disclose passwords and failed to practice safe computing.

Previous research links individual-level values, ethics, and ethical decision making to cultural focus (Beekun & Westerman, 2012; Fok et al., 2016). Recent attention over the past years has focused on formal and informal control mechanisms to manage employee's behavior. Such control mechanisms include policies, procedures, organizational culture, and the examination of how employees play a role in security. Most of these mechanisms have failed and are indicators of ineffective security

governance that do not address the individual values or beliefs by which decisions are made. Hence, this research focused on two critical issues that have received little to no attention in the literature: (a) identification of the factors that influence employee's cognitive decision making, and (b) investigation of the impact social influences and social pressures have on the intent to violate IS policy.

Goal

The main goal of this research study was to address, from a business and ethical orientation, why employees drift into a state in which they begin using neutralization techniques and, ultimately, violate employee IS security policy. The first specific goal of this study was to evaluate business orientation and its sub constructs—customer orientation, competitor orientation, and inter-functional coordination—and the relationship business orientation has to neutralization techniques (appeal to higher loyalties, defense of necessity, and metaphor of the ledger). The second specific goal of this research study was to evaluate ethical orientation and its subcomponents—personal belief, personal attitude, personal values, and moral orientation—and the relationship ethical orientation has to the neutralization techniques (condemnation of the condemners, denial of injury, and denial of responsibility). The third specific goal of this research study was to evaluate the social influences—attachment and involvement—and determine the effect of social bonds on the intent to violate IS policy. The fourth and final specific goal of this study was to evaluate the social pressures—subjective norms and descriptive norms—that influence employees' commitment to violate IS policy.

Research Questions

The main research question (RQ) this study addressed is: *Do employees knowingly make business or ethical decisions when accepting one of the six neutralization techniques with the intent to violate information security policy?* This question was addressed from the perspective of understanding employees' cognitive thinking from both a business and ethical orientation perspective. The study addressed this gap by explaining why employees drift into a state of neutralization and influence the intention to violate IS security policy. Therefore, this research will focus on the following research questions:

RQ1: What factors influence employees to accept neutralization techniques?

RQ2: What social factors influence employees to violate information security policy?

Relevance and Significance of the Study

Relevance

Due to employees being a key factor in IS breaches, research in this area continues to be relevant (D'Arcy et al., 2009; Sippeon & Vance, 2010; Furnell & Clarke, 2015). The proliferation of occurrences in breaches are directly or indirectly related to poor security practices by employees (Sippeon & Vance, 2010). Employees' individual perceptions, beliefs, and biases significantly influence security policy compliance behavior (Karyda & Kokolakis, 2015).

Crossler et al. (2013) noted that future direction in research regarding employee's intent to violate IS policy should address separating insider deviant behavior from insider misbehavior. Furthermore, Cheng et al. (2013) researched security incident occurrences

in the workplace through both formal and informal control factors as well as deterrence theory. The relevance of their study is twofold: (a) evaluate the influence that constructs business orientation and ethical orientation have on employees accepting neutralization techniques and, ultimately, violating IS policy; and (b) evaluate the influence the social constructs (attachment, involvement, subjective norm, and descriptive norm) have on the intent to violate IS policy.

This study was obviously influenced by Sippeon and Vance (2010), but it was also influenced by Cheng et al. (2013) and Herath (2009) in that constructs from their respective research models influenced the combining of the constructs of social influences and social pressures in this research model. The intent of this approach is to (a) better understand how employees make decisions from either an ethical or business perspective, and (b) combine social influences and social pressures constructs and evaluate their influence on the intent to violate IS policy. These constructs arguably can be used to evaluate the influence on accepting neutralization techniques, but the intent here is to only evaluate the impact of social influences and social pressures on the intent to violate IS policy.

With respect to business orientation and ethical orientation constructs in this research model, it is assumed that these specific neutralization techniques will relate to specific constructs in the mindset of employees accepting said techniques. The hypotheses are testable.

Significance

The significance of this research study is to gain a better understanding of the cognitive rationalization of employees as they make decisions from both a business and

ethical orientation. Notwithstanding, employees are the number one threat to an organization's security, and as a result, employees fall into neutralization techniques and commit security violations. This research provides an explanation for employees' cognitive thinking that enables them to make either business or ethical decisions to accept neutralization techniques and, ultimately, commit IS violations. As a result, this research will help practitioners, IS managers, and IS scholars in writing IS policy which can aid in reducing violations and thereby protect sensitive data.

Barriers and Issues

This study, like most studies, has typical limitations. First, the study collected data from a specified group of white-collar professionals working in either academia or the information technology and systems field. Therefore, some biases may exist to the sample and the generalizability to other organizations may not apply. Second, this survey study is an extension to previous research on the intent to violate IS policy, and the data collected is as only as good as the instrument used. In order to ensure a valid and reliable study, this research adopted valid instruments that have undergone rigorous validation for accurate data collection. Third, to ensure a good research design that participants clearly understand, it became important to conduct a pilot study to address any misleading questions. This research addressed this concern via pre-test of the survey instrument.

Limitations

As this study is based on questionnaire and scenario-based methodology, it is possible that results on the intent to violate IS policy may vary if an alternate scenario was presented that describes a different situation. This would ultimately affect content validity. Second, to manage this research, a small percentage of the population was

selected to capture data. Other industries and countries were not included in the scope of this research. Third, social influences and social pressures construct is only intended to evaluate their influences on the intent to violate IS policy. These constructs arguably can be used to measure the influence on accepting neutralization techniques. The intent here is only to evaluate the impact of social influences and social pressures on the intent to violate IS policy.

Delimitations

To manage the scope of this study, data were sent to three types of organizations: academic institutions, IT professional groups, and corporate organizations. Random sampling was used in this study to collect survey data and to make it generalizable to the population to avoid sampling bias. Since the only form of the survey is electronic, there exists sampling bias as paper-based surveys were not an option. Lastly, this study only considered organizations within the United States. It should be noted that similar organizations in other parts of the world may respond differently as security concerns are treated more rigorously in other countries.

Definitions of Terms

The following terms and definitions are used in this study.

Average Variance Extracted – measures the level of variance captured by a construct versus the level due to measurement error; values above 0.7 are considered very good, whereas the level of 0.5 is acceptable.

Construct Validity – is considered by Creswell (2002) as “a determination of the significance, meaning, purpose, and use of scores from an instrument” (p. 184).

Content Validity – is defined as “the extent to which the questions on the instrument and the scores from the questions are representative of all the possible questions that could be asked about the content or skills” (Creswell, 2002, p. 18).

Drift –can be defined as “a temporary period of irresponsibility or an episodic relief from moral constraint” (Maruna & Copes, 2005, p. 231).

Employee Commitment – is a sub-component of business orientation, suggest highly involved employees in the organization work hard and become highly involved in accomplishing the organizational goals (Arthur, 1994; Wood & De Menezes, 1998).

Ethical Orientation – “can be defined as a variable of study that refers to the approach an individual takes in making ethical judgment through ethical perceptions and sensitivity with the ability to recognize the ethical nature of a situation in a profession (Douglas et al., p. 102).

IT – is the abbreviation for “Information Technology.”

Inter-functional Coordination – “can be defined as the mechanism that facilitates the coordination between the various organizational units’ functionality” (Narver & Slater, 1990).

Neutralization –the act of rationalizing or justifying an immoral or illegal act (Silic et al., 2017).

Proportionate Stratified Random Sampling –is defined as a probability sampling design in which the number of sample subjects drawn from each stratum is proportionate to the total number of elements in a respective stratum.

Random Sampling – is “the collection of data where all possible subsets of a population or the sampling frame are given an equal probability of being selected” (Sekaran & Bougie, 2013, p. 245).

Reliability – “individual scores from an instrument should be nearly the same or stable on repeated administrations of the instrument, they should be free from sources of measurement error, and they should be consistent” (Creswell, 2002, p. 180)

Social influences – “employees in organizations that form bonds with the job, immediate supervisors, co-workers and the organization” Cheng et al. (2103, p. 451)

Stratified Random Sampling – is a probability sampling design that first divides the population into meaningful, non-overlapping subsets, and then randomly chooses the subsets from each subset.

Social Pressures – the subjective norms that refer to the perceived social pressure to perform the behavior in question” (Cheng et al., 2013)

Validity – “draws meaningful and justifiable inferences from scores about a sample or population” (Cresswell, 2002, p. 185)

Summary

The purpose of Chapter 1 was to introduce the existing research problem in the field of information technology security. This chapter identified the need to further explore why employees drift into a state in which they begin using neutralization techniques to violate IS policy. The research problem identified employees as still being the weakest link in the defense against internal attacks. Valid literature supporting the research problem and the need for this study was briefly presented. Chapter 1 also presented the main goal, specific goals, research questions, and hypotheses for this

research study. The main goal of this research study was to address the research questions from a business orientation and an ethical orientation. This chapter highlighted the conceptual model and hypotheses based on the research questions. The chapter also included barriers and issues that were encountered and noted. Four goals, along with the relevance and significance for this research study, were discussed. The chapter concluded with definitions of terms used for this research study.

Chapter 2

Literature Review

Introduction

In this chapter, a literature review will be presented to provide a synopsis of the relevant literature pertaining to violations of employee IS policy. A literature review is necessary to provide the foundation for research, and adequate knowledge of the history is necessary to have a comprehensive understanding of the body of knowledge. To acquire the knowledge, a comprehensive search of peer reviewed and secondary literature was performed to lay the necessary foundation for this research. Levy and Ellis (2006) said, “in any systemic approach, if the system input is either incorrect, of low quality, or irrelevant, the resulted output is going to be ineffective regardless of the quality of the processing stage or, colloquially, *garbage-in, garbage-out*” (p.185). From this process, it was determined the subject matter expands across interdisciplinary areas and, therefore, an extensive search was performed across multiple databases that included information systems domain, business, sociology, and psychology. This literature review presented four new constructs that were an extension to the Sippen and Vance (2010) research model: business orientation, ethical orientation, social influences, and social pressures. A comprehensive examination of these areas was conducted to address the critical need for organizations to understand why employees accept neutralization techniques and ultimately violate IS policy.

Theoretical Foundation

Information Systems Security Policy (ISSP) constitutes the written and defined statements an organization uses for security and management for their employees; it serves as guidelines for responsibility, obligations, sanctions, and countermeasures for non-compliance (Cheng et al., 2013). The increased interest of researchers in studying the factors that influence employees to violate IS practices has resulted in two major research streams: antecedents of ISSP violation behavior and factors leading to ISSP compliance behavior (Cheng et al., 2013). Vance and Siponen (2012) examined the effect of rational choice on ISSP violations; Hu et al. (2011) also tested employees' policy violation intention based on the rational choice theory and found perception of benefit had a significant influence on employees intended behavior. D'Arcy et al. (2009) proposed an extended deterrence model to examine the antecedents of insider IS misuse intentions. Ifinedo (2012) integrated protection motivation theory and the theory of planned behavior in an effort to better understand employees ISSP compliance intentions. Vance (2012) explored the extent of habit and protection motivation theories in driving employees IS security compliance. Siponen (2007) extended protection motivation theory to explain employees compliance towards ISSP and Siponen and Vance (2010) studied the compliance model and found coping appraisals did not significantly impact user attitudes toward compliance. Bulgurcu et al. (2010) found user's attitude towards ISSP compliance and their intentions are impacted by the cost, benefit assessment of compliance and non-compliance. Li, Zhang, and Sarathy (2010) also explored the effect of cost and benefit trade-off and personal norms on employees' internet use policy compliance intentions. Beautelement et al. (2009) found the key factors impacting employees' security policy

compliance decisions were the actual and anticipated cost and benefits of adherence for the individual employee. Herath and Rao (2009) demonstrated that security policy compliance intention can be influenced by intrinsic and extrinsic motivators and developed an integrated model based on the Taylor-Todd decomposed theory of planned behavior integrating the theories of general deterrence. Greene and D'Arcy (2010) examined the impact of security-related and employee organization relationship factors on employees IS security compliance decisions, while Bulgurcu et al. (2010) investigated the influence of employee's IS awareness and the perceived fairness of requirements of IS policy. Finally, Zhang and Reithel (2009) examined the impacts of perceived technical security policies.

These reviewed studies laid the foundation of the review of IS policy violations. Although the studies differ in terms of perspective, the extent in which the number of studies has drawn researchers' interest signifies the importance of the problem with employee violation of IS policy. Appendix A includes a summary of prior published research on employee IS security violations and a brief description of key aspects of each study. Figure 1 is a diagram of the research model. In the following sections, each construct is systematically inspected. The subsequent hypotheses required to test this model is drawn. Figure 1 includes a graphic depiction of the expansion of the neutralization model used in this study.

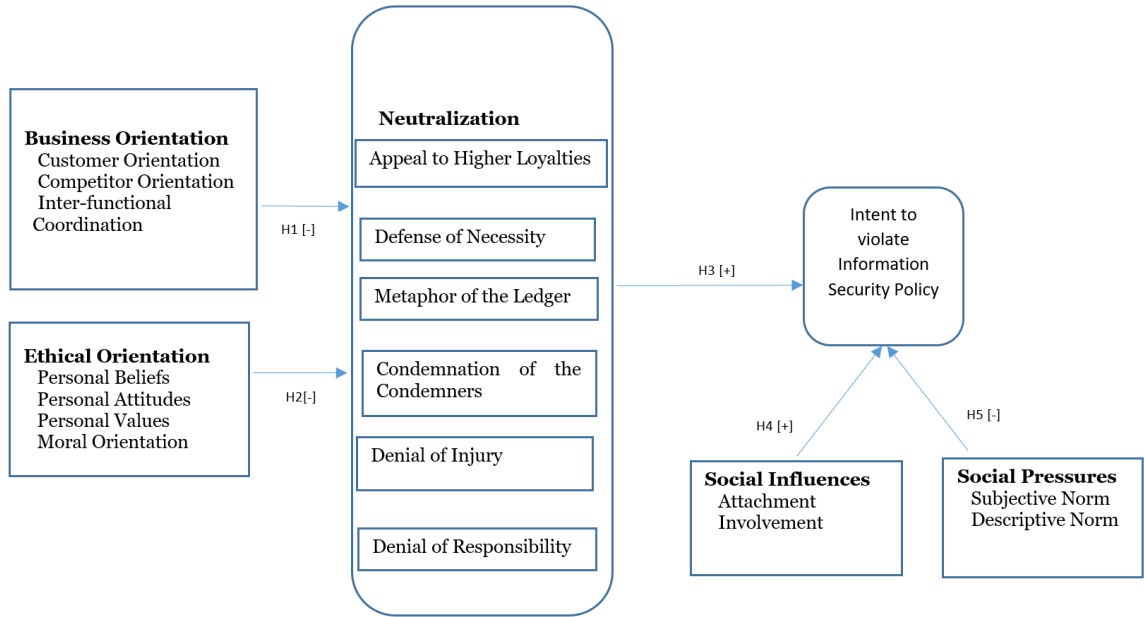


Figure 1. Research Model: Expansion of Neutralization Model

Business Orientation

Business orientation is closely related to market orientation in that both seek successful strategies for success (Narver & Slater, 1990). In this context, this research borrowed constructs from market orientation to fulfil business orientation components: customer orientation, competitor orientation, and inter-functional coordination. Business orientation can be defined as an organization-wide market of intelligence pertaining to current and future needs of customers, dissemination of intelligence horizontally and vertically within the organization, and organization-wide action or responsiveness to market intelligence (Kohli et al., 1993). No study, however, has explored the association between business orientation and the relationship with neutralization techniques in violating employee IS policy. These components may be critical in determining why some employees find themselves in a state of neutralization and begin using neutralization techniques. Customer orientation, competitor orientation, and inter-

functional coordination are sub-constructs that may affect employees when consciously or subconsciously making decisions to accept the neutralization techniques (denial of responsibility, denial of injury, defense of necessity, metaphor of the ledger, and condemnation of the condemners) and appeal to higher loyalties.

Narver and Slater (1990) identified literature in market orientation which consists of three behavioral components, customer orientation, competitor orientation, and inter-functional coordination, for organizations to achieve consistently and above-normal market performance. Customer orientation can be defined as the sufficient understanding of one's target buyers in the effort to continuously create superior value for them (Narver & Slater, 1990). Customer and competitor orientation involve all the activities that include the acquisition of information about buyers and competitors in a target market. This information is then disseminated throughout the business. Customer orientation can include various elements, which include measuring customer satisfaction, creating customer value, and understanding customer needs and commitment. More specifically, customer orientation is the sufficient understanding of one's target buyers to be able to create superior value. This requires the understanding of the entire value chain, not only as it relates to today but with the insight and understanding of how it will evolve over time subject to internal and market dynamics (Narver & Slater, 1990). The seller must understand not only its own cost and revenue dynamics, but also the cost and revenue dynamics of its immediate target buyer and the cost and revenue dynamics facing buyers from the demand in immediate market. Therefore, satisfying customer needs requires a comprehensive understanding of who the current potential customers are, who they may be in the future, what they want now, and what they may want in the future. Sin et al.

(2005) examined the economic ideology and industry type that moderate the impacts of market orientation and the relationship of market orientation on business performance.

Hooley et al. (2000) reviewed the transition of economies of Central Europe in testing the Narver and Slater market orientation scales. Their research focused on the transition economies that other business orientations may coexist with market orientation. Hart and Diamantopoulos (1993) focused on linking customer orientation, competitor orientation, and inter-functional coordination to company performance.

Competitor orientation, a sub-component of business orientation, suggests that highly involved employees in the organization work hard and become highly involved in accomplishing the organizational goals (Arthur, 1994; Wood & De Menezes, 1998). Competitor orientation means that a seller understands the short-term strengths and weaknesses and the long-term capabilities and strategies of both the current and the key potential competitors (Narver & Slater, 1990). Narver and Slater suggest that it is necessary to assess the current analysis of the customer as well as the analysis of the principal current and potential competitors to satisfy the expected needs of the seller's targeted buyers. In other words, it is extremely important to fully understand the entire technologies capable of satisfying current business needs and the needs of future targeted customers. Narver and Slater (1996) examined whether the competitive environment might have an impact on the effectiveness of different corporate objectives. Their research found none. Armstrong and Collopy (1996) conducted research on competitor orientation and the effects it has on objectives and information on managerial decisions and profitability. Their results suggest that the use of competitor objectives is detrimental to profitability. As a result, Armstrong and Collopy (1996) recommended firms should

ignore their competitors when setting objectives and focus directly on profit maximization. Dev et al. (2009) conducted an international research of hotels representing 37 brands from 56 countries in which market conditions of specific market strategies led to higher performance. Their research examined the circumstances under which customer orientation has higher pay off by simply investing resources on competitor orientation. Their results show that customer orientation had a greater effect on hotels performance than does a competitor orientation. Their research suggests customer orientation on performance is statistically positive and significant across all but one model (Dev et al., 2009).

Inter-functional coordination can be defined as the mechanism that facilitates the coordination between the various organizational units' functionality (Gatignon & Xuereb, 1997; Narver & Slater, 1990). Yang et al. (2012) defined inter-functional coordination in the context of an organization as the utilization of company resources in creating superior value for target customers. Rogerson and Sallnas (2017) defined inter-functional coordination as working together across functions to achieve common company goals. Rapp et al. (2012) studied the outcomes of different workplace structures. In particular, their study reviewed sales organizations' structure and e-learning and technological tools to determine the influence on coordination and the level of customer orientation within an organization. Their results indicated that organization structure type, coupled with e-learning and technological tools, led to greater positive outcomes. Jebarajakirthy et al. (2016) found that inter-functional coordination significantly and positively influenced corporate social responsibility. The authors study demonstrated that inter-functional coordination significantly and positively influenced the corporate social responsibility

involvement. Inter-functional coordination can be viewed as the mechanism that facilitates the coordination between the various organizational units' functionality.

Inter-functional coordination can be defined as the mechanism that facilitates the coordination between the various organizational units' functionality Gatignon and Xuereb (1997). Yang, Wang, Zhu, and Wu (2012) defined inter-functional coordination in the context of an organization as the utilizations of company resources in creating superior value for target customers. Rogerson and Sallnas (2017) defined inter-functional coordination as working together across functions to achieve common company goals. Rapp, Beitelspacher, Schillewaert, and Baker (2012) studied the outcomes of different workplace structures. In particular, their study reviewed sales organization's structure, e-learning and technological tools to determine the influence coordination and the level of customer orientation within an organization. Their results suggest that organization structure type, coupled with e-learning, and technological tools, lead to greater positive outcomes. Jebarajakirthy, Thaichon, and Yoganathan (2016) study found that inter-functional coordination significantly and positively influenced corporate social responsibility. The authors study found that inter-functional coordination significantly and positively influenced the corporate social responsibility involvement. Inter-functional coordination can be viewed as the mechanism that facilitates the coordination between the various organizational units' functionality. Appendix B includes a summary of published studies on business orientation and a brief description of key aspects of each study.

Ethical Orientation

The business community continues to struggle with issues surrounding ethical behavior. Studies have concluded that ethical judgements in situations of high moral intensity are affected by personal values (Douglas, Davidson, & Schwartz, 2001). Ethical orientation can be defined as a variable of study that refers to the approach an individual take in making ethical judgment through ethical perceptions and sensitivity with the ability to recognize the ethical nature of a situation in a profession (Clikeman et al., 2001). Beekun and Westerman (2012) recognized the rise in unethical business conduct and researched the need to better understand the antecedents to ethical decision-making with the influence of internal factors needing the most focus. Beekun and Westerman (2012) examined three sources of influence on ethical decision-making: personal spirituality, peer pressure, and national culture. The authors study examined the relationship between ethical decision-making and the behavioral norms. They used the social identity theory, that suggest a person's knowledges that he or she belongs to a social group. Fok et al. (2012) researched for a deeper understanding of the process in which cultural values influence ethical decisions.

According to (Payne et al., 2016; Fok et al., 2016), Ethical decision making from an individual level of analysis is more likely to adopt an act or rule from a utilitarian orientation. Payne et al. (2016) argued that most research in behavior ethics stems from four stages model of ethical decision making. The process starts with a person recognizing a particular issue or ethical dilemma, then eventually, the decision maker forms a moral intention by committing to a course of action. The final stage of the decision maker is to engage in moral action, that is acted upon (Hunt & Vitell, 1986).

Ethics is the foundation in which self-inquiries of morality, moral judgement, standards and rules of conduct of a person. Other words, ethics are the guidelines of human behavior one distinguishes between good and bad, right and wrong (Phatak, Bhagat, and Kashlak, 2009). Business ethics similarly concentrates on the moral standards as they apply to business, policies, organizations, and behaviors. In this context, ethical orientation is a decision justification that leads to the decision maker to consider different criteria and alternatives. Past research showed that individual's ethical orientation is directly associated with ethical judgement (Payne et al., 2016).

Individual factors, such as personal values, affect the ethical decision-making process and are the guidelines for doing ethical behavior (Turk & Avcilar, 2018). The most popular definitions used in the business literature for personal value is that "a value is an enduring belief that specific mode of conduct or end-state of existence is personally and socially preferable to an opposite or converse mode of conduct or end-state of existence" (Rokeach, 1973). Hyde and Weathington (2006) defined personal values as the beliefs or standards that individuals use to evaluate and define actions and events throughout the multiple domains in their lives. The importance of personal values on ethical decision-making have been studied in other disciplines like accounting and business literature for several years (Fritzsche & Oz, 2007; Mingzhi, 2008). (Rokeach, 1973; Hunt & Vitell, 1986) found ethical decision making and behavior to be potentially influenced by personal values in both the social psychology and organizational behavior literature (Rokeach, 1973). Moreover, empirical studies have shown a positive link between personal values and ethical sensitivity and judgement decisions (Fritzsche & Oz, 2007; Mingzhi, 2008). (Forsyth, 1980; Ferrell & Gresham, 1985) suggest that theoretical

models and theory of ethical decision-making demonstrate that personal values provide the bases for ethical judgement.

Attitude and beliefs are a subset of a group of constructs that name, define, and describe the structure and content of a mental state that are thoughts to drive a person's actions Richardson (1996). Wooten, Wontley, Singleton, and Euler (2012) suggest that personal beliefs are formed by the perceived effectiveness, consequences, and experiences of given situations. Attitudes can be defined as a mental and neutral state of readiness, organized through experience, exerting directive or dynamic influence upon the individual's response to all objects and situations with which it is related (Allport, 1967). Molina, Moreno, and Moreno (2013) define beliefs and attitudes as key perceptions that drive human behavior.

In this context, attitudes and beliefs will be evaluated as a sub-set of the construct ethical orientation. Attitudes and beliefs may further help determine factors that influence employees to violation information security policy. Prior research on information security has clearly indicated that information security can only be improved if organizations establish security controls that include the human factor (Kajtai, Benbasat, & Haftor, 2018). The authors argue that one of the most challenging decisions that an employee must make is whether to abandon a task that is too difficult to complete without violating information security policy. Bulgurcu et al. (2010) suggest that normative beliefs regarding information security policy noncompliance can help prevent policy violations. The authors mention that the mainstream of research of human perspective of information security is to find the factors that connect end user's behavior with information security in organizations. Kim, Yang, and Park (2014) researched an integrative behavior of

information security policy compliance. In their research, the authors in detail derived attitude, normal belief, and self-efficacy, based on the theory of reasoned action with seven factors of neutralization, and the response from the protection motivation theory.

Moral reasoning, a component of ethical orientation, can be defined as the process in which an individual applies moral principles to determine a course of action (Myyry, Siponen, Pahnla, Vartiainen, and Vance, 2009). The theory of moral reasoning is relevant to information security policies because the decision to violate security policy can be understood as a moral conflict. For example, a moral conflict can arise when an employee is obligated to follow security policy but decides not to and assist a co-worker at the cost of breaking security policy. A common instance of this is when an employee has logged off his or her computer because they are done for the day, but then realizes that they forgot to complete a task and ask another co-worker to gain access to the information through their log-in credentials. Whether such conflicts are minor or severe, theories of moral reasoning and values help explain why people choose to behave in certain ways. (Myyry et al., 2009) investigated moral reasoning to help explain compliance in IS security policy. The authors developed a model that integrated two well know theories: the theory of Cognitive Moral Development and the Theory of Motivational Types and Values. Their research supported the model and empirical test that significantly explained employee's compliance with information security policies.

According to Myyry et al. (2009), there are six stages in which one may deduce moral reasoning: the preconventional stage that suggest individuals act in order to avoid sanctions and penalties (stage 1), the individuals may receive something in exchange such as salary increase or reward (stage 2), the individuals behavior is based on

conforming to expectation of others as well as the expectation associated with the social role or profession (stage 3), the individuals follow the laws and norms for their own sake (stage 4), the decision is based on a utilitarian calculation, the individual should decide whether to comply with security policies for more satisfaction (stage 5), and the individuals apply the principle of universality, which means one must judge if a situation is right (stage 6). Fok et al., (2016) argued that values affect ethical decision making in a business context. Alteer, Yahya, and Haron (2013) also found ethical decisions are a result of personal values. The authors noted that these values are ideals that are abstract in one's mind and represents happiness and impacts behavioral decisions. As a result, we believe ethical orientation will influence neutralization.

Neutralization Theory

The study of neutralization theory is associated with the idea that people psychologically enable themselves to commit to the idea of breaking rules or committing anti-social actions (Sykes & Matza, 1957). Sykes and Matza demonstrated that offenders who might otherwise feel guilt and shame were able to neutralize their feelings by justifying their behaviors before committing the deviant act. Sykes and Matza (1957) suggested that the offenders negate the influence of internal norms and social censure. The term neutralization can be defined as the act of rationalizing or justifying an immoral or illegal act (Silic et al., 2017). Barlow, et al. (2018) defined neutralization as the use of rationalizations when violating a policy. In 1957, Gresham Sykes and David Matza introduced this theory in an effort to explain how juveniles were able to dismiss normative societal constraints so that deviant behavior can be committed (Hinduja, 2007). This theory originally derived from concepts from sociology and criminology in

which researchers attempted to explain crime and delinquency associated with social factors (Ball, 1966). Previous sociological theories fell short in explaining the readiness or the self-factor within the guidelines of acceptable behavior. As a result, the formulation that incorporated the recognition of the self-factor in delinquent behavior gave birth to the neutralization theory. Neutralization theory basically explains the justification of human behavior that is considered wrong under most circumstances but allows an individual to justify his or her self-concept while committing an act that is considered to be wrong (Costello, 2000). Participation at this point can then be justified and no deviant identity is assumed because the neutralization process has taken place (Hinduja, 2000).

Previous research of neutralization suggests theories of criminal behavior ascribe the importance of one's individual belief system in the context of whether their beliefs are in line with societal standards of conventional behavior. For example, Sykes and Matza (1957) called into question subcultural theories that claimed individuals are primarily allegiant to a normative belief system and must create justifications to engage in deviant behavior. Silic et al. (2017) studied the new perspective on neutralization in shadow IT usage. Their perspective on neutralization theory suggested those who commit illegal or illegitimate actions may use neutralization, while certain values may prohibit them from committing these same actions. From an organizational context, Silic et al. (2017) pointed out that employees may use one or more neutralization techniques to persuade himself or herself that policy violation does not represent a problem. Willingson et al. (2018) suggested techniques of neutralization is the process that serve to attenuate or deflect the disapproval one would otherwise experience from others in a social

environment. Thus, neutralization protects the violator from feeling self-blame and enabling him or her for deviant acts.

Prior research has viewed techniques of neutralization through theoretical lens for researching diverse forms of criminal behavior. Such forms have included tax evasion, car theft, drug abuse (Willingson et al., 2018)). In the context of IT, neutralization techniques have been used in cyber-loafing (Lim, 2002; Lim & Teo, 2005), digital piracy (Hinduja, 2007; Ingram & Hinduja, 2008; Morris & Higgins, 2009; Siponen et al., 2012) and IS security policy violations (Harrington, 1996; Siponen & Vance, 2010; Willison 2006).

Within the context of employee IS security policy violations, the neutralization theory can be used to offer new insights into how employees rationalize their behavior. Historically, neutralization theory has predominantly been used in criminology, but it can provide an explanation for IS security policy violations. For example, employee compliance to IS policy is reported as a key problem for organizations (Puhakainen, 2006). In fact, it is reported that over half of all IS security breaches are related to indirect or direct employee involvement (Siponen & Vance, 2010). Typically, deterrence theory was widely used as sanctions to overcome this problem; however, the use of such sanctions grounded in deterrence theory does not always provide or explain how fear of such sanctions affect employees because they may result in neutralization techniques (Sipson & Vance, 2010).

Siponen and Vance (2010) created a multi-dimensional second-order construct research model that illustrated the bearing that deterrence theory constructs (formal sanctions, informal sanctions, and shame) have on the intentions to violate IS security

policy. Their research model also illustrated the causal effect the first order constructs (appeal to higher loyalties, defense of necessity, metaphor of the ledger, condemnation of the condemners, denial of injury, and denial of responsibility) have on the intent to violate IS policy. These constructs initially proposed by Sykes and Matza formed the original formulation of neutralization theory. However, in 1974, Klockars added another component called *metaphor of the ledger* that represented the situation where an individual views past law-abiding behavior as a credit and the criminal or deviant behavior as a debit in his or her behavior ledger. Therefore, the offender may justify a debit in his or her ledger as insignificant compared to the numerous credits stored from past good behavior (Willison et al., 2018). Minor (1981) added the defense of necessity, in which an offender attempts to justify their actions based on the perceived necessity to commit the act. For example, an offender who has shoplifted may argue that he/she committed the deviant act because of the need to feed his children (Willison et al., 2018). In their study, Willison et al. utilized only three of the neutralization techniques (denial of injury, denial of victim, and the metaphor of the ledger) based on the argument that certain techniques of neutralization are better suited than others to particular deviant acts. Barlow et al. (2013) researched and investigated whether IT security communication forced on mitigating neutralization rather than deterrent sanctions reduced intentions to violate security policy. Their research examined only three neutralization techniques: denial of injury, metaphor of ledger, and defense of necessity. Siponen and Vance (2010) examined how six neutralization techniques can influence the intention to violate IS policy. Their research tested defense of necessity, appeal to higher loyalties, condemn the condemners, metaphor of the ledger, denial of injury, and denial of responsibility

alongside those described by the deterrence theory. Kim et al. (2014) researched the factors for organizations' members to comply with IS policy. Their study attempted to combined psychology and IS security research to achieve concrete definitions of influencing factors for IS compliance. Their research model included six neutralization techniques: denial of responsibility, denial of injury, condemnation, metaphor of ledger, appeal to loyalty, defense of necessity, and defense of ubiquity. Silic et al. (2017) examined the role of neutralization and deterrence in discouraging employees from using shadow IT tools, services, and systems within an organization that the IT department did not authorize. Six neutralization techniques were used in conjunction with deterrence constructs. Techniques used were denial of responsibility, appeal to higher loyalties, condemn the condemners, defense of necessity, denial of injury, and metaphor of the ledger (Silic et al., 2017). Teh and D'Arcy (2015) examined neutralization and social exchange theory from an industry banking perspective. Their study examined the factors that drive banking employees to violate IS policy. Their model specified previous untested relationships between job satisfaction, organizational commitment, role conflict, role ambiguity and neutralization techniques.

Prior research from Copes (2005) confirmed that only certain neutralization techniques should be used in any given study based on the likelihood that the technique would be used. In other words, all techniques are not applicable in every scenario. For example, Copes (2005) noted that the metaphor of the ledger was unlikely to be used and accepted by offenders who committed serious street crime but would be highly likely to apply within the workplace context. For this reason, the denial of victim will not be used

in this study because most users have difficulty pinpointing the victim of IS policy violation (Silic, et al. (2017).

In the context of this research, six techniques from the neutralization theory will be used: denial of responsibility, denial of injury, defense of necessity, metaphor of the ledger, condemnation of the condemners, and appeal to higher loyalties. Definitions and explanations of these techniques are displayed in Table 1.

Table 1

Definitions of Six Techniques from the Neutralization Theory

Neutralization Techniques	Definitions
Denial of Responsibility	A person committing deviant behavior defines himself as lacking responsibility.
Denial of Injury	A person justifying his action by minimizing the harm it causes.
Defense of Necessity	A person views the action as necessary and rationalizes that one should not feel guilty when committing the action. One may break the rule or policy because he feels that is unreasonable.
Metaphor of the Ledger	A person compensates bad action with good action. The individual believes that he has done a surplus of good so one bad action is okay.
Condemnation of the Condemners	A person blames those who are the target of the action. And believes the policy is unreasonable.
Appeal to Higher Loyalties	A person feels that they are in a dilemma and the problem must be resolved at the cost of violating policy.

Note: Taken from *Siponen & Willison, 2012*.

Neutralization Techniques

Justifications are commonly described as rationalizations. The term neutralization techniques can be defined as the techniques used to psychologically rationalize or justify an immoral or illegal act (Silic et al., 2017). In this context of IS policy, the following

techniques have been identified in which employees justify their actions prior to committing IS policy violations.

Denial of Responsibility

Denial of responsibility is the technique in which a person is committing a deviant act in which responsibility is rejected and believed that certain circumstances predisposed them to act as they did (Silic et al., 2017; Siponen & Vance, 2010). For example, a supervisor may ask an employee to complete a task that can only be efficiently accomplished using unapproved software. The employee may argue that he/she is a victim of circumstance because he/she was pushed beyond their control.

Denial of Injury

Denial of injury is the justification of action by minimizing the harm it causes (Leasure, 2017; Silic et al., 2018; Sykes & Matza, 1957). The offenders neutralize by suggesting that no one will be harmed by their action. For example, an employee may use shadow IT and create an Excel macro; he/she will argue that the simple macro will not do any damage to the system and, therefore, believe they have not caused any harm which justifies breaking IS policy (Silic et al., 2017).

Defense of Necessity

Defense of necessity is based on the justification that rule-breaking is necessary, and no other option was available. He/she does not feel guilty when committing the action (Barlow et al., 2013; Silic et al., 2017; Siponen & Vance, 2010). The offender feels that the choice is out of their hands; therefore, no guilt is experienced when violating the policy. For example, an organizational policy prohibits software download to flash drives, but, for the offender to complete a task, he/she downloads data to work

from home. In this case, the offender concludes that they had no rational choice but to violate policy (Barlow et al. (2013).

Metaphor of the Ledger

Metaphor of the ledger uses the idea of compensating bad behavior with acts of good behavior (Sipone & Vance, 2010). An employee who engages in delinquent behavior will strongly argue that all the good things they have done will make up for the bad (Silic et al., 2017). For example, an employee may get bored and is urging to do some online shopping. Although he/she knows that company policy prohibits surfing the internet during company hours, the employee rationalizes that the company owes them time because they have worked very hard and they deserve a break (Barlow et al., 2013).

Condemnation of the Condemners

Condemnation of the condemners is a technique that neutralizes one's actions by blaming those who are the target of the action (Siponen & Vance, 2010). In other words, the offender counterattacks by accusing the one that accused him/her. For example, there are two common sentiments that describe condemnation of the condemners: "Everyone else is doing it. Why focus on me?" and "You do the same thing, so don't point fingers at me" (Slic et al., 2017).

Appeal to Higher Loyalties

Appeal to higher loyalties is employed by those who feel they are in a dilemma and must resolve a task requiring violating policy (Leasure, 2017; Silc et al. 2017; Sykes & Matza, 1957). In an organizational context, an employee may argue that he/she must violate policy to get the work done (Siponen & Vance, 2010). For example, an employee may get into trouble by helping a friend and claim that he/she was not going to betray

their friend. In this case, any harm is justified if the individual remains within their group or friend's circle. He/she places the importance of such policy norms in second place (Silic et al., 2017). Appendix D includes a summary of neutralization research and a brief description of key aspects of each study.

Social Influences

Social influences can be defined as employees in organizations who form bonds with the job, immediate supervisors, co-workers, and the organization (Cheng et al., 2103). In other words, it is the extent in which social networks influence members behavior through messages and signals that helps form perceptions (Herath, 2009). Campbell et al. (2016) defined social influences as the change in attitude that one person invokes in another as a result of the way the changed person perceives his/her relationship to the influencer. Herath and Rao (2009) defined social influence as the extent to which social networks influence members' behavior through messages and signals that help form perceptions of an activity's value. Campbell et al. (2016) defined three broad forms of social influence: compliance, identification, and internalization. These three forms are defined as follows:

- Compliance –when individuals appear to agree with others, but actually keep their own contrary opinions private.
- Identification –when people are influenced by someone who is liked or respected in the community.
- Internalization –when people accept a belief or behavior and agree publicly and privately.

These characterizations can completely alter the opinions of individuals, which is consistent with the theorization that social influence is the result of the need to be right and the need to be liked (Deutsch & Gerard, 1955). Within the field of IS, the concept of social influence is often used to predict behavior and adopt technology (Venkatesh et al., 2003).

Social bonds may reflect the informal controls of social morality on an employee's individual behavior. Since norms are part of an organization, individuals form ties with the organization as well as receive pressure from others that influences his/her actions (Cheng et al., 2013). According to Chen et al., little research on information systems has been done to understand social bonds and how it affects employee's behavior regarding the intent to violate IS policy. Cheng et al. (2013) used Hirschi's (1969) social bond theory as one of the bases for their theoretical model for information control. Prior research from Hirschi suggested men are inherently more apt to commit deviant acts than women; however, Hirschi (1969) suggested that individuals with weaker bonds to the organization are more likely to commit deviant behavior. The social bond theory was originally developed to explain delinquency of adolescents. The theory focused on juvenile's attachment to conventional significant others, commitment to the actions of conventional goals, involvement in activities, and a belief in the moral validity of common value systems that influences behaviors such as cigarette smoking, drinking and driving, drug abuse, and misbehavior (Veenstra et al., 2010). Sims (2002) found that the impact of social bonds on employee's ethical rule-breaking was significantly impacted with the construct's attachment and involvement. Sims (2002) assessed the impact of social bonds on employee's ethical rule-breaking and found that

both attachment and involvement had significant impact on behavior. Lee (2004) found that insider computer abuse was strongly related to social bond factors, attachment, and involvement. Furthermore, earlier research from Hirsch (1969) found that people with stronger bonds with social groups are more likely to conform to group rules. His research also showed that the same effect works in organizational context which influences employee's IS policy violation intention.

Attachment can be defined as the affection and respect that an employee may develop to significant others within an organization (Hirschi, 1969). In the context of IS policy, Cheng et al. (2013) suggested that attachment has a negative impact on employee's IS policy violation intention. Employee attachment to the job may play a role in certain behaviors. For example, some employees are dedicated to the job and may work endless hours because they care about outcomes, whereas another employee may only see the job to make money. These two distinct attitudes play a role in an employee's commitment, and as a result, the employee with the deeper affection for the organization is more likely to safeguard the organization's interest (Cheng et al. 2013). In an organizational context, such attachments could be the employee's immediate supervisor, co-worker, the job, or the organization.

An employee's supervisor is an important person that plays a significant role in his/her work life. For example, the employee consistently seeks support, respect, and recognition from his/her supervisor. The supervisor is responsible for the evaluation and performance of the employee as well as the employee's promotion and rewards. Therefore, attachment to the supervisor may lead to the employee having a positive attitude and be less likely to engage in deviant behavior (Zhai et al., 2013).

Co-worker relationship is considered somewhat reflective of the employee-to-supervisor relationship in that a strong attachment with peer relations will serve as another dimension of an attachment bond. Employees who have a strong attachment to their co-workers are more likely to restrain their words and deeds and avoid negative behaviors (Cheng et al., 2013). Existing research suggests that two sources of social bonds influence IS violation behavior: subjective norms and co-worker (Herath & Rao, 2009). In this context, we will discuss the social attachment to co-worker followed by a discussion of subjective norms in the next paragraph. Co-worker behavior often describes co-worker's ISSP compliance (Herath & Rao, 2009). Co-workers often believe or do things that others do because behavior is reasonable and acceptable (Chen et al., 2013). For example, the use of opinions and actions of significant others often leads to the decision of others to determine what to do (Cheng et al., 2013). In criminology studies, it was found that peer behavior was an important predictor of one's crime (Rivis & Sheeran, 2003). In other words, employees in organizations are more likely to do the same things as other employees do (Rivis & Sheeran, 2003).

Cheng et al. (2013) found that job attachment plays a vital role in constraining delinquency in the workplace. For example, employees that work a lot are extremely enthusiastic about their work and their job. In contrast, some employees do not care as much about their job but work only to earn money. These are two distinct attitudes with different affection towards the workplace environment. Cheng et al. (2013) hypothesized that those who have strong attachment to their job will more likely be responsible and try harder to avoid mistakes in their work.

Attachment to one's organization reflects the loyalty the employee feels to the organization. For example, if the employee has deep affection for the organization, the more likely he/she is to safeguard the organization's interests (Cheng et al., 2013). Simply speaking, the attachment that an employee feels for his/her supervisor, organization, job, or co-workers is more likely to conform to the security policy.

Involvement, in this context, can be defined as organizational activities spent engaging in traditional activities within the organization (Cheng et al., 2013). Involvement pertains to the amount of time a person spends engaging in conventional activities. For example, involvement of highly involved people in conventional activities does not mean highly involved individuals are also highly committed. According to Hirschi (1969), employees who engage in conventional activities have less time left over to commit deviant acts. Therefore, employees who engage in more involvement in organizational activities are less likely to violate the security policies of the organization. Hearsh and Rao (2009) suggest that employee's commitment to an organization plays a role in engagement in security behaviors. Stanton (2003) believes that employees who are committed are less likely to enact counterproductive computer behaviors that may put the organization systems at risk. In a security context, Stanton (2003) and Kraemer et al. (2009) suggested that employees believe that their security-conscious behaviors are likely to impact the overall organizational IS security and, in fact, weaken security performance. Appendix E includes a summary of published studies on social influences and provides a brief description of key aspects of each study.

Social Pressures

Social pressures can be defined as the social networks that influence behavior through messages and signals that help form the perceptions of an activity (Vankatesh & Brown, 2001). Information technology has recognized the social influence role that plays in IS security policy violations. The role of social influence in technology acceptance decisions are complex and subject to a host of influences (Herath & Rao, 2009). Individuals are consistently influenced by the actions of messages and expectations observed by others. Previous research on social influence has identified the long-standing distinction between the descriptive and subjective meanings of social norms because the two are separate sources of motivation (Herath & Rao, 2009). People consciously and subconsciously consult the behavior of the people that are around them to find out what to do (Herath & Rao, 2009). In other words, people view other people's behavior as a source of information to help them define social reality. Such beliefs regarding what the majority of the people are doing in specified environments are referred to as descriptive norms (Herath & Rao, 2009).

Descriptive norms also influence employees' behavior. These behaviors are the extent that action one performs reflects the desired behavior of another. In other words, employees may replicate the believed behavior of others (Rivis & Sheeran, 2003). Fischer (2008) defined descriptive norms as characteristic behaviors displayed by most people within a culture as observed by members of that culture. In the context of IS security, employees who believe that their peers are following the organizational security policies may likely have positive intentions not to violate IS policy; likewise, if employees believe their peers and immediate supervisors do not follow IS policy, there

may be a negative intent to follow them as well. Herath and Rao (2009) found that the influence of one's peers encourages a person to do certain things under pressure. In other words, descriptive norms are the extent in which one believes that others are performing the desired behavior which focuses on the individual to replicate the belief of others (Rivis & Sheeran, 2003). In the context of this study, if an employee believes his/her colleagues follow IS policy, he/she is more likely to have a positive intention to follow the same.

As descriptive norms play a role influencing employees' behavior, so do subjective norms. A host of IS research has studied subjective norms, defined as the belief of whether or not a significant person wants the individual to do the behavior in question (Herath & Rao, 2009). Subject norms are based on normative beliefs and motivation to comply. This view of belief and motivation to comply is based on the findings in the technology acceptance literature. The technology acceptance model, (TAM, TAM2, TPB) innovation diffusion theory, and various other theories have a host of labels for subject norms constructs; all have the notion that the individual's behavior is influenced by what significant others expected them to do. Previous studies have examined particular settings in organizations and have found the influences of employees' perceptions of the expectations of supervisors, managers, and peers to be relevant in IS departments and have concluded that if an employee believe that their manager, IT personnel, or peers expect IS policy compliance, then he/she is more likely to comply (Venkatesh et al., 2003). According to Cheng et al. (2013), employee social bonding was found to have mixed impacts on the employee's intention to violate IS policy. The authors state that social pressures exerted by subjective norms and co-

worker's behaviors had significantly influenced employees' ISSP violation intentions. Cheng et al. (2013) analyzed formal sanctions and the perceived severity of sanctions and concluded that perceived severity sanctions were significant while perceived certainty of those sanctions was not. Research also suggested that subjective norms are pressures that influence individuals to perform or not perform certain behavior acts in question (Cheng et al., 2013; Herath & Rao, 2009). Subjective norms reflect the impact of opinions from others in the workplace that may positively or negatively influence one's opinion. From an IS context, employees can be influenced by the pressures from significant others that include, but are not limited to, immediate supervisor, co-workers, and the organization's expectations. Appendix F includes a summary of research on social pressures and provides details on each study.

Previous studies show that employees who are more enthusiastic about work will be more responsible in avoiding mistakes, and thus, more likely to safeguard the organization's interests (Cheng et al., 2013). Thus, employees with more involvement in the organizational activities will be less likely to violate IS policy. Siponen and Vance (2010) found neutralization as a strong indicator in predicting information security policy violations. However, they did not examine the factors that influenced employees to accept neutralization techniques. Their results showed the importance of neutralization as a factor that needs to be considered when developing and implementing organizational security policies and practices. Other factors, such as business orientation, was also an important driver for employees when making such decisions. This research investigated how business orientation affects employees' rational thinking when accepting neutralization techniques. Therefore, the following hypothesis were formulated:

H1: Business orientation will negatively influence acceptance of *neutralization techniques*.

In the context of this study, ethical orientation, a variable of study, can be described as “a continuum with relativism at one end and idealism at the other. Relativism describes an individual’s concern for a universal set of rules or standards, while idealism focuses on human welfare” (Greenfield, et al., 2008, p. 420). In this context, ethical judgement in corporate ethical culture is seen to influence personal values and the professional code of conduct. Fok et al., (2016) argued that values affect ethical decision making in business context. Alteer et al., (2013) found ethical decisions are a result of personal values. Hence, the following hypothesis were formulated:

H2: Ethical orientation will negatively influence the acceptance of *neutralization techniques*.

Research has shown Research has shown ISP violations in this industry as a major problem that plague organizations worldwide. Kim, Yang, and Park (2014) researched the factors for organizations members to comply with information security policy. Their study integrate research on information system security with relevant research in psychology to provide definitions of the underlying dimensions of neutralization. It is estimated that over half of all information systems security breaches are due directly or indirectly to the poor security practices of employees. Employees often rationalize their behavior when deciding whether to violate IS policy (Siponen & Vance, 2010). For this study, the neutralization construct is seen as a multidimensional, second-order construct that represents specific neutralization strategies. Siponen and Vance (2020) examined educational training interventions aimed at de-neutralizing techniques. Although their

research found that individuals who received their educational training used neutralization techniques substantially less, some individuals still used neutralization techniques. Hence, the following hypothesis was formulated for this study:

H3: Neutralization techniques will positively affect the intent to violate information security policy.

In the context of social bond theory in the workplace, employees are more likely to bond to conventional norms and are less likely to deviate from the conventional norms and participate in delinquent behavior. Stanton et al., (2003); Kraemer, Carayon, & Clem, 2009) suggest that employees believe that their security conscious behaviors are likely to impact the overall organizational information system security. In the context of this study, if an employee believes that her/his colleagues follow the organizational security policies, she/he is more likely to have a positive intention. Previous studies show that employees who are more enthusiastic about work will be more responsible in avoiding mistakes, and thus, more likely to safeguard the organization's interests (Cheng et al., 2013). Thus, employees with more involvement in the organizational activities will be less likely to violate IS policy. Therefore, the following hypothesis was formulated:

H4: Social influences will positively affect the intent to violate information security policy.

Social pressures, to the extent in which social networks influence members behavior through messages and signals, help form the perceptions and the activity in which employees may engage (Venkatesh & Brown, 2001). To this extent, employees often consult the behavior of others around them to find out what to do in a given situation (Herath & Rao, 2009). Employees in an organization's setting are further

influenced by the expectations of superiors, managers, and peers. Previous research on social bonding was found to have mixed impacts on the employee's intention to violate information security policy. Previous research show social pressures exerted by subjective norms and co-worker's behaviors had significantly influenced employees ISSP violation intentions. Subjective norms are pressures that influences individuals to perform or not perform certain behavior acts in question. Subjective norms reflect the impact of opinions from others in the workplace that may positively or negatively influence one's opinion. In other words, if an employee believes that their manager, IT personnel, or peers expect them to comply with IS policy, then, the likelihood that they will comply is increased. Therefore, the following hypothesis was formulated:

H5: Social Pressures [*expectations and behaviors of others*] will negatively affect the intent to violate information security policy.

Summary

A review of various aspects of the intent to violate employee information security policy was conducted to provide the foundation for this research study. After an exhaustive review of the relevant literature, the constructs, business orientation, ethical orientation, social influences, and social pressures were presented as viable constructs that described influences on the intent to violate information security policy. The literature review provided a description of what is known and unknown regarding the constructs of this research study. This research extended across a host of fields including information systems, sociology, and psychology.

Employees are key to maintaining a secure environment in an organization setting. It is estimated that over half of all the IS security breaches is indirectly or directly

caused by employee's poor IS security (Siponen & Vance, 2010). D'Arcy et al. (2009) investigated inside misuse and found that employees are the most significant threat to organizations. Siponen and Vance (2014) studied college students who were clear on safe practices and, still, they failed to comply with IS policy. Although advances in hardware and software have enhanced security managers' use of best practices in IS security, the biggest threat remains the insider employee (Siponen & Vance, 2010).

Although previous research has found that neutralization as an excellent indicator that significantly affects the predisposition to violate IS security policy, no research has examined why employees accept neutralization techniques in the first place. Previous research studied the intent to violate employee's IS policy using deterrence theory, formal and informal sanctions, and neutralization techniques; however, previous research has not studied factors that influence employees in accepting neutralization techniques.

Contributions of the Research Study

In this study, we have considered business and ethical orientation. Currently, no measures of business orientation exist, so this study borrowed elements from the construct market orientation: employee orientation, employee commitment, and inter-functional coordination. Although research exists on the effect personal values have on ethical decision making, research has failed to provide support for the effect personal values have on ethical judgement in the context of IS violation. Moreover, studies have not provided support on the effect of the four constructs of personal belief, personal attitudes, personal values, and moral reasoning on employees accepting neutralization techniques with the ultimate intention of violating employee IS policy. This research has filled that gap by adding these four constructs to the existing Siponen and Vance (2010)

research model to evaluate how employees consciously and unconsciously make decisions based on business orientation and ethical orientation perspectives. Additionally, the constructs of social influences and social pressures have been combined from the research of Cheng et al. (2013) and Herath and Rao (2009) to evaluate social involvement, social attachment, subjective norms, and descriptive norms. Therefore, this research was designed to address the need to examine business orientation, ethical orientation, social influences and social pressures on the intent to violate employee IS policy.

Chapter 3

Methodology

Research Method

This research adopted a quantitative perspective that examined human behavior from the perspective of both a business orientation and an ethical orientation. The purpose of this study was to better understand business and ethical factors that influence employees who consciously and subconsciously make decisions to accept neutralization techniques that ultimately impact the decision to violate IS policy. Furthermore, to explore the social influences and pressures more thoroughly, this research evaluated multiple dimensions by combining research constructs from Herath and Rao (2009), subjective and descriptive norms, and social attachment and involvement from Cheng et al. (2013) on the intent to violate IS policy.

A quantitative survey approach was pursued to examine the research model. The overall approach for this research was based on survey and scenario methodology for data collection. Sekaran and Bougie (2013) noted that survey research is a system for collecting information about people that describes and explains their knowledge, attitudes, and behaviors. According to Fink (2003), survey research involves setting objectives, collecting data, designing the study, preparing a reliable and valid survey instrument, managing and analyzing survey data, administering the survey, and reporting the results. In designing a hypothetical scenario for this research, the intent was to

describe a situation that was not uncommon to respondents. This method was denoted by Piquero and Hickman (1999) and Limayem and Hirt (2003). Siponen and Vance (2010) used this methodology and solicited security experts and IS managers for their most common violations. They found the most common and significant IS policy violations using an open-ended questionnaire that resulted in the response from 54 IS experts that identified the top four IS security policy compliance problems. This research borrowed from the work of Siponen and Vance (2010) as it ensured a scenario that reflected real-world problems that were important and relevant to IS security practice. In keeping with Siponen and Vance (2010), a scenario-based design ensures findings are generalizable across different IS security violation policies. Using validated and tested questions improves the reliability of results (Straub, 1989). To reduce the problems with the reliability and validity of questionnaires, this research adopted items from previously validated studies.

To describe the different sectors in the sample, descriptive statistics, including the mean, median, mode, and standard deviation of the demographic data, were used. The research design included the use of inferential statistics tools such as PLS and regression analysis. The use of such tools enabled decisions to support or not support the hypotheses.

Instruments and Measures

As mentioned by Devellis (2011), the key in selecting the most appropriate instrument for a research study is the type of data called upon based on the research questions and hypotheses. As this research was inspired by prior studies conducted in the

field of IS security, it utilized vetted survey instruments as well as questions from those studies. This was necessary to guarantee the validity and reliability of the study.

To measure the constructs business orientation and ethical orientation, a survey methodology was used to collect data from respondents. A previous validated instrument from Siponen and Vance (2010) were used with additional items added. Each item involved a 7-point Likert scale to indicate respondent's level of agreement and the likelihood to adopt neutralization techniques and, ultimately, violate IS policy. Each response scale ranged from (1-*strongly disagree*) to (7-*strongly agree*). The range captured the intensity of the respondent's feelings for a given item (DeVellis, 2012). The Likert scale was designed to specify the respondent's level of agreement or disagreement on a symmetric agree-disagree scale for a series of statements. Providing validated and tested questions improves reliability (Straub, 1989). Therefore, adopted survey instruments from previous validated studies were used that reflect real-world problems which are important and relevant to IS security practice. To measure business orientation and ethical orientation, instruments were borrowed from Hooley et al. (2000) and Sin et al. (2005). To measure neutralization, instruments were borrowed from (Siponen & Vance, 2010). To measure social influences, instruments were borrowed from Cheng et al., (2013). To measure social pressures, instruments were borrowed from (Siponen & Vance, 2014), Cheng et al. (2013), and (Hearth & Rao, 2009). Constructs and measures from vetted sources are listed on Table 2.

Table 2

Constructs and Instrument Source

Construct	Source
Intent to Violate IS Policy	Siponen & Vance, 2010
Business Orientation	Hooley et al., 2000; Sin et al., 2005)
Ethical Orientation	Allmon et al., 2000; Douglas et al., 2001
Neutralization	Siponen & Vance, 2010
Social Influences	Cheng et al., 2013
Social Pressures	Herath & Rao, 2009; Siponen & Vance, 2010; and Cheng et al., 2013

Business and Ethical Orientation Measures

The construct business orientation consists of three sub constructs: employee orientation, employee commitment, and inter-functional coordination. These components may be critical in determining why some employees find themselves in a state in which they accept neutralization techniques. This research adopted previously validated instruments from Hooley et al. (2000) to capture business orientation influences on neutralization. A 7-point Likert scale ranging from 1 to 7, where 1 indicates that an employee strongly disagrees and 7 indicates that an employee strongly agrees with such behavior.

The construct ethical orientation has four sub constructs that may be factors related to an employee's decision to violate IS policy. Bulgurcu et al. (2010) noted that it is important to connect end user's behavior with IS in the organization. As Kajtai et al. (2018) argued, employees are faced with difficult choices in deciding whether to abandon a task that is too difficult to complete without violating IS policy. To measure ethical

orientation, survey tools designed by Sin et al. (2005) were used to capture the influence ethical orientation has on neutralization.

Neutralization Measure

The construct neutralization derived from the theory that people psychologically enable themselves to commit to an idea of rule breaking. In the context of IS, employees are believed to consciously or subconsciously rationalize the idea that it is ok to violate IS policy, and in doing so, a neutralization technique is adopted to justify their actions. There are six neutralization techniques: appeal to higher loyalties, defense of the necessity, metaphor of the ledger, condemnation of the condemners, denial of injury, and denial of responsibility. Each neutralization sub-construct is correlated with constructs from business orientation and ethical orientation, which corresponds to employees making decisions to commit the intent to violate IS policy from either a business or ethical perspective. Items were adapted from previously validated instruments where possible and were measured on a 7-point Likert scale ranging from 1 to 7, where 1 indicates that an employee strongly disagrees 7 indicating that an employee strongly agrees with such behavior.

Social Influences Measure

In the context of ISSP violation, previous research has shown employees form bonds with their job, immediate supervisor, co-workers, and the organization. The construct social influences capture the sub constructs attachment and involvement. These constructs are believed to have a negative influence on the intent to violate IS policy. To measure this relationship, questions were borrowed and modified from Cheng et al. (2013) to reflect the intent of this study. Each item was measured on a 7-point Likert

scale to indicate a respondent's level of agreement with the statements regarding employee's involvement and attachment to their job, co-workers, their supervisors, and their organizations. The scale measures on a 7-point Likert scale ranging from 1 to 7, where 1 indicates that an employee strongly disagrees and 7 indicates that an employee strongly agrees.

Social Pressures Measure

The construct social pressures consists of subjective norms and descriptive norms. These sub constructs helped determine how employees may behave with other co-workers around them. People consciously and subconsciously consult the behavior of the people around them to find out what to do. Cheng et al. (2013) found that an employee's social bonding was found to have a mixed impact on the employee's intent to violate ISSP; therefore, this measure re-addressed the social pressures with survey-based methodology that assessed antisocial, ethical, and unethical behavior (D'Arcy et al., 2009; Siponen & Vance, 2010). To measure the social bond construct subjective norm, items were borrowed from Herath and Rao (2009) and Cheng et al. (2013). Each item was measured on a 7-point Likert scale to indicate a respondent's level of agreement with the statements regarding the likelihood of violating the organization's IS policy. The scale uses a 7-point Likert scale ranging from 1 to 7, where 1 indicates that an employee strongly disagrees and 7 indicating that an employee strongly agrees with such behavior. To measure the construct descriptive norm, questions were borrowed from Herath and Rao (2009) and Siponen and Vance (2014).

Intent to Violate Information Security (IS) Policy Measure

The dependent variable, intent to violate IS policy was measured using a single construct that was adopted from Siponen and Vance (2010). The response scale for this item ranged from 0 (*not likely at all*) to 10 (*extremely likely*). Siponen and Vance (2010) noted a reliability threat from a single measure. However, Straub et al. (2004) noted that in some situations a single measure is most appropriate. The weakness in using a single measure is the inability to validate whether the construct was accurately captured. Conversely, in the scenario method, previous research validated that respondents reported the probability that they would do as the scenario character did via a single measure that appeared directly following the scenario (Pogarsky, 2004). Measurement for the intent to violate IS policy was adapted from Siponen and Vance (2010).

Validity and Reliability

Sekaran and Bougie (2013) explains that instrumentation effects are another source of internal validity that results from a change in the measuring instrument between pretest and posttest, and not because of the treatment's differential impact at the end (Sekaran & Bougie, 2013). It is important to use constructs that have already been used and validated in prior research studies. Sekaran (2003) contended that reliability is important because it indicates the extent of un-bias and is an indication of stability and consistency. This study conducted various tests to validate data collected. A normality test was conducted to ensure there was a normal distribution of data for each measured construct. A skewness & kurtosis test was performed to ensure scores fell within the range of -1.96 to +1.96. Construct reliability was examined by calculating the Cronbach's alpha test. Reliable instruments should measure what it is intended to measure. To

confirm reliability of the instrument, it is important to compute the reliability coefficient. The coefficient range should be from zero (low reliability) to 1.0 (high reliability). The higher the coefficient, the more reliable the test.

Furthermore, a factor analysis was conducted to determine the convergent and discriminant validity. Convergent validity refers to the degree to which two measures of constructs that theoretically should be related are, in fact, related. Convergent validity, along with discriminant validity, is a subtype of construct validity. Convergent validity can be established if two similar constructs correspond with one another, while discriminant validity applies to two dissimilar constructs that are easily differentiated. To test for reliability of the survey, a pilot test was conducted on 10% of the target population. Based on the results from the pilot study, any questions that were not perceived as clear were fixed and finalized.

Straub (1989) contended that it is important to show evidence that an instrument is measuring what it intends to measure. Straub (1989) added that unrepresentative instruments would yield uncertain results. There are two types of validation used to establish credibility of results: content and construct (Creswell, 2002; Salkind, 2006; Sekaran, 2003; Straub, 1989). According to Creswell (2002), “content validity is the extent to which the questions on the instrument and the scores from the questions are representative of all the possible questions that could be asked about the content or skills (p.184).

Construct validity is considered by Creswell (2002) as “a determination of the significance, meaning, purpose, and use of scores from an instrument” (p. 184). Straub (1989) contended that construct validity “asks” whether the measures chosen are true

constructs describing the event or merely artifacts of the methodology itself (p.150).

Straub (1989) recommended that “researchers should use previously validated instruments wherever possible, being careful not to make significant alterations in the validated instrument without revalidating the instrument content, constructs, and reliability” (p. 161). Therefore, where appropriate, this research study used previously validated constructs from prior research (Cheng et al., 2013; Douglas et al., 2001; Herath & Rao, 2009; Hooley et al., 2000; Siponen & Vance, 2010, 2014).

To ensure all aspects of the study and research method, A pilot study that covered all aspects of the research was used to ensure a good research design for the final study. By using a pilot study any issues that might arise before the actual study could be worked out. The pilot study helped flush out questions that were misleading, any confusion to the participants, and a pretest of the survey instrument. The pilot study sampled approximately 10% of the overall target audience. This method allowed a final quality assurance check before commitment to the full study. The pilot test serves as a learning opportunity even for the most seasoned researcher. Although the survey instrument in the research study had been tested and vetted, a pilot study was essential for final quality assurance and research design.

Data Collection

Data collection methods are considered an integral part of the research design and each method has its advantages and disadvantages (Sekaran & Bougie, 2013). Data can be collected in a host of different ways, from a field to a lab setting, and from different sources. The primary data for this research was collected from organizational business units, academic institutions, and IT professionals. For the purpose of this research study,

the method of choice was electronic administration via online survey. Validated survey questions for business orientation were taken and modified from Hooley et al. (2000). Validated survey questions for ethical orientation were taken from Douglas et al. (2001). Validated survey questions for social influences and pressures were taken and adapted from Cheng et al. (2013), Herath & Rao (2009), and Siponen & Vance (2014).

To improve the generalizability of the findings across a variety of IS violations, a vetted scenario was borrowed from Vance and Siponen (2012). The scenario presented a realistic and commonplace situation for respondents. A hypothetical scenario method was used; it presented a hypothetical situation to respondents, followed by a question regarding the likelihood that the respondent would behave in the same way under similar circumstances (Nagin & Paternoster, 1993). This method was chosen because it helped alleviate respondent's tendency to conceal information or to respond to questions in socially desirable ways (Vance & Siponen, 2012). Additionally, scenario methods provided substantial theoretical benefits when applied to rational choice theory, which holds the potential for offenders to weigh probabilities of costs and benefits (Becker, 1968). Notwithstanding these benefits, the method was appropriate because it provided the indirect means of measuring socially undesirable behavior of respondents who may be intimidated to report their intentions (Harrington, 1996).

The aforementioned scenario derived from surveying IT security practitioners with opened-ended questions listing the four IS security policy violations that were both common and consequential. The top three IS security policy violations cited by practitioners were (a) sharing or writing down passwords, (b) failing to lock or log out of workstations when not in use, and (c) copying sensitive data to unsecure portable USB

storage devices. The focus was on participants from business organizations, academic institutions, and IT professionals. To measure the construct's business and ethical orientation, a scenario-based methodology was appropriate.

Population and Sample

The unit of analysis can be referred to as the level of aggregation of the data collected during the subsequent data analysis stage (Sekaran & Bougie, 2013). The unit of analysis for this research study was at the individual level. In this study, the research questions determined the unit of analysis since the interest was to find out the cognitive frame of mind employees have when consciously or subconsciously deciding to accept one of the six neutralization techniques from a business or ethical orientation perspective.

Sampling is an important aspect of this survey study, and it is important for it to be as generalizable as possible (Terrell, 2016). To closely match the population, stratified random sampling was used to represent the population as much as possible (Terrell, 2016). This method is unbiased and the most efficient amongst all probability sampling techniques. This means that it guarantees that the sample chosen is representative of the population and that the sample is selected in an unbiased way (Sekaran & Bougie, 2013). According to Terrell (2016), if a sample is not generalizable, the results based on the sample are likely not valid and they will not reflect the true values in the population, which creates sampling bias. For this research, all data were collected via electronic and online, and, therefore, some sampling bias may have been created, as paper-based surveys were not administered. The intent here was to collect data from sectors of administrative offices in the academic institutions, corporate organizations, and information technology professionals. Received survey responses were divided into

mutually exclusive groups, based on gender across organizations. Subjects drawn from each stratum were proportionately drawn for women and men, at 50% rate from each group. All subgroup (men, women) members were assigned numbers within their specific group, and a selection process determined the probability of selection of each member. All selections were completed using a random number generator.

Survey links were sent out randomly to various sectors that included academic institutions, corporate organizations, and IT professionals. The letter of invitation to participate is included in Appendix G. The intent of this research was that all possible subsets and sectors of the population or sampling frame were given an equal probability of being selected. Furthermore, this methodology increased the potential for generalization and improved external validity.

To decide the minimum sample size, Cohen's statistical power analysis, one of the most popular methods for calculating sample size, was used. According to Cohen (1992), determining adequate sample size required predetermined factors of the significance level, effect size, power, and estimated variance. First, we used Cohen's indexes and their values for small, medium, and large effects for this study. The statistical level of significance was set at .05, the acceptable level for the probability of wrongly rejecting the null hypothesis. Alpha was set at .05, considered the most conventional level of significance (Cohen, 1992). Second, we estimated the medium effect size, which is the degree to which the phenomenon is present in the population or the degree to which the null hypothesis is false (Cohen, 2013). The effect size used standardized values by Cohen (1992). For this study, the effect size index (f^2) for small, medium, and large sizes is $f^2 = .02, .15$, and $.35$, respectively. Cohen (1992) proposed that a medium effect size is

desirable as it would be able to approximate the average size of the observed effects in various fields. For this study, the maximum number of independent variables is eight, with an alpha of 0.05. Following the recommendations of Cohen (1992), the sample sizes for small, medium, and large samples are 50, 107, and 757, respectively. This study aimed for a medium effect size, and, therefore, the required sample size for this study was 107, based on Cohen (1992) table. The distribution of participants among the three organizational samples is presented in Table 3.

Table 3

Distribution of Organizational Samples

Sample	Frequency	Percent	Valid Percent	Cumulative Percent
Information Technology	34	16.5	16.5	16.5
Corporate Organization	63	30.6	30.6	47.1
Academic Institution	109	52.9	52.9	100.0
	206	100.0	100.0	

Data Analysis Strategy

Data were collected and analyzed from three different industry sectors: academic institutions, IT professionals, and corporate organizations. As previously mentioned, data was collected using SurveyMonkey®, a web-based tool, for data collection. The online instrument is included in Appendix H. To analyze the theoretical model, this research study used partial least squares (PLS) using SmartPLS, a structural equation modeling (SEM) technique (Siponen & Vance, 2010). PLS is better suited over covariance-based SEM techniques because of the ability to model second-order constructs that are formatively first-order factors (Siponen & Vance, 2010). This technique is more suitable when predicting rather than testing established theory. This strategy places minimal

restrictions on measurement scales, sample size, and residual distributions. PLS has been widely used in IS studies by Siponen & Vance (2010), Vance et al. (2012), Li et al. (2010), and Bulgurcu et al. (2010). Haenlein & Kaplan (2004) recommend PLS when the sample size is considered small.

The analysis to address the two research questions and five hypotheses was conducted using SmartPLS for measurement validation and to test the structural model. Herath and Rao (2009) noted that PLS is a component-based approach for estimation that places minimal restrictions on sample size. To analyze the effects, the researcher ran a PLS algorithm to determine the standardized regression weights, factor loading, and percentage of variance. The model explained the variance of employees' intent to violate IS policy. To determine if the aggression weights were significant, a bootstrap algorithm was run that produced t-statistics that addressed the five hypotheses on the intent to violate IS policy. T-statistics above the 1.96 at the 0.05 level are an indication of significance. The following hypothesis were tested for RQ₁.

RQ₁: What factors influence employees to accept neutralization techniques?

H₁: Business orientation will negatively influence employees to accept *neutralization techniques* and ultimately influence the intent to violate information security policy.

H₂: Ethical Orientation will negatively influence employees to acceptance *neutralization techniques*.

H₃: Neutralization will positively affect the intent to violate information security policy.

Next, to analyze the added effects of the constructs social influences and social pressures, SmartPLS was also used for measurement and validation. Descriptive statistics were used to report the mean, median, mode, and standard deviation on the demographic data collected from the different groups (administrative offices in academic institutions, IT professionals, and corporate organizations). Demographics included identifiers of gender (male/female), organizational type, and organizational size. Hypotheses four and five for RQ₂ were addressed:

RQ₂: What social factors influence employees to violate information security policy?

H₄: Social influences will positively affect intent to violate information security policy.

H₅: Social Pressures [*expectations and behaviors of others*] will negatively affect the intention to violate information security policy.

Resources Requirements

Resources required for this research study included: computer, internet access, Microsoft® Word, Microsoft® Excel, creation of email accounts to segregate study emails from personal emails, SurveyMonkey®, and Smart PLS. SmartPLS was used for further data analysis. As indicated earlier, this research drew from prior studies conducted in the field of IS security violations. Vetted survey instruments taken from previous research are noted in Table, which include, but are not limited to the hypothetical scenario methodology (Siponen & Vance, 2012), the theoretical framework for influence of security-related stress of (Siponen & Vance, 2012), and social influences and social pressures (Cheng et al., 2013).

To handle the responses from random individuals, questionnaires were created in SurveyMonkey® to collect and store data. A 7-point Likert scale was used to collect responses where 7 (*strongly agree*) to 1 (*strongly disagrees*). A pilot study to ensure the crucial elements of the research design of the final study included a sample of approximately 10% of the overall target audience.

Finally, this research study collected data from a target audience working in either academic institutions, corporate organizations, and IT professionals across various organizations in IT forums. The idea was to target individuals who were familiar with IS policies to gain a realistic perspective on how such individuals might respond in certain IS scenarios. Approval from the Institutional Review Board (IRB) was required. Lastly, respondents were expected to use their own personal computer and respond on their own personal time.

Summary

This chapter provided an overview of the methodology used for this study. This research is an extension of the Siponen and Vance (2010) research model. The study used a quantitative approach to collection and analysis of data to better understand business and ethical factors that influence employees to accept neutralization techniques and ultimately violate IS policy. This chapter included a review of the impact of social influences and social pressures on the dependent variable, intent to violate IS policy. Furthermore, this chapter included the two research questions and five hypotheses. The instrumentation presented included a validated instrument borrowed from Siponen and Vance (2010), Hooley et al. (2000), Douglas et al. (2000), Cheng et al. (2013), Allmon (2000), Sin et al. (2005), and Heath and Rao (2009). Issues pertaining to reliability and

validity were addressed including internal and external validity of the instrument. The population and sample were presented including the unit of analysis and the demographics. The data analysis was presented with a discussion on the analysis of the theoretical model using SmartPLS. The chapter concluded with identifying the resources that were used to conduct this study.

Chapter 4

Results

Pre-Analysis Data Screening

This study was a quantitative study that collected data through an online survey methodology via SurveyMonkey® that used a 7-point Likert scale for measurement analysis (see Appendix H). This study performed a pilot test on 10% of the targeted population to assess the reliability of the online survey methodology prior to data collection. The participants were identified from three targeted groups: employees from academic institutions, employees from corporate organizations, and employees from information technology professionals. The initial test was sent to 10% of the population to identify any oversight that may have been missed by the researcher. From the pilot test, it was determined that some questions required grammatical corrections, some questions were missing data, and some questions were not marked as required. Prior to beginning data collection, IRB approval was requested and approved. Appendix I includes the IRB approval document.

After addressing these issues, a final survey invitation was sent to the remaining targeted population for completion.

Data collection was conducted in the months of June 2020, July 2020, August 2020, and September 2020. The research used a cross sectional method to gather data once, over a period of weeks to answer research questions from a one-shot or cross-

sectional approach. An additional check using IBM SPSS was performed for missing values and frequency distribution. The test indicated that there were no missing data and the frequency distribution conformed to a normally shaped distribution as seen on through the histogram chart. The unit of analysis for this study was at the individual level. Invitations were sent to over 800 individuals were a total of 240 responded, a response rate of 30%. A stratified method was used to collect data from the targeted groups, where a random sampling of each stratum proportionately selected data from stratified groups that equaled 206 participants (see Appendix J). SPSS was used to analyze data reliability and validity as well as convergent and discriminant validity. Normality, box plots, stem-and-leaf plots, Q-Q plots were examined visually for any abnormal data (see Appendix K). Descriptive statistics were used to analyze the demographic data collected on employee, institution, and gender. Partial least squares was used for modeling, a regression-based approach that helped minimize residual variances of internal constructs. PLS also is a more robust approach with fewer identification issues, and it works well with smaller sample sizes (Hair et al., 2011).

Normality, Stem-and-Leaf, and Q-Plots

To test for normality, all variables were aggregated into independent and dependent variables. Normality was examined by generating descriptive statistics for all variables through the use of SPSS skewness and kurtosis tests. All variables fell within the acceptable range with some items slightly above the 1.0 value. To correct any items that peaked outside the range, an arithmetic log base 10 algorithm was used to align within the acceptable range. The acceptable range for skewness is between -1.96 to +1.96 (Hair et al., 2017). Data visualization techniques were used to help clearly and efficiently

communicate the analysis of the data including stem-and-leaf plots and Q-Plots that are used to graphically represent the data for variance (Mertler & Vannatta, 2013). In quantitative studies, stem and leaf plots are used as a device for representing quantitative data in a graphical format, similar to a histogram. In this study, stem-and-leaf was used visually to analyze the shape of the data distribution. Q-Q Plots were also used to graphically determine how well the data distribution was normally distributed. In this study, data points on the Q-plots were examined visually. The normality graph showed the cases were very close to the diagonal line, which indicated normality of data. Notwithstanding, through the use of these tools it was determined the values were representative and an indication of a normal data distribution. Thus, it is understood that the data for this study was normally distributed (see Appendix K).

Box Plots

In SPSS, box plots were used to visually examine data distribution for outliers. SPSS delineates two types of outliers, mild and extreme. Mild outliers are those cases in which participants may have responded outside the median but still fell within the range of scoring. Extreme outliers are cases in which respondents are far outside the range of scoring. In this study, box plots were used to examine the center and the spread of the data which allowed the ability to identify skewness and outliers. There was a total of 23 outliers that were found for cases 10, 15, 18, 19, 46, 56, 58, 64, 80, 93, 94, 99, 110, 111, 124, 137, 146, 119, 160, 162, 176, 177, and 180. All identified outliers were considered to be mild outliers and also considered legitimate outliers; therefore, the cases were not altered or deleted. A Likert scale ranging from 1-7 did not allow respondents to mistakenly select or enter an extreme score.

Data Analysis

Smart PLS software was used to further analyze the data for model fit, convergent validity, discriminant validity, construct reliability and validity, and factor loading. After running the PLS algorithm, with all initial loadings, the model fit SRMR was at 0.072, which is considered an acceptable level (See Appendix L). Any level less than 0.08 is considered a good fit (Hu & Bentler, 1998). Although the initial PLS algorithm produced an SRMR acceptable level, it was observed that N10, N7, and SI4 had factor loadings of 0.659, 0.654, and 0.621, respectively. After deleting N10, N7, and SI4 and rerunning the PLS algorithm, the model fit improved the SRMR to 0.069 (see Table 4 and Appendix M). Also see Appendix N for PLS analysis with bootstrapping for *t* statistics for significance. A value of zero indicates a perfect fit (HU & Bentler, 1998). This research study is survey based, and validation becomes important for the research community to have confidence in the methods used. Rigorous validity and reliability tests of this model were conducted and found it to be valid and reliable. Table 4 displays the values resulting from the tests.

Table 4

Model Fit and Accepted Values

Test	Saturated Model	Estimated Model
SRMR	0.069	0.088
d_ULS	1.672	2.699
d_G	0.905	0.920
Chi-Square	999.746	1010.954
NFI	0.714	0.711

Convergent Validity

Convergent validity is a quantitative measure of the degree to which two logically and theoretically related measures of a construct are related. Items that measure the same construct “converge” in strong relationships, whether direct or indirect. In other words, convergent validity refers to the degree to which a measure is correlated with other measures. High correlations indicate two or more measures are measuring the same construct. Convergent validity was measured with Cronbach’s α and Pearson correlations (r) to quantify relationships between survey items; Cronbach’s α values of .70+ indicate acceptable reliability. All items measured at the .70+; however, there was a noticeable change for ethical orientation’s Cronbach alpha score from the pilot study, which measured at .807 for 40 participants, then at .684 for 206 participants, which is borderline to the acceptable range. The loadings ranged from 0.733 to 0.879 indicating convergent validity (see Tables 5, 6 and Appendix P).

Table 5

Outer Model Loadings

	Business Orientation	Ethical _Orientation	Neutralization	Social Influences	Social Pressures
B01	0.733				
B02	0.785				
B04	0.830				
B06	0.833				
E02		0.870			
E03		0.874			
N1			0.825		
N11			0.704		
N2			0.839		
N3			0.751		
N4			0.840		
N5			0.796		
N6			0.768		
N8			0.844		
N9			0.862		
SI10				0.738	
SI5				0.811	
SI6				0.739	
SI7				0.814	
SI8				0.845	
SP1					0.879
SP3					0.733
SP4					0.831
SP5					0.866
SP6					0.743

The average variance extracted (AVE) is another measure of convergent validity. Fornell and Larcker (1981) recommended values higher than 0.50 to indicate convergent validity. Table 6 shows the average variance extracted for each latent variable. The values were greater than the .50 threshold indicating convergent validity.

Table 6

Construct Reliability and Validity

Constructs	Cronbach Alpha	Rho_A	Composite Reliability	Average Variance Extracted	Number of Items	Factor Loading
Business Orientation	.815	0.835	.874	.634	4	.733 - .833
Ethical Orientation	.684	0.684	.864	.760	2	.870 - .874
Neutralization	.932	0.938	.943	.647	9	.704 - .862
Social Influences	.851	0.873	.892	.625	5	.781 - .852
Social Pressures	.873	0.906	.906	.661	6	.738 - .845

Discriminant Validity

Conversely, discriminant validity is a quantitative measure of the degree to which two unrelated constructs are in fact differentiated by survey items. Well-differentiated items that measure different constructs have weak relationships, whether direct or indirect, because they measure distinct ideas. Lee et al. (2013) refers to the low correlations that exist between measurements designed to measure different constructs.

Discriminant validity also measures the degree of differences between the overlapping constructs, which can be evaluated by using cross-loading of indicators. However, the factor loading indicators on the assigned construct must be higher than all the loadings of the other constructs. A detailed breakdown of the discriminant validity statistics can be found in Table 7, and Table 8 displays results using the Fornell and Larcker Criterion and Table 9 has results using the Heterotrait-Monotrait Ratio (HTMT) (see Appendix Q).

Table 7

Discriminant Validity: Indicator and Item Cross Loadings

Construct	Business Orientation	Ethical Orientation	Neutralization	Social Influences	Social Pressures	Intent to Violate
B01	0.733	0.179	-0.095	0.279	0.404	-0.091
B02	0.785	0.208	-0.216	0.270	0.421	-0.134
B04	0.830	0.212	-0.212	0.228	0.391	-0.047
B06	0.833	0.205	-0.240	0.251	0.377	-0.115
E02	0.190	0.870	-0.308	0.393	0.319	-0.250
E03	0.252	0.874	-0.312	0.265	0.222	-0.088
N1	-0.181	-0.272	0.825	-0.312	-0.188	0.342
N2	-0.272	-0.329	0.839	-0.238	-0.263	0.429
N3	-0.131	-0.223	0.751	-0.295	-0.303	0.394
N4	-0.237	-0.347	0.840	-0.314	-0.243	0.417
N5	-0.228	-0.398	0.796	-0.380	-0.336	0.425
N6	-0.228	-0.269	0.768	-0.322	-0.304	0.343
N8	-0.196	-0.255	0.844	-0.270	-0.168	0.336
N9	-0.160	-0.209	0.862	-0.274	-0.167	0.382
N11	-0.196	-0.203	0.704	-0.279	-0.267	0.320
SI5	0.262	0.282	-0.296	0.811	0.337	-0.144
SI6	0.331	0.237	-0.268	0.739	0.537	-0.109
SI7	0.277	0.341	-0.0323	0.814	0.367	-0.175
SI8	0.256	0.298	-0.297	0.845	0.384	-0.130
SI10	0.099	0.323	-0.278	0.738	0.350	-0.107
SP1	0.422	0.205	-0.242	0.415	0.879	-0.256
SP3	0.409	0.285	-0.266	0.314	0.733	-0.127
SP4	0.373	0.232	-0.293	0.435	0.831	-0.234
SP5	0.415	0.280	-0.212	0.414	0.866	-0.219
SP6	0.413	0.317	-0.284	0.399	0.743	-0.153
Intent to Violate ISP	-0.122	-0.193	0.473	-0.173	-0.255	1.000

Table 8

Discriminant Validity (Fornell and Larcker Criterion)

	Business Orientation	Ethical Orientation	Intent to Violate	Neutralization	Social Influences	Social Pressures
Business Orientation	0.796					
Ethical Orientation	0.253	0.872				
Intent to Violate	-0.122	-0.193	1.000			
Neutralization	-0.257	-0.356	0.473	0.805		
Social Influences	0.314	0.357	-0.173	-0.372	0.790	
Social Pressures	0.492	0.310	-0.255	-0.312	0.489	0.813

Note: The diagonal is the square root of the AVE of the latent variables and indicate the highest in any column or row.

Table 9

Discriminant Validity Heterotrait-Monotrait Ratio (HTMT)

	Business Orientation	Ethical Orientation	Intent to Violate	Neutralization	Social Influences	Social Pressures
Business Orientation						
Ethical Orientation	0.335					
Intent to Violate	0.134	0.234				
Neutralization	0.268	0.434	0.485			
Social Influences	0.378	0.491	0.182	0.413		
Social Pressures	0.597	0.419	0.260	0.349	0.572	

Note: Kline, R.B. (2011) Principles and practice of structural equation modeling, New York:

Guilford Press; Gold, A. H., Malhotra, A. and Segars, A. H. (2001). Knowledge management: an organizational capabilities perspective. *Journal of Management Information Systems*, 18(1), 185-214

Descriptive Statistics

SPSS was used to run descriptive statistics on all data items collected through the data collector, SurveyMonkey®. The frequency function was used to measure the mean, mode, and standard deviation for each of the following groups: academic institutions, corporate organizations, and IT Professionals. Charts and graphic images were used to present the ratio between the groups, including male and female. Descriptive statistics described the detailed demographic information between groups with a total of 206 respondents making up responses from all groups. Of the 206 responses, information technology professionals included 34 respondents or 16.5%, corporate organizations included 63 respondents or 30.6%, and academic institutions included 109 respondents or 52.9% of the sample population (see Appendix O).

A linear model univariate test, which included a post hoc Tukey and homogeneity test, was performed to detail any significance between the groups. Results showed that there were no significant differences between the information technology group and corporate group, with $p = .220$, and there was no difference between the information technology group and the academic institution, with $p = .187$. Furthermore, results showed no difference between corporate organizations and the information professional group, with $p = .220$, however, there was a significant difference between corporate organizations and academic institutions, with $p = .000$.

Organizational size indicated that 16.5% of the sample population reported they worked for an organization with 1 – 49 employees, 37.4% worked for organizations with 50 – 999 employees, 19.4% said their worked for organizations with 1,000 – 4,999 employees, and 26%.7 indicated their organization had 5,000 or more employees.

Descriptive statistical information on gender had an even split with male respondents numbering 103 (50%) and female respondents numbering 103 (50%), totaling 206 respondents. Table 10 includes descriptive statistics for organizational groups. Table 11 includes descriptive statistics for gender and Table 12 includes descriptive statistics for organizational size.

Table 10

Descriptive Statistics for Organizational Groups

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Information Technology Professional	34	16.5	16.5	16.5
	Corporate organization	63	30.6	30.6	47.1
	Academic Institution	109	52.9	52.9	100.0
	Total	206	100.0	100.0	

Table 11

Descriptive Statistics for Gender

		Gender			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	103	50.0	50.0	50.0
	Female	103	50.0	50.0	100.0
	Total	206	100.0	100.0	

Table 12

Descriptive Statistics for Organizational Size

What are the approximate total number of employees for your organization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 - 49	34	16.5	16.5	16.5
	50 - 999	77	37.4	37.4	53.9
	1,000 - 4,999	40	19.4	19.4	73.3
	5,000 - More	55	26.7	26.7	100.0
	Total	206	100.0	100.0	

Descriptive statistics was used to provide the statistical breakdown for all constructs pertaining to the research model. SPSS was used to measure the mean, median, mode and standard deviation for business orientation, ethical orientation, neutralization, social influences, social pressures, and intent to violate. See Table 13 statistics for model constructs.

Table 13

Descriptive Statistics for Model Constructs

Constructs	Mean	Median	Std. Deviation	Range	Minimum	Maximum
Intent to Violate	5.1165	2.0000	4.44544	18.00	2.00	20.00
Business Orientation	5.3313	5.5000	1.13283	6.00	1.00	7.00
Ethical Orientation	5.8641	6.5000	.98202	4.50	2.00	6.50
Neutralization	23.0243	21.0000	12.15728	50.00	11.00	61.00
Social Influences	6.0922	6.1667	.83202	4.50	2.50	7.00
Social Pressures	31.3252	32.5000	4.05403	24.00	11.00	35.00

Hypotheses Testing

This study used SmartPLS to test the proposed hypotheses and the significance of all paths in the research model. The PLS algorithm was run to produce the standardized regression weights, factor loadings, and R^2 (i.e., the percent of variance explained by the explanatory variables). To test if regression weights were significant, a bootstrapping algorithm created t statistics to show significance. The independent constructs found variance in the dependent constructs neutralization, with 15% explained by business orientation and ethical orientation and intent to violate IS policy with 24% explained by neutralization, social influences, and social pressures (see Figure 2 and Appendix L).

From a data analysis perspective, intent to violate IS policy was positively influenced by neutralization ($t = 5.839, p = 0.000$), which explained 24% of intent to violate IS policy. See Table 14. This result was statistically significant. However, due to lower loadings, N10 and N7 were removed, and the significance increased to $t = 6.240, p = 0.000$, which resulted in the same influence of 24% of the intent to violate IS policy (see Appendix M). Business orientation ($t = 2.952, p = 0.003$) and ethical orientation ($t = 4.523, p = 0.000$) which explained 15% of variance on neutralization were both statistically significant. Social influences ($t = .796, p = 0.415$) and social pressures ($t = 1.533, p = 0.124$) were not significant on the intent to violate IS policy, as the t statistics did not reach 1.96 at the .05 level. See figure 2 for details on path coefficients.

The path coefficients are the standardized beta coefficients. As predicted, business orientation had a negative influence on the acceptance of *neutralization techniques* ($\beta = -0.179, p < 0.01$). Therefore, **H1** is support. The analysis of these results shows that, in most instances, the relationship between business orientation and neutralization is a

predictor of employees accepting neutralization techniques to violate IS policy. The results further show that most employees with a strong sense of customer satisfaction are not willing to compromise breaking the rule or policy. Ethical orientation had a negative influence on the *neutralization techniques* ($\beta = -0.310, p < 0.05$). Therefore, **H2** is supported. Results from ethical orientation are clear that the values of most, but not all employees, are overwhelming in agreement with ownership of individual actions that should not harm other employees or the organization. As per Siponen and Vance (2010), neutralization had a positive influence on the intent to violate information security policy ($\beta = 0.452, p < 0.001$). **H3** is supported. Results showed a positive impact on the intent to violate information security policy. Previous research from Siponen and Vance (2010) found neutralization to be an indicator of employee's information security behavior. Neutralization showed a positive and significant impact on ISSP. Social influence ($\beta = 0.067, p = 0.415$) did not have a significant impact on the intent to violate information security policy. Employee's involvement and attachment to their co-workers and organization did not result in a significant influence to violate ISSP. Results contradict the findings of Cheng et al., (2013) who found that social influence negatively impacted the intent to violate ISSP. This is an area certainly for future research, as results are inconclusive. **H4** was not supported. Lastly, social pressures ($\beta = -0.146, p = 0.124$) did not have a significant impact on the intent to violate information security policy. Therefore, **H5** is not supported. These results indicate supervisors, managers, and peers influence employees through messages and expectations in adhering to IS policies. Moreover, these results show that employees have a negative intent to violate IS policy through the influence of pressures by their peers (see Appendix M). Table 14 summarizes

the statistical results of the analyses and Figure 2 displays a graphic of the results of the analysis.

Table 14

Summary of Hypothesis Tests

Path	Path			
	Coefficient	t Value	p Value	Support
Business Orientation -> Neutralization Techniques	-.0179	2.952	0.009	Yes
Ethical Orientation -> Neutralization Techniques	-0.310	4.523	0.001	Yes
Neutralization -> Intent to Violate Information Security Policy	.452	5.839	0.000	Yes
Social Influences -> Intent to Violate Information Security Policy	.067	0.796	0.415	No
Social Pressures -> Intent to Violate Information Security Policy	-.146	1.533	0.124	No

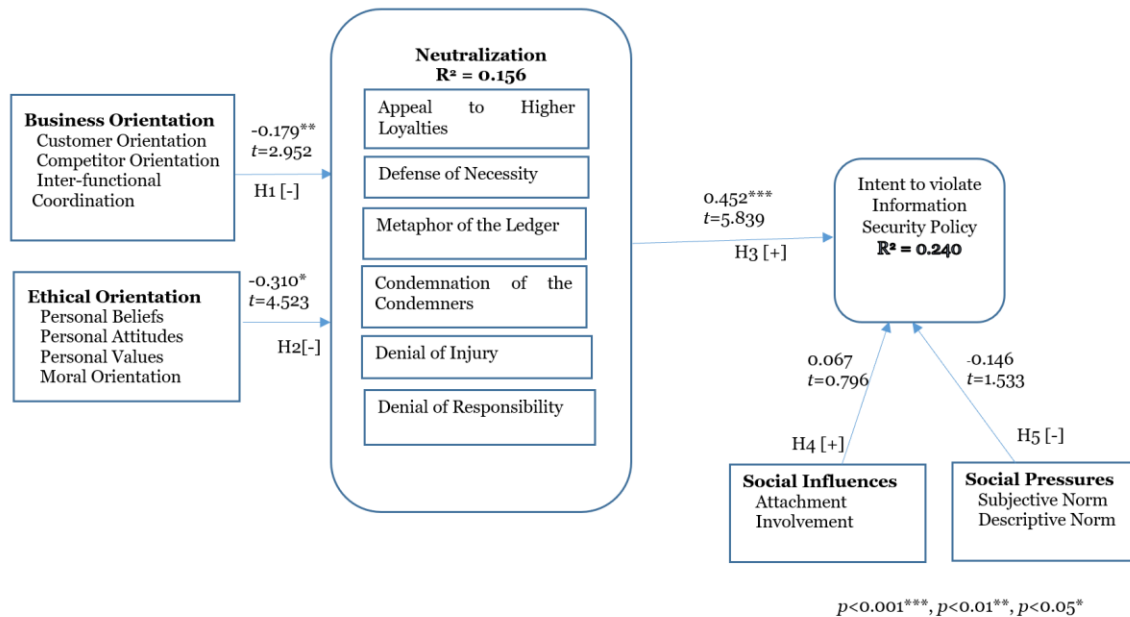


Figure 2. PLS Analysis Results for Intent to Violate Information Security Policy

Summary

A quantitative study was conducted using an online survey methodology. A pilot test provided excellent feedback for refining the final study. A total of 206 participants volunteered to complete an online survey using SurveyMonkey® which constituted the final data collection. All data were tested for normality using tests for skewness and kurtosis; stem-and-leaf, Q Q-Plots were also used. SurveyMonkey® was used to collect random data through the outreach program. To correct any items that peeked outside the range, an arithmetic log base 10 was used to align within acceptable range. Smart PLS provided the model fit, convergent validity, discriminant validity, construct reliability and validity, and factor loadings. Descriptive statistics were used to model constructs, organizational groups, and gender.

Results revealed variance in neutralization with 15% explained by business orientation and ethical orientation. Intent to violate information security policy had a variance of 24%, which was explained by 24% from neutralization, social influences and social pressures. Hypotheses H4 and H5, were rejected, while H1, H2, and H3 were supported.

Chapter 5

Conclusions

Complying to an organization's IS policy is critical in protecting sensitive information. Research has shown that employees are the key to the IS compliance problem for organizations. It is estimated that over half of all IS security breaches are due directly or indirectly to employee's poor security practices. This research built on the Siponen and Vance (2010) model that found neutralization as an excellent indicator of predisposition to violate IS policy. This research added the constructs of business orientation, ethical orientation, social influences, and social pressures to the Siponen and Vance (2010) model that addressed the phenomenon of why employees drift into a state in which they begin using neutralization techniques to violate IS policy. To address this drift, this research adopted a quantitative methodology that used survey methodology. Data were collected from academic institutions, corporate organizations, and information technology professionals. A stratified method for data collection was used to ensure equal representation of the population. Partial least squares was used to evaluate and test the research model. The significance of the study lies in providing insight that will help practitioners and IS managers better understand why employees make decisions to violate IS policy from both a business and ethical perspective. Additionally, social influences and pressures were applied to better understand the magnitude in which social pressure and influences aid employees to violate IS policy.

Discussion

Based on the results of this research, neutralization and social influences played a vital role in positively influencing the intent to violate IS policy. Surprisingly and contrary to the hypothesis, business orientation had significance with negative influences on neutralization techniques. The analysis of these results shows, in most instances, that the relationship between business orientation and neutralization is a predictor of employees accepting neutralization techniques to violate IS policy. Results further suggests that most employees with a strong sense of customer satisfaction are not willing to compromise breaking the rule or policy. It was predicted that business orientation would negatively influence employees to accept neutralization techniques and violate IS policy, but it was shown that employees, when faced with the decision from a business orientation perspective, were not willing to accept neutralization techniques and violate IS policy.

As hypothesized, ethical orientation had negative influence on neutralization techniques. Bulgurcu et al. (2010) noted that it is important to connect end user's behavior with an organization's security policy when evaluating difficult choices by employees. Employees, when faced with difficult decisions, were not willing to cross the line and violate information security policy. Furthermore, employees were not willing to violate information security policy when faced with a task that was too difficult to complete. This research demonstrated that when employees were faced with ethical decisions they were not willing to cross the line and violate IS policy.

Social influences did not have a significant impact on intent to violate IS policy. The research showed employee's involvement and attachment to their organization and

co-workers resulted in the bond employees have with their co-workers and organization. These findings agree with Cheng et al. (2013), who found social influences negatively impacted the intent to violate IS policy. Sims (2002) found ethical rule breaking with involvement and attachment had significant impact. This is an area certainly for future research, as results are inconclusive.

Previous research found social pressures to have mixed impacts on employee's intent to violate ISSP. Hearsh and Rao (2009) found social pressures to have a positive influence, while Cheng et al. (2013) found social pressures to have a negative influence on intent to violate IS policy. This research predicted employees' social pressures (subjective norms and descriptive norms) would have a negative impact on the intent to violate information security policy. Results reveal supervisors, managers, and peers did not have a significant influence on employees through messages and expectations. Previous research has shown employees form bonds with their job, immediate supervisors, co-workers, and the organization.

As predicted, neutralization had a positive impact on the intent to violate IS policy. Previous research from Siponen and Vance (2010) also found neutralization to be an indicator of employee's IS behavior. Employees are believed to consciously or subconsciously rationalize the idea that it is ok to violate IS policy, and in doing so, a neutralization technique is adopted to justify their actions. Neutralization was positive and significant on the intent to violate IS policy with all initial loadings. After the removal of N7 and N10, the significance decreased.

Overall, the results indicated there were no significant differences in the intent to violate IS policy between the information technology group and the academic group, and

there was no difference between corporate organization and information technology group; however, results did indicate there was a significant difference between corporate organizations and academic institution groups. Accepting neutralization techniques was explained by 15% from business and ethical orientation. The relationship between these two constructs showed t values of business orientation to be $t = 2.952$. As noted by Hair et al. (1995), values for a study with two-tailed test of 5% significance level is acceptable when the t -value is greater than or equal to 1.96. High t values are an indication that there is a strong relationship between constructs. This means it is important for practitioners and IS managers to have a full understanding of an employee's cognitive process when faced with decisions relating to complying with IS policy. Results indicate the academic institution group was more likely to violate IS policy. Furthermore, results show that organizational size was a better than organization type in predicting the intent to violate IS policy. This research found that significance did not exist between academic institutions and IT professionals on the intent to violate IS policy; however, there was a significant difference in comparing academic institutions and corporate organizations. Corporate organizations had a negative impact with an unstandardized coefficient of -1.809 and significance $p = .010$. Also, results showed there was no significance between corporate organizations and IT professionals. In terms of organizational size, results showed organizations with 1 – 49 employees are more likely to violate IS policy, while larger organizations showed significantly less likely to violate IS policy. These results may indicate organizations with fewer resources and less structure tend to violate policy in an effect to complete tasks and get the job done, while larger organizations with more resources and structure are less likely to commit such acts. Lastly, results indicated that

across gender there was no significant difference between gender type on the intent to violate IS policy.

Implications

This study clearly identified areas in which IS policy can be compromised by employees. It is recommended that corporate organizations, academic institutions, and IT professionals consider the following:

- Deploy behavioral analytics. This will provide more insight in understanding how employees act and why. It will enable accurate predictions about how they will likely act in the future.
- Train employees for best defense. Employees can unknowingly pose risks to the organization. Proper training should cover poorly designed passwords, surfing the web, and social engineering awareness, which may lead to employees divulging confidential information leakage. Similarly, proper training of employees can become an organization's strongest asset.
- Provide a work environment with IS as a focal point which embraces a healthy security culture.

Moreover, this study showed that intent to violate IS policy was totally explained by 24% of variance from neutralization, social influences, and social pressures, with 15% from neutralization, and the remaining accounted for by social influences and social pressures. This confirms neutralization significantly affects the predisposition to violate IS security policy, which is also consistent with previous research on neutralization studies in other disciplines. For example, Harrington (1996) found that rationalizations were strongly correlated with the intent to commit computer abuse. Similarly,

Puhakainen (1996) found that employees fail to comply with IS security policies because they perceived workloads were too high and argued security policies slowed them down.

Social influences had a positive, but not significant, effect on intent to violate IS policy with a *t*-value of 0.762. This implies attachment to one's co-workers, job, or organization did not have a significant effect on policy violation intentions. This is in keeping with findings from Cheng et al. (2013) who found that involvement in organizational activities does not inevitably result in less policy disobedience.

Likewise, social pressures had a negative influence on intent to violate IS policy, with a *t*-value of 1.539. The construct did not reach the significant level of 1.96. This finding was inconsistent with prior research from Herath and Rao (2009). They found normative beliefs related to expectations from relevant others had a significant impact on employee's behaviors with respect to the expectations of supervisors, peers, or IT personnel. This research showed social pressures (subjective norms, descriptive norms) to have a negative effect on the intent to violate IS policy.

Limitations and Future Studies

To limit the scope of this study, constructs from business orientation were selected to capture some idea of how employees cognitively accept neutralization techniques. In doing so, some questions were omitted. It is hoped that future studies will include more sub constructs and expand business orientation. Ethical orientation initially used four measures in the pilot study to capture employee's ethical decision making regarding accepting neutralization techniques. Two of the four items were removed to improve the Cronbach alpha score to .807 using data from 40 participants. After the final data collection with 206 participants, the Cronbach alpha score dropped to .684 just

below the minimum cutoff set at .70. As these questions were previously vetted, and well tested, the decision was made to continue with vetted questions. The neutralization construct had 11 survey items, but due to low factor loadings, two variables, N7 and N10, were removed which resulted in representation of nine items. Neutralization measures were consistent with Siponen and Vance (2010) results in that this study found neutralization to significantly affect the predisposition to violate IS policy. Social influences initially had six items but, due to low factor loading, SI4 was removed. As a result, social influences were found to have a positive influence on the intent to violate IS policy. Thus, it is suggested that future research focus further on ethical orientation, neutralization, and social influences constructs. Lastly, this study collected data from organizations within the United States only, and therefore, it is suggested that future studies focus on data collected from different populations from different parts of the world, as IS is handled differently by other countries.

Stratified random sampling was used in this study to collect survey data to improve the study generalizability. Two strata were created to represent men and women across all groups. Individual records were randomly removed from the data to create an even distribution of male and female respondents. A total of 240 respondents were collected and then reduced to 206, which created a representation of 103 males and 103 females. Although stratified random sampling was used, the scope and audience of the study remained limited. This is a result of the preselected groups: corporate organizations, academic institutions, and IT professionals. This study did not consider government organizations or the U.S. military, as these groups handle IS differently. Notwithstanding, this study focused on a small percentage of the population. It is hoped

that future studies will expand to different countries and different groups, as IS may be handled differently and in a more rigorous way.

Conclusion

This study addressed the phenomenon of why employees drift into a state in which they begin using neutralization techniques to justify violations of IS policy. This study adopted the Siponen and Vance (2010) model and expanded it to address factors that influenced employees in cognitive decision making from a business and ethical orientation perspective. Additional constructs, social influence, and social pressures were also added to measure their impact on the intent to violate IS policy. A brief overview of how neutralization played a role in the predisposition on the intent to violate IS policy was described. A brief overview of the employee's cognitive mind set from a business and ethical perspective was discussed to provide some context. Lastly, the integration of social influences and social pressures into the model to provide additional influences on the intent to violate IS policy was described.

Research questions were developed for this study and based on the research questions, the study highlighted and proposed hypotheses. A conceptual model was created to provide a visual perspective of constructs and how they influenced neutralization and the intent to violate IS policy, respectively.

The literature review highlighted prior studies that created the fundamental foundation for this research. Siponen and Vance (2010) explored new insights into how employees rationalized their behavior. The authors were the first to use the neutralization model to explain IS security behavior. Cheng et al. (2013) focused on explaining employees information system security policy violations behavior through the

consideration of deterrence and social bond theories. Herath and Rao (2009) focused on IS adoption, protection-motivation theory, deterrence theory, and the adoption of IS practices and policy. These authors focused on the framework for security policy compliance in organizations and how employees are affected by the organization, environment, and behavior factors.

The research method of this study highlighted the research design, the instrument, data collection technique, sample data, and reliability and validity of instruments used. This study used a quantitative survey approach to analyze the independent variables (business orientation, ethical orientation, neutralization, social influences, and social pressures) and the intent to violate IS policy. Data was collected from three specific groups: corporate organizations, academic institutions, and IT professionals. A stratified random sampling was conducted, and descriptive statistics were used to provide the mean, median, and mode. Inferential statistics included *t* statistics, ANOVA, and factor analysis on the data collected. A pilot study was conducted with 40 participants to validate data. A final collection of data was conducted and based on results of the analyses, evidence either supported or rejected the hypotheses. In conclusion, limitations and recommendations for future studies were highlighted.

The main goal of this research is to add to the current body of knowledge in the IS security policy context. Therefore, it is believed that this research will contribute to the body of knowledge on the intent to violate IS policy. Additionally, it is hoped that this body of knowledge will help practitioners, CIOs, and IS professionals write and expand current and future IS policies to reduce violations of IS policy.

Appendix A

Summary of Prior Research on Employees IS Security Violations

Study	Objective of Study	Theory	Instrument or Construct	Main Finding
Bulguru et al. (2009)	Investigated the influence of employee's information security awareness (ISA) and perceived fairness of required information security policy	Theory of Planned Behavior (TPB)	Survey method 462 participants	Found both ISA and perceived fairness significantly influenced attitude; Attitude positively impacted the intention to comply
Bulgurcu et al. (2010)	Identifies the antecedents of employee compliance with IS policy of organizations	Rational choice theory	Pilot testing; online questionnaires	Employee's intention to comply with the ISP is significantly influenced by attitude, normative beliefs, and self-efficacy to comply.
Chan et al. (2005)	Examines the effects of social contextual factors on employee's compliance with organizational security policies	Compliance behavior theory	28 item survey instrument using structured modeling	ISSP compliance behavior intention is influenced by end user's perception of information security climate and self-efficacy of breaching security.
Herath and Rao (2009)	Evaluated the effect of organizational commitment on employee security compliance intentions	Protection motivation theory; deterrence theory; organizational behavior	Survey responses of 312 employees from 78 organizations	Security policy compliance intention can be influence by both intrinsic and extrinsic motivators, including penalties, social pressures, and perceived effectiveness.
Hu et al. (2011)	Tested employee's policy violation intention based on the rational choice theory	Rational choice theory	Scenario-based survey methodology	The perception of benefit had a significant influence on employees' intended behavior.

Study	Objective of Study	Theory	Instrument or Construct	Main Finding
Ifinedo (2012)	Integrated protection motivation theory and theory of planned behavior to better understand employees ISSP compliance intentions	Motivation theory and planned behavior	Efficacy, self-efficacy, response cost	Both appraisals and threat appraisals have significant influences in ISSP compliance.
Li et al. (2010)	Explored the effect of cost-benefit trade-off and personal norms on employee internet use policy compliance intentions	Rational choice theory	Variable measurement	Perceived benefits, formal sanctions, and security risks significantly influenced an employee's intention to comply with internet use policy
Myyry et al. (2009)	Integrated theory of cognitive moral development and theory of motivational values	Theory of moral reasoning	Preconventional reasoning, Conventional reasoning, postconventional reasoning, values	Preconventional moral reasoning is positively related to both hypothetical and actual compliance
Siponen & Van (2010)	Applied neutralization theory to IS	Neutralization theory	Policy capturing	Neutralization significantly affects predisposition to violate IS security policy
Siponen & Vance (2012)	Examined the effects of rational choice on ISSP	Rational choice theory	Contextual information scenarios	Impacts of informal sanctions on moral beliefs; perceived benefits are predictors
Siponen & Vance (2014)	Authors argue that IS behavioral research can improve its practical relevance without loss of rigor by carefully addressing contextual issues in instrumentation design. Presents 5 criteria to meet rigor and relevance to increase contextual	N/A	(1) inform study respondents that a behavior is an ISP violation, (2) measure examples of ISP violations, (3) ensure ISP violations are important ISP problems in practice, (4) ensure the applicability of IS security violations to organizational context, (5) consider	No existing study meets more than three of these five guidelines. By applying their guidelines where applicable, IS scholars can increase the contextual relevance of their instrumentation, yielding results more likely to address important problems in practice.

Study	Objective of Study	Theory	Instrument or Construct	Main Finding
	relevance of field survey research		appropriate level of specificity and generalizability for instrumentation	

Appendix B

Summary of Prior Research on Business Orientation

Study	Objective of Study	Theory	Instrument or Construct	Main Findings
Customer Orientation	Atuahene-Gima (1996)	Empirical study of 158 manufacturing and 117 services firms in Australia	Examined influence of market orientation on innovation characteristics and performance.	Market orientation has significant relationships with innovation characteristics such as innovation-marketing fit, product advantage, and inter-functional teamwork, but with product newness and innovation-technology fit.
Customer Orientation	Kohli, Jaworski, & Kumar (1993)	500 executives, 13 excluded from final response calculation, leaving 487. 230 responded with a response rate of 47.2%	Developed a measure of market orientation and assessed its psychometric properties.	MARKOR assesses the degree to which a SBU (1) engages in multi-department market intelligence generation activities (2) disseminates intelligence vertically and horizontally through informal and formal channels (3) develops and implements marketing programs based on intelligence generated
Customer Orientation	Greenly (1995)	A total of 280 were obtained; 240 fully completed questionnaires	Built on the limited empirical evidence about a relationship by achieving new insights	Market orientation does not have direct effect on performance
Customer Orientation	Narver & Slater (1990)	140 business units	Developed a valid measure for market orientation	Infer from literature that market orientation consists of 3 behavior components customer orientation, competitor

Study	Objective of Study	Theory	Instrument or Construct	Main Findings
Customer Orientation	Wanous & Reichers (2001)		Study of new employee orientation programs: (a) stress theory/coping methods, (b) attitude theory/change methods, (c) RJP theory/methods; close the gap between common practice vs. the scholarly	orientation, and inter-functional coordination Researchers need to agree on the parameters of what constitutes orientation and proceed with field experiments. Experiments represent the strongest design for assessing the effects of orientation, and seem particularly feasible
Competitor Orientation	Armstrong & Collopy (1996)	U.S. schools: 73 undergraduates, 846 MBAs, 42 executive MBAs; Argentinian business schools: 20 MBAs, 35 executives	Study measured the effects of objectives and information on managerial decisions and profitability	Use of competitor-oriented objectives is detrimental to profitability
Competitor Orientation	Dev, Zhou, Brown, & Agarwal (2007)	558 surveys to hotel general or senior managers who were club members reporting on their individual hotels; they knew relevant information on their hotel's strategic orientation, performance benchmarks, and surrounding environment; 32.9 % response rate	Authors identified, for the first time in an international context, the circumstances when customer orientation (acquisition, satisfaction, and retention of customers) alone has a higher payoff or when simply investing resources on competitor orientation (monitoring, managing, and outflanking competitors) alone is the better strategy	Customer orientation has a greater effect on hotel performance than does a competitor orientation; customer orientation on performance is statistically positive and significant; across all but one of the models, neither the effects of a competitor orientation nor inter-functional coordination is significant for any model
Competitor Orientation	Lewrick, Omar, & William (2011)	Acquired data from over 200 Chief Operating Officers (CEO's) and managing directors from both start-up	Investigates the effects of parameters of market orientation on radical and incremental innovation in start-up and mature companies. This	Illustrate differences in both types of company and reveals new insights on market orientation and its constituent elements and its relationship with incremental and radical innovations. Key results

Study	Objective of Study	Theory	Instrument or Construct	Main Findings
		and mature companies	contrasts to other research by distinguishing between start-up and mature companies; yields new insights about the transformation process in the growth of innovative companies	are that strong competitor orientation, a key ingredient of market orientation, has positive relationship to incremental innovation for start-up companies but is contra productive for mature companies.
Competitor Orientation	Sousa & Marques (2013)	197 Brazilian Firms	Addresses gap in the literature to test a model that examines whether customer and competitor orientation have linear or quadratic relationships with export performance. Investigate if competitive intensity moderates the linear and quadratic relationships	Empirical evidence reveals that, while customer orientation has a U-shaped relationship with export sales, the competitor orientation, export profit relationship, is linear.
Competitor Orientation	Sin, Tse, Yau, Chow, & Lee (2004)	226 firms completed surveys, a rate of 26.6%	Examined how economics ideology and industry type moderate the impacts of market orientation on business performance	Two sets of ideas/findings distinguish this study from previous studies (1) Developed constructs and measures of MO and RMO for data collection; validates MO and RMO scales in a Chinese context using data obtained from market decision makers at corporate level.
Competitor Orientation	Hooley, Cox, Shipley, Beracs, Fonfara, & Snoj (2000)	NA	Develop ed and refined earlier market orientation scales to create useful tools for measuring the degree of market orientation that Western firms exhibit.	Demonstrated that the overall Narver and Slater (1990) MO scale is both valid and reliable as a measure of market orientation in the transition economies of central Europe.
Inter-functional Coordination	Jebarajakirthy, Thaichon, & Yoganathan (2016)	250 managers of microcredit institutions operating in the	Investigated the influence of market orientation on corporate social	Market culture enhanced positive influences of both customer orientation and inter-

Study	Objective of Study	Theory	Instrument or Construct	Main Findings
		rural areas of Sri Lank.	responsibility among microcredit institutions	functional coordination on CSR; findings are useful for microcredit institutions and marketers operating in bottom of pyramid (BOP) market to enhance their CSR through market orientation practices.
Inter-functional Coordination	Micheli, Perks, & Beverland (2018)	53 in-depth interviews with key informants, representing a range of 12 companies, including large multinational companies as well as small and medium-sized enterprises	Studied unreal and detail critical practices and potential tensions influencing the elevation of design's status in firms	Findings show how six practices (top management support, leadership of the design function, generating awareness of design's role and contribution, inter-functional coordination, evaluation of design, and formalization of product and service development processes) affected the design elevation process; revealed the same practice can play both positive and negative roles and there are fundamental tensions, which should be reconciled
Inter-functional Coordination	Narver & Slater (1990)	140 business units	Develop a valid measure for market orientation	Infer for literature that market orientation consists of 3 behavior components -customer orientation, competitor orientation and inter-functional coordination
Inter-functional Coordination	Rapp, Beitelspacher, Schillewaert, & Baker (2012)	156 sales organizations	Examined outcomes of different workplace structures	Reviewed sales force structure, e-learning and technological tools that influence coordination and the level of customer orientation; Suggested this type of structure leads to greater positive outcomes.
Inter-functional Coordination	Rogerson & Sallus (2017)	Data from three Swedish companies -case study	Developed matrix to show the differences in applying various coordination	Different coordination mechanisms are useful in different categories and can also be applied

Study	Objective of Study	Theory	Instrument or Construct	Main Findings
			mechanisms in eight categories, according to intra functional or inter-functional coordination, sequential or reciprocal interdependencies, and the number of activities	differently; for example, coordination mechanisms that aim to exert control are more suitable for intra-functional than for inter-functional coordination. Inter-functional coordination relies more on mechanisms that aim to increase understanding of transport-related issues among non-logistics activities in organizations.
Inter-functional Coordination	Yang, Wang, Hengyuan, & Wu (2012)	More than 500 senior executives in a wide range of manufacturing and service firms in China	Aim to evaluate (1) whether a focus on customer, technology, competitor, or inter-functional coordination will have the greatest impact on new product success; (2) if effectiveness of a specific SO varies with environment	Found positive relationship between technology orientation and new product performance, did not expect to find technology orientation so dominant, both in terms of the level of significance and the magnitude of influence across all environmental conditions.

Appendix C

Summary of Prior Research on Ethical Orientation

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Alteer, Yahya, and Haron	General Ethics Theory	AICPA members sample		Personal values, ethical climate, ethic sensitivity, ethical judgement	Finding of this study suggest there are several ethical theories a model provide a significant understanding of ethical issues and suggested factors that may affect ethical judgement decision.
Beekun and Westerman (2012)	Data were collected from business students (n=149) at state universities in Norway	Sociology		Justice, utilitarianism, and relativism	Results indicate that intention to behave ethically was significantly related to spiritually, national culture, and the influence of peers. Americans were significantly less ethical than Norwegians based on the three dimensions of ethics, yet more spiritual overall.
Bulgurcu, Cavsoglu, and Benbasat (2009)	Theory of Planned Behavior (TPB)	PLS analysis of data collected from 464 participants	IS security, psychology	ISP awareness, ISA general, attitude, fairness, intent to comply	ISA and perceived fairness positively affect attitude, and in turn attitude positively affects intention to comply. ISA also has an indirect impact on attitude since it positively influences perceived fairness.
Cohen, Pant, and Sharp (2001)	Ethical theory Justice deontology,	Items were selected from those identified by	Business ethics	Ethical awareness, ethical orientation, and intention to	Tests for differences in responses between the eight questionnaire

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
	relativism, utilitarianism, egoism	Reidenbach and Robin (1988) from a survey of the moral philosophy literature, and subsequently refined and validated in an accounting context by Flory et al. (1992) and Cohen et al. (1993, 1996).		perform questionable acts.	versions indicated no order or sequence effects. No significant differences emerged among the responses of the five firms, or among the five universities
Douglas, Davidson, and Schwartz (2001)	Belief system theory	304 accountants	Business ethics	Idealism, realism, judgment,	Measures of idealism and relativism show no significant correlation with age or position; relativism and idealism are significantly correlated with gender
Ferrell and Gresham (1985)	Differential association theory	Survey n=1200	Marketing	Ethical issues, individual factors, significant others, individual decision making, behavior, evaluation of behavior	Integrated the key determinants of ethical and unethical behavior in multistage contingency
Fok, Payne, and Corey (2016)	Rule Utilitarianism, Act Utilitarianism, Theory of Moral Rights, Theory of Justice	Students taught in Southern city in U.S. and students in Puerto Rico EMBA program	Business ethics	Instrument adopted from a Brenner and McGuire (Brenner and McGuire 2003; McGuire et al. 2006) study	Evidence shows that one means through which cultural values impact ethical decision-making
Fritzsche, and Oz (2007)	Theory of planned behavior	Data were gathered from 174 working professional	Business ethics	Altruistic, Openness, self-enhance, traditional	First study to link values directly to the ethical dimension of decision making and

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
		s attending part-time graduate programs at an Eastern graduate school			will hopefully attract interest to this area of exploration.
Hunt and Vitell (1986)	Theory of marketing ethics	Scenario techniques	Macromarketing	Cultural environment, industry environment, organizational environment, personal experience, ethical judgement	Develop a theory of marketing ethics to guide empirical research and analysis
Hyde and Weathington (2006)			Social and general psychology	Personal value, work sphere, behavior	Results suggested varying relationships between value placement and work attitudes. The authors discussed implications and directions for future research.
Kajtazi, Cavusoglu, Benbasat, and Haftor (2018)	Prospect theory	500 respondents ; pre-test, pre-study, main study	Information & Security		Antecedents that explain the escalation of commitment behavior in terms of the effect of lost assets, such as time, effort and other resources, give us a new lens to understand noncompliance behavior
Kim, Yang, and Sunyoung (2014)	Neutralization theory Planned behavior theory, motivation theory, rational choice theory	194 out of 207 questionnaires	Psychology, Information security	Attitude, subjective norm, perceived control of actions.	Derived attitude, normal belief, and self-efficacy based upon the theory of reasoned action, seven factors from neutralization theory, and response efficacy from the protection motivation theory.

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Theory of Cognitive Moral Development by Kohlberg and the Theory of Motivational Types of Values by Schwartz		Survey of two subsamples sets	Social psychology	Preconventional reasoning, Conventional reasoning, Postconventional reasoning, openness to change, Conservation Hypothetical compliance.	Empirical findings suggest that preconventional moral reasoning is positively related to both hypothetical and actual compliance
Utilitarian ethical theory		176 business students	Business management	Instrument is a 150-item self-report questionnaire on nine cultural values and beliefs	Results indicated that act and rule utilitarian orientations significantly mediated the effects of universalism on EDM.
Theory of marketing ethics		406 valid questionnaires were obtained from voluntarily participated students in this research	Psychology	Analysis was carried out by using Partial Least Squares technique; justice, deontology, relativism, and utilitarianism	Found that instrumental value positively affects students' ethical decision-making criteria (e.g. justice, relativism, utilitarianism, and deontology) in five scenarios; found that utilitarianism positively affects students' intention to perform ethical behaviors for the five of the six scenarios

Appendix D

Summary of Prior Research on Neutralization

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Barlow, Warkentin, Ormond, and Dennis (2013)	Neutralization theory	Factorial survey method. Random set of 4 out of 36 scenarios increased total sample by four using Qualtrics; 90 employees completed survey; total size=360	Information Technology	Defense of necessity, Denial of injury, Metaphor of the ledger	Security communication and training that focuses on neutralization techniques is just as effective as communication that focuses on deterrent sanctions in persuading employees not to violate policies
D'Arcy (2015)	Neutralization. Social exchange theory	Malaysian banking employees	Banking/ financial sector	Organizational commitment, role conflict, neutralization	Extended the reach of neutralization theory beyond North American and European cultures; found positive role conflict and neutralization of ISP violations
Hinduja (2007)	Neutralization theory	anonymous and voluntary questionnaire; logistic regression analyses on cross-sectional data collected from a sample of university students in the United State	Sociology, criminal-ogy	Denial of injury, denial of victim, denial of responsibility, condemnation of the condemners, appeal to higher loyalties	Denial of Injury, Appeal to Higher Loyalties, Denial of Negative Intent, and Claim of Relative Acceptability were the only techniques significantly related to having pirated software at least once. Generally speaking, neutralization was found to be weakly related to experience with online software piracy
Ingram and	Neutralization	Sampled 2,000 undergraduate students	Criminology, sociology	Denial of responsibility, denial of injury,	Findings indicated that greater acceptance of the techniques

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Hinduja (2008)				denial of victim, appeal to higher loyalties, condemnation of condemners	associated with denial of responsibility, denial of injury, denial of victim, and appeal to higher loyalties significantly predicted moderate levels of piracy participation. Additionally, effect of appeals to higher loyalty on piracy was found to be conditioned by the respondent's approval of the behavior
Kim, Yang, and Sunyoung (2014)	Neutralization theory, Planned behavior theory, motivation theory, rational choice theory	194 out of 207 questionnaires	Psychology Information security	Attitude, subjective norm, perceived control of actions.	Derived attitude, normal belief, and self-efficacy based upon the theory of reasoned action, seven factors from neutralization theory, and response efficacy from the protection motivation theory.
Leasure (2017)	Neutralization	Instrumental case study; sampled 22 participants from 5 different companies	U.S. retail banking industry		Results indicate that neutralization theory does generalize to the retail banking context
Minor	Neutralization theory	N/A	Criminology	Defense of necessity	Added the defense of necessity, in which an offender attempts to justify their actions based on the perceived necessity to commit the act
Morris and Higgins (2009)	Neutralization,	Data were collected from undergraduate students from multiple universities (n = 585)	Sociology, criminology	Neutralization, willingness to engage in video piracy	Neutralization construct was found to have a statistically significant direct effect on willingness (prospective) to engage in illegally downloading a music CD but not on potential video piracy. neutralization was

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Silc, Barlow, and Back (2017)	Neutralization	Field study; Four organizations; Banking, Information technology, Insurance, financial company	Information & Management	Metaphor of the ledger	found to have the strongest direct effect compared to the other theoretical predictors Studied the effects of neutralization on both intentions (self-reported) and actual behavior. Found metaphor of ledger predicts shadow IT intention
Siponen and Vance (2010)	Neutralization Theory	60 according to "rule of ten" (Barclay et al. (1995). Administrative personnel from three organizations	Criminology	Survey 11-point	Neutralization significantly affects predisposition to violate IS security. (2) Although informal sanctions significantly predict intention, the presence of neutralization make informal sanctions on intention insignificant. (3) Data suggest formal sanctions do not predict IS security policy violations. (4) provided security managers with most important and common IS security violations
Sykes and Matza (1957)	Neutralization theory	N/A	American Sociology	N/A	Originators of neutralization techniques. Provide reasoning to juvenile delinquency justification behavior
Willison, Warkentin, and Johnson (2018)	Neutralization theory, deterrence theory, Justice theory	Scenario design; 968 responses; 45% male, 30% age 35-44; 44% reported 25 or more years of professional work experience		Denial of victim, metaphor of ledger, and denial of injury	Employees may form intentions to commit computer abuse if presence of procedural injustice and techniques of neutralization and certainty of sanctions.

Appendix E

Summary of Prior Research on Social Influences

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Camp-bell, Stylianou, and Shropshire (2016)	Theories of idealism perceived organization al risk, social influence, and managerial position	Survey 315 American workers tested the proposed hypotheses and research model using structural equation modeling.	Information Technology	Perceived organizational risk, social influence, mgmt. position, idealism, intent to report internet abuse	Each of the attitudinal factors had a significant impact on employee willingness to report Internet violations.
Chen, Li, Li, Holm, and, Zhai (2013)	Social control and deterrence theory	Survey data of 185 employees	IS, sociology	Social bonds, social pressures, perceived sanctions	Formal and informal have significant effect on employee's ISSP violation intentions. Social bonds have mixed impacts on employee's intentions. Subjective norms and co-worker's behavior have significantly influence
Deutsch and Gerard (1955)	Social Psychology	101 students from New York University psychology course	Psychology	Social influence -normative, informational	Data provide strong support for the prediction that the normative social influence upon individual judgments will be greater among individuals forming a group than among individuals who do not compose a group.
Ifinedo (2012)	Theory of planned behavior and protection motivation theory	Survey 124 business managers and IS professionals	IS, psychology	Self-efficacy, attitude toward compliance, subjective norms, response efficacy and perceived vulnerability positively influence	Study showed factor such as self-efficacy, attitude toward compliance, subjective norms, response efficacy and perceived vulnerability positively influence ISSP behavioral compliance intentions of employees. Data did not support perceived

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Hearth and Rao (2009)	Protection-motivation theory, deterrence theory, and organizational behavior	Survey responses of 312 employees from 78 organizations.	IS, sociology	Subjective norm, descriptive norm; Construct reliability, convergent validity, and discriminant validity	severity and response cost as being predictors of ISSP behavior compliance intentions. Develop an Integrated Protection Motivation and Deterrence model of security policy compliance under the umbrella of Taylor-Todd's Decomposed Theory of Planned Behavior; evaluated the effect of organizational commitment on employee security compliance intentions
Kraemer, Carayon, and Clem (2009)		(2) 5member group focus group sessions	IS	External influences, human error, management, organization, performance and resource management, policy issues, technology, and training.	Focus group participants identified 66 human and organizational factors (21) factors in group 1 and group (2) 50 pathways
Lee, Lee, and Yoo (2004)	Social control theory (SCT)	Pilot study, the survey questionnaires were distributed to 500 computer users who were MBA students, most with full time jobs, at five universities all located in Kore	IS, sociology	Organizational trust -attachment, commitment, involvement	The results show that deterrence factors influence SDI and organizational factors significantly affect ICI and ICI decreases insiders' abuse. Interestingly, SDI negatively affects both insiders' and invaders' abuses
Rivis and Sheeran (2003)	Theory of Planned Behavior	335 UK students survey concerning their "views about aspects of students' lifestyles; Two weeks later 225	Psychology	Descriptive norms, subjective norms attitudes	Findings supported the utility of the TPB, descriptive norms, prototype similarity, and past behavior in predicting intentions and behavior. Importantly, prototype

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Stanton	Reaction formation	participants completed a second questionnaire where they reported their exercise behavior Survey of 298 workers and managers who routinely used IT on the job	Sociotechnical approach to information security	Job attitude, organizational commitment	similarity was directly associated with behavior, both on its own and through its relationship with descriptive norms, even after controlling for the TPB and past behavior Results show organizational commitment successfully predicted seven out of nine of the common behaviors, but only three out of nine unique behavior
Veenstra, Lindenbergh, Tinga, and Ormel (2010)	Goal-framing theory, social control, cognitive psychology	2000 boys and girls and combined information from pre-adolescence and early adolescenc	Psychology	Attachment, truancy	Findings show that children from disadvantaged social backgrounds (in particular family breakup) and with inadequate social bonds (lack of attachment to parents and teachers
Venkatesh, Morris, Davis, and Davis (2003)	Theory of planned behavior, Social cognitive theory, theory of reasoned action	N/A	IS, psychology. Sociology	N/A	The present work advances individual acceptance research by unifying the theoretical perspectives.

Appendix F

Summary of Prior Research on Social Pressures

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
Venkatesh, Morris, Davis, and Davis (2003)	Theory of planned behavior, Social cognitive theory, theory of reasoned action	N/A	IS, psychology. Sociology	N/A	The present work advances individual acceptance research by unifying the theoretical perspectives common in the literature
Chen, Li, Li, Holm, and, Zhai (2013)	Social control and deterrence theory	Survey data of 185 employees	IS, sociology	Social bonds, social pressures, perceived sanctions	Formal and informal and informal controls have significant effect on employee's ISSP violation intentions. Social bonds have mixed impacts on employee's intentions. Subjective norms and co-worker's behavior have significantly influence employees ISSP intention
Hearth and Rao (2009)	Protection-motivation theory, deterrence theory, and organizational behavior	Survey responses of 312 employees from 78 organizations.	IS, sociology	Subjective norm, descriptive norm; Construct reliability, convergent validity, and discriminant validity	Develop an Integrated Protection Motivation and Deterrence model of security policy compliance under the umbrella of Taylor-Todd's Decomposed Theory of Planned Behavior; evaluated the effect of organizational commitment on employee security compliance intentions
Rivis and Sheeran (2003)	Theory of Planned Behavior	335 UK students survey on their "views	Psychology	Descriptive norms, subjective	Findings supported the utility of the TPB, descriptive norms, prototype similarity, and

Original Source	Theory	Sample	Field	Instrument or Main Constructs	Main Findings or Contribution
		about aspects of students' lifestyles; 2 weeks later 225 participants completed a second questionnaire on their exercise behavior		norms attitudes	past behavior in predicting intentions and behavior. Importantly, prototype similarity was directly associated with behavior, both on its own and through its relationship with descriptive norms, even after controlling for the TPB and past behavior
Myry, Siponen, Pahlila, Vartiainen, and Vance (2009)	Theory of Cognitive Moral Development by Kohlberg and the Theory of Motivational Types of Values by Schwartz	Survey of two subsamples sets	Social psychology	Preconventional reasoning, Conventional reasoning, Postconventional reasoning, openness to change, Conservation Hypothetical compliance, Actual compliance	Empirical findings suggest that pre-conventional moral reasoning is positively related to both hypothetical and actual compliance in the given IS context
Merhi and Ahluwalia (2019)	Theory of reasoned action	Data were collected from 133 employees of 10 organizations spanning four industries and the hypotheses were tested and validated using PLS-SEM	IS, Criminology	Descriptive, moral, certainty, resistance, severity	Provided research on real-world situations in which compliance of ISS policies are often mandatory, enforced by technology

Appendix G

NSU Consent to be in a Research Study



Orientation and Social Influences Matter: An Expansion of Neutralization Model

This person doing this study is Frank King with College of Engineering and Computing, Nova Southeastern University. They will be helped by Dr. Souren Paul. You are being asked to take part in this research study because you are associated in one of the following industries: Academia, Corporate, or Information technology professionals.

The purpose of this study is to find a better understanding of employee's cognitive rationalization when making decisions from both a business and an ethical orientation. Employees are seen as the number one threat to an organization's security, and as a result, employees fall into neutralization techniques and commit information security policy violations. This research will provide an explanation to employee's cognitive thinking that enable them to make either business or ethical decisions to accept neutralization techniques and ultimately commit information security violations. As a result, this research will help practitioners, information security managers, and information security scholars in writing information security policy which may aid in reducing violations and ultimately protect sensitive data.

If you are willing to participate and you are 18 years of age and older, this will be a one-time, anonymous survey. The survey will take approximately 12 minutes to complete. Responses to this survey are completely anonymous and no personal identifiable information (PII) will be collected.

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life. You can decide not to participate in this research, and it will not be held against you. You can exit the survey at any time. Participation in this study is totally voluntary.

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Participation of this survey is anonymous and not personal identifiable (PII) will be collected. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any granting agencies (if applicable). All confidential data will be kept securely. Data will be kept with a secure cloud service provider and all data will be kept for 36 months from the end of the study. All records must be kept for a minimum of

36 months. After that time, all data will be erased and permanently deleted and destroyed. I will clear all data collected from databases and ensure that all backup copies are also deleted and destroyed.

If you have questions, you can contact Frank King at XXX-XXX-XXXX Monday thru Friday from 9am – 6pm EST or via e-mail fk145@mynsu.nova.edu

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

If you have read the above information and voluntarily wish to participate in this research study, you may access the survey by clicking on the link below:

https://www.surveymonkey.com/r/infosec_policy_violations

Appendix H

Survey Questionnaire

Participant Letter for Anonymous Surveys

Nova Southeastern University Consent to be in a Research Study Entitled

Orientation and Social Influences Matter: An Expansion of Neutralization Model

The person doing this study is Frank King with the College of Engineering and Computing, Nova Southeastern University under the guidance of Dr. Souren Paul.

You are being asked to take part in this research study because you are associated in one of the following industries: Academia, Corporate, or Information Technology Professionals.

The purpose of this study is to find a better understanding of employee's cognitive rationalization when making decisions from both a business and ethical orientation. Employees are seen as the number one threat to an organization's security, and as a result, employees fall into neutralization techniques and commit information security policy violations. This research will provide an explanation to employee's cognitive thinking that enable them to make either business or ethical decisions to accept neutralization techniques and ultimately commit information security violations. As a result, this research will help practitioners, information security managers, and information security scholars in writing information security policy which may aid in reducing violations and ultimately protect sensitive data.

If you are willing to participate and you are 18 years of age and older, this will be a one-time, anonymous survey. The survey will take approximately 12 minutes to complete. Responses to this survey are completely anonymous and no personal identifiable information (PII) will be collected.

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

You can decide not to participate in this research, and it will not be held against you. You can exit the survey at any time. Participation in this study is completely voluntary.

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. This data will be available to the researcher, the Institutional Review Board (IRB) and other representatives of this institution, and any granting agencies (if applicable). All confidential data will be kept securely. Data will be kept with a secure cloud service provider and all data will be kept for 36 months from the end of the study. All records must be kept for a minimum of 36 months. After that time, all data will be erased and permanently deleted and destroyed. All data collected will be cleared from databases and all backup copies will be deleted and destroyed.

If you have questions, you can contact Frank King at 202-841-6195 Monday thru Friday from 9am – 6pm EST or via e-mail fk145@mynsu.nova.edu

If you have questions about the study but want to talk to someone else who is not a part of the study, you can

call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

If you have read the above information and voluntarily wish to participate in this research study, you may proceed to the survey below:

--

*

In our organization our commitment to serving customer needs is closely monitored

[illegible]

* In our organization it is important that customer satisfaction is frequently assessed

[illegible]

* In our organization we achieve rapid response to competitive actions

[illegible]

* In our organization business functions are integrated to serve market needs

[illegible]

* A person should make certain that their actions never intentionally harm another even to a small degree

[illegible]

* *Hypothetical Scenario 2*

Hannu is a low-level manager in a small company where he was recently hired. His company has a strong policy that each computer workstation must be password-protected and that passwords are not to be shared. However, Hannu is on a business trip and one of his co-workers needs a file on his computer. Hannu expects that sharing his password could save his company a lot of time. He also knows that the firm has mandatory information security training. Hannu shares his password with his co-worker.

What is the likelihood you would do as Hannu

[illegible]

*

It is OK to violate the organizational information security policy to get the job done

[illegible]

* It is ok to violate the organizational information security policy under circumstances where it seems like you have little to no choice

[illegible]

* It is ok to violate organizational information security policy when you are in a hurry

[illegible]

* I feel my general adherence to organization information security policy compensates for occasionally violating information security policy

[illegible]

* I feel my hard work compensates for occasionally violating information security policy

[illegible]

* It is not wrong to violate information security policy that is unreasonable

	Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
N6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* It is not wrong to violate information security policy that requires too much time to comply

	Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
N7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* It is ok to violate information security policy if it does not harm the organization

	Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
N8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* It is ok to violate information security policy if no one gets hurt

	Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
N9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* It is OK to violate the organization's information security policy if you are not aware of what it is

	Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
N10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* It is ok to violate the organization's information security policy if it is not advertised

	Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
N11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Demographic Information

Which principal industry best describe your organization or work profession?

☐ Information Technology Professional

☐ Corporate organization

☐ Academic Institution

* What are the approximate total number of employees for your organization

- ☐ 1 - 49
- ☐ 50 - 999
- ☐ 1,000 - 4,999
- ☐ 5,000 - More

* Gender

- ☐ Male
- ☐ Female

Appendix I

IRB Approval



NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Frank King**
From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board
Date: **November 19, 2019**
Re: **IRB #: 2019-541; Title, "Orientation and Social Influences Matters"**

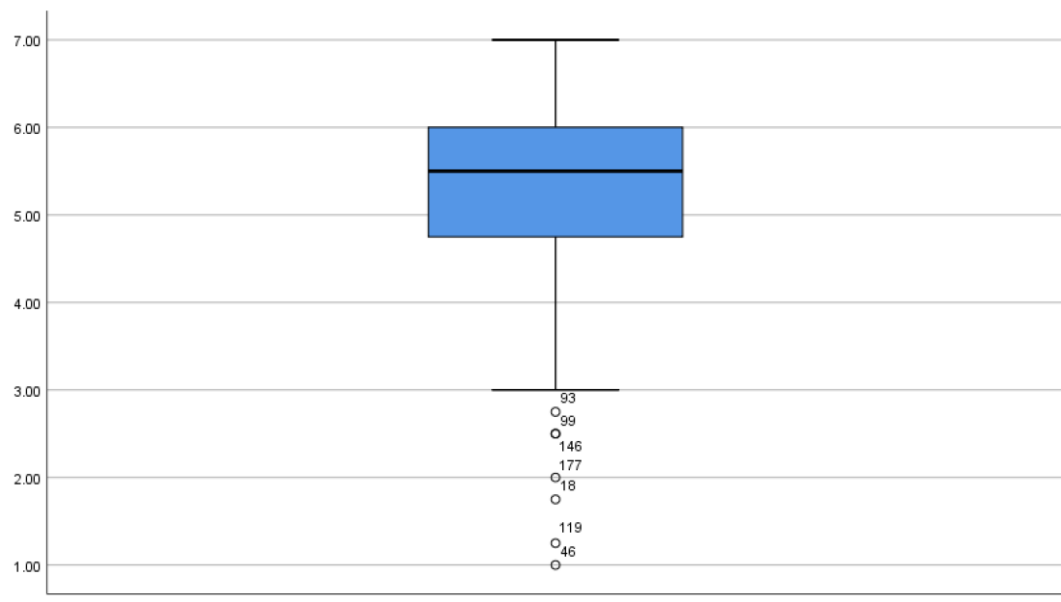
I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

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

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

Cc: **Souren Paul, Ling Wang, Ph.D.**

Appendix K
Stem & Leaf, Q-Q Plots, Histogram



Business_Ave_Score Stem-and-Leaf Plot

Frequency	Stem &	Leaf
7.00 Extremes (=<2.8)		
1.00	3 .	0
14.00	3 .	555557777777777
12.00	4 .	022222222222
30.00	4 .	555555555555555777777777777777777
34.00	5 .	000000000000000000000000022222222222222
33.00	5 .	55555555555555555555577777777777777
40.00	6 .	00000000000000000000000000000000022222222222222
16.00	6 .	555555555577777
19.00	7 .	00000000000000000000
Stem width: 1.00		
Each leaf: 1 case(s)		

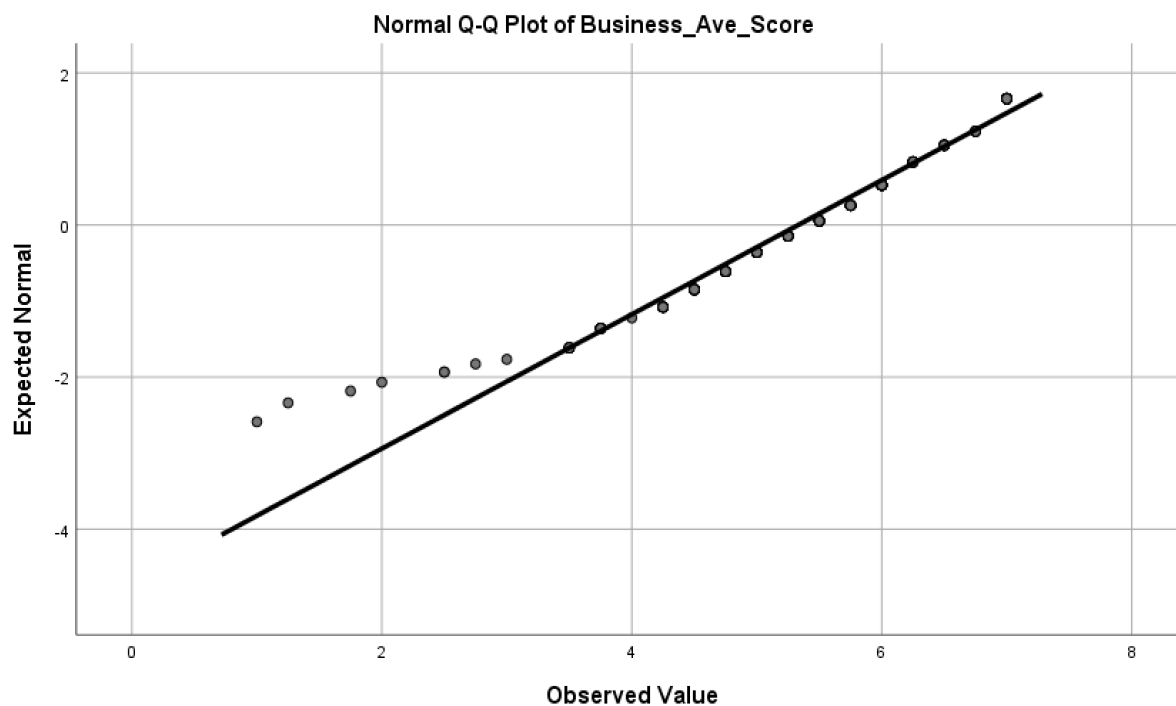
Descriptives

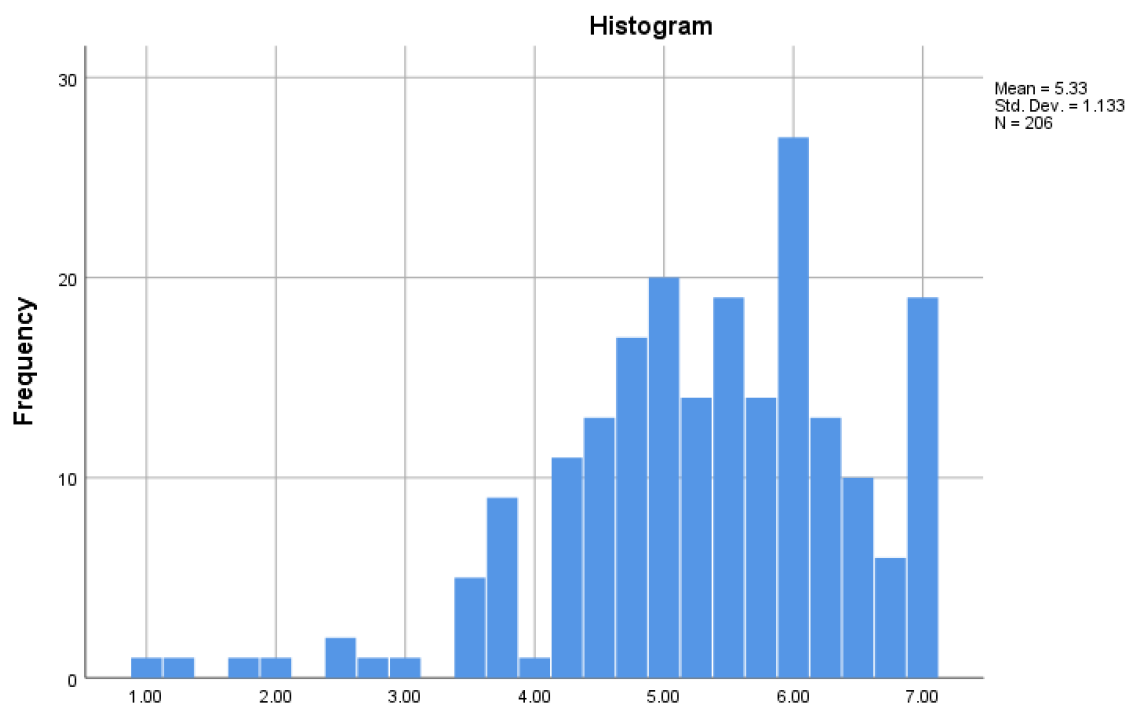
			Statistic	Std. Error
Business_Ave_Score	Mean		5.3313	.07893
	95% Confidence Interval for Mean	Lower Bound	5.1757	
		Upper Bound	5.4869	
	5% Trimmed Mean		5.4010	
	Median		5.5000	
	Variance		1.283	
	Std. Deviation		1.13283	
	Minimum		1.00	
	Maximum		7.00	
	Range		6.00	
	Interquartile Range		1.25	
	Skewness		-.884	.169
	Kurtosis		1.421	.337

Tests of Normality

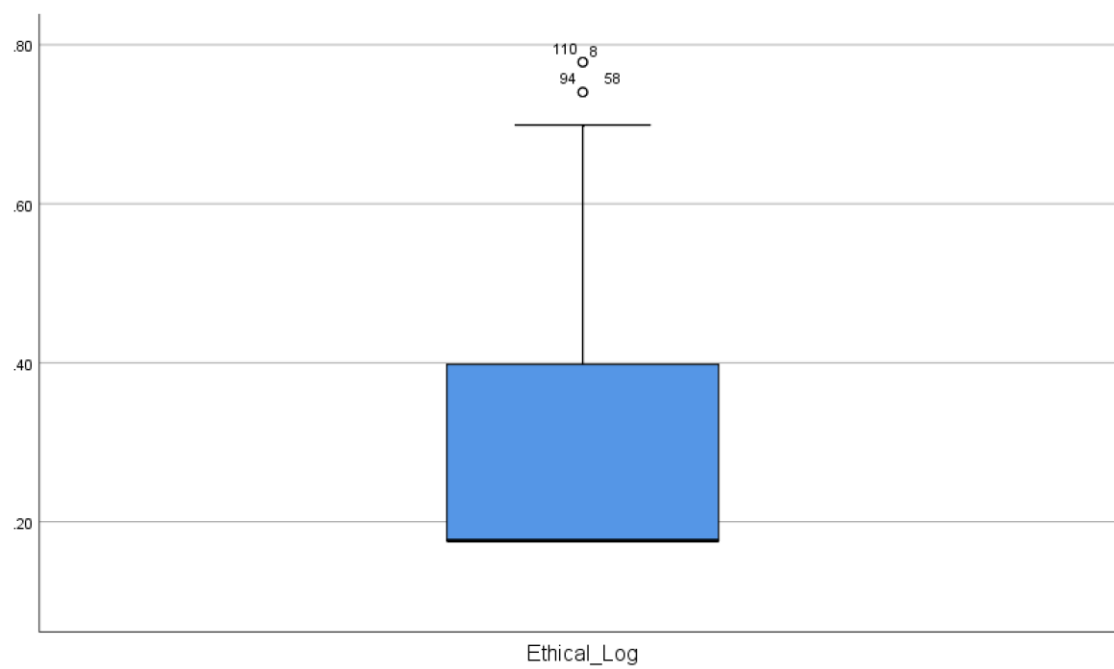
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Business_Ave_Score	.087	206	.001	.944	206	.000

a. Lilliefors Significance Correction





Ethical Orientation Stem & Leaf, Q-Q Plots, Histogram



Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Ethical_Log	206	100.0%	0	0.0%	206	100.0%

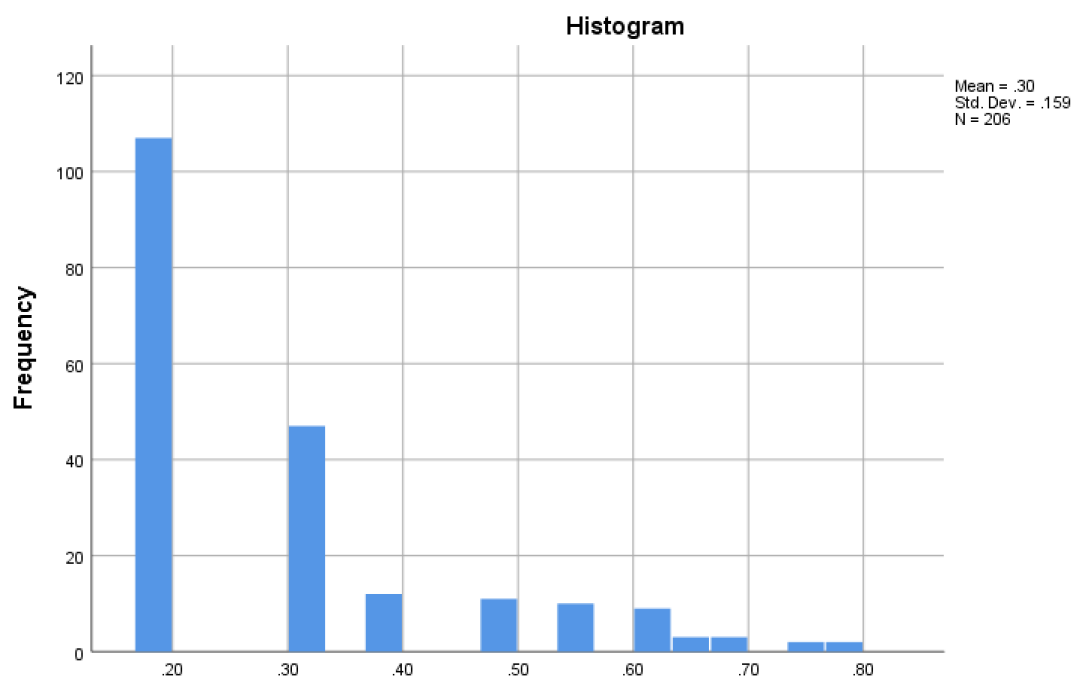
Descriptives

		Statistic	Std. Error
Ethical_Log	Mean	.2960	.01111
	95% Confidence Interval for Mean	Lower Bound	.2740
		Upper Bound	.3179
	5% Trimmed Mean	.2798	
	Median	.1761	
	Variance	.025	
	Std. Deviation	.15947	
	Minimum	.18	
	Maximum	.78	
	Range	.60	
	Interquartile Range	.22	
	Skewness	1.260	.169
	Kurtosis	.577	.337

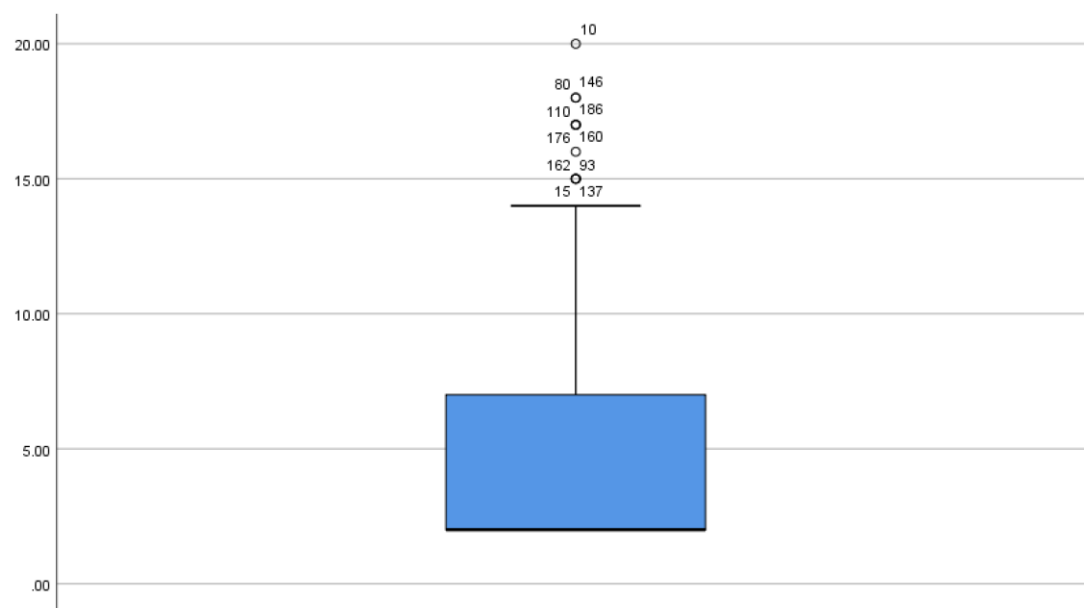
Tests of Normality

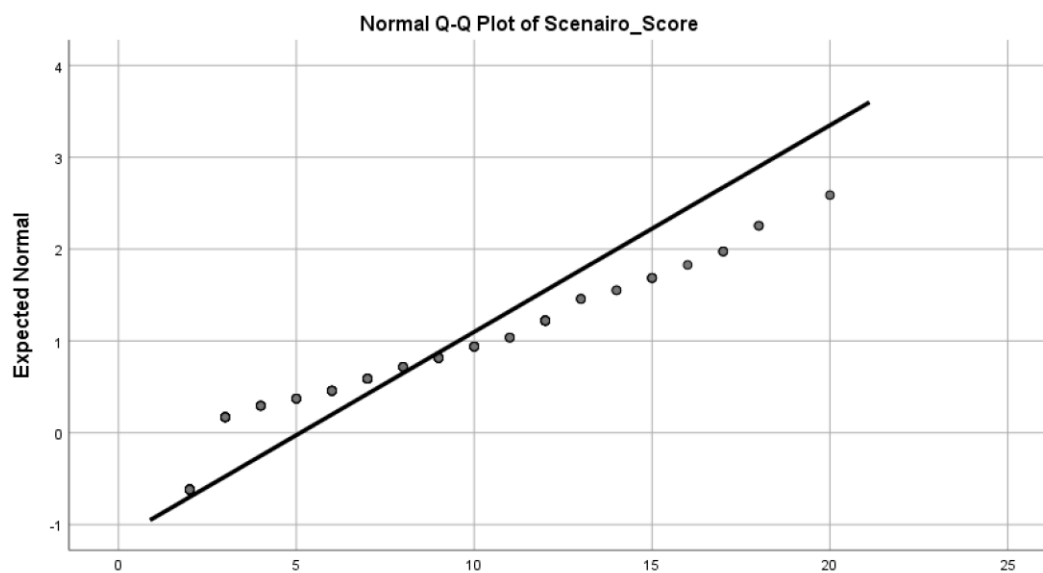
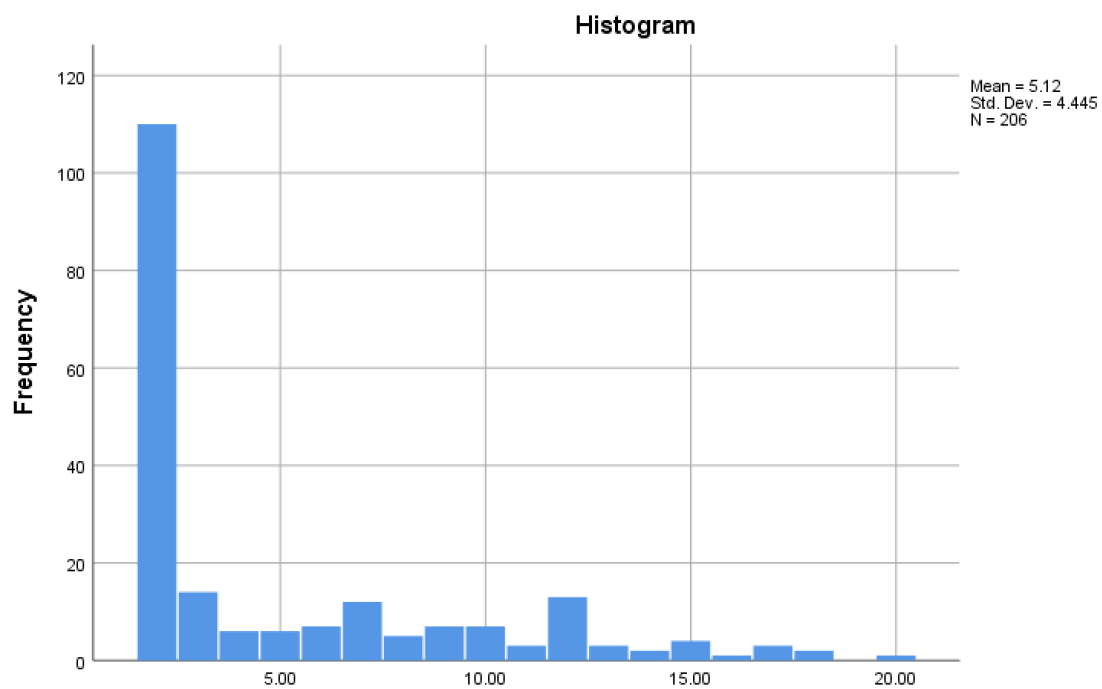
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Ethical_Log	.293	206	.000	.759	206	.000

a. Lilliefors Significance Correction



Scenarios Stem & Leaf, Q-Q Plots, Histogram





Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Neutralization_Ave_Score	206	100.0%	0	0.0%	206	100.0%

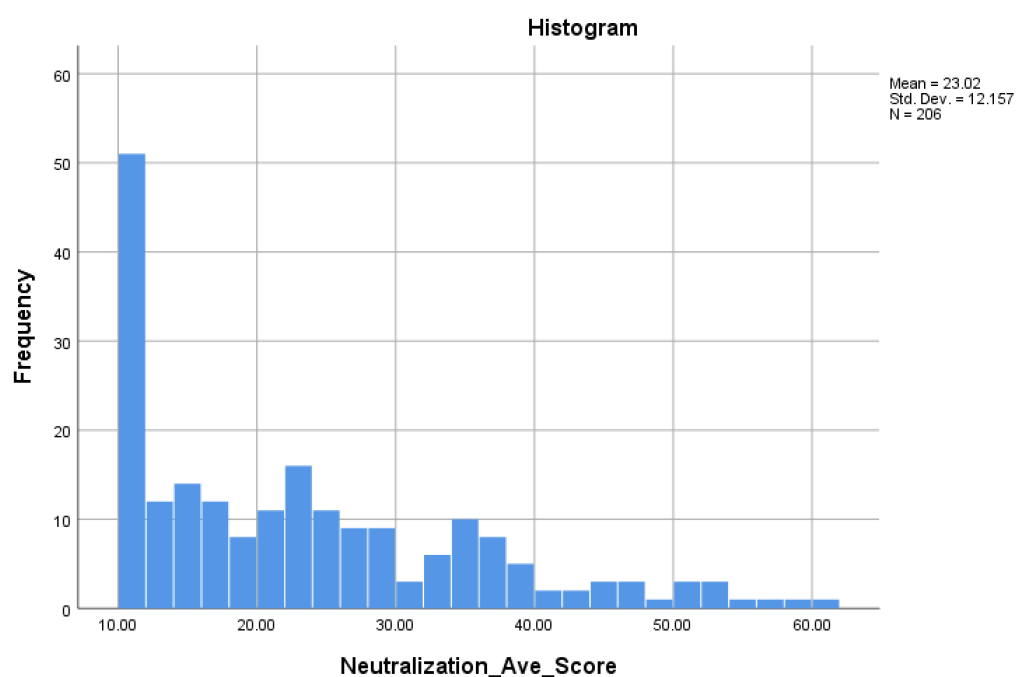
Descriptives

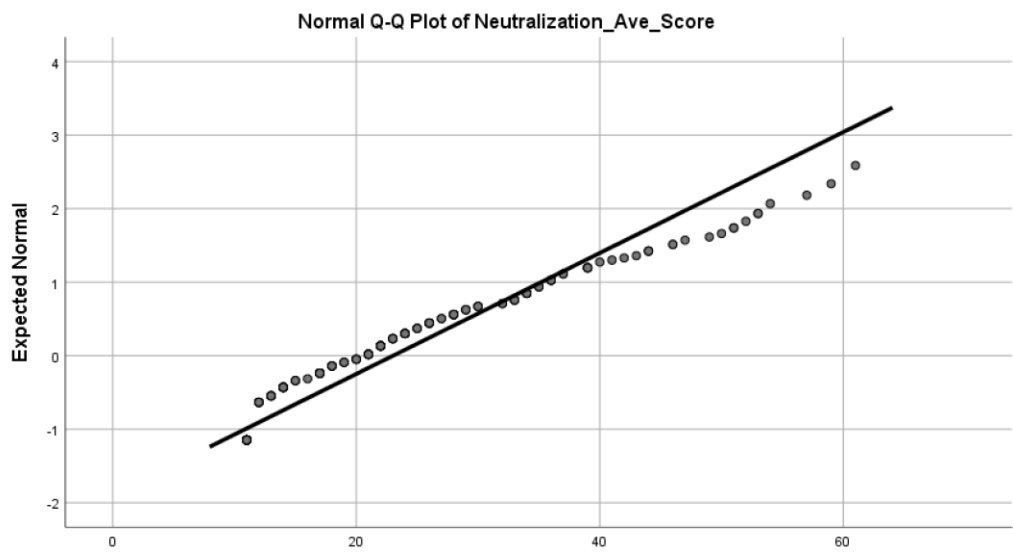
			Statistic	Std. Error
Neutralization_Ave_Score	Mean		23.0243	.84704
	95% Confidence Interval for Mean	Lower Bound	21.3542	
		Upper Bound	24.6943	
	5% Trimmed Mean		21.9741	
	Median		21.0000	
	Variance		147.799	
	Std. Deviation		12.15728	
	Minimum		11.00	
	Maximum		61.00	
	Range		50.00	
	Interquartile Range		18.25	
	Skewness		1.003	.169
	Kurtosis		.315	.337

Tests of Normality

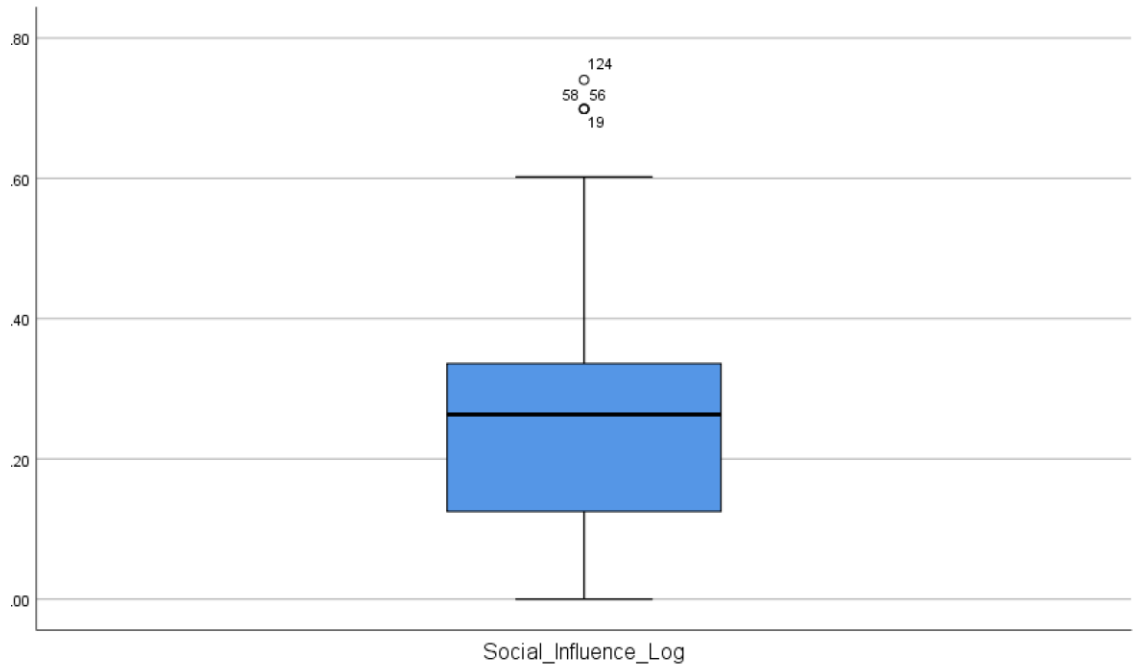
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Neutralization_Ave_Score	.161	206	.000	.877	206	.000

a. Lilliefors Significance Correction





Social Influences Stem & Leaf, Q-Q Plots, Histogram



Social_Influence_Log Stem-and-Leaf Plot

Frequency	Stem &	Leaf
30.00	0 .	000000000000000000000000000000
17.00	0 .	666666666666666666
22.00	1 .	22222222222222222222
12.00	1 .	777777777777
19.00	2 .	2222222222222222222
20.00	2 .	66666666666666666666
36.00	3 .	00000000000000000000003333333333333333
18.00	3 .	66666666666699999999
5.00	4 .	22222
7.00	4 .	5555777
12.00	5 .	000000222444
1.00	5 .	8
3.00	6 .	000
4.00	Extremes	(>=.70)

Stem width: .10

Each leaf: 1 case(s)

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Social_Influence_Log	206	100.0%	0	0.0%	206	100.0%

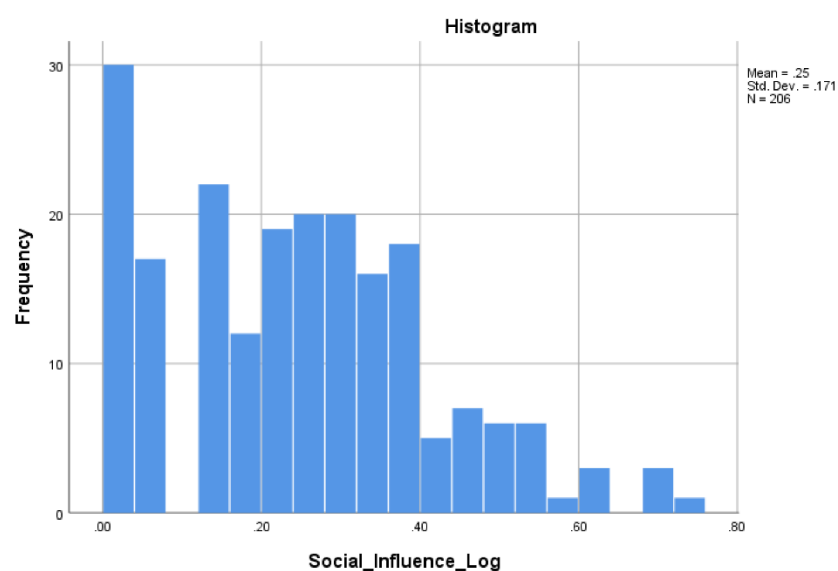
Descriptives

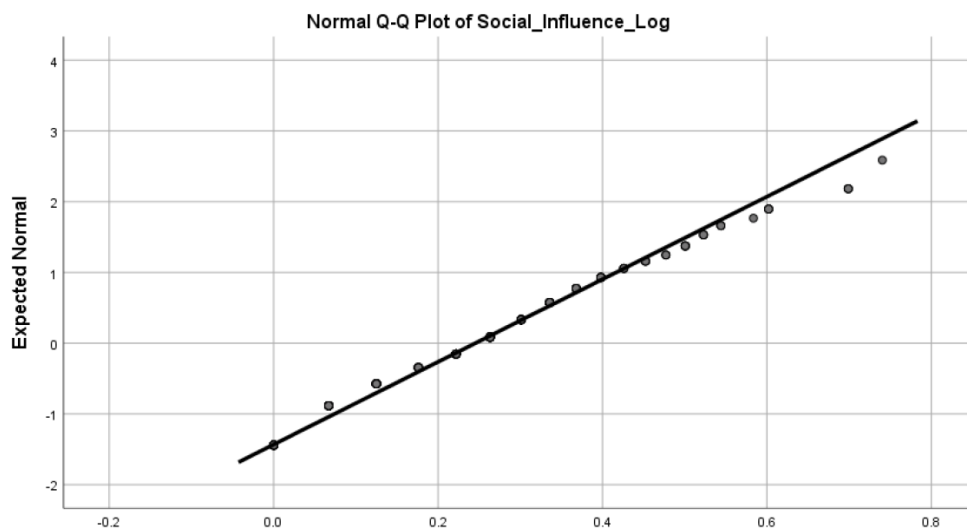
		Statistic	Std. Error
Social_Influence_Log	Mean	.2453	.01193
	95% Confidence Interval for Mean	Lower Bound	.2218
		Upper Bound	.2689
	5% Trimmed Mean	.2376	
	Median	.2632	
	Variance	.029	
	Std. Deviation	.17127	
	Minimum	.00	
	Maximum	.74	
	Range	.74	
	Interquartile Range	.21	
	Skewness	.395	.169
	Kurtosis	-.266	.337

Tests of Normality

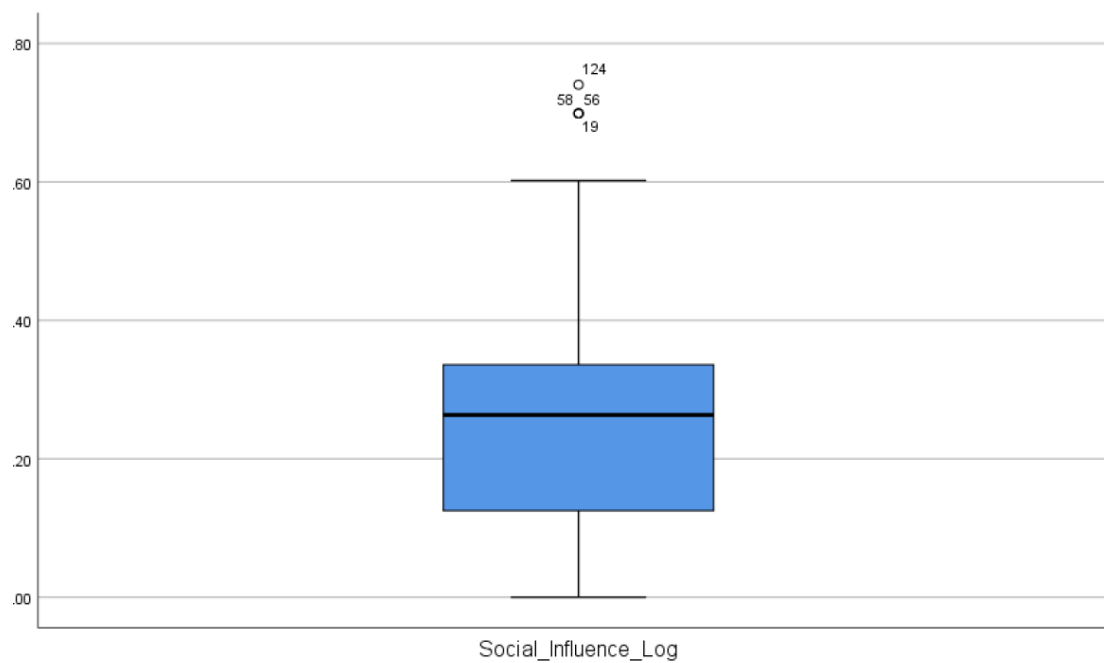
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Social_Influence_Log	.094	206	.000	.958	206	.000

a. Lilliefors Significance Correction





Social Pressures Stem & Leaf, Q-Q Plots, Histogram



Social_Influence_Log Stem-and-Leaf Plot

```

Frequency      Stem & Leaf

    30.00      0 .  000000000000000000000000000000
    17.00      0 .  6666666666666666
    22.00      1 .  22222222222222222222
    12.00      1 .  777777777777
    19.00      2 .  2222222222222222
    20.00      2 .  666666666666666666
    36.00      3 .  00000000000000000003333333333333
    18.00      3 .  666666666699999999
     5.00      4 .  22222
     7.00      4 .  5555777
    12.00      5 .  000000222444
     1.00      5 .  8
     3.00      6 .  000
     4.00 Extremes      (>=.70)

```

Stem width: .10
Each leaf: 1 case(s)

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Social_Influence_Log	206	100.0%	0	0.0%	206	100.0%

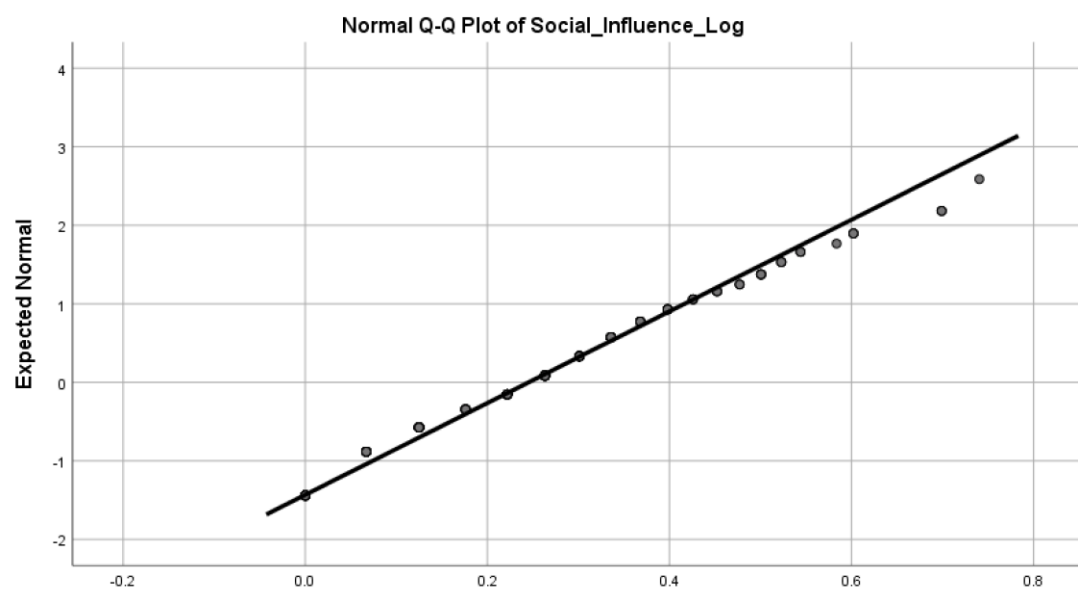
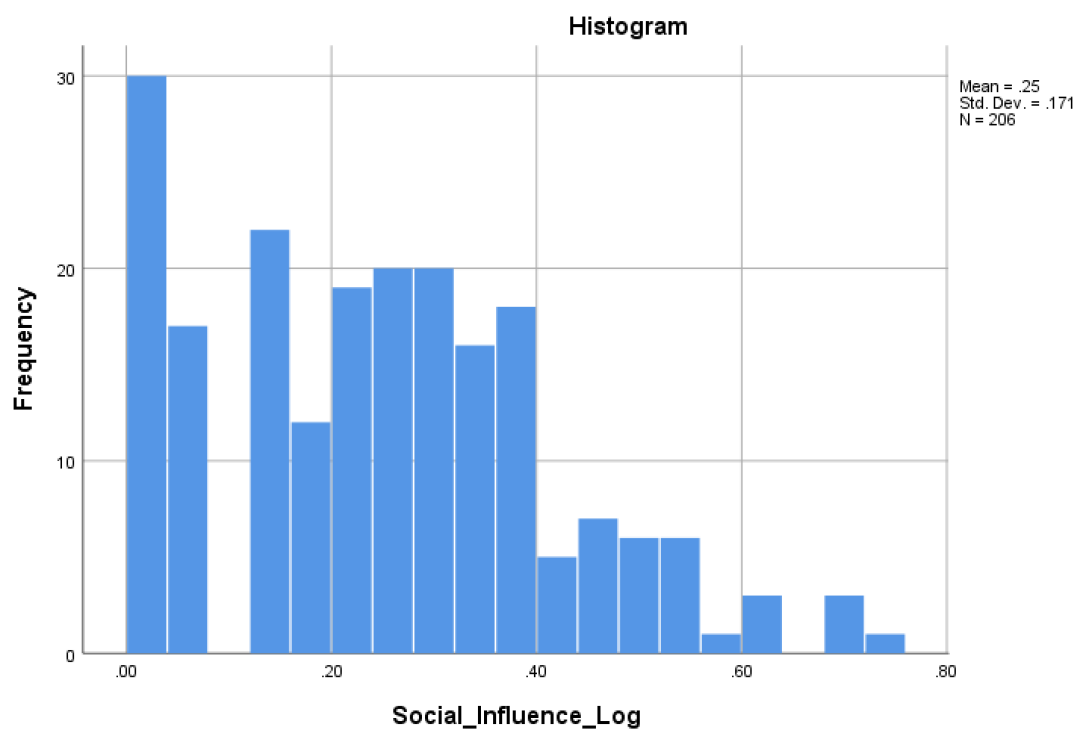
Descriptives

		Statistic	Std. Error
Social_Influence_Log	Mean	.2453	.01193
	95% Confidence Interval for Mean	Lower Bound	.2218
		Upper Bound	.2689
	5% Trimmed Mean	.2376	
	Median	.2632	
	Variance	.029	
	Std. Deviation	.17127	
	Minimum	.00	
	Maximum	.74	
	Range	.74	
	Interquartile Range	.21	
	Skewness	.395	.169
	Kurtosis	-.266	.337

Tests of Normality

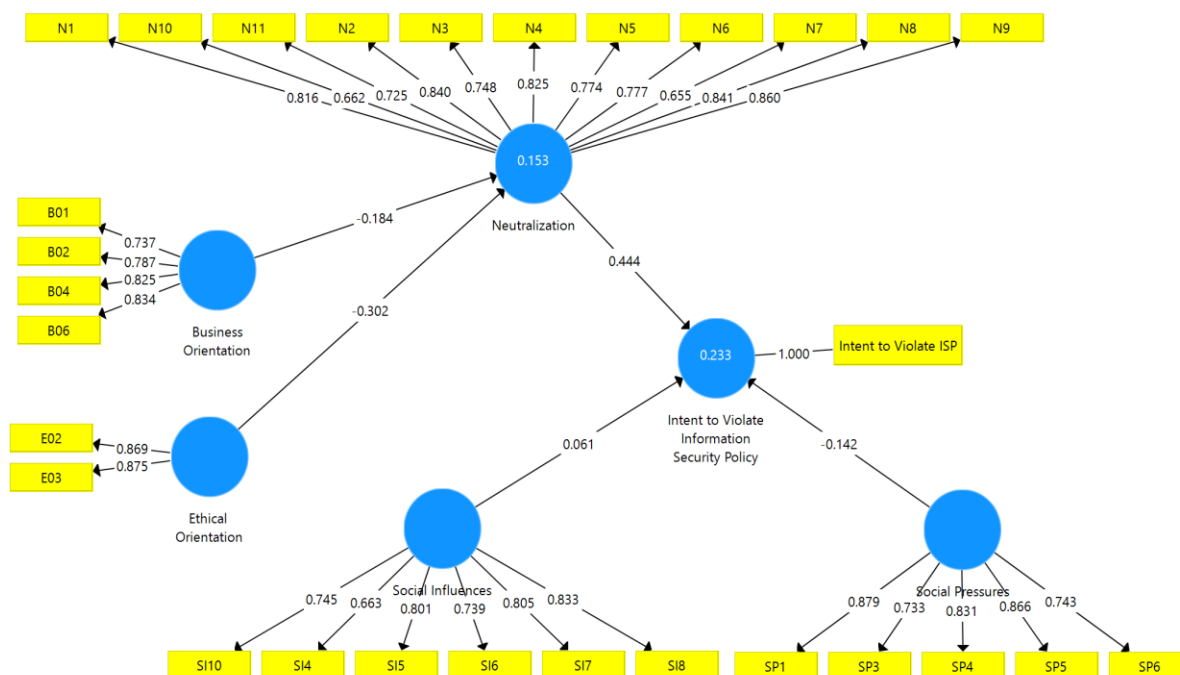
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Social_Influence_Log	.094	206	.000	.958	206	.000

a. Lilliefors Significance Correction



Appendix L

PLS Analysis, Model Fit, Reliability, Validity, Coefficient and Outer loading



Model_Fit

	Fit Summary	rms Theta	
		Saturated Model	Estimated Model
SRMR		0.072	0.091
d_ULS		2.255	3.573
d_G		1.166	1.181
Chi-Square		1233.295	1244.898
NFI		0.692	0.689

Construct Reliability and Validity

Matrix	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
	Cronbach's Alpha	rho_A	Composite Relia...	Average Variance Extracted (AVE)
Business Orient...	0.815	0.837	0.874	0.635
Ethical _Orientat...	0.684	0.685	0.864	0.760
Intent to Violate...	1.000	1.000	1.000	1.000
Neutralization	0.934	0.943	0.944	0.605
Social Influences	0.861	0.888	0.895	0.587
Social Pressures	0.873	0.906	0.906	0.661

Discriminant Validity

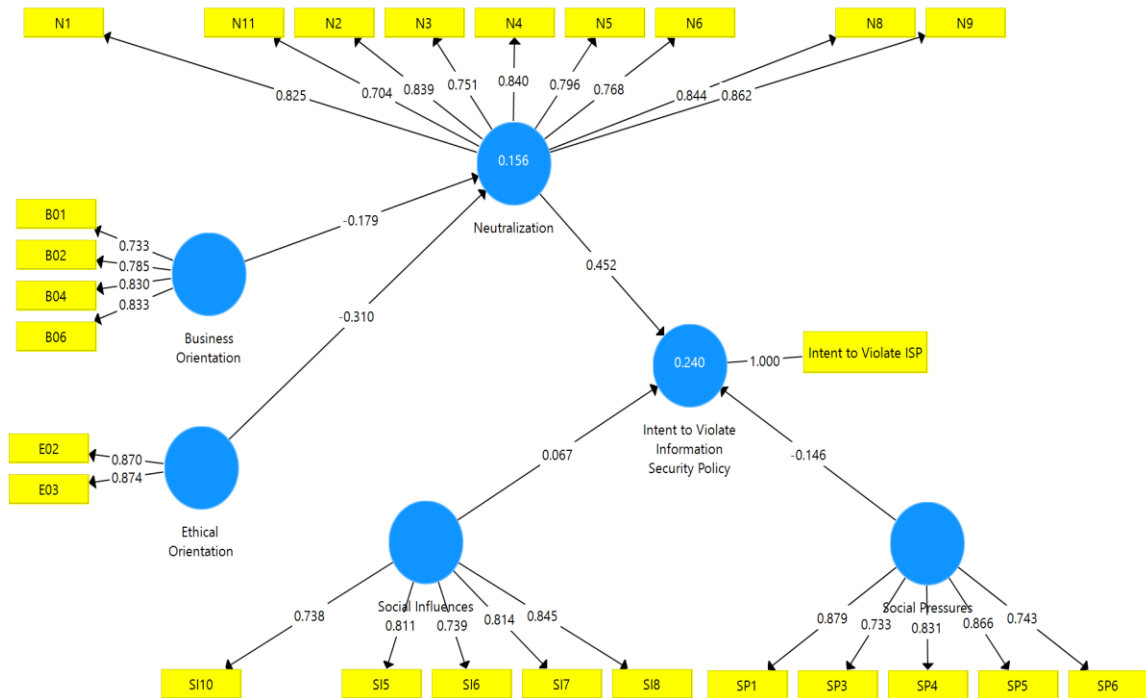
	Business Orient...	Ethical _Orientat...	Intent to Violate...	Neutralization	Social Influences	Social Pressures
Business Orient...	0.797					
Ethical _Orientat...	0.253	0.872				
Intent to Violate...	-0.123	-0.192	1.000			
Neutralization	-0.260	-0.348	0.467	0.778		
Social Influences	0.308	0.359	-0.170	-0.368	0.766	
Social Pressures	0.492	0.310	-0.255	-0.318	0.475	0.813

Outer Loadings

	Business Orient...	Ethical _Orientat...	Intent to Violate...	Neutralization	Social Influences	Social Pressures
B01	0.737					
B02	0.787					
B04	0.825					
B06	0.834					
E02		0.869				
E03		0.875				
N1				0.817		
N10				0.659		
N11				0.724		
N2				0.839		
N3				0.750		
N4				0.824		
N5				0.773		
N6				0.777		
N7				0.657		
N8				0.842		
N9				0.860		
SI10					0.745	
SI4					0.663	
SI5					0.801	
SI6					0.739	
SI7					0.805	
SI8					0.833	
SP1						0.879
SP3						0.733
SP4						0.831
SP5						0.866
SP6						0.743
Scenario1			1.000			

Appendix M

PLS Analysis After Deleting N7, N10, and SI4



Model_Fit

Fit Summary		rms Theta	
	Saturated Model	Estimated Model	
SRMR	0.069	0.088	
d_ULS	1.672	2.699	
d_G	0.905	0.920	
Chi-Square	999.746	1010.954	
NFI	0.714	0.711	

R Square

Matrix	R Square	R Square Adjusted
	R Square	R Square Adjusted
Intent to Violate...	0.240	0.228
Neutralization	0.156	0.148

Discriminant Validity

Fornell-Larcker Criterion		Cross Loadings		Heterotrait-Monotrait Ratio (HTMT)		Heterotrait-Monotrait Ratio (HTMT)	
	Business Orient...	Ethical _Orientat...	Intent to Violate...	Neutralization	Social Influences	Social Pressures	
Business Orient...	0.796						
Ethical _Orientat...	0.253	0.872					
Intent to Violate...	-0.122	-0.193	1.000				
Neutralization	-0.257	-0.355	0.473	0.805			
Social Influences	0.314	0.377	-0.173	-0.372	0.790		
Social Pressures	0.492	0.310	-0.255	-0.312	0.489	0.813	

Construct Reliability and Validity

Matrix	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
	Cronbach's Alpha	rho_A	Composite Relia...	Average Varianc...
Business Orient...	0.815	0.835	0.874	0.634
Ethical _Orientat...	0.684	0.684	0.864	0.760
Intent to Violate...	1.000	1.000	1.000	1.000
Neutralization	0.932	0.938	0.943	0.648
Social Influences	0.851	0.873	0.892	0.625
Social Pressures	0.873	0.906	0.906	0.661

Path Coefficients

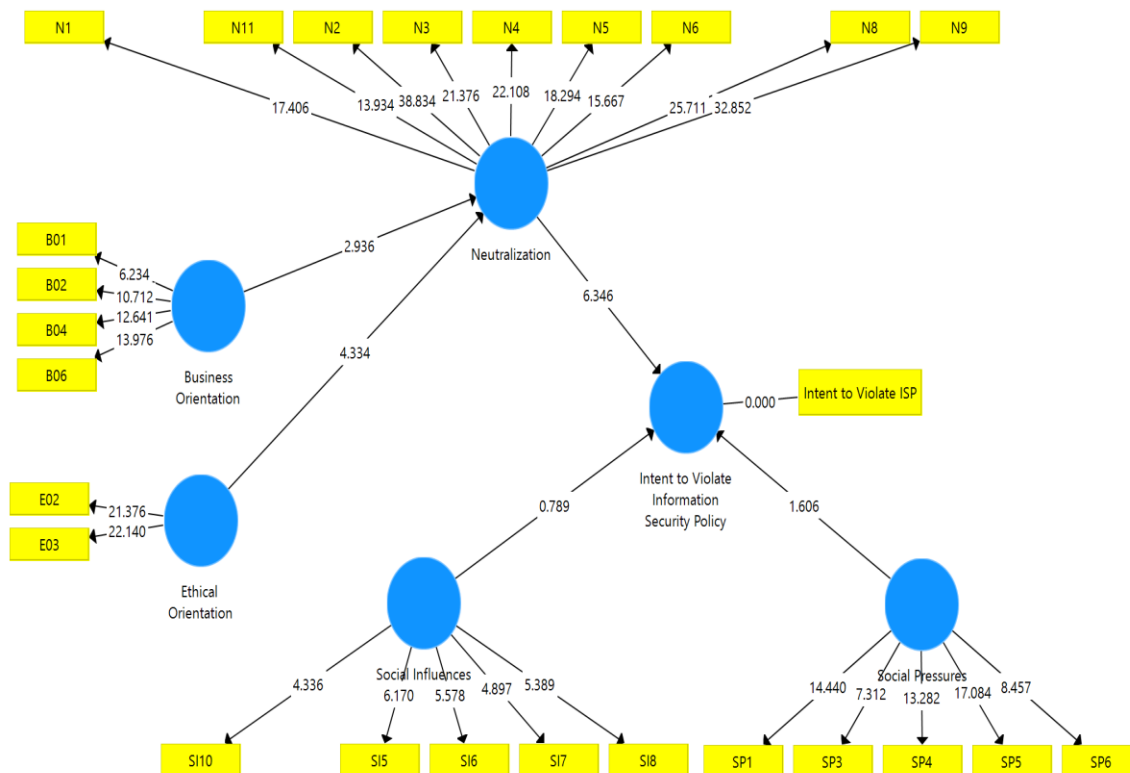
Matrix	Path Coefficients
	Business Orient... Ethical _Orientat... Intent to Violate... Neutralization Social Influences Social Pressures
Business Orient...	-0.179
Ethical _Orientat...	-0.310
Intent to Violate...	
Neutralization	0.452
Social Influences	0.067
Social Pressures	-0.146

Outer Loadings





Matrix						
	Business Orient...	Ethical _Orientat...	Intent to Violate...	Neutralization	Social Influences	Social Pressures
B01	0.733					
B02	0.785					
B04	0.830					
B06	0.833					
E02		0.870				
E03		0.873				
N1				0.825		
N11				0.704		
N2				0.839		
N3				0.752		
N4				0.839		
N5				0.796		
N6				0.768		
N8				0.844		
N9				0.863		
SI10					0.738	
SI5					0.811	
SI6					0.739	
SI7					0.814	
SI8					0.845	
SP1						0.879
SP3						0.733
SP4						0.831
SP5						0.866
SP6						0.743
Scenario1			1.000			

Appendix N

PLS Analysis with Bootstrapping



Total Effects

 Mean, STDEV, T-Values, P-Values	 Confidence Intervals	 Confidence Intervals Bias Corrected	 Samples		
	Original Sample...	Sample Mean (...)	Standard Deviat...	T Statistics (O/S...	P Values
Business Orient...	-0.081	-0.081	0.027	2.940	0.003
Business Orient...	-0.179	-0.186	0.061	2.907	0.004
Ethical _Orientat...	-0.140	-0.139	0.040	3.514	0.000
Ethical _Orientat...	-0.310	-0.316	0.075	4.144	0.000
Neutralization -...	0.452	0.440	0.072	6.248	0.000
Social Influence...	0.067	0.043	0.078	0.853	0.394
Social Pressures ...	-0.146	-0.147	0.097	1.501	0.134

Appendix O

Organizational Statistical Information

Multiple Comparisons

Dependent Variable: Business_Ave_Score

Tukey HSD

(I) Demographic InformationWhich principal industry best describe your organization or work profession?	(J) Demographic InformationWhich principal industry best describe your organization or work profession?	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Information Technology Professional	Corporate organization	-.3859	.23124	.220	-.9318	.1601
	Academic Institution	.3751	.21345	.187	-.1289	.8790
Corporate organization	Information Technology Professional	.3859	.23124	.220	-.1601	.9318
	Academic Institution	.7609*	.17197	.000	.3549	1.1670
Academic Institution	Information Technology Professional	-.3751	.21345	.187	-.8790	.1289
	Corporate organization	-.7609*	.17197	.000	-1.1670	-.3549

Based on observed means.

The error term is Mean Square(Error) = 1.181.

*. The mean difference is significant at the .05 level.

Statistics

a

Demographic InformationWhich principal industry best describe your organization or work profession?

N	Valid	206
	Missing	0
Mean		2.3641
Median		3.0000
Mode		3.00
Std. Deviation		.75124

Demographic InformationWhich principal industry best describe your organization or work profession?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Information Technology Professional	34	16.5	16.5	16.5
	Corporate organization	63	30.6	30.6	47.1
	Academic Institution	109	52.9	52.9	100.0
	Total	206	100.0	100.0	

Organizational Size Statistics

Statistics

What are the approximate total number of employees for your organization

N	Valid	206
	Missing	0
Mode		2.00
Range		3.00
Minimum		1.00
Maximum		4.00

What are the approximate total number of employees for your organization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 - 49	34	16.5	16.5	16.5
	50 - 999	77	37.4	37.4	53.9
	1,000 - 4,999	40	19.4	19.4	73.3
	5,000 - More	55	26.7	26.7	100.0
	Total	206	100.0	100.0	

Gender Statistics

Statistics

Gender

N	Valid	206
	Missing	0
Mode		1.00 ^a
Range		1.00
Minimum		1.00
Maximum		2.00

a. Multiple modes exist.
The smallest value
is shown

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	103	50.0	50.0	50.0
	Female	103	50.0	50.0	100.0
	Total	206	100.0	100.0	

Appendix P

Reliability and Validity

Pilot Study Ethical Orientation

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.807	.809	2

Item Statistics

	Mean	Std. Deviation	N
EO2	6.3750	1.05460	40
EO3	5.6250	.95239	40

Final Data Collection Ethical Orientation

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.677	.684	2

Item Statistics

	Mean	Std. Deviation	N
EO2	6.3398	1.02223	206
EO3	5.3883	1.22759	206

Neutralization

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.930	.934	11

Business Orientation

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.814	.815	4

Item Statistics

	Mean	Std. Deviation	N
BO1	5.5631	1.41539	206
BO2	5.8010	1.31935	206
BO4	4.8786	1.44824	206
BO6	5.0825	1.46770	206

Social Influences**Reliability Statistics**

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.857	.861	6

Item Statistics

	Mean	Std. Deviation	N
SI4	6.0971	1.09557	206
SI5	6.1408	.89147	206
SI6	6.0825	.93077	206
SI7	6.0097	1.23758	206
SI8	5.8981	1.24324	206
SI10	6.3252	1.08921	206

Social Pressures**Reliability Statistics**

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.859	.873	5

Item Statistics

	Mean	Std. Deviation	N
SP1	6.5485	.78714	206
SP3	6.1117	1.21461	206
SP4	6.4709	.89259	206
SP5	6.3932	.88110	206
SP6	5.8010	1.21543	206

Appendix Q

Discriminant Validity of Constructs

	Business Orient...	Ethical _Orientat...	Intent to Violate...	Neutralization	Social Influences	Social Pressures
Business Orient...	0.797					
Ethical _Orientat...	0.253	0.872				
Intent to Violate...	-0.184	-0.200	0.848			
Neutralization	-0.259	-0.345	0.590	0.778		
Social Influences	0.315	0.365	-0.198	-0.369	0.763	
Social Pressures	0.496	0.317	-0.224	-0.314	0.475	0.815

Discriminant Validity of Business Orientation and Ethical Orientation

Correlation Matrix^a

		BO1	BO2	BO4	BO6	EO2	EO3
Correlation	BO1	1.000	.643	.476	.485	.140	.171
	BO2	.643	1.000	.477	.437	.166	.196
	BO4	.476	.477	1.000	.624	.133	.235
	BO6	.485	.437	.624	1.000	.163	.193
	EO2	.140	.166	.133	.163	1.000	.520
	EO3	.171	.196	.235	.193	.520	1.000
Sig. (1-tailed)	BO1		.000	.000	.000	.022	.007
	BO2	.000		.000	.000	.009	.002
	BO4	.000	.000		.000	.028	.000
	BO6	.000	.000	.000		.010	.003
	EO2	.022	.009	.028	.010		.000
	EO3	.007	.002	.000	.003	.000	

a. Determinant = .161

Discriminant validity of Business Orientation and Social Influences

		B01	B02	B04	B06	SI4	SI5	SI6	SI7	SI8	SI10
Correlation	B01	1.000	.643	.476	.485	.043	.246	.264	.261	.252	.045
	B02	.643	1.000	.477	.437	.078	.235	.256	.228	.264	.062
	B04	.476	.477	1.000	.624	.155	.153	.235	.218	.158	.130
	B06	.485	.437	.624	1.000	.156	.226	.306	.209	.178	.066
	SI4	.043	.078	.155	.156	1.000	.435	.456	.442	.441	.505
	SI5	.246	.235	.153	.226	.435	1.000	.709	.494	.554	.455
	SI6	.264	.256	.235	.306	.456	.709	1.000	.393	.450	.488
	SI7	.261	.228	.218	.209	.442	.494	.393	1.000	.692	.475
	SI8	.252	.264	.158	.178	.441	.554	.450	.692	1.000	.623
	SI10	.045	.062	.130	.066	.505	.455	.488	.475	.623	1.000
Sig. (1-tailed)	B01		.000	.000	.000	.269	.000	.000	.000	.000	.260
	B02	.000		.000	.000	.134	.000	.000	.000	.000	.187
	B04	.000	.000		.000	.013	.014	.000	.001	.012	.031
	B06	.000	.000	.000		.013	.001	.000	.001	.005	.175
	SI4	.269	.134	.013	.013		.000	.000	.000	.000	.000
	SI5	.000	.000	.014	.001	.000		.000	.000	.000	.000
	SI6	.000	.000	.000	.000	.000	.000		.000	.000	.000
	SI7	.000	.000	.001	.001	.000	.000	.000		.000	.000
	SI8	.000	.000	.012	.005	.000	.000	.000	.000		.000
	SI10	.260	.187	.031	.175	.000	.000	.000	.000	.000	

Discriminant validity of Ethical Orientation and Social Influences

		E02	E03	SI4	SI5	SI6	SI7	SI8	SI10
Correlation	E02	1.000	.520	.171	.279	.268	.337	.315	.360
	E03	.520	1.000	.023	.213	.147	.258	.205	.204
	SI4	.171	.023	1.000	.435	.456	.442	.441	.505
	SI5	.279	.213	.435	1.000	.709	.494	.554	.455
	SI6	.268	.147	.456	.709	1.000	.393	.450	.488
	SI7	.337	.258	.442	.494	.393	1.000	.692	.475
	SI8	.315	.205	.441	.554	.450	.692	1.000	.623
	SI10	.360	.204	.505	.455	.488	.475	.623	1.000
Sig. (1-tailed)	E02		.000	.007	.000	.000	.000	.000	.000
	E03	.000		.374	.001	.018	.000	.002	.002
	SI4	.007	.374		.000	.000	.000	.000	.000
	SI5	.000	.001	.000		.000	.000	.000	.000
	SI6	.000	.018	.000	.000		.000	.000	.000
	SI7	.000	.000	.000	.000	.000		.000	.000
	SI8	.000	.002	.000	.000	.000	.000		.000
	SI10	.000	.002	.000	.000	.000	.000	.000	

Discriminant validity of Ethical Orientation and Social Pressures

		E02	E03	SP1	SP3	SP4	SP5	SP6
Correlation	E02	1.000	.520	.246	.205	.284	.284	.278
	E03	.520	1.000	.112	.291	.122	.205	.274
	SP1	.246	.112	1.000	.517	.707	.686	.523
	SP3	.205	.291	.517	1.000	.464	.661	.557
	SP4	.284	.122	.707	.464	1.000	.582	.500
	SP5	.284	.205	.686	.661	.582	1.000	.602
	SP6	.278	.274	.523	.557	.500	.602	1.000
Sig. (1-tailed)	E02		.000	.000	.002	.000	.000	.000
	E03	.000		.055	.000	.041	.002	.000
	SP1	.000	.055		.000	.000	.000	.000
	SP3	.002	.000	.000		.000	.000	.000
	SP4	.000	.041	.000	.000		.000	.000
	SP5	.000	.002	.000	.000	.000		.000
	SP6	.000	.000	.000	.000	.000	.000	

Discriminant validity of Neutralization and Social Influences

		N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	SI4	SI5	SI6	SI7	SI8	SI10
Correlation	N1	1.000	.724	.660	.641	.550	.563	.531	.675	.665	.430	.512	-.095	-.255	-.243	-.292	-.233	-.190
	N2	.724	1.000	.580	.659	.543	.615	.515	.660	.655	.555	.594	-.084	-.177	-.203	-.213	-.193	-.149
	N3	.660	.580	1.000	.489	.560	.549	.549	.602	.669	.391	.373	-.269	-.160	-.202	-.242	-.291	-.285
	N4	.641	.659	.489	1.000	.793	.609	.397	.580	.608	.498	.583	-.122	-.276	-.224	-.268	-.230	-.234
	N5	.550	.543	.560	.793	1.000	.547	.334	.562	.593	.421	.483	-.197	-.333	-.269	-.285	-.291	-.333
	N6	.563	.615	.549	.609	.547	1.000	.667	.615	.628	.427	.439	-.117	-.216	-.249	-.313	-.238	-.243
	N7	.531	.515	.549	.397	.334	.667	1.000	.578	.542	.304	.386	-.081	-.186	-.196	-.299	-.272	-.183
	N8	.675	.660	.602	.580	.562	.615	.578	1.000	.905	.476	.588	-.080	-.194	-.128	-.271	-.251	-.192
	N9	.665	.655	.669	.608	.593	.628	.542	.905	1.000	.529	.595	-.120	-.222	-.180	-.239	-.226	-.204
	N10	.430	.555	.391	.498	.421	.427	.304	.476	.529	1.000	.721	-.149	-.244	-.204	-.182	-.166	-.151
	N11	.512	.594	.373	.583	.483	.439	.386	.588	.595	.721	1.000	-.118	-.291	-.237	-.211	-.196	-.159
	SI4	-.095	-.084	-.269	-.122	-.197	-.117	-.081	-.080	-.120	-.149	-.118	1.000	.435	.456	.442	.441	.505
	SI5	-.255	-.177	-.160	-.276	-.333	-.216	-.186	-.194	-.222	-.244	-.291	.435	1.000	.709	.494	.554	.455
	SI6	-.243	-.203	-.202	-.224	-.269	-.249	-.196	-.128	-.180	-.204	-.237	.456	.709	1.000	.393	.450	.488
	SI7	-.292	-.213	-.242	-.268	-.285	-.313	-.299	-.271	-.239	-.182	-.211	.442	.494	.393	1.000	.692	.475
	SI8	-.233	-.193	-.291	-.230	-.291	-.238	-.272	-.251	-.226	-.166	-.196	.441	.554	.450	.692	1.000	.623
	SI10	-.190	-.149	-.285	-.234	-.333	-.243	-.183	-.192	-.204	-.151	-.159	.505	.455	.488	.475	.623	1.000
Sig. (1-tailed)	N1		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.088	.000	.000	.000	.000	.003
	N2	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.116	.006	.002	.001	.003	.016
	N3	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.011	.002	.000	.000	.000
	N4	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.040	.000	.001	.000	.000	.000
	N5	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.002	.000	.000	.000	.000	.000
	N6	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.047	.001	.000	.000	.000	.000
	N7	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.122	.004	.002	.000	.000	.004
	N8	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.126	.003	.034	.000	.000	.003
	N9	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.043	.001	.005	.000	.001	.002
	N10	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.016	.000	.002	.004	.009	.015
	N11	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.045	.000	.000	.001	.002	.011
	SI4	.088	.116	.000	.040	.002	.047	.122	.126	.043	.016	.045		.000	.000	.000	.000	.000
	SI5	.000	.006	.011	.000	.000	.001	.004	.003	.001	.000	.000	.000		.000	.000	.000	.000
	SI6	.000	.002	.002	.001	.000	.000	.002	.034	.005	.002	.000	.000	.000		.000	.000	.000
	SI7	.000	.001	.000	.000	.000	.000	.000	.000	.000	.004	.001	.000	.000	.000		.000	.000
	SI8	.000	.003	.000	.000	.000	.000	.000	.000	.001	.009	.002	.000	.000	.000	.000		.000
	SI10	.003	.016	.000	.000	.000	.000	.004	.003	.002	.015	.011	.000	.000	.000	.000	.000	

Discriminant validity of Neutralization and Social Pressures

		N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	SP1	SP3	SP4	SP5	SP6
Correlation	N1	1.000	.724	.660	.641	.550	.563	.531	.675	.665	.430	.512	-.148	-.178	-.172	-.121	-.167
	N2	.724	1.000	.580	.659	.543	.615	.515	.660	.655	.555	.594	-.178	-.233	-.274	-.175	-.240
	N3	.660	.580	1.000	.489	.560	.549	.549	.602	.669	.391	.373	-.297	-.130	-.353	-.168	-.232
	N4	.641	.659	.489	1.000	.793	.609	.397	.580	.608	.498	.583	-.206	-.211	-.223	-.152	-.219
	N5	.550	.543	.560	.793	1.000	.547	.334	.562	.593	.421	.483	-.264	-.247	-.306	-.255	-.314
	N6	.563	.615	.549	.609	.547	1.000	.667	.615	.628	.427	.439	-.252	-.236	-.286	-.218	-.254
	N7	.531	.515	.549	.397	.334	.667	1.000	.578	.542	.304	.386	-.129	-.147	-.197	-.162	-.188
	N8	.675	.660	.602	.580	.562	.615	.578	1.000	.905	.476	.588	-.077	-.227	-.142	-.126	-.181
	N9	.665	.655	.669	.608	.593	.628	.542	.905	1.000	.529	.595	-.123	-.168	-.155	-.103	-.161
	N10	.430	.555	.391	.498	.421	.427	.304	.476	.529	1.000	.721	-.188	-.272	-.204	-.186	-.289
	N11	.512	.594	.373	.583	.483	.439	.386	.588	.595	.721	1.000	-.186	-.291	-.179	-.197	-.260
	SP1	-.148	-.178	-.297	-.206	-.264	-.252	-.129	-.077	-.123	-.188	-.186	1.000	.517	.707	.686	.523
	SP3	-.178	-.233	-.130	-.211	-.247	-.236	-.147	-.227	-.168	-.272	-.291	.517	1.000	.464	.661	.557
	SP4	-.172	-.274	-.353	-.223	-.306	-.286	-.197	-.142	-.155	-.204	-.179	.707	.464	1.000	.582	.500
	SP5	-.121	-.175	-.168	-.152	-.255	-.218	-.162	-.126	-.103	-.186	-.197	.686	.661	.582	1.000	.602
	SP6	-.167	-.240	-.232	-.219	-.314	-.254	-.188	-.181	-.161	-.289	-.260	.523	.557	.500	.602	1.000
Sig. (1-tailed)	N1		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.017	.005	.007	.042	.008
	N2	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.005	.000	.000	.006	.000
	N3	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.031	.000	.008	.000
	N4	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.001	.001	.001	.014	.001
	N5	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N6	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.001	.000
	N7	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.032	.018	.002	.010	.003
	N8	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.136	.001	.021	.036	.005
	N9	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.039	.008	.013	.069	.010
	N10	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.003	.000	.002	.004	.000
	N11	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.004	.000	.005	.002	.000
	SP1	.017	.005	.000	.001	.000	.000	.032	.136	.039	.003	.004		.000	.000	.000	.000
	SP3	.005	.000	.031	.001	.000	.000	.018	.001	.008	.000	.000	.000		.000	.000	.000
	SP4	.007	.000	.000	.001	.000	.000	.002	.021	.013	.002	.005	.000	.000		.000	.000
	SP5	.042	.006	.008	.014	.000	.001	.010	.036	.069	.004	.002	.000	.000	.000		.000
	SP6	.008	.000	.000	.001	.000	.000	.003	.005	.010	.000	.000	.000	.000	.000	.000	

References

- Ab Hamid, M. R., Sami, W., & Sidek, M. M. (2017, September). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. *Journal of Physics*, 890(1), 012163.
- Agnew, R. (1994). The techniques of neutralization and violence. *Criminology*, 32(4), 555-580.
- Alarcón, D., Sánchez, J. A., & De Olavide, U. (2015, October 22). Assessing convergent and discriminant validity in the ADHD-R IV rating scale: User-written commands for Average Variance Extracted (AVE), Composite Reliability (CR), and Heterotrait-Monotrait ratio of correlations (HTMT) [Conference presentation]. Spanish STATA Meeting. Universidad Pablo de Olavide, Seville, Spain.
- Allmon, D. E., Page, D., & Roberts, R. (2000). Determinants of perceptions of cheating: Ethical orientation, personality and demographics. *Journal of Business Ethics*, 23(4), 411-422. <https://doi.org/10.1023/A:1006087104087>
- Allport, G. (1967). Attitudes. In M. Fishbein (Ed.), *Readings in attitude theory and measurement* (pp. 1-13). New York: John Wiley & Sons.
- Alteer, A. M., Yahya, S. B., & Haron, M. H. (2013). Auditors' personal values and ethical judgement at different levels of ethical climate: A conceptual link. *Journal of Asian Scientific Research*, 3(8), 862.
- Arkes, H. R., & Blumer, C. (1985). The psychology of sunk cost. *Organizational Behavior and Human Decision Processes*, 35(1), 124-140.
- Armstrong, J. S., & Collopy, F. (1996). Competitor orientation: Effects of objectives and information on managerial decisions and profitability. *Journal of Marketing Research*, 33(2), 188-199. <https://doi.org/10.1177/002224379603300206>
- Arthur, J. B. (1994). Effects of human resource systems on manufacturing performance and turnover. *Academy of Management Journal*, 37, 670-687. <https://doi.org/10.2307/256705>
- Ashar, M., Ghafoor, M., Munir, E., & Hafeez, S. (2013). The impact of perceptions of training on employee commitment and turnover intention: Evidence from Pakistan. *International Journal of Human Resource Studies*, 3(1), 74. <https://doi.org/10.5296/ijhrs.v3i1.2924>

- Atuahene-Gima, K. (1996). Market orientation and innovation. *Journal of Business Research*, 35(2), 93-103. [https://doi.org/10.1016/0148-2963\(95\)00051-8](https://doi.org/10.1016/0148-2963(95)00051-8)
- Ball, R. A. (1966). An empirical exploration of neutralization theory. *Criminology*, 4(2), 22-32. <https://doi.org/10.1111/j.1745-9125.1966.tb00147.x>
- Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, 39, 145-159. <https://doi.org/10.1016/j.cose.2013.05.006>
- Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't Even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for IS*, 19(8), 689-715. <https://doi.org/10.17705/1jais.00506>
- Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *The Data Base Advances IS*, 48(3), 1-24. <https://doi.org/10.1145/3130515.3130519>
- Beautement, A., Sasse, M. A., & Wonham, M. (2009, August). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (pp. 47-58). ACM. <https://doi.org/10.1145/1595676.1595684>
- Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2), 169-217. <https://www.jstor.org/stable/1830482>
- Beekun, R. I., & Westerman, J. W. (2012). Spirituality and national culture as antecedents to ethical decision-making: a comparison between the United States and Norway. *Journal of Business Ethics*, 110(1), 33-44. <https://doi.org/10.1007/s10551-011-1145-x>
- Blau, P. M. (1964). *Exchange and power in social life*. New York: Wiley.
- Bommer, M., Gratto, C., Gravander, J., & Tuttle, M. (1987). A behavioral model of ethical and unethical decision making. *Journal of Business Ethics*, 6(4), 265-280.
- Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in IS research. *MIS Quarterly*, 25(1), 1-14. <https://doi.org/10.17705/1CAIS.01324>
- Bowers, D. G., & Seashore, S. E. (1966). Predicting organizational effectiveness with a four-factor theory of leadership. *Administrative Science Quarterly*, 238-263. <http://doi.org/10.2307/2391247>

- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009, August 6). *Roles of information security awareness and perceived fairness in information security policy compliance*. Americas Conference on Information Systems, San Francisco, CA, United States.
- 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.
- Brum, S. (2007). *What impact does training have on employee commitment and employee turnover?* (Seminar Research Paper Series, No. 45).
http://digitalcommons.uri.edu/lrc_paper_series/45
http://digitalcommons.uri.edu/lrc_paper_series/45
- Campbell, M., Stylianou, A. C., & Shropshire, J. (2016). The impact of attitudinal factors on intention to report workplace Internet abuse. *Journal of Information Privacy and Security*, 12(2), 68-83. <https://doi.org/10.1080/15536548.2016.1160677>
- Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3), 18-41.
<http://doi.org/10.1080/15536548.2005.10855772>
- Cialdini, R. B., Kallgren, C. A., & Reno, R. R. (1991). A focus theory of normative conduct: A theoretical refinement and reevaluation of the role of norms in human behavior. *Advances in Experimental Social Psychology*, 24, 201-234.
[https://doi.org/10.1016/S0065-2601\(08\)60330-5](https://doi.org/10.1016/S0065-2601(08)60330-5)
- Cohen, A., Fehr, E., & Maréchal, M. A. (2014). Business culture and dishonesty in the banking industry. *Nature*, 516(7529), 86-89. <https://doi.org/10.1038/nature13977>
- Cohen, J. (1992). A power primer. *Psychological Bulletin*, 112(1), 155.
<https://doi.org/10.1037//0033-2909.112.1.155>
- Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. Abingdon, England: Routledge.
- Cohen, J. R., Pant, L. W., & Sharp, D. J. (1998). The effect of gender and academic discipline diversity on the ethical evaluations, ethical intentions and ethical orientation of potential public accounting recruits. *Accounting Horizons*, 12(3), 250. <https://doi.org/10.1007/s10551-005-0277-2>

- Cohen, J. R., Pant, L. W., & Sharp, D. J. (2001). An examination of differences in ethical decision-making between Canadian business students and accounting professionals. *Journal of Business Ethics*, 30(4), 319-336. <https://doi.org/10.1023/A:1010745425675>
- Costello, B. J. (2000). Techniques of neutralization and self-esteem: a critical test of social control and neutralization theory. *Deviant Behavior*, 21(4), 307-329. 10.1080/016396200404113
- Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39, 447-459. 10.1016/j.cose.2013.09.009
- Chin W.W. (1998). *The partial least squares approach for structural equation modeling*. New York: Lawrence Erlbaum Associates.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks: Sage.
- Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Upper Saddle River: Merrill Prentice Hall.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101. 10.1016/j.cose.2012.09.010
- Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing*, 19(1), 20-26. <https://doi.org/10.1509/jppm.19.1.20.16944>
- D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management IS*, 31(2), 285-318. <https://doi-org.ezproxylocal.library.nova.edu/10.2753/MIS0742-1222310210>
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on IS misuse: A deterrence approach. *IS Research*, 20(1), 79-98,155,157. <https://doi.org/10.1287/isre.1070.0160>
- Dev, C., Zhou, K. Z., Brown, J., & Agarwal, S. (2009). Customer orientation or competitor orientation: Which marketing strategy has a higher payoff for hotel brands? *Cornell Hospitality Quarterly*, 50(1), 19-28. <https://doi.org/10.1177/1938965508320575>

- DeVellis, R. F. (2012). *Scale development: Theory and applications*. Thousand Oaks, CA: Sage.
- Deutsch, M., & Gerard, H. (1955). A study of normative and informational social influences upon individual judgment. *The Journal of Abnormal and Social Psychology, 51*(3), 629–636. <https://doi.org/10.1037/h0046408>
- Diamantopoulos, A., & Hart, S. (1993). Linking market orientation and company performance: Preliminary evidence on Kohli and Jaworski's framework. *Journal of Strategic Marketing, 1*(2), 93-121. <https://doi.org/10.1080/09652549300000007>
- Douglas, P.C., Davidson, R.A., & Schwartz, B.N. (2001). The effect of organizational culture and ethical orientation on accountant's ethical judgements. *Journal of Business Ethics, 34*(2), 101-121. <https://doi.org/10.1023/A:1012261900281>
- Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived organizational support. *Journal of Applied Psychology, 71*, 500–507. <https://doi.org/10.1037/0021-9010.71.3.500>
- Ferrell, O. C., & Gresham, L. G. (1985). A contingency framework for understanding ethical decision making in marketing. *Journal of Marketing, 49*(3), 87-96. <https://doi.org/10.2307/1251618>
- Fink, A. (2003). *The survey handbook* (2nd ed.). Thousand Oaks: Sage.
- Fischer, R. (2006). Congruence and functions of personal and cultural values: Do my values reflect my culture's values? *Personality and Social Psychology Bulletin, 32*(11), 1419-1431. <https://doi.org/10.1177/0146167206291425>
- Fischer, R. (2008). Multilevel approaches in organizational settings: Opportunities, challenges and implications for cross-cultural research. *Individuals and Cultures in Multi-Level Analysis, 173-196*.
- Fok, L. Y., Payne, D. M., & Corey, C. M. (2016). Cultural values, utilitarian orientation, and ethical decision making: A comparison of US and Puerto Rican professionals. *Journal of Business Ethics, 134*(2), 263-279. <https://doi.org/10.1007/s10551-014-2426-y>
- Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. <https://doi.org/10.2307/3151312>
- Forsyth, D. R. (1980). A taxonomy of ethical ideologies. *Journal of Personality and Social Psychology, 39*(1), 175. <http://dx.doi.org/10.1037/0022-3514.39.1.175>

- Fritzsche, D., & Oz, E. (2007). Personal values' influence on the ethical dimension of decision making. *Journal of Business Ethics*, 75(4), 335-343.
<https://doi.org/10.1007/s10551-006-9256-5>
- Gatignon, H., & Xuereb, J. M. (1997). Strategic orientation of the firm and new product performance. *Journal of Marketing Research*, 77-90.
<https://doi.org/10.1177/002224379703400107>
- Grasmick, H. G., & Bursik Jr, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law and Society Review*, 837-861.
- Greene, G., & D'Arcy, J. (2010, June 16). *Assessing the impact of security culture and the employee-organization relationship on IS security compliance* [Conference presentation]. Annual Symposium on Information Assurance, Albany, NY, United States.
- Greenfield, A. C., Norman, C. S., & Wier, B. (2008). The effect of ethical orientation and professional commitment on earnings management behavior. *Journal of Business Ethics*, 83(3), 419-434. <http://www.jstor.org/stable/25482387>
- Haenlein, M., & Kaplan, A. M. (2004). A beginner's guide to partial least squares analysis. *Understanding Statistics*, 3(4), 283-297.
https://doi.org/10.1207/s15328031us0304_4
- Hair, J.F., Hult G.T.M., Ringle, C.M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks: Sage.
- Hair, J.F., Ringle, C.M., & Sarstedt, M. (2011). PLS-SEM: Indeed, a silver bullet. *The Journal of Marketing Theory and Practice*, 19(2), 139-152.
<https://doi.org/10.2753/MTP1069-6679190202>
- Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, 257-278. <https://doi.org/10.2307/249656>
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of IS*, 18(2), 106-125. 10.1057/ejis.2009.6
- Herath, T., Yim, M. S., D'Arcy, J., Nam, K., & Rao, H. R. (2018). Examining employee security violations: Moral disengagement and its environmental influences. *Information Technology & People*, 31(6), 1135-1162.
<https://doi.org/10.1108/ITP-10-2017-0322>

- Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology*, 9(3), 187-204.
<https://doi.org/10.1007/s10676-007-9143-5>
- Hirschi, T. (1969). *Causes of delinquency*. Berkeley: University of California Press.
- Hollinger, R. C. (1986). Acts against the workplace: Social bonding and employee deviance. *Deviant Behavior*, 7(1), 53-75.
<https://doi.org/10.1080/01639625.1986.9967695>
- Hooley, G., Cox, T., Fahy, J., Shipley, D., Beracs, J., Fonfara, K., & Snoj, B. (2000). Market orientation in the transition economies of central Europe: Tests of the Narver and Slater market orientation scales. *Journal of Business Research*, 50(3), 273-285. [https://doi.org/10.1016/S0148-2963\(99\)00105-8](https://doi.org/10.1016/S0148-2963(99)00105-8)
- Hu, L.T., Bentler, P.M. (1998). Fit Indices in covariance structure modeling: Sensitivity to under parameterized model misspecification. *Psychological Methods*, 3, 424-453.
- 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.
- Hunt, S. D., & Vitell, S. (1986). A general theory of marketing ethics. *Journal of Macromarketing*, 6(1), 5-16. <http://dx.doi.org/10.1177/027614678600600103>
- Hyde, R. E., & Weathington, B. L. (2006). The congruence of personal life values and work attitudes. *Genetic, Social, And General Psychology Monographs*, 132(2), 151-190. <https://doi.org/10.3200/MONO.132.2.151-192>
- Ifinedo, P. (2012). Understanding IS security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95. <https://doi.org/10.1016/j.cose.2011.10.007>
- Ingram, J. R., & Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior*, 29(4), 334-366. 10.1080/01639620701588131
- Jebarajakirthy, C., Thaichon, P., & Yoganathan, D. (2016). Enhancing corporate social responsibility through market orientation practices in bottom of pyramid markets: With special reference to microcredit institutions. *Journal of Strategic Marketing*, 24(5), 398-417. <https://doi.org/10.1080/0965254X.2015.1063680>
- Jehanzeb, K., Rasheed, A., & Rasheed, M. F. (2013). Organizational commitment and turnover intentions: Impact of employee's training in private sector of Saudi Arabia. *International Journal of Business and Management*, 8(8), 79.
<https://doi.org/10.5539/IJBM.V8N8P79>

- Jung, W. H., Prehn, K., Fang, Z., Korczykowski, M., Kable, J. W., Rao, H., & Robertson, D. C. (2016). Moral competence and brain connectivity: A resting-state fMRI study. *Neuroimage*, 141, 408-415.
<http://dx.doi.org/10.1016/j.neuroimage.2016.07.045>
- Kajtazi, M., Cavusoglu, H., Benbasat, I., & Haftor, D. (2018). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information & Computer Security*, 26(2), 171-193. <https://doi.org/10.1108/ICS-09-2017-0066>
- Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of IS security effectiveness. *International Journal of Information Management*, 23(2), 139-154.
[https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1016%2FS0268-4012\(02\)00105-6](https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1016%2FS0268-4012(02)00105-6)
- Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*.
<https://doi.org/10.1155/2014/463870>
- Klepper, S., & Nagin, D. (1989). The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology*, 27(4), 721-746.
<https://doi.org/10.1111/j.1745-9125.1989.tb01052.x>
- Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *IS Journal*, 28(1), 227-261.
<https://doi.org/10.1111/isj.12131>
- Kohli, A. K., Jaworski, B. J., & Kumar, A. (1993). MARKOR: a measure of market orientation. *Journal of Marketing Research*, 30(4), 467-477.
<https://doi.org/10.1177%2F002224379303000406>
- Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7), 509-520. <https://doi.org/10.1177%2F002224379303000406>
- Leasure, P. (2017). Neutralizations in Retail Banking: A Qualitative Analysis. *Deviant Behavior*, 38(4), 448-460. <https://doi.org/10.1080/01639625.2016.1197018>
- Lee, H., Park, J., & Lee, J. W. (2013). Role of leadership competencies and team social capital in IT Services. *The Journal of Computer IS*, 53(4), 1-11.
<https://doi.org/10.1080/08874417.2013.11645645>
- Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707-718. <https://doi.org/10.1016/j.im.2003.08.008>

- Lengler, J. F., Sousa, C. M., & Marques, C. (2013). Exploring the linear and quadratic effects of customer and competitor orientation on export performance. *International Marketing Review*. <https://doi.org/10.1108/IMR-03-2011-0087>
- Lewrick, M., Omar, M., & Williams Jr, R. L. (2011). Market orientation and innovators' success: An exploration of the influence of customer and competitor orientation. *Journal of Technology Management & Innovation*, 6(3), 48-62. <https://doi.org/10.4067/S0718-27242011000300004>
- Levinson, H. (1965). Reciprocation: the relationship between man and organization. *Administrative Science Quarterly*, 9, 370-390. <https://psycnet.apa.org/doi/10.2307/2391032>
- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of IS research. *Informing Science Journal*, 9, 181-212. <https://doi.org/10.28945/479>
- Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635-645. <https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1016%2Fj.dss.2009.12.005>
- Lim, V. K., & Teo, T. S. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information & Management*, 42(8), 1081-1093. <https://doi.org/10.1016/j.im.2004.12.002>
- Limayem, M., & Hirt, S. G. (2003). Force of habit and IS usage: Theory and initial validation. *Journal of the Association for IS*, 4(1), 3.
- Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research? *Crime and Justice*, 32, 221-320. <http://www.scopus.com/inward/record.url?scp=33645465637&partnerID=8YFLogxK>
- Mason, E. S., & Mudrack, P. E. (1996). Gender and ethical orientation: A test of gender and occupational socialization theories. *Journal of Business Ethics*, 15(6), 599-604. <https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1007%2FBF00411793>

- Marta, J., Singhapakdi, A., & Kraft, K. (2008). Personal characteristics underlying ethical decisions in marketing situations: A survey of small business managers. *Journal of Small Business Management*, 46(4), 589-606.
<https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1111%2Fj.1540-627X.2008.00258.x>
- Merhi, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to IS Security. *Computers in Human Behavior*, 92, 37-46.
<https://doi.org/10.1016/j.chb.2018.10.031>
- Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods* (4th ed.). Glendale: Pyrczak.
- Mertler, C., & Vannatta, R. (2013). *Advanced and multivariate statistical methods: Practical application and interpretation* (5th ed.). Glendale: Pyrczak Publishing
- Meyer, J. P., Becker, T. E., & Vandenberghe, C. (2004). Employee commitment and motivation: a conceptual analysis and integrative model. *Journal of Applied Psychology*, 89(6), 991. <https://psycnet.apa.org/doi/10.1037/0021-9010.89.6.991>
- Micheli, P., Perks, H., & Beverland, M. B. (2018). Elevating design in the organization. *Journal of Product Innovation Management*, 35(4), 629-651.
<https://doi.org/10.1111/jpim.12434>
- Mingzhi, Liu, M. (2008, May 31). *The effect of personal values on individuals 'ethical behavioral intentions: evidence from professional auditors in people's Republic of China* [Session presentation]. Canadian Academic Accounting Association Annual Conference, Winnipeg, Canada.
- Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency*, 18(2), 295-318.
<https://doi.org/10.1177%2F002242788101800206>
- Molina, C. M., Moreno, R. R., & Moreno, M. R. (2013). Previous beliefs and continuance intention. *International Entrepreneurship and Management Journal*, 9(2), 199-216.
<https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1111%2Fj.1540-627X.2008.00258.x>
- Moore, T. T., & Chang, J. C. J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly*, 167-180.
<https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.2307%2F25148722>

- Morris, R. G., & Higgins, G. E. (2009). Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review*, 34(2), 173-195. <https://doi.org/10.1177%2F0734016808325034>
- Mowday, R. T. (1998). Reflections on the study and relevance of organizational commitment. *Human Resource Management Review*, 8(4), 387-401. [https://doi.org/10.1016/S1053-4822\(99\)00006-6](https://doi.org/10.1016/S1053-4822(99)00006-6)
- Myyry, L., Siponen, M., Pahnla, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of IS*, 18(2), 126-139. <https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1057%2Fejis.2009.10>
- Nagin, D. S., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law & Soc'y REV.*, 27, 467. <https://doi.org/10.2307/3054102>
- Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, 39(4), 865-892. <https://doi.org/10.1111/j.1745-9125.2001.tb00943.x>
- Narver, J. C., & Slater, S. F. (1990). The effect of a market orientation on business profitability. *Journal of Marketing*, 54(4), 20-35. <http://dx.doi.org/10.2307/1251757>
- Ocen, E., Francis, K., & Angundaru, G. (2017). The role of training in building employee commitment: the mediating effect of job satisfaction. *European Journal of Training and Development*, 41(9), 742-757. <https://doi.org/10.1108/EJTD-11-2016-0084>
- O'Connor, P. (2007). Online consumer privacy: An analysis of hotel company behavior. *Cornell Hospitality Quarterly*, 48(2), 183-200. <https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1177%2F0010880407299541>
- Park, S., Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2012). Towards understanding deterrence: Information security managers' perspective. In *Proceedings of the International Conference on IT Convergence and Security 2011* (pp. 21-37). Cham Switzerland: Springer.
- Payne, D., Corey, C. M., & Fok, L. Y. (2016). The Indirect Effects of Cultural Values on Ethical Decision Making via Utilitarian Ethical Orientation. *American Journal of Management*, 16(1), 19-34.

- Phatak, A. V., Bhagat, R. S., & Kashlak, R. J. (2005). *International management: Managing in a diverse and dynamic global environment*. New York: McGraw-Hill Irwin.
- Piquero, A. R., & Hickman, M. (1999). An empirical test of Tittle's control balance theory. *Criminology*, 37(2), 319-342. <https://doi.org/10.1111/j.1745-9125.1999.tb00488.x>
- Plakoyiannaki, E., Tzokas, N., Dimitratos, P., & Saren, M. (2008). How critical is employee orientation for customer relationship management? Insights from a case study. *Journal of Management Studies*, 45(2), 268-293. <https://doi.org/10.1111/j.1467-6486.2007.00740.x>
- Pogarsky, G. (2004). Projected offending and contemporaneous rule-violation: Implications for heterotypic continuity. *Criminology*, 42(1), 111-136. <https://doi.org/10.1111/j.1745-9125.2004.tb00515.x>
- Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, 51(5), 551-567. <https://doi.org/10.1016/j.im.2014.03.009>
- Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management IS*, 32(4), 179-214. <https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.25300%2FJMISQ%2F2013%2F37.4.09>
- Puhakainen, P., & Ahonen, R. (2006). *Design theory for information security awareness* [Unpublished doctoral dissertation]. University of Oulu.
- Rapp, A., Beitelspacher, L. S., Schillewaert, N., & Baker, T. L. (2012). The differing effects of technology on inside vs. outside sales forces to facilitate enhanced customer orientation and interfunctional coordination. *Journal of Business Research*, 65(7), 929-936. <https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1016%2Fj.jbusres.2011.05.005>
- Rest, J. R. (1986). *Moral development: Advances in research and theory*. Elmwood Park: Praeger.
- Rokeach, M. (1973). *The nature of human values*. New York: Free Press.

- Richardson, V. (1996). *The role of attitudes and beliefs in learning to teach*. In J. Sikula, Ed. *Handbook of Research on Teacher Education* (2nd ed.), pp. 102-119. New York: Simon & Schuster Macmillan.
- Rivis, A., & Sheeran, P. (2003). Social influences and the theory of planned behaviour: Evidence for a direct relationship between prototypes and young people's exercise behaviour. *Psychology and Health*, 18(5), 567-583.
<https://doi.org/10.1080/0887044032000069883>
- Rogerson, S., & Sallnäs, U. (2017). Internal coordination to enable high load factor. *The International Journal of Logistics Management*, 28(4), 1142-1167.
- Rokeach, M. (1973). *The nature of human values*. New York: Free Press.
- Salkind, N. J. (2006). *Exploring research* (6th ed.). Upper Saddle River: Pearson Education.
- Schwaig, K. S., Kane, G. C., & Storey, V. C. (2005). Privacy, fair information practices and the fortune 500: The virtual reality of compliance. *The DATA BASE for Advances in IS*, 36(1), 49-63.
<https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1145%2F1047070.1047075>
- Sekaran, U. (2003). *Research methods for business: A skill building approach* (4th ed.) New York: John Wiley & Sons.
- Sekaran, U., & Bougie, R. (2013). *Research Methods for Business* (6th ed.). New York: John Wiley & Sons.
- Sheehan, K. B. (2005). In poor health: An assessment of privacy policies at direct-to-consumer websites. *American Marketing Association*, 24(2), 273-283.
<https://doi.org/10.1509%2Fjppm.2005.24.2.273>
- Sheeran, P., & Rivis, A. (2017). Descriptive norms as an additional predictor in the theory of planned behavior: A meta-analysis. In C. J. Armitage & J. Christian, Eds. *Planned Behavior* (pp. 49-68). Abingdon: Routledge.
- Sherif, E., Furnell, S., & Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 436-448). San Francisco: Springer.
- Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management*, (in press), 1-15. <https://doi.org/10.1016/j.im.2017.02.007>

- Sims, R. L. (2002). Ethical rule breaking by employees: A test of social bonding theory. *Journal of Business Ethics*, 40(2), 101-109.
<https://doi.org/10.1023/A:1020330801847>
- Sin, L. Y., Tse, A. C., Yau, O. H., Chow, R. P., & Lee, J. S. (2005). Market orientation, relationship marketing orientation, and business performance: The moderating effects of economic ideology and industry type. *Journal of International Marketing*, 13(1), 36-57.
- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee IS security policy violations. *MIS Quarterly*, 487-502.
<https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.2307%2F25750688>
- Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of IS*, 23(3), 289-305.
<https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1057%2Fejis.2012.59>
- Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management*, 49(7-8), 334-341.
<https://doi.org/10.1016/j.im.2012.06.004>
- Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), 296-302. <https://doi.org/10.1016/j.im.2011.07.002>
- Stanton, J. M., Stam, K. R., Guzman, I., & Caledra, C. (2003, October 8). Examining the linkage between organizational commitment and information security. In *Systems, Man and Cybernetics* (vol. 3, pp. 2501-2506). Washington, DC, United States: IEEE. <https://doi.org/10.1109/ICSMC.2003.1244259>
- Straub, D. W., Jr. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147-169. <https://doi.org/10.2307/248922>
- Straub, D. W., Jr., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 45-60.
<https://doi.org/10.2307/249307>
- Straub, D. W., Jr., Boudreau, M., & Gefen, D. 2004. Validation guidelines for IS positivist research. *Communications of the Association for IS*, 13(24), 380-427.
<http://dx.doi.org/10.17705/1CAIS.01324>

- Storey, V. C., Kane, G. C., & Schwaig, K. S. (2009). The quality of online privacy policies: A resource-dependency perspective. *Journal of Database Management*, 20(2), 19-37. <http://doi.org/10.4018/jdm.2009040102>
- Sykes G, Matza D. (1957). Techniques of neutralization: a theory of delinquency. *American Sociological Review*, 22(6):664-70. <https://doi.org/10.2307/2089195>
- Teh, P. L., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees?: Insights from neutralization and social exchange theory. *Journal of Global Information Management (JGIM)*, 23(1), 44-64. 10.4018/jgim.2015010103
- Terpstra, D. E., Rozell, E. J., & Robinson, R. K. (1993). The influence of personality and demographic variables on ethical decisions related to insider trading. *The Journal of Psychology*, 127(4), 375-389. <https://doi.org/10.1007/s10551-005-3327-x>
- Terrell, S. R. (2016). *Writing a proposal for your dissertation: Guidelines and Examples*. New York: Guilford Press.
- Trevino, L. K. (1992). Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly*, 121-136. <https://doi.org/10.2307/3857567>
- Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & Security*, 52, 128-141. <https://doi.org/10.1016/j.cose.2015.04.006>
- Turk, Z., & Avcilar, M. Y. (2018). An investigation of the effect of personal values on the students' ethical decision-making process. In *Eurasian Business Perspectives* (pp. 245-262). Cham, Switzerland: Springer.
- Vance, A., Siponen, M., & Pahnla, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49(3), 190-198. <https://doi.org/10.1016/j.im.2012.04.002>
- Vance, A., & Siponen, M. T. (2012). IS security policy violations: a rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, 24(1), 21-41. <https://doi.org/10.4018/joeuc.2012010102>
- Venkatesh, V., & Brown, S. A. (2001). A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges. *MIS Quarterly*, 71-102.
- Veenstra, R., Lindenberg, S., Tinga, F., & Ormel, J. (2010). Truancy in late elementary and early secondary education: The influence of social bonds and self-control—

- the TRAILS study. *International Journal of Behavioral Development*, 34(4), 302-310. <https://doi.org/10.1177%2F0165025409347987>
- Venkatesh, V., & Brown, S. A. (2001). A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges. *MIS Quarterly*, 71-102. <https://doi.org/10.2307/3250959>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478. <https://doi.org/10.2307/30036540>
- Wanous, J. P., & Reichers, A. E. (2001). New employee orientation programs. *Human Resource Management Review*, 10(4), 435-451. [https://doi.org/10.1016/S1053-4822\(00\)00035-8](https://doi.org/10.1016/S1053-4822(00)00035-8)
- Watson W., (1999). *WorkUSA 2000: Employee commitment and the bottom line*. Bethesda: Watson Wyatt.
- Whitener, E. M. (2001). Do “high commitment” human resource practices affect employee commitment? A cross-level analysis using hierarchical linear modeling. *Journal of Management*, 27(5), 515-535. <https://doi.org/10.1177%2F014920630102700502>
- Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and organization*, 16(4), 304-324. <https://doi.org/10.1016/j.infoandorg.2006.08.001>
- Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 1-20. <http://www.jstor.org/stable/43825935>
- Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *IS Journal*, 28(2), 266-293. <https://doi.org/10.1111/isj.12129>
- Wood, S., & de Menezes, L. (1998). High commitment management in the U.K.: Evidence from the Workplace Industrial Relations Survey and Employers' Manpower and Skills Practices Survey. *Human Relations*, 51, 485-515. <https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1023%2FA%3A1016941914876>
- Wooten, K. G., Wortley, P. M., Singleton, J. A., & Euler, G. L., (2012). Perceptions matter: Beliefs about influenza vaccine and vaccination behavior among elderly white, black, and Hispanic Americans. *Vaccine*, 30(48), 6927-6934. <https://doi.org/10.1016/j.vaccine.2012.08.036>

- Yang, Y., Wang, Q., Zhu, H., & Wu, G. (2012). What are the effective strategic orientations for new product success under different environments? An empirical study of Chinese businesses. *Journal of Product Innovation Management*, 29(2), 166-179.
<https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1111%2Fj.1540-5885.2011.00900.x>
- Zhai, Q., Lindorff, M., & Cooper, B. (2013). Workplace guanxi: Its dispositional antecedents and mediating role in the affectivity–job satisfaction relationship. *Journal of Business Ethics*, 117(3), 541-551. <https://doi.org/10.1007/s10551-012-1544-7>
- Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, 17(4), 330-340.
<https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1108%2F09685220910993980>