Winter 12-2021

Exploring High-Power Distance Among Other Variables in Information Security Policy Compliance

Erasmus Ekpo Etim
Dakota State University

DAKOTA STATE UNIVERSITY

EXPLORING HIGH-POWER DISTANCE AMONG OTHER VARIABLES IN INFORMATION SECURITY POLICY COMPLIANCE

A doctoral dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Information Systems

December 2021

By
Erasmus Ekpo Etim

Dissertation Committee:

Dr. Kevin Streff
Dr. Insu Park
Dr. Gabe Mydland

DEDICATION

Navigating life is a difficult task, thanks to my mother who has been there all the way. This is the result of your love and commitment to all of us. Thank you, Ma May for everything. I love you.

DISSERTATION APPROVAL FORM

We certify that we have read this dissertation and that, in our opinion, it is satisfactory in scope and quality as a dissertation for the degree of Doctor of Philosophy in Information Systems.

Student Name: Erasmus Ekpo Etim

Dissertation Title: **Exploring High-Power Distance among other Variables in Information Security Policy Compliance**

Dissertation chair: Dr. Kevin Streff Date: October 29, 2021

Committee member: Insu Park Date: October 29, 2021

Committee member: Gabe Mydland Date: October 29, 2021

ACKNOWLEDGMENT

First, I thank my Lord and Savior Jesus Christ for giving me the strength to complete this task.

My sincere thanks to the dissertation chair Dr. Kevin Streff for his guidance throughout this process. I appreciate the help of the committee members, Dr. Insu Park, Dr. Pam Rowland, and Dr. Gabe Mydland. I would not be this far in the project without all of you.

I thank my wife Gerri for putting up with me and her encouragement at every turn. Thanks to my children, Ofiong, Efiom, and Nsa for taking up my part of the family chores to see me free to take up this challenge.

I thank my sisters, Immaculata and Felicitas, and their families for their help in handling some of the essential tasks needed for this project.

To my Church family at Key to Faith Ministries I say thank you for your prayers and encouragement.

ABSTRACT

Information security threat is one of the significant challenges organizations must deal with, and one component of that challenge is information security policy compliance. Data breaches sometimes happen because employees do not adhere to information security policies. The purpose of the exploratory study was to determine if power distance had a role in information security policy compliance; power distance is the understanding that power distribution is unequal. The research required survey data collected from a high-power distance index country, Nigeria. The Nigerian working class was the population sample; a model was developed based on compliance, descriptive norms, moral beliefs, normative beliefs, power distance, self-efficacy, sanctions as the independent variables, and intent to comply as the dependent variable. General deterrence theory, protection motivation theory, rational choice theory, theory of reasoned action, and theory of planned behavior were the applicable theories. The analysis was performed using Partial least squares-structural equation modeling, and the preferred software was SmartPLS version 3.3.3. The significance of power distance playing a role in information security compliance would mean that organizations could cultivate the idea of using employees with the cultural characteristic as influencers and could incorporate power distance into the training program. The results showed that power distance was significant in information security policy compliance.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

_____

Erasmus Ekpo Etim

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The year 2018 witnessed incredible technological innovation (Expert Panel, 2019; Winick et al., 2018), and most organizations have boarded the new technological train. Unfortunately, the increase in technology also inspired new cybercrimes as cybercriminals invented new ways to compromise the latest technologies; according to Deloitte (2019), more data breaches occurred in the same year. The report cites the Facebook data breach scandal and the acquisition by Cambridge Analytica of about 87 million Facebook users' information without authorization. Nigerian businesses were not exempt as they were subject to some of the same waves of criminal acts, including the well-known Nigerian scams (Deloitte, 2019). Due to the increase in digital crime worldwide, a Nigerian agency, National Information Technology Development Agency (NITDA), was mandated to chart a country's data security policy. The agency's ultimate goal is to foster international cooperation to enforce legislation that protects personal data ((NITDA, 2019).

Information security is one of the most significant challenges faced by organizations today, and information security policy (ISP) is one of the tools employed to mitigate the problem. Employees' violations of ISP are serious concerns (D'Arcy, Hovav, & Galletta, 2009; Kim, Yang, & Park, 2014; Vance & Siponen, 2012). In 2,216 confirmed breaches by Verizon 2018 investigation report, 28% involved internal actors, and partners are responsible for 2% (Verizon Business, 2018). Further analysis of the top 20 action varieties in 1,799 confirmed breaches produced the following results: Social engineering – 350, misuse – 256, and human error – 312 (Verizon Business, 2018). In 255 confirmed breaches, the following internal actors are involved in order: System admin (72), end-users (62), other (62), doctor or nurse (32), developer (15), manager (9), executive (8), cashier (6), finance (6) and human resources (5), (Verizon Business, 2018). Without human cooperation, ISP has no chance of successfully protecting organizations' information (Doherty & Fulford, 2005; Pahnila, Siponen, & Mahmood, 2007b).

The early research on factors that positively affect employees' behaviors toward ISP compliance was based on sanctions and fear appeals (Bulgurcu, Cavusoglu, & Benbasat,

2010; Herath & Rao, 2009a). Recent ISP research focuses on employees' behavior, linking information protection to what employees do or do not do, as Da Veiga and Eloff (2010) argued. Pahnila et al. (2007) provide empirical data on factors that explain employees' adherence to information security policies: normative beliefs, threat appraisal, self-efficacy, visibility, sanctions, rewards, and response efficacy. Password sharing, not following correct procedures by taking shortcuts, visiting wrong websites, and downloading potentially harmful materials from the internet (Alfawaz, Nelson, & Mohannak, 2010), are behaviors that expose organizations' data to external compromise. Some employees excuse their ISP violations by saying everybody does it and that it is their first time, basically making excuses to justify their actions (Kim et al., 2014). Sommestad, Hallberg, Lundholm, and Bengtsson (2014) conducted extensive reviews of research on factors that influence ISP compliance; out of over 60 variables reviewed, there was no clear front runner; each concentration was on a small part of human behavior.

Definition of Terms

Information security: "Information security is the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional " (Peltier, 2004), and successful security depends on several factors one of which is a well written and disseminated information security policy (ISP).

Information security policy: Lowry and Moody (2015) define information security policies as *"*a set of formalized procedures, guidelines, roles, and responsibilities to which employees are required to adhere to safeguard and use the information and technology resources of their organizations properly. "

Culture: Hofstede, Jan Hofstede, and Minkov (2010, p. 6) define culture as "the collective programming of the mind that distinguishes the members of one group or category of people from others. "

Sanctions: These measures discourage employees from violating organizations' policy prescriptions (Johnston, Warkentin, McBride, & Carter, 2016).

Moral beliefs: D'Arcy and Herath (2011) define moral beliefs as "the extent to which one perceives an illicit act to be morally offensive. "

Benefits of compliance: Bulgurcu et al. (2010) define perceived benefits of compliance as "the overall assessment of consequences to an employee for complying with the requirements of the ISP. "

Self-efficacy: Bandura (1997: p. 3) defines self-efficacy as "beliefs in one's capabilities to organize and execute the courses of action required to produce given attainments. "

Descriptive norms: The perception that others who are significant are performing the behavior (Smith & Louis, 2009).

Normative beliefs: The acceptable or expected behaviors in a workplace or social setting (Rousseau, 1990).

Power distance: The "the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally " (Hofstede et al., 2010: p. 61).

Intention to comply: An "employee's intention to protect the information and technology resources of the organization from potential security breaches " (Bulgurcu et al., 2010).

Culture in Context

Information security is a global phenomenon. Thus, national culture should be a part of information security research on how much culture could affect ISP compliance. Businesses seek worldwide reach, and one way to achieve it is to establish branches in different countries for quick market access, which requires managing security risks. Management has to address both national and organizational cultures to be successful and corporate cultures are easier to manage than national cultures (Hofstede, 1994). Understanding national culture starts with understanding employees' backgrounds, which predicts present and future behavior (Hofstede, 1994). An example of a cultural difference would be comparing the plight of single women in the United States of America to those in Nigeria. In the United States women seem to choose when they marry without pressure from family or society (Goldstein & Kenney, 2001; Moran, 2004). In contrast, the pressure on single women and single mothers in Nigeria has driven some of them to do the unthinkable, such as polygamously marrying a man who is already married (Chinwuba, 2015).

Culture affects how people think and behave; its effects are not limited to marriage but extend to technology and, specifically, information security. Cultures come in different forms: national, organizational, and workplace cultures (Gefen & Straub, 1997; Hofstede et al., 2010). Studies from over 50 countries and 20 organizational units point out the following findings: National culture and organizational culture are similar, but national culture has more influence on employees than organizational culture. Further, while organizational cultures changes with each employment, national culture is independent of the employment environment (Dols & Silvius, 2010; Hofstede, 1994, 2011). Hofstede (2011) provides a framework for the understanding needed in dimensionalizing national cultures. National culture as seen through the lenses of Hofstede's six dimensions are defined in table 1.1:

Table 1.1 Definition of Cultural Dimensions

Cultural Dimension	Definition	Source
Power Distance Index (PDI)	Members of organizations accept that power distribution is unequal, and subordinates must obey their superiors' instructions. This characteristic is acquired as children, educated to be obedient to parents, and taught to look up to teachers as authority figures in high PDI societies. The opposite is true in a low PDI society where subordinates can challenge superiors' decisions.	Hofstede, 1991, 2011.
Individualism versus Collectivism (IDV)	Individualist culture has no strong bonds, and each person looks out for him/herself and his/her family. By contrast, a collective culture is one in which people integrated into a robust and cohesive group.	
Masculinity versus Femininity (MAS)	Men's values are different from women's, and from one culture to another, women's values vary minimally; men's values range maximally, from very assertive to modest and caring.	
Uncertainty Avoidance (UAI)	Uncertainty avoidance is defined - "as the extent to which the members of a culture feel threatened by uncertain or unknown situations." - In a high uncertainty avoidance culture, members set rules and laws to reduce the possibilities of uncertainty. On the opposite end, low uncertainty avoidance cultures tend to be more trusting and make fewer laws.	
Long Term versus Short Term Orientation (LTO)	Values ascribed to the long term are thrift and perseverance, and the short-term value is concerned with tradition, fulfilling social obligations, and protecting one's - "face."	
Indulgence versus Restraint (IND)	Indulgence culture allows free gratification of human desires; restraint culture, on the other hand, controls gratifications and regulates by imposing strict social norms.	

As defined in table 1.1, high power distance translates into respect for elders and superiors, which leads to employees' acceptance and execution of instructions without challenge (Hofstede, 1994), which is what an organization wants in an employee. In the age of technology and failure to protect an organization's assets, there is a need for employee loyalty to reverse this trend. Roehling, Roehling, and Moen (2001) argued that commitment is a challenge for an organization, and the lack of it shows that employees have no vested interest in the business.

Nigerian Culture

In this research, Hofstede's PDI is the applicable dimension as Nigeria is one of the countries with high PDI, as indicated in figure 1.1 below. Six cultural dimension indicators are representing Nigeria standing in Hofstede's analysis compared to the United States. The research is based on Nigerian national culture because of its uniqueness compared to other countries. It is a country with over 300 ethnic groups and 500 tribes, each with its own unique culture, yet it manages to develop and maintain a national culture of respect for elders, employers, and superiors (Falola, 2001, p. 139; Lawan & Zanna, 2013). The respect for authority and rules in Nigerian national culture is the foundation of this research on behavior favorable to ISP compliance. The high PDI indicates dependence on superiors to lead and have the employees follow. Power distance, with other psychological and sociological factors that positively or negatively affect an employee's behavior toward ISP compliance to compare its effect in a broad perspective considering those well-researched factors, will be investigated. The following constructs (input variables) are explored in this research: Sanctions, moral beliefs, benefits of compliance, self-efficacy, descriptive norms, normative beliefs, and power distance. The data from the six variables will be compared to the data from power distance to understand its importance.

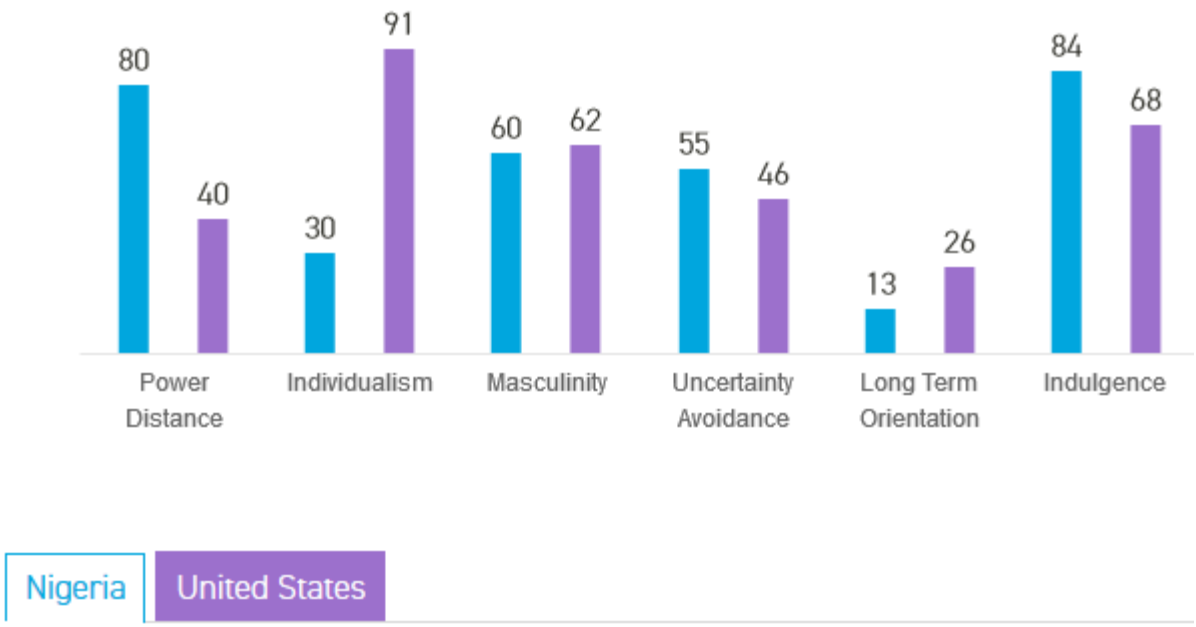


Figure 1.1 Hofstede six cultural dimensions- Nigeria/USA Comparison (Hofstede, 2017)

Statement of the Problem

Data breaches resulting from phishing emails are common; they cost businesses $4.5 billion in 2014 globally, and the conversion rate for email fraud is at 45% (Derouet, 2015). The data breach at Target happened because criminals had access to heating, ventilation, and air conditioning contractor's credentials obtained through phishing email attacks (Krebs, 2014; Olavsrud, 2014). The credentials gave them access to Target through the corporate intranet (Krebs, 2014; Olavsrud, 2014). The increase in technological innovation had been exceptional, followed by the rise in information security violations resulting from human failures as demonstrated in the above statements. Organization information is related to its business and is well known to its employees and contractors; the organization uses it to gain a competitive advantage (Peltier, 2004, p. 49).

Early research based on sanctions and fear appeals affect how employees behaved toward ISP compliance (Bulgurcu et al., 2010; Herath & Rao, 2009a). The present research focuses on how employees' behaviors contribute to information protection or information breaches (Da Veiga & Eloff, 2010). Pahnila et al. (2007) provide empirical evidence on factors that explain employees' adherence to information security policies:

normative beliefs, threat appraisal, self-efficacy, visibility, sanctions, rewards, and response efficacy. Several other researchers have conducted studies that involved other factors which explained employees' behaviors toward information protection in response to ISP. Employees' behaviors toward ISP have been at the core of all the studies. If National culture is a way to assess human behavior, it demands investigation to determine the adequate security measures needed to manage a global organization.

The above brief literature review summary on employees' behaviors has not included culture, one of the determinants of human behavior (Gastil, 1961). The role of power distance (PD), a derivative of culture (Hofstede, 1994; Mathew & Perreault, 2016), in ISP compliance has not been investigated and this study is designed to accomplish that. This research is an exploration of how national culture – power distance specifically affects behavior toward ISP compliance.

The approach to the study is to develops and validates an empirical model based on testable hypotheses. The model will consist of power distance and other variables as independent variables, and intention to comply as the dependent variables. The tests to evaluate and validate the model and hypotheses involve using statistical software based on partial least squares – structural equation modeling (SEM).

Research Questions and Hypotheses

- RQ1 - What effect does power distance have on employees' behavior toward ISP compliance intention?
- RQ2 - How significant are the data on power distance?
- RQ3 - How do the data on power distance compare with the data on other constructs in the survey?
- H1: Self-efficacy will positively impact employees' attitudes toward ISP compliance.
- H2: Benefits of compliance will positively impact employees' attitudes toward ISP compliance.
- H3: Descriptive norms will positively impact employees' attitudes toward ISP compliance.
- H4: Sanctions will positively impact employees' attitudes toward ISP compliance.
- H5: Moral beliefs will positively impact employees' attitudes toward ISP compliance.

- H6: Normative beliefs will positively impact employees' attitudes toward ISP compliance.
- H7: High power distance positively impacts employees' attitudes toward ISP compliance.

Purpose of the Research

The problem statement points out the gap in the studies done so far in ISP compliance, and the purpose of this research is to fill that gap. Investigation the role of power distance in ISP compliance will help employers develop sensitivity to national culture and relate that to appropriate job assignments and security awareness training.

In addition, this research creates an opportunity for other researchers to study the role of power distance in information security in different organizations and countries.

Theoretical Background and Constructs Description

These theories apply to this research: Protection Motivation Theory (PMT), Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), and Rational Choice Theory (RCT).

Protection Motivation Theory (PMT): States that fear appeal can motivate people to comply or learn what is required to comply with directives. The cost of taking the right action outweighs any benefits derived from the violation. The second point is that the proper knowledge facilitates compliance in the case of self-efficacy (Herath & Rao, 2009a; B. A. C. Johnston & Warkentin, 2010; Lee, Lee, & Yoo, 2004; Vance, Siponen, & Pahnila, 2012a).

Theory of Reasoned Action (TRA): Posits that that person's intentions drive individual behavior. Behavioral intentions point to how the person feels about their behavior and those connected to them. The attitude toward the behavior is either positive or negative about performing the behavior. Finally, the person must weigh whether he/she desires to accept the consequences of the behavior (Bulgurcu et al., 2010; Fishbein & Ajzen, 1975; Hale, Householder, & Greene, 2003).

Theory of Planned Behavior (TPB): This theory is related to a person's behavioral intention, resulting from a person's attitude and willingness to take opportunities (Ajzen, 1991).

General Deterrence Theory (GDT): Posits that violations could be discouraged by using countermeasures in the form of sanctions proportional to the act (Straub & Weike, 1998).

Rational Choice Theory (RCT): This theory explains that a person chooses based on his/her moral beliefs and that acts on those beliefs may be wrong or right. It links choice to preference which indicates that people should behave purposefully according to their values. Recently the theory has been extended to include a positive spectrum of moral obligation, doing right instead of wrong (Akers, 1990; Vance & Siponen, 2012b).

Table 1.2 Description of Constructs

Construct	Description	Source and Theory
Sanctions	The employee punished in proportion to the violation of information security (IS) policy	Bulgurcu et al., 2010; Pahnila et al., 2007 GDT
Moral beliefs	The moral obligation that compels an employee to do right. The rules guide a person's action in choosing between right and wrong.	Al-Omari, Deokar, El-Gayar, Walters, & Aleassa, 2013; Vance et al., 2012; Cronan & Al-Rafee, 2008) RCT
Benefits of compliance	The employee believes that compliance with IS policy will bring benefits to him/her, such as continuous employment	Bulgurcu et al., 2010. TPB, TRA
Self-Efficacy	Employee assesses his/her ability to perform tasks that are required to comply with IS policy.	Maddux & Rogers, 1983. PMT
Descriptive Norms	An employee who sees that his/her co-workers follow the organization's IS policy will likely do the same.	Herath & Rao, 2009. TPB
Normative beliefs	The employee receives social pressure from colleagues and those over him/her to comply with IS policy as a part of the expected behavior.	Ajzen, 1991; Ajzen et al., 1980. TPB
Power distance	A factor that indicates how a person will respond to authority based on how low or high the power distance is.	Zhang & Begley, 2011; Sideridis, Kaissidis, & Padeliadu, 1998. RCT, TRA
Intention to comply	The employee desires to protect an organization's resources from potential security breaches.	Ajzen, 1991; Ajzen et al., 1980. TPB

Contribution

This investigation will contribute to research, theory, and practice. It fills the gap in ISP compliance research by introducing power distance as one of the variables that positively affect behavior. In the case of theory, (RCT) has been criticized because people make decisions based on environmental and other constraints, which would indicate that those people have no other options (Burns & Roszkowska, 2016; Coleman, 1992). People have choices; they choose to operate within the cultural bounds though exposed to alternatives, and the research will provide an extension to RCT. The theory of reasoned action, as explained, is voluntary, based on a person's beliefs, which parallels culture (Ajzen & Fishbein, 1980; Moody, 2018). This research offers an extension to TRA. The people of most cultures view the consequences of their actions as reasonable.

For practice, the research will help businesses build national and personal profiles leading to decisions on investments and job assignments. The practical implications could extend beyond the borders of Nigeria as employers would trust and favor people from the country to handle sensitive information. Management in every business depends on other people to carry out their objectives; to do that, they have to know what has to be done and know the people who have to do them (Hofstede, 1994). Employees profiled as protectors of the organization's information should be positioned to influence others and help the organization design appropriate ISP awareness programs. Placement of employees in influencing situations is a form of risk aversion for businesses.

Limitations

The study is not generalizable outside of Nigeria, because of differences in national cultures. The survey was taken during the global lockdown with only a few people allowed to work outside their homes; therefore, access was limited. Each construct was limited to three questions in the survey to encourage many people to complete the survey. Only respondents with ISP programs in their organizations are considered for this study. In a self-reporting survey, there is the problem of reliability and this study did not escape it. People understand questions differently and the responses to such questions may be questionable. There are possibilities that some respondents might have answered some questions without reading them. Answering questions on survey forms does not allow the respondents to explain the reasons for their answers.

How the Paper is Organized

The introduction presents the problem statement, the definition of culture in the Nigerian context, theoretical background, construct description, motivation, research questions, contribution, and limitations. The rest of the paper's organization is as follows: Chapter 2 – present a review of literature; chapter 3 – describes the methodology, including the research model, hypotheses, data collection, and standards for data analysis, Chapter 4 – provides the analysis and results, including demographics, model assessments, and hypothesis testing; finally, chapter 5 – closes with a discussion, recommendations, and conclusions. The results are summarized, limitations are listed, implications examined, and suggestions for future research are made.

Summary

There is a limit to what technology can accomplish in terms of protecting an organization's information. Human behavior is central in information security compliance, and this research explores the role of power distance as a contributor to that behavior. The underlying theories in the study are protection motivation theory, rational choice theory, the theory of reasoned action, the theory of planned behavior, and general deterrence theory. The selection of a country with a high PDI for this study was to discover the effect of power distance on people's behavior toward information security policy compliance.

Chapter 2 is the literature review from different disciplines that have researched the role of power distance in some form. The literature reviewed included cultural research and has some significant effects on business and technology. The knowledge gained from these research studies applies to study information security policy compliance. The literature review ends with theories used in information security research, which have their origins from criminology and psychology, which deal with behaviors.

CHAPTER 2

LITERATURE REVIEW

Introduction

Many factors must be considered to stem the tide of data breaches that are on the rise yearly. Based on research conducted in other disciplines, cultural dimensions have featured prominently in technology adoption, business, advertising, and job performance in several countries and other factors affecting how employees respond to organizations' information protection issues. The related literature review will concentrate on how power distance and different cultural dimensions affect how people behave and how these factors affect behaviors that result in ISP compliance or non-compliance.

Factors that influence how employees behave toward ISP compliance, except PD, have been well researched. The literature review will attempt to include the roles of national culture and power distance impacts in other disciplines that could apply to ISP compliance.

Power Distance and Organizational Learning Culture

Škerlavaj, Su, and Huang's (2013) work on national cultural dimensions determined their moderating effects on information acquisition, information interpretation, and behavioral changes. Four national cultural dimensions, power distance, individualism, masculinity, and uncertainty avoidance, were the moderating constructs used in the research. They moderate the relationship between information acquisition and information interpretation and between information interpretation and behavioral and cognitive changes. The authors' intended to demonstrate empirically that organizational learning was a multilevel process affected by the four national cultural dimensions.

Škerlavaj et al. (2013) found that contrary to expectations, the four national cultural dimensions did not significantly moderate the relationship between information acquisition and information interpretation. They confined themselves to researching the effects of the four national cultural dimensions and could not exclude the possibility that the remaining dimensions might not positively affect the relationship. Nevertheless, the impact of national culture on the positive relationship between information interpretation and

behavioral and cognitive changes was significant. The effects were behavior modification and new cognitive beliefs.

Power distance strengthened the positive influence of information interpretation on behavior and cognitive changes, and individualism weakened the relationship, like masculinity and uncertainty avoidance. The effect of information interpretation was significant in a high power distance organization as it translated into employees' behavioral and cognitive changes (Škerlavaj et al., 2013). This finding indicated that employees from high power distance cultures took organizational learning seriously enough to alter their behaviors to align with their expectations.

Power Distance Moderating Effect on Employee Empowerment and other Variables

Different types of employee empowerment would lead to better team participation, resulting in improved performance in an organization. Empowerment can be psychological. It might manifest, for example, as a supervisor showing concern for subordinates, permitting them to voice concern on issues, or encouraging them to participate in decision making.

Zhang and Begley (2011) researched the moderating impact of power distance on employee empowerment and team participation based on a survey of employees of Chinese companies in China and Chinese-based American companies. The authors described empowerment as an organization giving employees discretion and autonomy to carry out their functions under the organization's guidelines. Team participation meant that employees had the freedom of association, cooperated, and shared information to improve processes and products (Zhang & Begley, 2011). One of the expected findings was the acculturation of Chinese employees working for Chinese-based American companies (Zhang & Begley, 2011). As a low power distance society, the expectation implied that the United States might transmit that state of mind to Chinese employees that could change their behaviors.

Several findings were apparent from Zhang and Begley's (2011) research. One was that Chinese-based American companies had changed their values to become more Americanized. The significance was that they had become more assertive than those from a low power distance society. In addition team participation was not significantly impacted by empowerment in a high power distance setting, while low power setting, the opposite was true in a low power distance setting(Zhang & Begley, 2011). The importance of this finding

centered on the point that employees in a high-power distance setting responded to instructions, and empowerment did not make much difference to them compared to those in the low power distance setting.

The main objective of the research conducted by Fock, Hui, Au, and Bond (2013) was to examine the moderation effects of power distance on the relationship between three types of empowerment; discretion, psychological and leadership empowerment, and employee satisfaction. Discretion empowerment, also referred to as structural empowerment, is the extension of the decision-making process to powerless employees to encourage effective job performance (Fock et al., 2013). Empowerment that goes beyond job autonomy to include improving the feeling of self-efficacy among other employees leads to self-worth and psychological empowerment (Fock et al., 2013). Fock et al. (2013) also explained that leadership empowerment happened when a supervisor stepped into a supportive role that engendered subordinates' trust. This type of empowerment involves coaching, encouragement, and showing concern for subordinates' welfare. The authors conducted their research by a survey of employees in Canada, a low power distance society, and China, a high-power distance society.

The conclusion drawn by researchers showed that empowerment did not apply to high power distance society motivated Fock et al. (2013) to investigate the effect of power distance on the relationship between different types of empowerment and employee satisfaction. The finding was that discretion empowerment did not affect job satisfaction in high power distance, which was the same conclusion arrived at by other researchers (Fock et al., 2013). The relationship between psychological empowerment and employee satisfaction in low and high power distance cases was significant (Fock et al., 2013). High power distance had a more pronounced effect on the relationship between leadership empowerment and employee satisfaction (Fock et al., 2013). It is worth noting that employees who obey orders will not be affected by being given discretion empowerment. Employees welcomed psychological empowerment, which makes them human, and leadership empowerment is beneficial primarily to employees whose experiences are usually limited to management dictate.

To study the mediating and moderating effects of employee empowerment on the relationship between trust of supervisor and job satisfaction in a high distance organization,

Lim and Lau (2017) surveyed employees of banks in Kuala Lumpur. The cultural factor in this research was that Kuala Lumpur was a high power distance society (Lim & Lau, 2017).

In a high-power organization, employees who had personal trust in their superiors had some sense of higher job satisfaction (Lim & Lau, 2017). In addition, employee empowerment in a high power distance organization creates a sense of belonging, which significantly affects interpersonal trust and employee job satisfaction (Lim & Lau, 2017). This research's critical point is that trust reduces anxiety and fear in the organization, creating a great work environment that improves performance.

Power Distance in Advertising

Does advertising content mirror cultural differences (Albers-Miller & Gelb, 1996)? The authors wanted to answer the question by conducting research based on Hofstede's cultural model. Eleven countries with PDIs ranging between 13 and 81 were chosen for their advertising appeals; out of 30 appeals, eight were related to power distance. The remaining 22 related to three other cultural dimensions: individualism, uncertainty avoidance, and masculinity. Albers-Miller and Gelb (1996), based on power distance, hypothesized the following:

- Ornamental appeals: beauty is more associated positively with country high scores on power distance dimension.
- Vein appeals: acceptable social appearance is associated positively with country high scores on power distance dimension.
- Expensive appeals: luxurious items that show wealth are associated positively with country high scores on power distance dimension.
- Status appeals: social status is associated positively with country high scores on power distance dimension.
- Cheap appeals: inexpensive is associated negatively with country low scores on power distance dimension.
- Plain appeals: simple is associated negatively with country low scores on power distance dimension.
- Humility appeals: unassuming is associated negatively with country low scores on power distance dimension.

- Nurturance appeals: charity is associated negatively with country low scores on power distance dimension.

The findings were significant; out of the 30 hypotheses, ten supported, and five out of eight appeals coded for power distance were supported (Albers-Miller & Gelb, 1996). Ornamental, vain, expensive, and status appeals related positively to power distance dimension and cheap appeal related negatively. The authors did not recommend standardized advertisement across cultures based on their findings.

Jung, Polyorat, and Kellaris (2009) studied how young adults would respond to an ad that featured people who were not authority figures. The authority-based promotion believed consumers would respond positively to an ad featuring an authority figure (Jung et al., 2009). The expectation was that the recommendations of authority figures had more significant sway in high power distance cultures than low power cultures (Jung et al., 2009). Jung et al. (2009) conducted two experiments: one involved undergraduate business students from South Korean universities and undergraduate business students from an American university. The second group was undergraduate business students from a Thai university. Jung et al. (2009) required students to listen to radio advertisements. The script varied to represent high, medium, and low authority levels; Jung et al. (2009) measured spokesperson source credibility, while the respondents' power distance, culture, and demography were controls.

The findings clearly showed reverse authority effects among young adults Koreans and reduced authority effects among young Americans (Jung et al., 2009). Dissatisfaction with authorities was prevalent in other high power distance Asian countries as traditional values were weakened, attributable to accelerated economic development (Jung et al., 2009). Among young Thai consumers, responses were negative toward the spokesperson of high authority, even when they believed the person to be credible (Jung et al., 2009). Based on economic disparity between the two countries, the authors had to rule out economic development as the source of rejection of authority figures in each advertisement.

The consequences of culture have become a concern in advertising and marketing in recent years (Mooij & Hofstede, 2007). This paper, written by the authors,

directed at the essential aspects of Hofstede's model applicable to branding and advertisement and the review of research that applied the model in advertising and branding.

In search of an effective global advertising model, researchers had undertaken the study of culture to resolve the issues of efficiency that resulted from standardization or yield to local consumer desires (Mooij & Hofstede, 2007). Effective advertising makes consumers the primary objective, and as stated by Mooij and Hofstede (2007), cultural values shape consumers' personalities. Mooij and Hofstede (2007) agreed that there was no universal advertising model and offered some valuable suggestions through cultural dimensions configuration to improve the research hypotheses.

Power distance is not only about power being unequal between people, but it also spells the distinction between classes of people, therefore, the need for luxury brands to demonstrate status in high power distance cultures (Mooij & Hofstede, 2007). combining masculinity and individualism produces success, which means that masculinity does not go well with collectivism since masculinity emphasizes personal achievement (Mooij & Hofstede, 2007). Taking risk is the way of innovation which is very low in uncertainty avoidance culture, but in combination with high PD, it will encourage innovation leading to modernity, therefore, status (Mooij & Hofstede, 2007).

Culture and Technology

The influence of culture on the widespread adoption of social media in the operation of rural businesses was the focus of the research conducted by Lekhanya (2013). In the study, the author intends to uncover the cultural factors responsible for the adoption and use of the modern communication system in KwaZulu-Natal (KZN), a rural community in South Africa. Lekhanya (2013) interviewed 175 business owners/managers and had them complete survey questionnaires. The author applied a mixed method of qualitative and quantitative techniques. Business models had become highly complicated, and consumers were subjected to influences from many sources, including word-of-mouth communication (Lekhanya, 2013), which would drive the adoption and diffusion of the prevalent technological platform to improve competition.

Lekhanya (2013) argued that culture could be an engine that drove innovation on the one hand. The other could stifle innovation by spreading fear, lack of knowledge, and different cultural beliefs counterproductive to free thinking. Cultural norms and beliefs

played essential roles in people's decisions to use new technology, 51 percent strongly agreed with the statement, and 23 percent agreed (Lekhanya, 2013). The exact number of respondents subscribed to the opinion that social media technology was not trustworthy. Prompting the conclusion arrived by Lekhanya (2013), culture affected the diffusion and adoption of technology in society. It recommended training at the local level to encourage local businesses and residents to feel free to engage in the social media revolution.

The word digital divide refers to the difference between nations with unrestricted access to the internet and those without (Nath & Murthy, 2004). Many factors may contribute to the technological disparity between nations to the exclusion of culture. Still, Nath and Murthy (2004) saw that argument as incomplete as nations with high uncertainty and masculinity index seemed slow to adopt new technology, thereby lagging the more progressive cultures. The authors assessed that there was extremely little research that focused on the role of culture in adopting the Internet and their research was an attempt to fill that gap. Nath and Murthy (2004) chose five of Hofstede's cultural dimensions, power distance, individualism versus collectivism, uncertainty avoidance, masculinity versus femininity, and long term versus short term orientation, for their research.

The data used in the research by Nath and Murthy (2004) were secondary data obtained from The Global Information Technology Report 2001 – 2002, The Global Competitiveness Report 2001 – 2002, and a few other sources for accuracy. In addition, the authors included the following technological, economic, and political variables to contribute to the Internet adoption rate.

The findings showed that uncertainty avoidance and masculinity negatively affected the Internet adoption rate (Nath & Murthy, 2004). The empirical evidence showed that national culture significantly affected any other factors cited as the primary sources of the problem (Nath & Murthy, 2004).

The influence of culture in Executive Information Systems (EIS) was the research undertaken by Leidner, Carlsson, and Elam (1995). The application of information systems and communication technology is not uniform across cultures, necessitating better studies to understand how to implement them in other cultures (Leidner et al., 1995). The authors drew attention to Group Decision Support System (GDSS), an example of technology applicable in some countries and not others, China.

Leidner et al. (1995) surveyed EIS users in the United States and Sweden on how each used the system, decision-making styles, and the type of outcome they experienced. The comparisons used Hofstede's four cultural dimensions: Uncertainty avoidance, individualism, power distance, and masculinity. The authors based their hypotheses on the four cultural dimensions. Contacts were 29 US and 20 Swedish organizations to distribute surveys, and respondents were from 22 US and 20 Swedish organizations. Out of 450 surveys distributed, 200 returned the survey.

Country effects on EIS use were significant as Americans operated under higher time pressure than Swedish executives (Leidner et al., 1995). Information availability and perceived competition were the same for the two countries. Still, significant cultural differences were evident in how EIS was used: Swedish executives used it mainly to analyze data and evaluate decisions, while Americans used it primarily to monitor (Leidner et al., 1995). The American executives experienced an increase in problem identification and the Swedish executives. The Americans also experienced a rise in decision-making, but decision-making for Swedish executives was slower (Leidner et al., 1995). The findings lead to the conclusion by Leidner et al. (1995) in the comparison of the two countries on the use of EIS that culture did play a vital role as the perceived expected outcomes were different.

Culture and Job Performance

Oghojafor, George, and Owoyemi (2012) attempted to investigate the impact of culture on the function of corporate governance. Corporate governance was instituted to protect stakeholders' interests in the organization they studied, and every corporate officer had to promise to execute such governance to the letter (Oghojafor et al., 2012).

Data used for the paper by Oghojafor et al. (2012) came from secondary sources showing the beginning of economic democracy in Nigeria. The authors used the case study done on Cadbury (Nigeria) Plc. They chronicled the company's history as a division of Cadbury Pty. Ltd., United Kingdom, from its establishment to the accounting irregularities that brought focus to the practices of division executives. Investigation into business practices uncovered some corrupt practices. The Personnel Manager employed his relatives and people from his clan, which resulted in loyalty to him. The Managing Director/Chief Executive Officer overstated the businesses financial health, and employees who knew about the corrupt practices were afraid that the organization would not survive. Employees knew all

the details but had no avenue to express their feelings (Oghojafor et al., 2012). In a high PD culture, the people at the top declare themselves gods by their positions, and those at the bottom would not present any challenge (Oghojafor et al., 2012). Oghojafor et al. (2012), in an interview, asked 20 Nigerian employees of Cadbury (Nigeria) Plc the following questions: 1. "Do you fear your manager or respect him/her? " 2. "Do you disagree with your managers? " The 20 respondents stated that they feared and respected their managers and had no reason to disagree with their managers. Their answers were quite different from those of British origin working for Cadbury Worldwide UK. In the research, the significant result was that poor job performance in a high PD culture was possible when the people at the top were culpable in criminal acts and unaccountable.

Aluko (2003) had four objectives when he decided to study the impact of culture on organizational performance: cultural variables responsible for high performance, discern the nature of the relationship between culture and performance, find other variables that may be contributors, and determine the combined effects of culture and other variables on performance. Unfortunately, there has been minimal research on the impact of culture on performance. By extension, very little about Nigerian culture and its effect on performance is available (Aluko, 2003).

Data for the study came from both qualitative and quantitative methodology, which involved interviews, observations, and survey questionnaires (Aluko, 2003). The total number of respondents in the author's research was 630 from three textile mills in three regions. Those interviewed were personnel managers, customers, and owners/shareholders. Documents accessed included annual reports, accounting records of the past five years, and other relevant materials (Aluko, 2003). The culture was used as an independent variable, performance as the dependent variable, and to minimize error, multiple indicators served as measures of the concepts (Aluko, 2003).

There was significant empirical evidence revealed in this research by Aluko (2003), and they were as follows:

- Workers showed positive attitudes toward work.
- Lateness, absenteeism, and labor turnover were very rare.
- Personal commitment to work was high.

- Power, wealth, and prestige were achievements that caused the workers to strive more at work.

A culture of hard work and excellence as a part of responsibility and respect was well expressed by one of the tribes in Nigeria – "work is the antidote of poverty" (Aluko, 2003).

The author showed through his research that in the Nigerian society, with differences in the local culture based on the three largest ethnic groups, the Yoruba, the Hausa, and the Igbo, there were no significant differences in their work performances. They all were highly productive, even with limited or non-existent technology resources. Although his findings were not in the field of information security policy, comparison to information security policy compliance is obvious; the effect of culture about obedience to rules would apply to any discipline.

Culture and Business

Two people from different cultures in any business have to communicate with and understand each other. The way to accomplish that, their messages have to be decoded correctly, and it is an essential factor in marketing (Rosenbloom & Larsen, 2003). The question then is how do variations in national culture dictate communication protocols (Rosenbloom & Larsen, 2003)? In an attempt to answer the question, Rosenbloom and Larsen (2003), understanding that culture affects human behavior, referred to Hofstede's cultural dimensions while relying on Hall's version of cultural differences.

Rosenbloom and Larsen (2003), in their research, divided culture into two types, low-context (LC) and high-context (HC). The low-context culture expects every communication wholly expressed and explicit with nothing left out and on the contrary high-context culture only requires implicit transmission where inference is essential. They also explained the concepts of small and large cultural distance; if members of LC or HC cultures communicate with members in similar LC or HC cultures, they are in a small cultural distance situation. The alternative is the opposite, which is a large cultural distance situation. The authors hypothesized the following about business communications based on the distinction between the two cultural contexts:

- Expect a high frequency of fax communication when the cultural distance is large,
- Telephone communication increases when the cultural distance is large.

- E-mail communication increases when the cultural distance is large; and
- Business letter writing increases when the cultural distance is large.

A survey conducted the research; out of 250 firms contacted, 60 responded, and out of the 60, 54 were used for the analysis as six survey questionnaires were incomplete (Rosenbloom & Larsen, 2003). The respondents were 35 from HC cultural context countries, and 19 were from LC culture countries, and one of those 19 was the United States. The survey used a five-point Likert scale to indicate the frequency of communication for four weeks (Rosenbloom & Larsen, 2003).

Fax communication in both directions when the cultural distance was large was above 70%. For small cultural distance, the US and another LC country's fax communication ranged between 30% and 41%, respectively. The hypothesis was supported (Rosenbloom & Larsen, 2003). Telephone communication was supported: phone traffic was 40% from the US and 34% from the distant partner compared to 12% and 18% between the US and another LC culture country (Rosenbloom & Larsen, 2003). E-mail communication increased on the small cultural distance partners instead of large cultural distance partners; the hypothesis was not supported. Business letter writing was also not supported. The significance of this study was that conducting business across cultures requires knowledge of how each culture operates.

In a global reach, businesses serve themselves well by deploying expatriates who are the product of the home culture where business branches are established. An example would be sending a Chinese trained in the United States to China (Brock, Shenkar, Shoham, & Siscovick, 2008). Therefore culture features in multinational corporation decision making (Brock et al., 2008).

The impact of culture on business organizations was the objective of the research by Aigbomian and Oboro (2015). Understanding international culture in business is vital since it determines whether the company will progress or fail; therefore, business practices reflect the culture of the nation where that business is established (Aigbomian & Oboro, 2015). The global nature of companies means that one standard does not fit all as management has to be sensitive to different practices of other nations (Aigbomian & Oboro, 2015; Hofstede, 1994). An international business has to deal with two different types of cultures, national and organizational. Membership is permanent in national and voluntary in an organization (Hofstede, 1994), meaning that if an employee leaves an organization, he/she

will have to take up membership in a new organizational culture while remaining true to the national culture.

Barring other conditions that may affect productivity, Nigerian national culture has consistently contributed to performance improvement (Aigbomian & Oboro, 2015). An international business system of management has to be adaptive in its practices taking into account the location of each branch as it seeks to extract maximum benefit from the employees (Aigbomian & Oboro, 2015; Hofstede, 1994).

Culture and Security

This paper is a study by Dols and Silvius (2010) on national culture as one factor influencing information security non-compliance. Data protection is a serious venture that has not yet been under control despite the measures tried; it is reasonable to look at another approach (Dols & Silvius, 2010). There are many sources of security threats to businesses, and some have human components, which could be carelessness or flagrant disregard for instruction (Dols & Silvius, 2010).

The authors adopted Hofstede's cultural dimensions to explain the national culture and surveyed one of the Big Four accounting firms in The Netherlands and Belgium. People from The Netherlands are characterized as having medium IDV, low PDI, medium to high UAI, and medium to high MAS. Belgian people are described as having high IDV, medium to high PDI, high UAI, and medium MAS (Dols & Silvius, 2010). They distributed 653 surveys, 361 in The Netherlands and 292 in Belgium, and 246 were completed (Dols & Silvius, 2010).

Dols and Silvius (2010) research on the influence of national cultures on non-compliance behavior resulted in some noteworthy findings:

- The Dutch were likely to disobey rules if they did not understand them. Well explained rules and the consequences of violations helped to mitigate the problems.
- A Belgian would readily obey a partner or a manager if requested to bend IT security rules contrary to what a Dutch would do. Comparing them, The Netherlands had low PDI, and Belgium had a high PDI. The best solution to this problem was to have managers involved in the IT security program understand the perils of such a request.

- In both countries, employees would sometimes transport data in an unsecured manner using a USB. Security policies may not have emphasized the risks as a part of the awareness Program.
- Employees from both countries were willing to correct colleagues on security issues. They both score medium on IDV.
- There was no difference in the question of masculinity.
- Companies in a country with low UAI will more likely see their policies or rules challenged. This assertion is confirmed with The Netherlands employees as their UAI was low compared to Belgium's high UAI.

The structure of information awareness training does not include cultural factors related to people from diverse backgrounds (Kruger, Drevin, Flowerday, & Steyn, 2011). There is no successful information security plan without proper controls, and humans play an integral part in that control (Kruger et al., 2011). Human involvement calls into question knowledge and behavior appropriate for the task (Kruger et al., 2011). This paper intended to extend the traditional awareness program to include cultural factors of people from different backgrounds. Understanding individual and group behavior should improve the management of information security. The primary intended outcome of the research was to establish if cultural differences among university students affected how they understood information security (Kruger et al., 2011).

Kruger et al. (2011) suggested that if a person did not elaborate on information security terms, such a person was susceptible to cybercrime. To assess the information security knowledge of university students, Kruger et al. (2011) administered a vocabulary test based on the following cognitive skills:

- Knowledge of facts, how to process them, and how they are related.
- Know when to apply the right processes and concepts; and
- use proper reasoning ability.

The breakdown of the questionnaire consisted of two sections: The first section was on general security questions, for example, spam, virus, and phishing. The second section questions were scenario type to assess behavior and reasoning ability. There were biographical questions for the respondents to complete, which helped inform cultural diversity

in information security awareness. They experimented with two South African universities, and 180 responses were received (Kruger et al., 2011).

The general findings were that the respondents had good knowledge associated with threats linked to e-mail. They understood what constituted a strong password and the meaning of hacking (Kruger et al., 2011). However, more than half the students did not understand the term "security incident," and almost half did not know the meaning of social engineering. Furthermore, the concept of phishing was foreign to 40% of the students, while 64% did not understand the word vishing (Kruger et al., 2011). The cultural factors that influence information security awareness, the findings were as follows:

- the indigenous language of the student;
- the high school attended by the student, whether private or government;
- the number of years the student had access to a computer; and
- the field of study and the gender of the respondent.

The most significant cultural factors affecting information security awareness was different language groups (Kruger et al., 2011). Based on their findings, the authors concluded that security awareness programs should include the cultural difference of indigenous languages when preparing students to enter the world of information security.

Sanctions and ISP Compliance

Herath and Rao (2009) argue that organizational information security goes beyond technology, processes, and people to include the behaviors of end-users. Factors that influence end-users behaviors were the focus of Herath and Rao's (2009) research. They explored the effectiveness of employee's actions, the role of penalties, and social pressures from subjective and descriptive norms. Computer security policies have become the de facto method to control behaviors that cannot be controlled through technology (Herath & Rao, 2009a).

The data collected for this research by Herath and Rao (2009) came from 77 organizations and 312 employees from those organizations were respondents. The authors proposed the following hypotheses:

- The understanding that there will be severe punishment and the certainty of being detected will be positively associated with the intention to comply with the organizational ISP.

- The pressure exerted by subjective norms – the expectation to do what is right and descriptive norms – observation of the actions of other employees will be positively associated with the intention to comply with the organizational ISP.
- The understanding that security behavior will be beneficial will be positively associated with the intention to comply with the organizational ISP.

One of the key findings of this research was that the severity of the penalty undermined the intention to comply with organizational ISP. The understanding that there was a certainty of detection had a positive effect on the intention to comply with ISP. In the case of social pressures, subjective and descriptive norms had positive effects on the intention to comply with organizational ISP. Security behavior was also beneficial and had a positive influence on the intention to comply with organizational ISP (Herath & Rao, 2009a). Based on the above findings, Herath and Rao (2009) suggested that penalty or severity would negatively impact compliance and generate hostilities toward the organization, making it counterproductive. On the contrary, Myyry, Siponen, Pahnila, Vartiainen, and Vance (2009) argued that people who were certain of the consequences for security violations would usually choose to comply with the organization's ISP. The conclusions reached had not provided insights into why people might not be persuaded by the certainty of penalty but by detection.

Moral Beliefs

Religious beliefs and ethical behaviors are factors that have been rarely investigated in connection with information security policy compliance (Al-Omari et al., 2013; Borena & Bélanger, 2013). According to Borena and Bélanger (2013), religiosity is the belief in a higher power that can inhibit behaviors that are counter to societal norms. Al-Omari et al. (2013) explain ethics as a reach into the concept of morality, the understanding of morality means upholding standards and rules that conform to expected societal norms.

Al-Omari et al. (2013) collected data from banks in Jordan to test their proposed hypotheses:

- An employee's moral obligation positively affects the intention to comply with organizational ISP.
- An employee's ethical egoism negatively affects the intention to comply with organizational ISP.

The findings were that an employee's moral obligation took precedence over every other feeling to violate organizational ISP. Ethical egoism would always result in the employee satisfying self-interest, therefore, violating organizational ISP (Al-Omari et al., 2013). In conclusion, Al-Omari et al. (2013) argued that ISP compliance was an ethical behavior prompting guilty feelings when highly moral employees acted contrary to set policy.

Borena and Bélanger (2013) argued that actions taken by users including non-compliance were rational in the value-based compliance model. The authors asserted that values and religiosity had a very strong relationship, leading to the following hypotheses: Religiosity will positively affect ISP compliance intention. Religiosity will positively influence attitude. Finally, religiosity will positively affect the relationship between conservative values and ISP compliance intention. The proposed hypotheses were tested using survey questionnaires distributed to 215 students; 120 completed questionnaires were returned.

The findings supported the hypothesis that religiosity positively affected the relationship between conservative value and ISP compliance intention. Religiosity positively affected attitude, affecting ISP compliance intention (Borena & Bélanger, 2013). In most cases resulting from religious upbringing or affiliation, moral beliefs affected employee's behavior toward ISP compliance (Borena & Bélanger, 2013).

Benefits of Compliance

Information security policy compliance is not a choice. That is what an organization's management gets across to all employees. There are severe consequences for failure, but employees may decide on their own to comply with the policy or not, which means they have to consider the cost or benefit of such decisions. Bulgurcu, Cavusoglu, and Benbasat's (2010) investigation was conducted to shed light on the perceived benefit of compliance based on rationality-based beliefs with roots in rational choice theory. The authors found three definite outcomes related to RCT: understanding the benefit of compliance, awareness of the cost of compliance, and what the cost would be for noncompliance. The perceived benefit of compliance is what an employee sees as a favorable outcome for complying with ISP. The expected cost of ISP compliance could be a form of inconvenience to an employee. For example, compliance takes extra time to comply, the cost of noncompliance is unfavorable outcome (Bulgurcu et al., 2010). An employee's attitude

toward compliance with ISP is positively affected by perceived benefit, negatively affected by the perceived cost of compliance, and positively affected by perceived consequences of noncompliance (Bulgurcu et al., 2010).

The findings were significant as they support the three hypotheses. Employees derived some satisfaction from knowing that they have contributed to protecting the organization's information by complying with ISP, which led to some intrinsic benefits (Bulgurcu et al., 2010).

Vance and Siponen (2012) argued that perceived benefits, in sharp contrast to Bulgurcu et al. (2010), positively affected a person's decision to violate rules or policy as predicted by RCT, indicating that the person derived a certain gratification from such action. They used a hypothetical scenario used in criminology to let respondents reveal undesirable behaviors in a nonthreatening environment. The authors' first step was to solicit from 111 IT professionals the common ISP violations known to them. From 54 respondents, the three listed were "(1) sharing and writing down password, (2) failing to lock or log out of workstations when not in use, and (3) copying sensitive data to unsecured portable USB storage devices." The second step was to design scenarios based on those violations. Vance and Siponen (2012) collected data from two sources, a high-tech service company and a bank in Finland. Both had security policies and sanctions in place, which is one the reason they were chosen.

The hypotheses that formal and informal sanctions had significant negative effects on the intention to violate ISP were not supported (Vance & Siponen, 2012b). On the other hand, moral beliefs were more than likely to have significant negative effects on ISP violation intention, and the finding on moral beliefs was supported (Vance & Siponen, 2012b). Intention to violate ISP involves weighing the consequences resulting from sanctions and the potential benefits derived from a violation, indicating that perceived benefits significantly affect violation intention (Vance & Siponen, 2012b).

The perceived benefit of ISP compliances was one of the factors investigated by Kadir et al. (2017) and posited a positive correlation between the perceived benefit of compliance and compliance behavior. Tests conducted by the authors confirmed the correlation between benefit and behavior. In contrast to Vance and Siponen's (2012) finding

that perceived benefit would promote ISP violation, Kadir et al. (2017) stated that perceived benefit would lead to compliance.

Behavior and Information Security

Certain behaviors run counter to ISP compliance. Some of them are well known: password sharing, not following correct procedures by taking shortcuts, visiting wrong websites, and downloading potentially harmful materials from the internet (Alfawaz et al., 2010). Some may believe that security is the function of the Information Technology personnel. Therefore they view ISP compliance as an intrusion into their everyday work routines (Alfawaz et al., 2010). To violate ISP, some employees may resort to the reasoning that their actions are not serious, that everybody does it, and that it is their first time, basically making excuses to justify their actions (Kim et al., 2014). ISP materials should take full advantage of employees' culture to maximize their effectiveness, resulting in maximum compliance behavior (Bada, Sasse, & Nurse, 2015). A perfect behavior changer is when ISP is mandatory. In such a case, the management will have to vigorously enforce the policy by making it known to employees that they are being monitored (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). In a cross-cultural investigation, participants from France exhibited the most secure behavior.

In contrast, participants from Asia behaved less securely, and in that investigation, confidence proves to be more significant than knowledge in promoting better safe behavior (Sawaya, Sharif, Christin, & Kubota, 2017). Chua, Wong, Low, and Chang (2018) stated that demographic characteristics such as age, working industry, and education level significantly affected awareness and behavior toward ISP compliance. D'Arcy et al. (2009), in their investigation, contradicted some of the other researchers in asserting that the general deterrence theory (GDT) considering perceived severity (PS) and perceived certainty (PC) of sanction impacted ISP compliance. Herath and Rao (2009), in their findings, discovered that the severity of the penalty had a negative impact on ISP compliance, while certainty of detection and social pressure were more effective at preventing ISP violations.

Descriptive Norms

Descriptive norms are the feelings that other people may be performing the behavior in question (White, Smith, Terry, Greenslade, & Blake, 2009). They are regular events with positive results that motivate a person to act appropriately (White et al., 2009).

Descriptive norms depend on what people we trust or affiliate with do, which signals that it is appropriate and can also do it (Rivis & Sheeran, 2017). Descriptive norms did not influence attitude, behavioral change, or behavior (Smith & Louis, 2009); they speculated that the results could be based on sources considered and different levels of measurements for the research. Though they did not directly affect descriptive norms, they argue that descriptive group norms play a moderating role in injunctive group norms. Interaction between descriptive norms and injunctive norms resulted in group attitudes change, behavioral willingness, and behaviors (Smith & Louis, 2009). Norman, Clark, and Walker (2005) took surveys of soccer and hockey fans to study their behaviors toward opposing teams. Their findings were that descriptive norms had a significant impact on the amount of variance explained in intention scores and injunctive norms had nothing to do with the result. In agreement with some of the researchers, they found that descriptive norms would track behavior and not attitude.

Merhi and Ahluwalia (2019) reviewed several research publications to find that intention to comply with information systems security (ISS) policies has always been the dependent variable, decided to change that position. They reversed that and developed a model which showed moral and descriptive norms as mediators between punishment and resistance. The authors hypothesized that "descriptive norms for violating ISS policies positively related to the moral norms of ISS policies compliance" and "descriptive norms for violating ISS policies are negatively related to employees' resistance of ISS policies." They analyzed data from 133 professionals from 10 organizations. They found that descriptive norms were that the descriptive norms for violating ISS policies positively related to moral norms, and the direct impacts of descriptive norms on resistance to ISS policies were minimal.

Normative Beliefs

Rousseau (1990) investigated normative beliefs in fund-raising organizations based on two hypotheses: (1) that security-oriented beliefs negatively impact both fund-raising success and staff job attitudes, and (2) that team-work-oriented norms had a positive effect on staff attitudes. The hypotheses were confirmed, and the reason for security-oriented beliefs was scarce resources; therefore, staff units could not interact. The author characterized what happened as dysfunctional normative beliefs. In the final assessment, normative beliefs

and the organization's performance are linked (Rousseau, 1990). Claudia (2012), meanwhile, found direct and moderating effects of normative beliefs on online buying. In their study, normative beliefs affected the decisions to buy online, and referent groups strengthened the online buying decisions. One of the hypotheses proposed for online shopping was that people were influenced by those they believed were important and felt the need to fit in (Eri, Aminul Islam, & Ku Daud, 2011). Analysis of their data indicated support for their hypothesis.

Barlow, Warkentin, Ormond, and Dennis (2018), in their research on information security compliance, asserted that normative communication positively affected employees' decision not to violate information security. The proposed communication was based on the belief that employees used other people's actions to guide their behaviors; the communication would motivate employees to comply when they thought others were complying (Barlow et al., 2018). The hypothesis was not supported, though some research they cited indicated the opposite effect of normative beliefs. Subjective norms will positively impact information systems security policy (ISSP) compliance (Ifinedo, 2014), and the model for the investigation had other variables. His study involved 124 responses that he analyzed to confirm that subjective norms positively affected ISSP compliance. The hypothesis that a stronger ISP compliance norm will lead to a stronger behavioral intention to comply was confirmed after an analysis of data from 148 respondents. (Hu, Dinev, Hart, & Cooke, 2012).

Self-efficacy

Information security cannot be brought under control if the users do not have the proper knowledge or skills to ward off threats (Hameed & Arachchilage, 2018). Self-efficacy is a significant component of information systems security (Hameed & Arachchilage, 2018). Choi, Levy, and Anat (2013) investigated the role of self-efficacy, cybersecurity skills, and other variables on computer misuse. They pointed out that 60% of organizations' computer crimes are insider attacks. Their primary findings were that cybersecurity skills mediated monitoring reduced misuse intention and computer self-efficacy influence. Yoon, Hwang, and Kim (2012) explored factors that influenced students' behaviors in information security with the desire to confirm that self-efficacy affected students' information security behavior. They analyzed survey data from 202 students from a South Korean university and produced the following finding. Self-efficacy had a strong effect on student's intention to practice information security. Chan, Woon, and Kankanhalli (2005) investigated the

perception of information security at the workplace, intending to show that perception and self-efficacy promoted information security best practices. They performed analysis on survey data from 104 respondents. They found the following outcome: employees who perceive that other employees, including management, practiced safety in combination with their self-efficacy would exhibit positive information security behaviors. Pham, Brennan, and Furnell (2019) studied the factors that contributed to information security compliance burnout and hypothesized that security self-efficacy had a negative effect on information security compliance burnout. They conducted a survey that resulted in 443 participants, and their data analysis did not confirm their hypothesis.

Theoretical Background

Merriam-Webster., n.d. defines a theory as "a plausible or scientifically acceptable general principle or body of principles offered to explain phenomena." Theory can be explained in terms of vitamins: some people consume them in excess, and some take just take enough to do some good, but no one can live without them (Collins & Stockton, 2018). A practical sense theory is needed to have an informed discussion on important topics, such as topics in information security policy (Kawulich, 2009).

Rational choice theory, first developed in criminology, has been applied by Hu, Xu, Dinev, and Ling (2011) in information security to determine if deterrence could reduce ISP abuse. Protection motivation theory which resulted from research in psychology has been adopted by many researchers in ISP, such as Herath and Rao (2009b).

Protection Motivation Theory

Rogers (1975) understood fear appeal as a compelling motivator for avoiding adverse conditions by changing unsafe behaviors or engaging in actions that would prevent such harmful events. His protection motivation theory charts a path that originates from fear appeal and ends with the implementation of recommended mitigating strategies. First a fear appeal will provoke a thought pattern to assess the severity of the event, and the next step in the process is to analyze the probability of the event's occurrence. The last step is assessing the recommended remedy to ascertain its effectiveness, referred to as its efficacy (Rogers, 1975).

Rogers (1983) revision to the original postulates included persuasive communication and the following extensions:

- extensive statements about sources of information that begin the coping process.
- inclusion of additional mediating process; and
- providing extensive clarity on modes of coping.

Observations of what happens to others and verbal persuasion have been identified as sources of the cognitive mediating process (Rogers, 1983, p. 167). Much can be learned by observing what has happened to others, taking heed to verbal warnings, and even reflecting on past life events. The cognitive initiation process starts when information is received from environmental or intrapersonal sources.

Cognitive mediation consists of two processes: threat appraisal and coping appraisal. First, the cognitive process is assessed as maladaptive or adaptive, and the results of that assessment could lead to a decreased or increased response (Rogers, 1983). Second, in threat appraisal, a maladaptive response could be any form of behavior that generates a reward, intrinsic or extrinsic (for example, smoking or drinking excessively). The social benefits of some of the actions may lead to a decreased response, while adverse effects like health or family problems may increase the response. The mediated protective response could be attributed to a physiological change following the appraisal of the severity of the danger (Rogers, 1983).

The coping appraisal process involves assessing a person's ability to cope with imminent danger and overcome or avert it. The view is that increased probability of adaptive response is the equivalent of accepting that the recommended coping mechanism works and the person can successfully perform the coping response (Rogers, 1983).

In summary, maladaptive response and adaptive response follow different paths to protection motivation. A maladaptive response involves behavior that increases rewards, resulting in severe or vulnerable conditions, which will finally trigger a threat appraisal. On the other hand, an adaptive response first assesses the response efficacy followed by self-efficacy and then the cost of carrying out the recommended remedy leads to coping appraisal (Rogers, 1983). The theory was first applied to psychology and it has found acceptance in other disciplines, including information systems, more recently.

The underlying principle behind the protection motivation theory is a fear appeal (Herath & Rao, 2009b; Maddux & Rogers, 1983; Moody, Siponen, & Pahnila, 2018; Vance, Siponen, & Pahnila, 2012; Woon, Tan, & Low, 2005). If a person knows that there is

impending danger, the responsible action is to evade the danger by following a prescribed course of action. Maddux and Rogers (1983) proposed this theory in connection to a health problem, but it is also applicable to other disciplines, especially information security. The essential components of this theory are that information about impending danger invokes fear which in turn activates cognitive processes to the appraisal of the severity of the threat resulting in protection motivation. The assumption is that the individual can understand and respond to the threat in a manner that would resolve the problem effectively (Maddux & Rogers, 1983; Moody et al., 2018), which leads to the individual self-efficacy.

Herath and Rao (2009b) developed an integrated model encompassing protection motivation theory and deterrence theory to investigate ISP compliance. During their research, they evaluated the effect of organizational commitment on employee security compliance intentions.

Herath and Rao (2009b) preferred method for data collection was a web-based survey. Out of 690 organizations contacted, 120 expressed interest in participating in the survey, and 312 samples were obtained for the test. The four constructs under protection motivation theory tested were severity of security breach, the certainty of a security breach, security breach concern, and effectiveness of a person's action (Herath & Rao, 2009b).

The research indicated that it significantly affected their sense of security breaches when employees understood the severity of security threats. There was no security concern in terms of the certainty of security breaches. Employees viewed the impact of policy compliance on everyday job operation in the form of hinderance negatively. The perceived effectiveness of employee response positively affected behavior toward ISP compliance intentions. The employees understanding that their ISP compliance had positive effects or resulted in some type of benefit would encourage a positive attitude toward security policy. Response efficacy and self-efficacy were found to significantly impact the attitude of employees toward ISP compliance intentions (Herath & Rao, 2009b).

Vance, Siponen, and Pahnila (2012b) in research to motivate ISP compliance combined habit with all six protection motivation theory constructs. The three constructs of threat appraisal used were vulnerability, perceived severity, and rewards, and the coping appraisal constructs were response efficacy, self-efficacy, and response cost.

Their empirical study a web-based survey instrument that targeted a 500 employees organization in Finland, resulting in 210 completed returns (Vance et al., 2012b). Their approach was to design a hypothetical scenario-based event describing an action or decision after presenting respondents with questionnaires to assess their ethical/unethical behavior regarding information security. The scenario had to be validated by a panel of information security experts and information security managers before being released to the public. Some of the proposed hypotheses tested by the authors included the following:

- Vulnerability positively influences employees' ISP compliance intentions.
- Perceived severity positively influences employees' ISP compliance intentions.
- Rewards negatively influence employees' ISP compliance intentions.
- Response efficacy positively influences employees' ISP compliances intentions.
- Self-efficacy positively influences employees' ISP compliance intentions.
- Response cost negatively influences employees' ISP compliance intentions.

Vance et al. (2012b) Analyzed the survey data collected using SmartPLS 2.0 and their findings were as follows:

Habit towards ISP compliance had a significant impact on all the components of PMT. Vulnerability had no demonstrable effect on employees' ISP compliance intentions. The severity of threat to security had a significant effect on employees' ISP compliance intentions. Self-efficacy had a positive impact on employees' ISP compliance intentions. Rewards negatively impacted employees' ISP compliance: the reward, in this case, was based on maladaptive responses. Response cost negatively influenced employees' ISP compliance intentions since they viewed ISP as an intrusion that inconvenienced them if they were to adhere to it. Response efficacy significantly negatively impacted employees' ISP compliance intentions, which contrasted with the expected result since it was positively correlated with intentions ($r = 0.21$). Further tests revealed that both self-efficacy and perceived severity acted as suppressors for response efficacy and tested alone it had a positive effect on employees' ISP intentions.

Woon et al. (2005) Adopted five constructs from PMT in their research on security measures for home wireless systems. The understanding is that remote access to workplace networks to perform daily tasks has expanded security concerns to the home network or wireless systems. Employing survey as a research methodology, Woon et al.

(2005) collected data from 189 home users out of 215 respondents based on a 31-item questionnaire to test, evaluate and report on the adopted constructs.

The hypothesis that perceived vulnerability would be significant in the determination of behavior was not supported, leading to the explanation that a person may not be able to avert danger in the case of vulnerability (Woon et al., 2005). Self-efficacy was significant as it was linked to a person's knowledge and skill to enable security measures on the wireless system. Response efficacy was significant as a predictor of behavior as well as response cost. Perceived severity was a significant predictor of behavioral change in computer security, with the impact uniform compared to a discipline like healthcare (Woon et al., 2005).

General Deterrence Theory

Deterrence theory was initially proposed to explain criminal behavior and the effort to curb crime, as Bailey and Smith (1972) wrote on their research on punishment – its severity and certainty. They waded through several historical debates asserting that punishment did not reduce crime and found that critics of the death penalty pointed to homicide rates as evidence that there was no difference before and after abolishing capital punishment. Bailey and Smith (1972) explained the suggestion that the severity and certainty of punishment associated with deterrence theory as additive factors to represent punishment administered with certainty resulted in maximum deterrence. The inverse of that finding was thought to be true.

Bailey and Smith (1972) used secondary source data from every state in the United States for their investigation.

Three periods, 1950-1960, 1951-1964 and 1960-1964 were used to compute changes in the levels of certainty of punishment for each offense (Bailey & Smith, 1972). First correlation coefficients between severity and certainty of punishment during the same periods were calculated. Then another set of correlations was calculated between changes in levels of severity and certainty of punishment during the same periods. Tests of significance were not run since the researchers used of random sampling (Bailey & Smith, 1972).

Findings indicated that for certain offenses (example, assault, burglary, and larceny), the correlations were moderate for 1960 and 1964. Correlation coefficients were positive for rape, car theft, and homicide but the overall correlations were very low (Bailey & Smith, 1972). One very significant finding was that the severity and certainty of punishment

are inversely related in the case of capital punishment (Bailey & Smith, 1972). The more severe a punishment was, the less likely it was to be applied, allowing certain violations to thrive.

Straub and Weike's (1998) approach to deterrence used countermeasures and awareness training. Their whole argument was that abusive behaviors toward information systems could be thwarted by implementing information security measures. The authors enumerated some of those deterrent techniques, such as policies and guidelines on proper system use. However, they also realized that their recommended countermeasures included no enforcement provision leaving it for users to comply voluntarily. An awareness training program should also include the two important aspects of general deterrence theory, sanction certainty, and severity of the sanction.

Straub and Weike's (1998) set up comparative studies in two companies to examine two propositions: (1) that managers were not aware of the range of actions available to them to mitigate systems risk and (2) that managers exposed to well-researched planning techniques would include them in their risk mitigation processes. The studies involved interviews for 4 months followed by action research for 15 months. Their approach was to institute three intervention programs: The security planning phase, the security awareness phase, and the countermeasure phase. In the first phase, security planning was conducted to recognize security problems, perform a risk analysis, generate alternatives, and implement the plans to match the threat. The security awareness program was the education of management and professionals in the proper use of systems assets. The final phase was to develop a countermeasure matrix that entailed deterrence, prevention, detection and remedies (Straub & Weike, 1998).

One of the effects of the study and recommendations was the implementation of the programs and the company spent more effort in areas that yielded a long-term impact on security (Straub & Weike, 1998). In addition top management agreed unanimously to prosecute any employee who abused the system vigorously, and the effect of such action and others should provide feedback into the system (Straub & Weike, 1998). In conclusion, there was empirical evidence that practitioners would adopt tools generated from sound theoretical based research to implement security planning (Straub & Weike, 1998).

Hu, Xu, Dinev, and Ling (2011) researched the effect of deterrence of ISP violations that focus on sanctions. Citing 2008 Computer Crime and Security Survey data at the time of their research, 44% was insider abuse and 49% was due to virus incidents. Their research interest was to delve into human behavioral aspects of information security, use available theories to provide causal relationships and prescribe useful guidelines for security management mitigation.

Hu et al.'s (2011) data came from a survey of employees of five organizations in China. About 250 surveys were distributed, 227 were received and 207 were viewed as complete and useable. The analysis of the data was performed using SmartPLS.

The result pointed to the fact that people who intended to violate ISP would weigh the consequences, and the benefits of such a violation would tip the scale (Hu et al., 2011). The finding made it difficult to conclude that deterrence worked (Hu et al., 2011). They further tested certainty, severity, and celerity from deterrence constructs linked to the intention to comply with ISP to confirm or reject the previous finding on deterrence. Since the result was insignificant, the previous finding was accepted (Hu et al., 2011). Deterrence alone was not enough to dissuade the intention to violate ISP (Hu et al., 2011).

Rational Choice Theory (RCT)

Becker (1974) considered criminal law through rational choice theory and that individuals who intend to violate laws do so with a full understanding of the benefits they will derive. Paternoster and Simpson (2009) noted that the theory was first proposed for street crime and not corporate crime, but Rational choice theory (RCT), also known as Choice Theory, has applications in various disciplines, including sociology, psychology, and economics. According to Levin and Milgrom (2004), "rational choice is defined to mean the process of determining what options are available and then choosing the most preferred one according to some consistent criterion. " Thus, the choice would be viewed as optimizing a real-valued utility function (Levin & Milgrom, 2004), which results in maximum benefit.

Li, Zhang, and Sarathy's (2010) research involved the application of RCT to investigate deviant behavior concerning compliance with internet use policy (IUP) in an organization. They argued that users determined to violate IUP perform a cost-benefit analysis to assess any benefits derived from intrinsic or extrinsic motivation. One of the

hypotheses proposed in the research was that "perceived benefits of internet abuses had a negative impact on IUP compliance intention. "

The methodology for the research was by survey questionnaires and a total of 246 responses were analyzed using partial least squares (PLS) (Li et al., 2010). The analysis yielded a significant result that supported the hypothesis that if users could derive benefits from violation they would take advantage of it (Li et al., 2010).

Aytes and Connolly (2011), meanwhile, concluded a study to determine the reasons users who were aware of the consequences of insecure behaviors were engaged in such acts from the perspective of RCT. Some of these unsafe behaviors included failing to backup data, password disclosure and password sharing (Aytes & Connolly, 2011). The respondents claimed to be knowledgeable about safe computing practices and the consequences of violating them (Aytes & Connolly, 2011).

The authors designed their study based on three behavioral settings: password usage, email usage, and data backup. In the case of password usage, the central questions were how often they shared passwords with others and how often they changed their passwords. In the case of email, they wanted to know how frequently users opened email attachments without first checking them for viruses. Finally, the authors needed to understand how frequent users backed up data to mitigate data loss. The questionnaires were distributed to university students based on the knowledge that they had a fair understanding of computing systems and a total of 167 completed the survey.

Aytes and Connolly (2011) presented the respondents' ratings: 93% considered themselves knowledgeable, very knowledgeable, or expert on email, 69% on protecting against viruses, and 70% on the issue of defending against a computer crash. The significant finding in this research was that the knowledge the users acquired did not persuade them to practice safe computing, indicating that they chose to do what was expedient in this case (Aytes & Connolly, 2011).

Theory of Reasoned Action (TRA)

Fishbein and Ajzen (1975, p. 511) studied the relationship between intentions and behaviors and developed a model that showed the antecedent of behavioral intention that finally resulted in the behavior was the attitude a person had toward that behavior. Their framework showed beliefs about the outcome of the action which resulted in the attitude

toward the action, on the other component of that model normative beliefs that resulted in subjective norms, and how both branches combined to form an attitude. Attitude toward behavior led to acting on the behavior, as depicted in figure 2.1. Sideridis, Kaissidis and Padeliadu (1998) presented a slightly different model. In their model, belief strength, outcome evaluation, normative beliefs, and motivation to comply represented independent variables that pointed to intermediate variable intention, and intention indicated dependent variable behavior.

An example by Mykytyn and Harrison (1993) explained the process of decision-making applying TRA. A chief information officer (CIO) wanted to convince the president of an organization to develop and deploy a strategic information system (IS) for competitive advantage, which was the stimulus (Mykytyn & Harrison, 1993). The next phase of the process was to determine what the president believed the outcome of the decision would be and would proceed to evaluate several good and bad outcomes which would lead to his/her attitude about the IS project (Mykytyn & Harrison, 1993). The evaluation of the outcomes would be based on several factors, including contacts, experiences, or observations. The formation of attitude was only one component of the intention process; the other was subjective norms (Mykytyn & Harrison, 1993).

The subjective norm component might come from the board of directors, executive board, new project committee members, customers, and other employees. These different groups might be for or against the project and they made up the subjective norm component. The input provided by all the people involved resulted from normative beliefs and motives to comply in one way or the other (Mykytyn & Harrison, 1993). The president's intention will be known as he/she followed through, with the behavior (Mykytyn & Harrison, 1993).

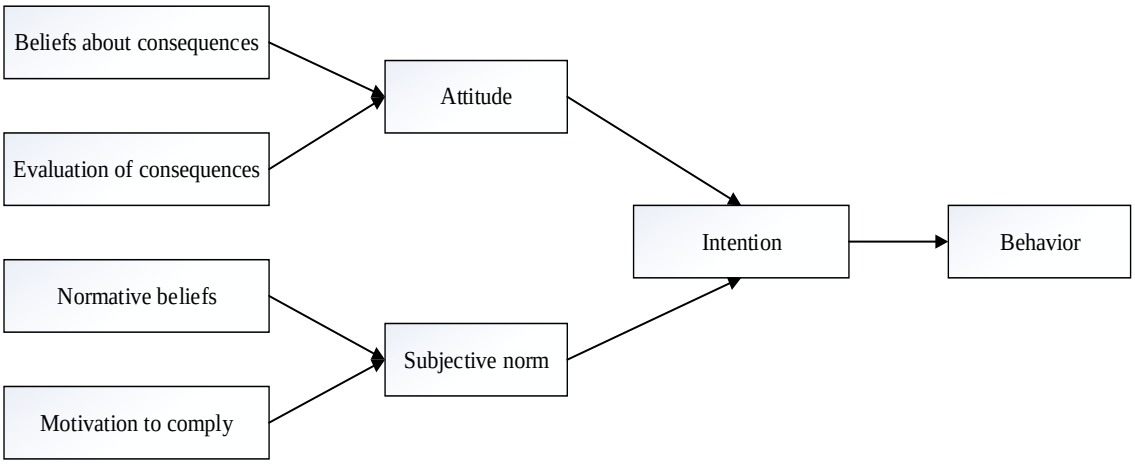


Figure 2.1 TRA (Fishbein & Ajzen, 1975)

Theory of Planned Behavior (TPB)

The theory of planned behavior is an extension of TRA, as depicted in figure 2.2 (Ajzen, 1991). The new construct is perceived control which consists of various components such as time, money, the right skills, and help from other people (Ajzen, 1991). Moody et al. (2018) argued that TPB simply underscores that self-efficacy is an important, positive attitude toward behavior, and norms are insufficient without the right skills.

George (2004) provided an explanation for TPB by studying internet purchases.

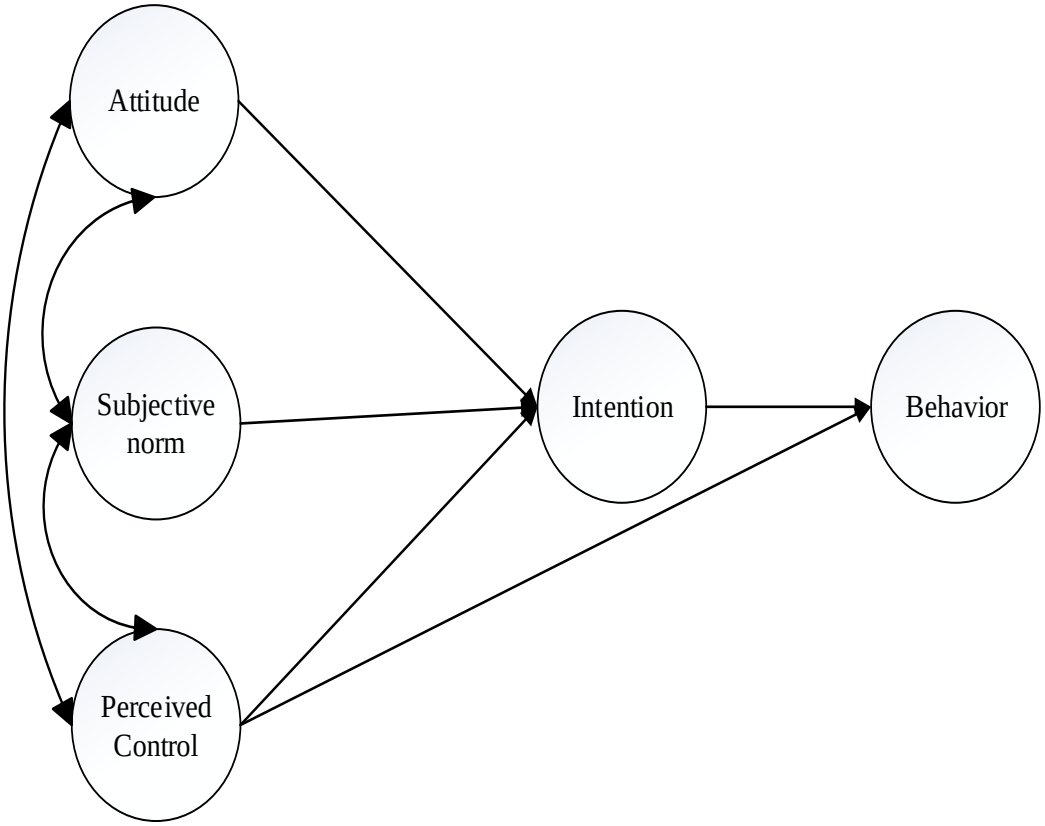


Figure 2.2 TPB (Ajzen, 1991)

(see figure 2.3). He based the research on TPB components to propose the following hypotheses.

- The belief in internet trustworthiness would influence internet purchasing.
- The unauthorized use of and sharing of personal information would negatively impact internet purchasing.
- Positive attitudes toward the internet would encourage online purchasing behavior.
- What important others think about internet purchasing should influence an individual's subjective norms about internet purchasing.
- Subjective norms should have a positive influence on internet purchasing.
- Positive self-efficacy of making internet purchases would influence perceived behavioral control on making internet purchases.
- Positive beliefs about behavioral control would encourage internet purchasing.

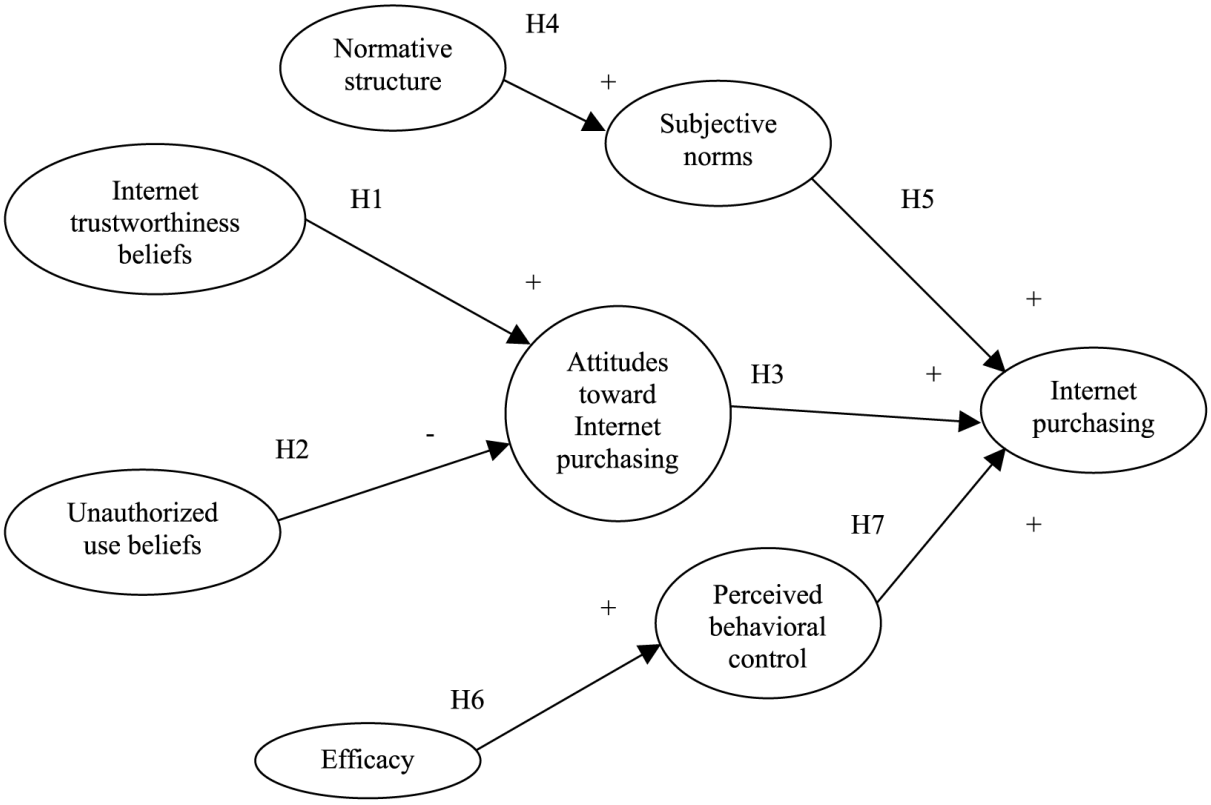


Figure 2.3 TPB Research Model (George, 2004)

His data came from 193 university students and yielded the following findings. Trustworthiness was more important than unauthorized use and sharing of personal information for internet purchasing. The following were supported, trustworthiness, attitude to purchase, normative beliefs to subjective norms, efficacy, and perceived control to purchasing; the remaining two components were not supported. His findings were like those of some other researchers.

Literature Search

Literature for the research came from several sources, Dakota State University Karl Mundt Library, IEEE, Google Scholar, CiteSeerX, Academia, ResearchGate, Mendeley reference management system. Initially, the search was limited to peer-reviewed literature but expanded to include conference papers cited in the extant literature and the date preference was mainly from 2000 to the present. The search included power distance in advertising, power distance in business, power distance and its moderating effects on employee empowerment, power distance, and organizational learning culture. The search was expanded to include culture in business, culture and technology, culture and job performance,

and culture and security. On reviewing the literature obtained, the search was further expanded to include factors that influence behavior toward information security policy compliance, descriptive norms, normative beliefs, and self-efficacy.

A search was conducted for theories that would apply to the research, including deterrence theory, protection motivation theory, the theory of planned behavior and rational choice theory. The theories originated from other disciplines, such as criminology, health, sociology, and psychology, and have since been adopted to explain events in information systems security.

Summary

The literature review paints a picture of the role of power distance and culture in every part of business, from communication to technology. The research is based on human behavior in the workplace and the proper instruments to employ are theories that focus on behavior. PMT, GDT, RCT, TRA, and TPB are very appropriate as they are based on criminology and psychology. The effect of power distance on advertising, employee empowerment, and education yielded significant findings. Culture is featured in business as a platform to explain the relationship between management, lower ranked employees, and job performance. Culture exposed different points of view in technology adoption and security.

The concept of behavior as it relates to information security policy is well-examined in the previous literature. Many constructs have been investigated as factors contributing to the problem, and but power distance has not been featured as one of those constructs. This research includes power distance as one of the constructs to bridge the gap.

Chapter 3 describes the methodology employed to collect and analyze the data, the research model, and the hypotheses development. The operationalization of the construct is also accomplished. The procedures used to perform the two main assessments must be satisfied to validate the research model are explained in this chapter.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

This quantitative research adopts a positivist philosophy, as it develops and validates an empirical model based on testable hypotheses to clarify the effect of power distance and related variables on employees' information security policy compliance. It is exploratory research, and the statement of the problem points out the gap in the studies done so far in ISP compliance, and the purpose of this research is to fill that gap. Furthermore, investigating the role of high-power distance in ISP compliance will help employers develop sensitivity to national culture and relate that to appropriate job assignments and security awareness training.

This research creates an opportunity for other researchers to study the role of power distance in information security in different organizations and countries.

Data Collection

The data collection method was survey instruments, which gathered extensive information and provided anonymity. The survey was distributed to employees in the South-Eastern part of Nigeria, with a very good representation of all the major ethnic groups in Nigeria. Employees in private and public organizations were targeted for participation. The measurement of the latent variables was on a 7-point Likert scale: (1) strongly disagree, (2) disagree, (3) somewhat disagree, (4) neither agree nor disagree, (5) somewhat agree, (6) agree, (7) strongly agree.

Population

The population for this research was the Nigerian working class employed by public and private business organizations that have ISP. Every member of an organization is responsible for the protection of that organization's information. The proper representation of the population was determined to be a random sampling of employees that would be ethnically diverse encompassing the major tribes in Nigeria. The choice of Nigerian

employees was made based on the country's high PDI and the best way to capture the effect of power distance was to collect samples from the country.

Population Sampling

The sampling process was based on the random distribution of survey questionnaires in a metropolitan city with a large concentration of businesses that employed people from every ethnic diversity. The proper approach was to seek consent from individuals, to participate in the survey which was strictly anonymous to comply with ethical standards. Bootstrapping, a resampling technique, differs from classical confidence intervals, that providing population parameter estimations (Chin & Dibbern, 2010; Goodhue, Lewis, & Thompson, 2012). It is also one of the functions of SmartPLS which is structural equation modeling (PLS-SEM) software. In the place of a confidence interval, bootstrapping was used in population parameter estimation.

Sample Size

Sample size estimation is one of the vexing problems in quantitative research, and guidelines must be adhered to for a study to be acceptable (Mccrum-gardner, 2010; Westland, 2010). Minimum size estimation is difficult; as Kock and Hadaya (2018) explained, if the researcher finds that the minimum size is not met, additional data must be collected. According to Hair, Hult, Ringle, and Sarstedt's (2017) rule of thumb, the minimum sample size should be minimally 10 times the number of independent variables. That was their initial suggestion but later revised to include the following: significance level, statistical power, minimum coefficient of determination (R^2), and the minimum number of arrows pointing at an endogenous construct in the PLS path model (pp. 24-26). Peng and Lai (2012) suggested that researchers should perform power analysis before estimating the required sample size and that the number of items for each construct should be increased. A researcher must know the sample size to attain the statistical power for the specified significance level and hypothesized effect size (Cohen, 1992). The sample size is directly proportional to the desired power and inversely proportional to the effect size and significance level (Cohen, 1992).

The computation results presented in figure 3.1 are based on the statistical power of 80% for different significance levels and R^2 values. The best approach to determining sample size was based on a table provided by Hair et al. (2017, p. 26), (see figure

3.1). A significance level is a cut-off point chosen before the data test, 5% for most research, that protects against accidentally rejecting the null hypothesis when it is true (Mccrum-gardner, 2010). Statistical power makes it possible to reject the null hypothesis when the alternative hypothesis is true (Mccrum-gardner, 2010). The minimum statistical power is 80%, signifying an 80% chance of detecting the difference of the specified effect size (Mccrum-gardner, 2010). The sample size for this research was based on the table in figure 3.1. The significance level of 5%, the minimum R^2 value of 0.25, and the value of 0.20 are considered high for behavior studies (Hair et al., 2017: p. 199). Seven independent variables, a statistical power of 80%, and the minimum sample size of 51 are shown below.

Exhibit 1.7 Sample Size Recommendation in PLS-SEM for a Statistical Power of 80%

Maximum Number of Arrows Pointing at a Construct (Number of Independent Variables)	Significance Level											
	10%				5%				1%			
	Minimum R^2				Minimum R^2				Minimum R^2			
	0.10	0.25	0.50	0.75	0.10	0.25	0.50	0.75	0.10	0.25	0.50	0.75
2	72	26	11	7	90	33	14	8	130	47	19	10
3	83	30	13	8	103	37	16	9	145	53	22	12
4	92	34	15	9	113	41	18	11	158	58	24	14
5	99	37	17	10	122	45	20	12	169	62	26	15
6	106	40	18	12	130	48	21	13	179	66	28	16
7	112	42	20	13	137	51	23	14	188	69	30	18
8	118	45	21	14	144	54	24	15	196	73	32	19
9	124	47	22	15	150	56	26	16	204	76	34	20
10	129	49	24	16	156	59	27	18	212	79	35	21

Source: Cohen (1992): A Power Primer. Psychological Bulletin 112: 155–159.

Figure 3.1 (Hair et al., 2017: p. 26)

Data Analysis

The collected data was analyzed using SmartPLS version 3.3.3 (Ringle, Wende, & Becker, 2015), suitable for analyzing small samples following some PLS application guidelines. The report should include the following based on the initial assessment of the PLS-SEM model for reflective measurement (Wong, 2013):

- The main endogenous variable variance
- The inner model path coefficient sizes and significance
- The outer model loadings and significance
- Indicator reliability

- Internal consistency reliability
- Convergent validity
- Discriminant validity
- Structural path significance in bootstrapping
- Variance inflation factor (VIF)

Participants' demographics were analyzed using descriptive statistics, showing type of organization, years at the present position, type of position, age, gender, and education.

Conceptual Model

The literature review points to the variables considered in the research, the effects of descriptive and subjective norms, penalty, coping appraisal in shaping behavioral intention as shown in the conceptual model in figure 3-2. Descriptive and subjective norms are internal forces that motivate a person to act in a way that satisfies moral and personal obligations (Doran & Larsen, 2016). The penalty is an external force that encourages conformity to rules and regulations (Herath & Rao, 2009a). A coping appraisal is a self-assessment of a person's ability to carry specific procedures to effectively counter a threat (Maddux & Rogers, 1983; Woon et al., 2005). The research also explores the relationship between all the constructs under planned behavior, rational choice theory, protection motivation theory, and deterrence theory, which should lead to ISP compliance intention as presented in the conceptual model in figure 3-3. Benefits of compliance, descriptive norms, and normative beliefs are placed under the theory of planned behavior; rational choice theory has moral beliefs and power distance; self-efficacy is under the protection motivation theory; formal sanction is under the deterrence theory. The constructs in combination should affect a person's behavior that would lead to ISP compliance.

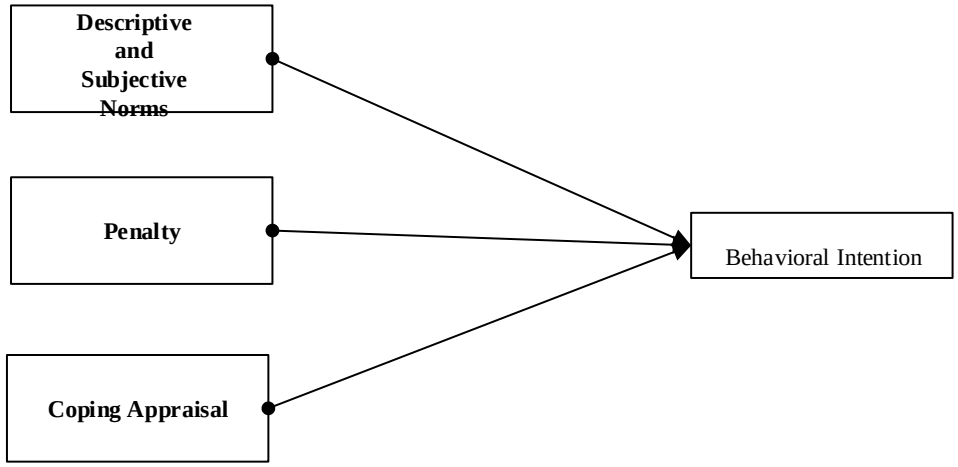


Figure 3.2 Conceptual Model 1

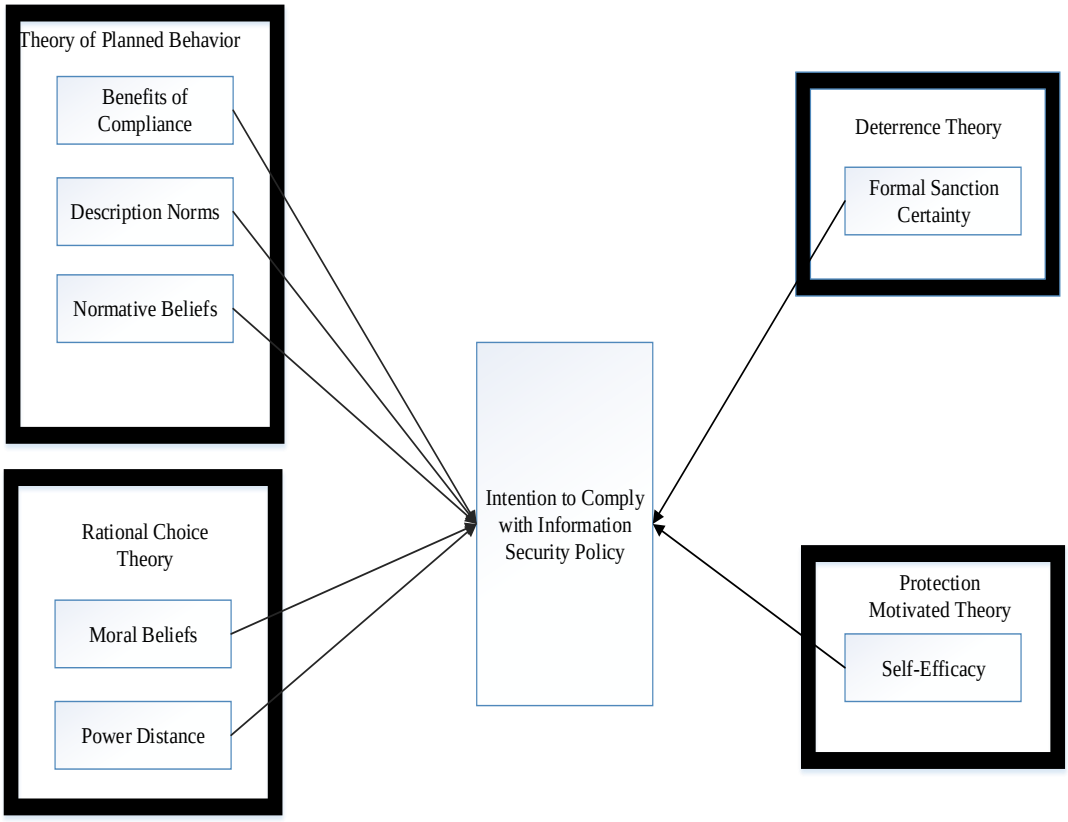


Figure 3.3 Conceptual Model 2

Research Model and Hypotheses

There are 8 constructs in the research, 7 of which are independent variables and one dependent variable (figure 3.4). Independent variables are Sanctions, moral beliefs, benefits of compliance, self-efficacy, descriptive norms, normative beliefs, and power distance. The dependent variable is the intention to comply. The research model used to find how the different constructs function together and the uniqueness of the model is the inclusion of power distance. However, based on based on searches that have been conducted power distance is not associated with ISP compliance research.

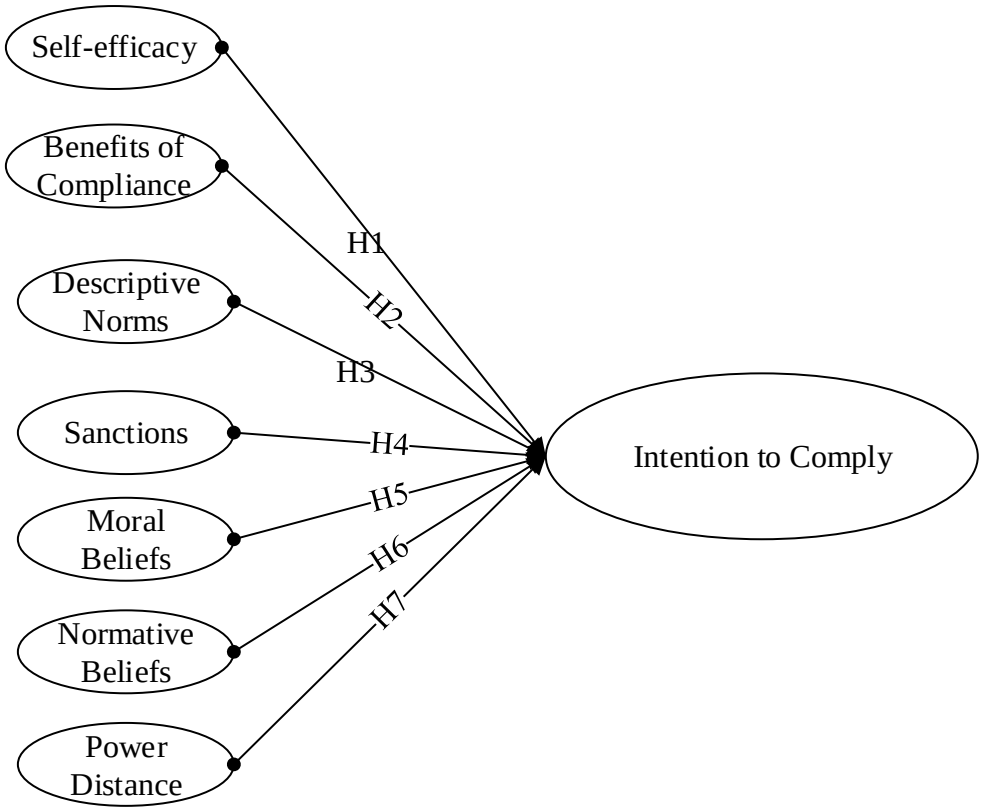


Figure 3.4 Research Model

Woon et al. (2005) Adopted five constructs from PMT in their research on security measures for home wireless systems. The understanding is that remote access to workplace networks to perform one's daily tasks has expanded security concerns to the home network and wireless systems. Employing survey as a research methodology, Woon et al. (2005) collected data from 189 home users out of 215 respondents based on a 31-item

questionnaire to test, evaluate and report on the adopted constructs. The hypothesis that perceived vulnerability would be significant in the determination of behavior was not supported, leading to the explanation that a person may not be able to avert danger in the case of vulnerability (Woon et al., 2005). Self-efficacy is an indication that a person has the capability and confidence to perform tasks, to protect an organization's information assets (Awofala et al., 2019; Bandura, 1977). Self-efficacy has a significant effect on employee's expected results from the use of information security, and the expectation depends on the level of self-efficacy (Compeau & Higgins, 1995). In a study conducted by Bandura (1977), self-efficacy positively correlates to a change in behavior. Information security issues require competence and confidence which come from self-efficacy. In other studies, self-efficacy is found to have a direct link to how an employee responds to assigned tasks, and information security (Ariff, Yeow, Zakuan, Jusoh, & Bahari, 2012; Bulgurcu et al., 2010; Herath & Rao, 2009a; Workman, Bommer, & Straub, 2008). Hence, we hypothesize that

- H1: Self-efficacy will positively impact employees' attitudes toward ISP compliance.

People seem to do things that bring some benefits and shy away from efforts that may negatively impact them. There are different types of benefits. One is being able to protect assets by using adequate security controls and, in the process be recognized (Blythe, Coventry, & Little, 2015; Bulgurcu et al., 2010). An example by Mykytyn and Harrison (1993) explained the process of decision-making by applying TRA. A chief information officer (CIO) wanted to convince a president of an organization to develop and deploy a strategic information system (IS) for competitive advantage; this was the stimulus (Mykytyn & Harrison, 1993). The next phase of the process was to determine what the president believed the outcome of the decision would be after evaluating several good outcomes and several bad ones, which would inform his/her attitude about the IS project (Mykytyn & Harrison, 1993). The examination of the outcome would be based on several factors, some of which could include contacts, experience, or observations. The formation of attitude was only one component of the intention process; the other was subjective norms (Mykytyn & Harrison, 1993). If employees feel that their work may be impeded and little benefit is derived from security requirements, they may violate ISP (Koloseni, Lee, & Lee, 2018). Considering an action, a person weighs the consequences of that action and determines to fully take

responsibility before engaging in it (Ajzen, 1991; Ajzen & Fishbein, 1975). Hence, we hypothesize that

- H2: Benefits of compliance will positively impact employees' attitudes toward ISP compliance.

Surrounded by colleagues who comply with ISP would prompt an employee to do the same. Descriptive norms are beliefs about other people's behaviors, good or bad (Forward, 2009; Goldsmith, Montford, & Goldsmith, 2014). Descriptive norms could be used as social control, letting society know that if most people are performing acts, everyone should be (Cialdini, 2007). As other behavior researchers have shown, this behavior is planned (Ajzen, 1991; Herath & Rao, 2009b). Hence, we hypothesize that

- H3: Descriptive norms will positively impact employees' attitudes toward ISP compliance.

Straub and Weike's (1998) approach to deterrence involved more countermeasures and awareness training. Their whole argument was that abusive behaviors toward information systems could be thwarted by implementing information security measures. The authors then enumerated some of those deterrent techniques, such as policies and guidelines on proper system use. They also realized that their recommended countermeasures included no enforcement provision leaving it for users to comply voluntarily. An awareness training program should also include the two essential aspects of general deterrence theory: sanction certainty and severity of the sanction. Sanctions, by their nature invoke the image of punishment in the minds of employees, whether tangible or intangible.

Hu, Xu, Dinev, and Ling (2011), in their research on the effect of ISP violation deterrence, found that companies tend to focus on sanctions. Citing 2008 Computer Crime and Security Survey data at the time of their research, 44% was insider abuse and 49% was due to virus incidents. Their research interest was to delve into human behavioral aspects of information security using available theories to reveal causal relationships and prescribe guidelines for the mitigation of security management. Punishment has a negative effect on employees' involvement in non-malicious information systems security deviant behavior (Ifinedo & Idemudia, 2017). Researchers have shown sanctions to effectively move

employees to ISP compliance (Bulgurcu et al., 2010; Pahnila et al., 2007a; M. Siponen, Vance, & Willison, 2012; D. W. Straub & Weike, 1998). Therefore, we hypothesize that

- H4: Sanctions will positively impact employees' attitudes toward ISP compliance.

Moral beliefs are concerned with making choices based on a person's beliefs indicating deliberate acts that could involve a choice between good and bad, (Al-Omari et al., 2013; Vance & Siponen, 2012b). Moral beliefs could be an impetus to do good or resist what people believe is evil, such as forming a neighborhood watch to prevent crime. Aytes and Connolly (2011) presented the respondents ratings: 93% considered themselves knowledgeable, very knowledgeable, or expert on email, 69% on protecting against viruses, and 70% on protecting against a computer crash. The significant finding in this research was that the knowledge the users acquired did not persuade them to practice safe computing, indicating that they chose to do what was expedient in this case (Aytes & Connolly, 2011). Moral strength is required to do what is right when a person may not feel like behaving that way. Rules are not for employees only; management should not set security rules and do the opposite (Siponen, 2000). Therefore, we hypothesize that

- H5: Moral beliefs will positively impact employees' attitudes toward ISP compliance.

Normative beliefs have been assessed primarily by considering the pressures exerted at the workplace by colleagues, managers, (Ajzen, 1991; Ajzen & Fishbein, 1980; Bulgurcu et al., 2010). The extension of this construct should include the fact that in some countries, like Nigeria, people care more about family honor and community opinion of them than the pressures at work (Idang, 2015). Failure for them is not an option, so family honor and being viewed positively by the community will push them to do what is right by complying with ISP. Hence, we hypothesize that

- H6: Normative beliefs will positively impact employees' attitudes toward ISP compliance.

Dinev, Goo, Hu, and Nam (2009) suggest that cultural factors should be firmly integrated into any type of ISP design. Culture is acquired through a slow process over years, starting from birth, as Jones and Alony (2007) argued. Its acquisition is not easily discarded. Based on the above assertions and the context of the national culture considered in this research, it is not out of place to imply that the antecedent of behavior is culture. Lovett

(2006) looks at the two prevailing explanations of RCT: Intentional pursuit of self-interest by social actors, their choice is for their optimal benefits. The other explanation is that there are general social benefits of individual pursuits. RCT is more of a social benefit than an individual outcome (Hechter & Kanazawa, 1997). In methodological individualism, the social structure does not restrict human behavior; instead, structural individualism includes social structures that affect individual decisions and behavior (Wittek, 2013). Li, Zhang, and Sarathy (2010) applied RCT to investigate deviant behavior concerning compliance with internet use policy (IUP) in an organization. They argued that users determined to violate IUP perform a cost-benefit analysis to assess benefits derived from intrinsic or extrinsic motivation. One of the hypotheses proposed in the research was that " perceived benefits of internet abuses had a negative impact on IUP compliance intention. " Sideridis, Kaissidis, and Padeliadu (1998) presented a slightly different model than presented by Fishbein and Ajzen's. In their model, belief strength, outcome evaluation, normative beliefs, and motivation to comply represented independent variables that pointed to intermediate variable intention, and intention indicated dependent variable behavior. Whether it is individual or social, a beneficial choice has to be made. Hence, we hypothesize that

- H7: High power distance positively impacts employees' attitudes toward ISP compliance.

Operationalization of Constructs

The constructs in this research are operationalized by the assignment of indicators to latent (unobservable) variables (Hair, Hult, Ringle, & Sarstedt, 2017, p. 6). The indicators are observable and can be measured using a survey instrument (Hair et al., 2017; Hu et al., 2011). The constructs from the conceptual model are further developed into measurement items on a 7-point Likert scale. The measurement items used in the research are adopted from extant literature, as they have been tested and used several times, minimizing the possibility of bias and maximizing reliability and validity as is highly recommended by Straub, Boudreau, and Gefen (2004), which constitutes content validity.

Table 3.1 Measurement Item Sources			
Construct	Item	Item Description	Source
Sanctions	SN1	I will be demoted if I do not comply with information security policy.	Bulgurcu, Cavusoglu, & Benbasat 2010
	SN2	I will be reprimanded if I do not comply with information policy.	
	SN3	I will incur financial loss if I do not comply with information policy.	
Moral Beliefs	MB1	It is morally right to comply with information security policy.	Al-Omari, Deokar, El-Gayar, Walters, & Aleassa, 2013; Vance et al., 2012; Cronan & Al-Rafee, 2008
	MB2	I feel obligated to comply with information security policy.	
	MB3	I will feel guilty if I do not comply with information security policy.	
Benefits of Compliance	BC1	I will feel satisfied if I comply with information security policy.	Bulgurcu et al. 2010
	BC2	I will feel accomplished if I comply with information security policy.	
	BC3	I will feel content if I comply with information security policy.	
Self-efficacy	SE1	I have the required knowledge to comply with information security policy.	Al-Omari et al. 2013
	SE2	I have the required skills to comply with information security policy.	
	SE3	I have the required competencies to comply with information security policy.	
Descriptive Norms	DN1	I believe that other employees comply with information security policy.	Herath & Rao 2009
	DN2	I know that other employees comply with information security policy.	
	DN3	I have a strong opinion that majority of employees comply with information security policy.	
Normative Beliefs	NB1	Upper management believes that I should comply with information security policy.	Bulgurcu et al. 2010
	NB2	My immediate superiors believe that I should comply with information security policy.	
	NB3	My colleagues believe that I should comply with information security policy.	
Power Distance	PD1	Organization rules should not be broken; therefore, I must comply with information security policy.	Zhang & Begley 2011; Sideridis et al., 1998.

	PD2	I respect management decisions; therefore, I must comply with information security policy.	
	PD3	Management has the right to expect complete obedience in work-related matters; therefore I must comply with information security policy.	
Intention to Comply	IC1	I intend to comply with information security policy.	Bulgurcu et al. 2010
	IC2	I intend to help others comply with information security policy.	
	IC3	I encourage others to comply with information security policy.	

Data Analysis Plan

The analysis of the collected data was in two parts, descriptive statistics, and inferential statistics. Microsoft Excel software was used to calculate the descriptive statistics, which were the demographic data obtained from the questionnaires. Partial least squares structural equation modeling (PLS-SEM) was used to calculate inferential statistics and the preferred software was SmartPLS version 3.3.3 (Ringle et al., 2015). There are a few reasons for the adoption of the PLS-SEM mode of data analysis as stated below:

- PLS is an appropriate form of analysis for exploratory research; it provides a graphical indication of relationship proxies; the observations will be on the path coefficients (Ainuddin, Beamish, Hulland, & Rouse, 2007; Henseler, 2018; Henseler, Ringle, & Sinkovics, 2009).
- PLS is suitable for small sample size analysis when others may not be (Birkinshaw, Morrison, & Hulland, 1995; Henseler et al., 2009; Mintu-Wimsatt & Graham, 2004).
- PLS is suitable for estimating complex models with many latent and manifest variables (Henseler et al., 2009).
- PLS does not require normally distributed data to perform analysis. It performs well with nonparametric data (Acedo & Jones, 2007; Henseler et al., 2009).
- PLS is capable of handling both reflective and formative models (Henseler et al., 2009).

Reflective Measurement Model Assessment

The established theoretical measurements provide guidelines on what standards the measurement model should meet to be included in the path model (Hair et al., 2017, p. 105). The reliability and validity of construct measures are established by the assessment of the reflective measurement model, which shows how indicators are related to latent constructs (measurement models) and how constructs are related to each other (structural model) (Hair et al., 2017, p. 105). There are two assessment models to be evaluated, and the structural model evaluation must follow the measurement model evaluation (Hair et al., 2017).

Detmar Straub et al.'s (2004) mandated tests for exploratory research, as previously pointed out, are content validity, construct validity, and internal consistency reliability. Reliability is an indication that a tool will be stable and the results obtained from it valid is that measurements from the constructs will be of exactly what should be measured (Hair et al., 2017, p. 107). The components of reflective measurement model reliability are internal consistency reliability and indicator reliability. The two components of validity associated with reflective measurement are convergent validity and discriminant validity

Internal Consistency Reliability

Cronbach's alpha has been traditionally used as the criterion to assess internal consistency reliability. Subsequently, it was discovered to underestimate internal consistency reliability leading to the acceptance of composite reliability as a better measure of internal consistency reliability (Hair et al., 2017, p. 111). The acceptable composite reliability values for exploratory research are between 0.6 and 0.70, while the values for more established research should be between 0.70 and 0.90 (Bagozzi & Yi, 1988; Hair et al., 2017: p. 112).

Indicator Reliability

Indicators associated with each construct have higher loading and the size of the outer loading is referred to as indicator reliability (Hair et al., 2017, p. 113). For the outer loading to be statistically significant, the rule of thumb is that the standardized value should be 0.708 or higher. The indicator reliability is obtained by squaring the standardized indicator's outer loading (Hair et al., 2017). Although the standardized value is considerably lower for exploratory research, 0.4 and higher are acceptable (Hulland, 1999).

Convergent Validity

The measure of convergent validity is based on the average variance extracted (AVE) of each latent variable (Hair et al., 2017, p. 114; Wong, 2019, p. 33). An acceptable AVE is 0.50 or higher (Bagozzi & Yi, 1988; Hair et al., 2017, p. 115) which indicates that more than 50% of AVE is explained by the construct associated with it.

Discriminant Validity

Discriminant validity refers to the empirical distinction between constructs (Hair et al., 2017, p. 115). The traditional method of testing for this distinction are cross-loadings and the **Fornell-Larcker criterion;** the **Fornell-Larcker criterion** requires that the square root of each construct AVE should be greater than the AVE of other correlated constructs (Fornell & Larcker, 1981; Hair et al., 2017, p. 115). When two constructs are highly correlated, cross-loadings fail to address the lack of discriminant validity. The Fornell-Larcker criterion depends on the distinctions provided by cross-loadings, and if cross-loadings fail, Fornell-Larcker will also fail (Hair et al., 2017: p. 118). Henseler, Ringle, and Sarstedt (2014), proposed a remedy to the problem of discriminant validity. They suggested assessing the heterotrait-monotrait ratio (HTMT) of the correlations. The summary of the reflective measurement model assessment is presented in table 3.2, adopted from Wong (2013).

Table 3.2 Checking Reliability and Validity (Wong, 2013)			
What to check?	What to look for in SmartPLS?	Where is it in the report?	Is it OK?
Reliability			
Indicator Reliability	"Outer loadings" numbers	PLS → Calculation Results → Outer Loadings	Square each of the outer loadings to find the indicator reliability value. 0.70 or higher is preferred. If it is exploratory research, 0.4 or higher is acceptable. (Hulland, 1999)
Internal Consistency Reliability	"Reliability" numbers	PLS → Quality Criteria → Overview	Composite reliability Should be 0.7 or higher. If it is exploratory research, 0.6 or higher is acceptable. (Bagozzi & Yi, 1988)
Validity			
Convergent validity	"AVE" numbers	PLS → Quality Criteria → Overview	It should be 0.5 or higher (Bagozzi & Yi, 1988)
Discriminant validity	"AVE" numbers and Latent Variable Correlations	PLS → Quality Criteria → Overview (for the AVE number as shown above) PLS → Quality Criteria →Latent Variable Correlations	Fornell and Larcker (1988) suggest that the "square root " of AVE of each latent variable should be greater than the correlations among the latent variables

Structural Model Assessment

Structural model measurement represents the relationship between constructs (Hair et al., 2017, p. 13). The evaluation of the following criteria must be satisfied for an assessment to be valid (Hair et al., 2017, pp. 191-209; Hair, Ringle, & Sarstedt, 2011):

- Coefficients of determination (R^2)
- Predictive relevance (Q^2)
- Size and significance of path coefficients
- Model's f^2 effect size
- Model's q^2effect size

- Collinearity issues of structural model (Inner VIFs)
- The standardized root mean square residual (SRMR)

Coefficients of Determination (R^2)

R-square value is an effect size measure in path modeling, it is the most common effect size, and its value appears in the endogenous latent variables (Garson, 2016: p. 59). The R- square value of 0.620, for example is interpreted as 62% of the variance in the endogenous variable is explained by the model that is by the exogenous variables linked to it (Garson, 2016: p. 59). The R-square value called the coefficient of determination may be substantial, moderate, or weak, and the term "high" is relevant to the study (Garson, 2016: p. 80). R-square value is also known as a measure of a model predictive power. Using the rule of thumb, the R^2 values of 0.75, 0.50 or 0.25 for the endogenous construct are classified as substantial, moderate, and weak respectively (Hair et al., 2017: p. 199).

Predictive Relevance (Q^2)

Predictive Relevance is known as Stone-Geisser's Q^2 value. It measures how well the path model predicts the observed values; it applies only to the endogenous constructs of the reflective models (Garson, 2016: p. 117). There are four types of cross-validation output (Garson, 2016: p. 118):

- Construct cross-validated redundancy
- Construct cross-validated communality
- Indicator cross-validated redundancy
- Indicator cross-validated communality

The construct output represents the inner model, which comprises connections between latent variables. The indicator output is obtained from the relationship between indicators and their respective constructs (Garson, 2016: p. 118). The Q^2 statistics are from the redundancy output, calculated in a SmartPLS blindfolding operation (Garson, 2016: p.118). A blindfolding calculation is performed using the specified omission distance D to obtain Q^2 values. The process omits the d^{th} data point and uses the estimate obtained to predict the omitted data (Hair et al., 2011). The rule in choosing distance D, which is between 5 and 10, is that when the number of observations is divided by D the result should not be an integer (Hair et al., 2011). The rule of thumb requires the value of Q^2 to be larger than 0 to

show that the exogenous constructs have predictive relevance for the endogenous variable linked to them.

Size and Significance of Path Coefficients

The path coefficient in combination with the p-value indicates the significance to the model; PLS does not assume normal or any other distribution so bootstrapping, which is a sample and replace method, is employed to simulate a normal distribution and calculate a p-value (Garson, 2016: p. 62). The bootstrapping process involves the choice of 5000 subsamples which is the recommended number and a default value in SmartPLS. As a rule of thumb for a two-tailed test, the critical t-values are 1.65 for a 10% significance level, 1.96 for a 5% significance level, and 2.5% for a 1% significance level. Alternatively, a *p*-value less than 0.10 for a 10% significance level, less than 0.05 is a 5% significance level, and less than 0.01is a 1% significance level. The recommended significance level for research is 5% (Garson, 2016: pp. 192 -193).

Model's f^2 Effect Size

A change in R^2 value when an exogenous variable is omitted from a model is referred to as an f-square effect size. The larger the change in R^2 the less the explained variance of the endogenous variable (Garson, 2016: p. 83). Effect size f^2 is calculated to assess the effect of eliminating exogenous construct from a model and the calculation is performed as shown:

$$f^2 = \frac{R_i^2 - R_e^2}{1 - R_i^2}$$

Where {subscripts *i* means included and *e* means excluded }, the denominator is the unexplained part of the variance; the f^2 calculation shows how large the unexplained portion is accounted for by a change in R^2 (Garson, 2016: p. 84).

Variance Inflation Factor

The presence of collinearity makes it impossible for a researcher to use the structural path coefficient to assess the relative importance of predictor variables in the structural model (Garson, 2016: p. 81). The assessment of collinearity is based on tolerance, and tolerance is (1 - R^2). If tolerance is < 0.20, then R^2 is > 0.80, suggesting collinearity problem (Garson, 2016: p. 81). Collinearity is a condition in which two independent variables in a model are so correlated that they fail to predict the value of the response variable

independently; based on the above-suggested tolerance, the acceptable R^2 has to be <0.80 resulting in the variance inflation factor (VIF) of < 5), according to the formula below (Hair et al., 2017: p. 143).

$$VIF = \frac{1}{1 - R^2}$$

Model's q^2 Effect Size

The q^2 effect size is calculated to assess the contribution of an exogenous construct to the endogenous variable's Q^2 values; in another way, it is used to assess the predictive relevance of the inner model paths to the endogenous construct (Garson, 2016: p. 121). The calculation is performed in the same way as f^2, replacing R^2 with Q^2. The formula is shown below. The values of 0.02, 0.15 and 0.35 respectively, are indications that the exogenous construct has small, medium, or large predictive relevance to the related endogenous variable; (Hair et al., 2017: pp. 207 - 208).

$$q^2 = \frac{Q_i^2 - Q_e^2}{1 - Q_i^2}$$

Standardized Root Mean Square Residual (SRMR)

SRMR is a means of measuring the goodness of fit (GoF), which means understanding the difference between the observed or estimated values of the dependent variables of the model and the values predicted by the PLS model (Wong, 2019). The acceptable value is (<0.080); any value below the recommended threshold shows that the model has a good fit.

Survey Taking Ethics

The survey was issued and collected voluntarily and anonymously. I am a qualified survey taker certified after completing the Collaborative Institutional Initiative (CITI Program) training, Basic Institutional Review Board (IRB) – Record ID: 33537490, Personal ID: 4429965. The Institutional Review Board (IRB) approval number is 20210211.

Summary

Chapter 3 presented the complete methodological approach of the research, including the data collection, population samples, and data analysis plan. Nigeria was selected as the high PD country for the random survey. The model was developed to represent the influence of pd in combination with other variables on intention to comply with information security policy. The operationalization of the constructs provided means of

measuring the latent variables which could not be observed directly. The development of hypotheses provided clear focus on the type of analysis required to produce meaningful results. the plan for data analysis was to present the two required statistical results, descriptive and inferential statistics. The descriptive statistics were to highlight the demography of the survey questionnaire respondents. the inferential statistics were to comply with requirements that would render the model useful and satisfy the reflective and structural measurement assessments. The final section discussed ethics in the survey process; the survey questionnaires were distributed and collected anonymously, and the questions did not request any identifying information.

CHAPTER 4

Analysis and Results

Introduction

The purpose of this study was to explore the role of high-power distance in information security compliance using a quantitative method. The approach was to develop an empirical model to test the following hypotheses:

- H1: Self-efficacy will positively impact employees' attitudes toward ISP compliance.
- H2: Benefits of compliance will positively impact employees' attitudes toward ISP compliance.
- H3: Descriptive norms will positively impact employees' attitudes toward ISP compliance.
- H4: Sanctions will positively impact employees' attitudes toward ISP compliance.
- H5: Moral beliefs will positively impact employees' attitudes toward ISP compliance.
- H6: Normative beliefs will positively impact employees' attitudes toward ISP compliance.
- H7: High power distance positively impacts employees' attitudes toward ISP compliance.

The need to answer the following research questions was also at the core of the study:

- RQ1 - What effect does power distance have on employees' behavior toward ISP compliance intention?
- RQ2 - How significant are the data on power distance?
- RQ3 - How do the data on power distance compare with the data on other constructs in the survey?

Protection motivation theory, general deterrence theory, rational choice theory, theory of reasoned action and theory of planned behavior all played roles in validating the model and testing the hypotheses.

Data Collection

A total of 1000 survey questionnaires were distributed; 597 responses were received, and 187 were discarded for incomplete answers. The 410 that were useable constituted a 41 percent completion rate. The demographics of respondents were generated using the 410 respondents which constituted the descriptive statistics, which were used to calculate inferential statistics.

Descriptive Statistics

The demographic classifications shown in table 4.1 are divided into eight sections, including gender, age, education, and job role. There were 54.63 percent male and 45.37 percent female participants. The largest age group was between 30 and 39 years. The employees in information technology were only18.78 percent of the total, eliminating bias in the analysis.

Table 4.1 Demographics (n = 410)			
Demographic		**Frequency**	**Percentage**
Gender	Male	224	54.63
	Female	186	45.37
Age	18 - 29	78	19.02
	30 - 39	123	30.00
	40 - 49	106	25.85
	50 - 59	40	9.76
	> 59	63	15.37
Education	< High School	10	2.44
	Completed High School	38	9.27
	Some College Credits	28	6.83
	Bachelor's Degree	146	35.61
	Graduate Degree	123	30.00
	Other	65	15.85
Job Role	Information Technology	77	18.78
	Other	333	81.22
Time in the Present Organization	< 1 Year	46	11.22
	1 -5 Years	101	24.63
	6 - 10 Years	75	18.29
	11 - 15 Years	74	18.05
	> 15 Years	114	27.80
Time in the Present Position	< 1 Year	92	22.44
	1 - 5 Years	145	35.37
	6 - 10 Years	59	14.39
	11 - 15 Years	57	13.90
	> 15	57	13.90
Number of Employees in your Organization	< 100	136	33.17
	100 - 500	109	26.59
	501 - 1000	58	14.15
	> 1000	107	26.10
Organization's Sector	Education	82	20.00
	Government	67	16.34
	Financial Services	98	23.90
	Health Care	55	13.41
	Information Technology	38	9.27
	Telecommunications	21	5.12
	Manufacturing	24	5.85
	Nonprofit	18	4.39
	Other	7	1.71
	Total	**410**	100.00

Inferential Statistics

The next process was the model analysis employing partial least squares-structural equation modeling using SmartPLS software version 3.3.3 (Ringle et al., 2015). The model was developed by assigning indicators to latent variables to measure relationships between indicators and variables (Hair et al., 2017: p. 6). The empirical results obtained help compare theoretical model and structural measurements to physical measurements, showing how the theory fits the data (Hair et al., 2017: p. 105). The two models evaluated were measurement models and structural model (Hair et al., 2017: p. 106).

Evaluation of the Measurement Models

The evaluation of the measurement models require the assessment of the reflective measurement models which includes the following (Hair et al., 2017: p. 106):

- internal consistency – Cronbach's alpha and composite reliability;
- convergent validity – indicator reliability, average variance extracted (AVE); and
- discriminant validity – Fornell-Larcker criterion and Heterotrait-Monotrait Ratio of Correlation.

Assessment of Reflective Measurements

Indicators NB2, and NB3, were dropped for cross-loading (i.e., loading high across other variables), with high correlations to other indicators from other variables (Hair et al., 2017: pp. 115 - 116; Hair, Black, Babin, & Anderson, 2015: pp. 116 - 118).

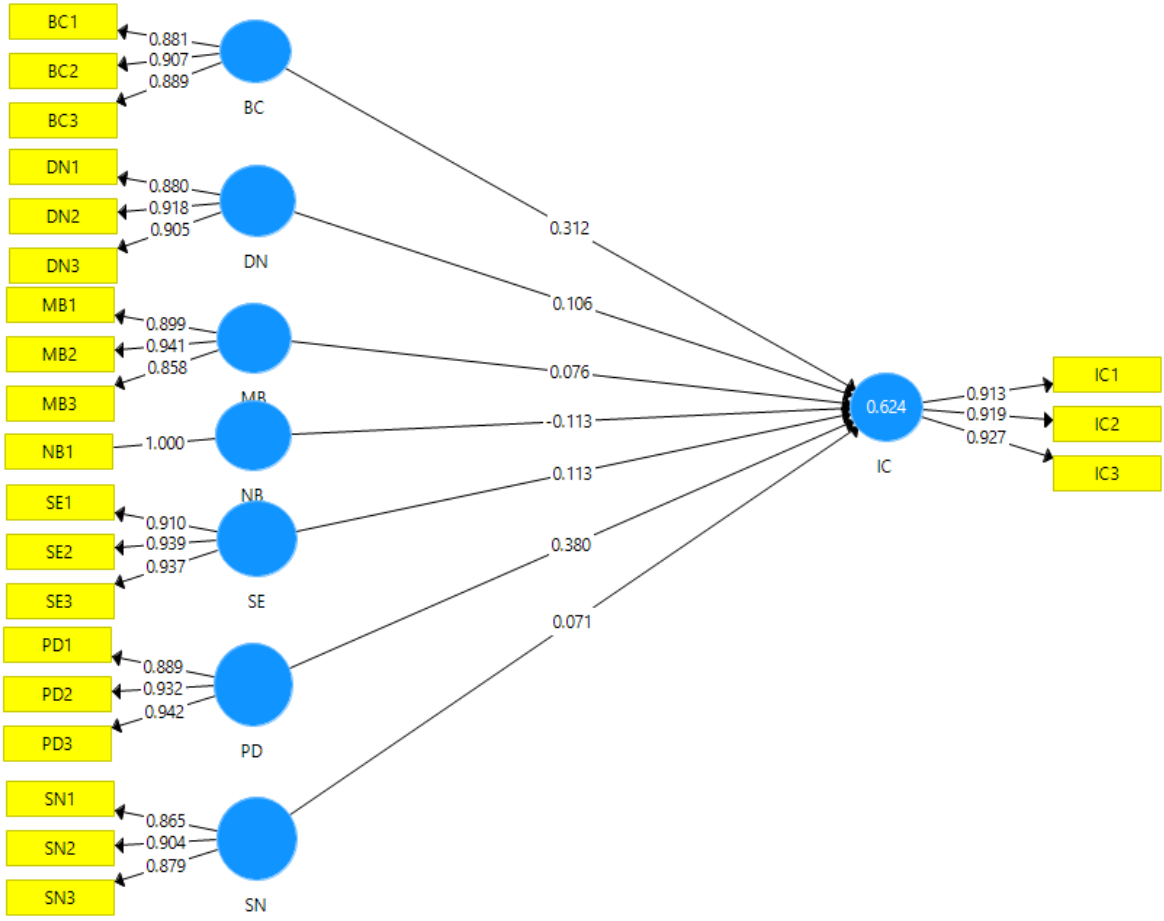


Figure 4.1 PLS Path Model from SmartPLS

There is a true value and a measurement value in every measurement, and the difference is the error; a random error threatens reliability and systematic error threatens validity (Hair et al., 2017: p. 107). Reliability is when a tool will produce consistent and stable results; composite reliability is the better estimate of a construct's internal consistency (Hair et al., 2011). The values of 0.60 to 0.70 for composite reliability in exploratory research are acceptable, advanced research values of 0.70 to 0.90 are expected, and values below 0.60 show a lack of reliability (Hair et al., 2011). The path model after a PLS algorithm calculation is shown in figure 4.1. Table 4.2 shows Cronbach's alpha and composite reliability values above the 0.7 thresholds, signifying a high level of consistency (Bagozzi, R. P., Yi, 1988).

The flow chart in figure 4.4 provides the steps to retain or eliminate indicators based on their values. The values are represented in figures 4.2 and 4.3.

Table 4.2. Internal Consistency - Cronbach's Alpha and Composite Reliability

	Cronbach's Alpha	Composite Reliability
BC	0.872	0.921
DN	0.884	0.928
IC	0.909	0.943
MB	0.882	0.928
NB	1	1
PD	0.911	0.944
SE	0.920	0.950
SN	0.859	0.914

Convergent Validity

A valid construct measures what it is supposed to measure, and to establish convergent validity, the test procedures of figure 4.4 should be performed. According to Hair et al. (2017: p. 112), "convergent validity is the extent a measure correlates positively with the alternative measures of the same construct, ". Domain sampling modeling regards each indicator of a reflective construct as different to measure the construct, and the indicators (measures) of a reflective construct should converge (Hair et al., 2017: p. 113). A latent variable should explain at least 50% of indicator's variance and the required value for the

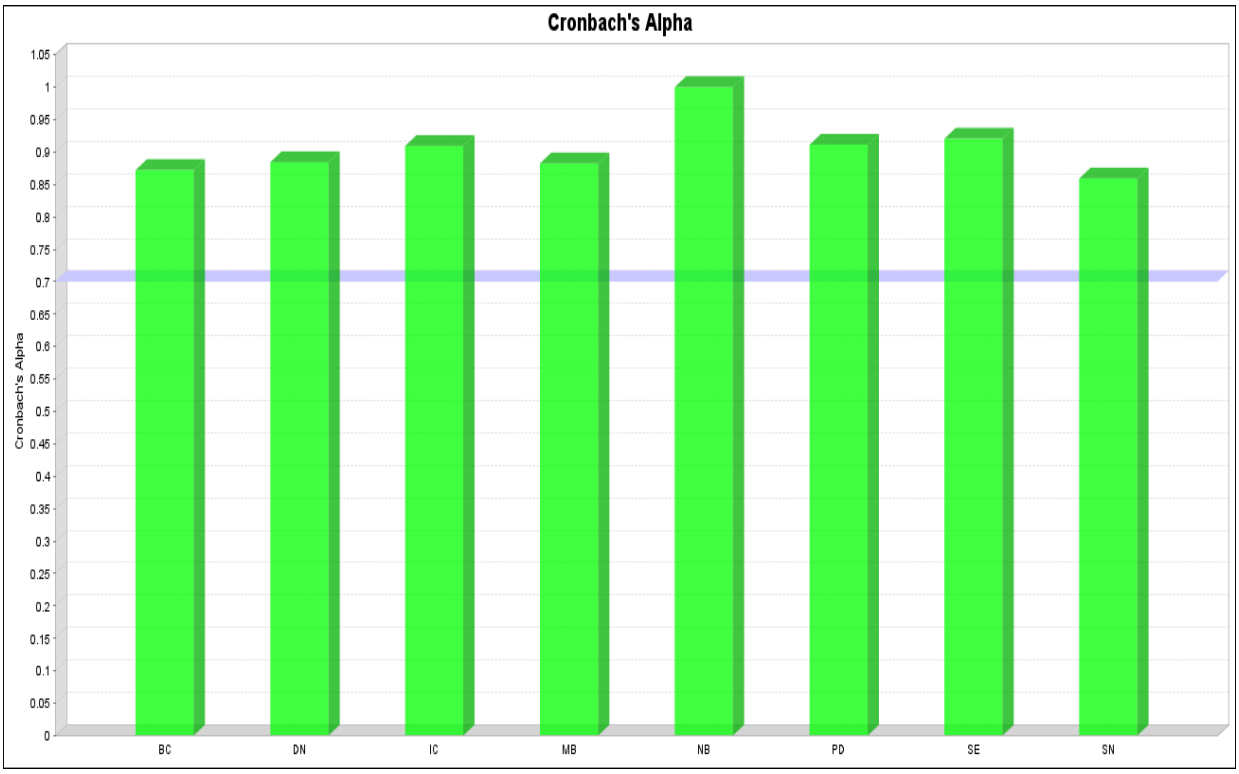


Figure 4.2 Cronbach's Alpha form SmartPLS

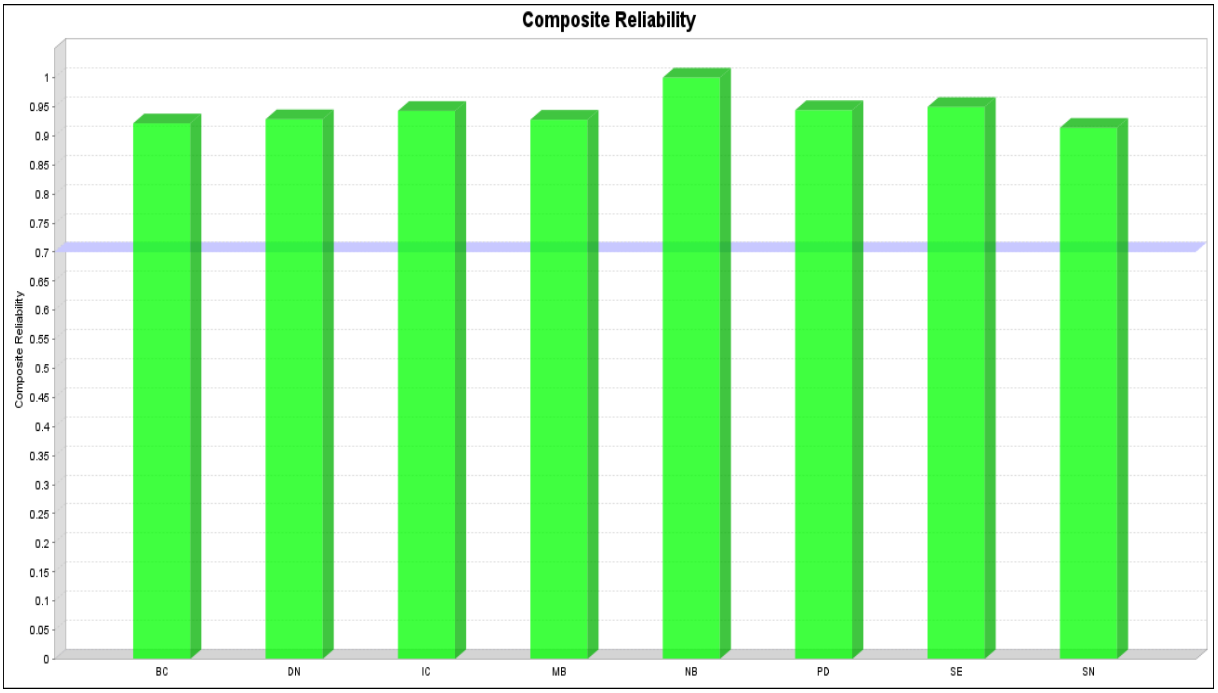


Figure 4.3 Composite Reliability from SmartPLS

indicator's outer loading should be at least .708 when squared is 0.50 (Hair et al., 2017: p. 113)

The outer loading of 0.4 is acceptable for exploratory research (Hulland, 1999). Average variance extracted (AVE) is another standard measure to establish convergent validity; for validity, the value should be 0.50 or greater (Hair et al., 2017: pp. 114 - 115). The values in table 4.3 show outer loading greater than the 0.708 threshold, and the values of the AVE in table 4.4 is greater than the required minimum of 0.50. Therefore, convergent validity is established (see figure 4.5).

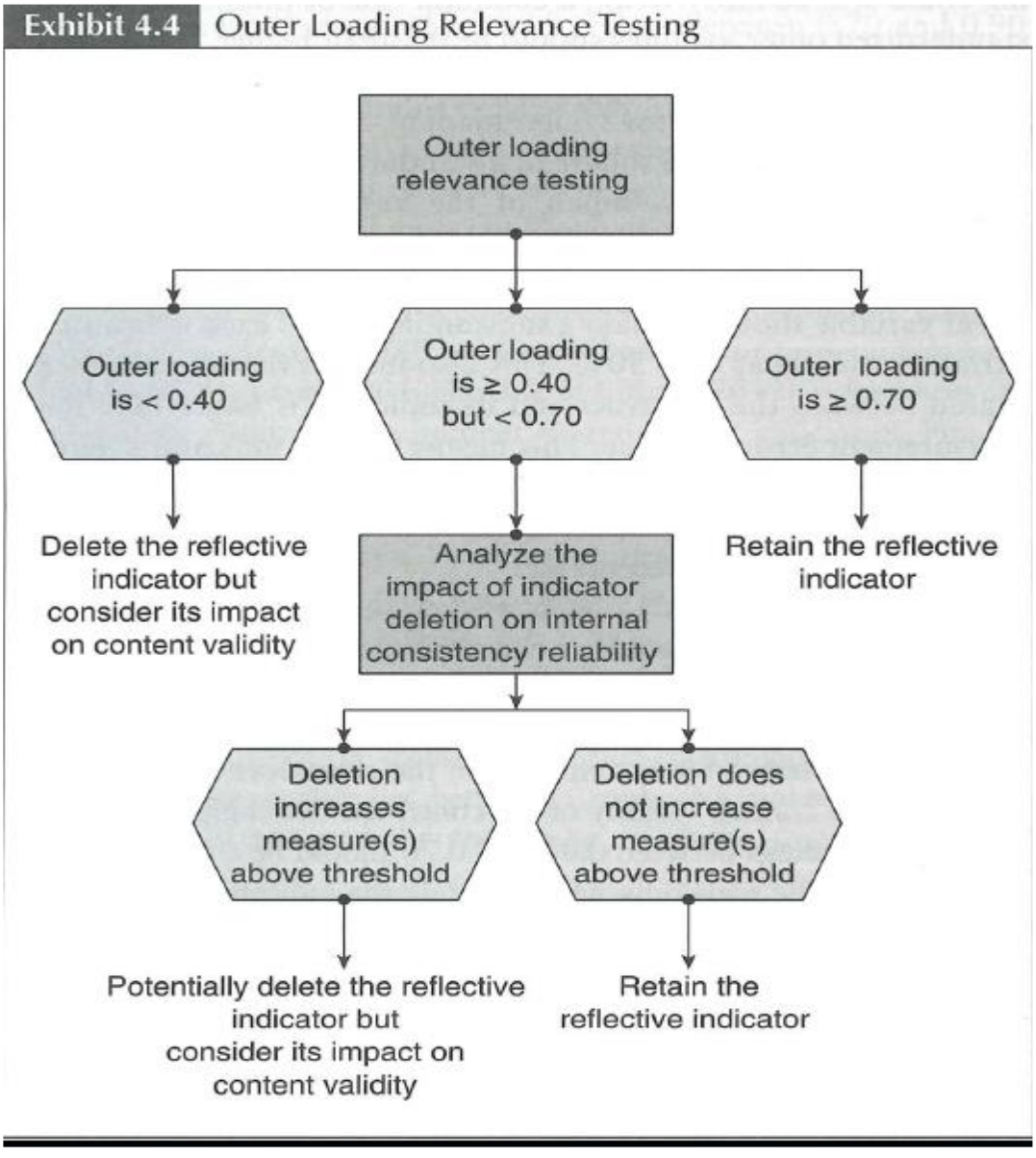


Figure 4.4 (Hair et al., 2017: p. 114)

Table 4.3. Outer Loadings Showing Indicator Reliability								
	BC	DN	IC	MB	NB	PD	SE	SN
BC1	0.881							
BC2	0.907							
BC3	0.889							
DN1		0.880						
DN2		0.918						
DN3		0.905						
IC1			0.913					
IC2			0.919					
IC3			0.927					
MB1				0.899				
MB2				0.941				
MB3				0.858				
NB1					1.000			
PD1						0.889		
PD2						0.932		
PD3						0.942		
SE1							0.910	
SE2							0.939	
SE3							0.937	
SN1								0.865
SN2								0.904
SN3								0.879

Table 4.4. AVE for Convergent Validity	
	Average Variance Extracted (AVE)
BC	0.796
DN	0.812
IC	0.846
MB	0.811
NB	1.000
PD	0.849
SE	0.863
SN	0.779

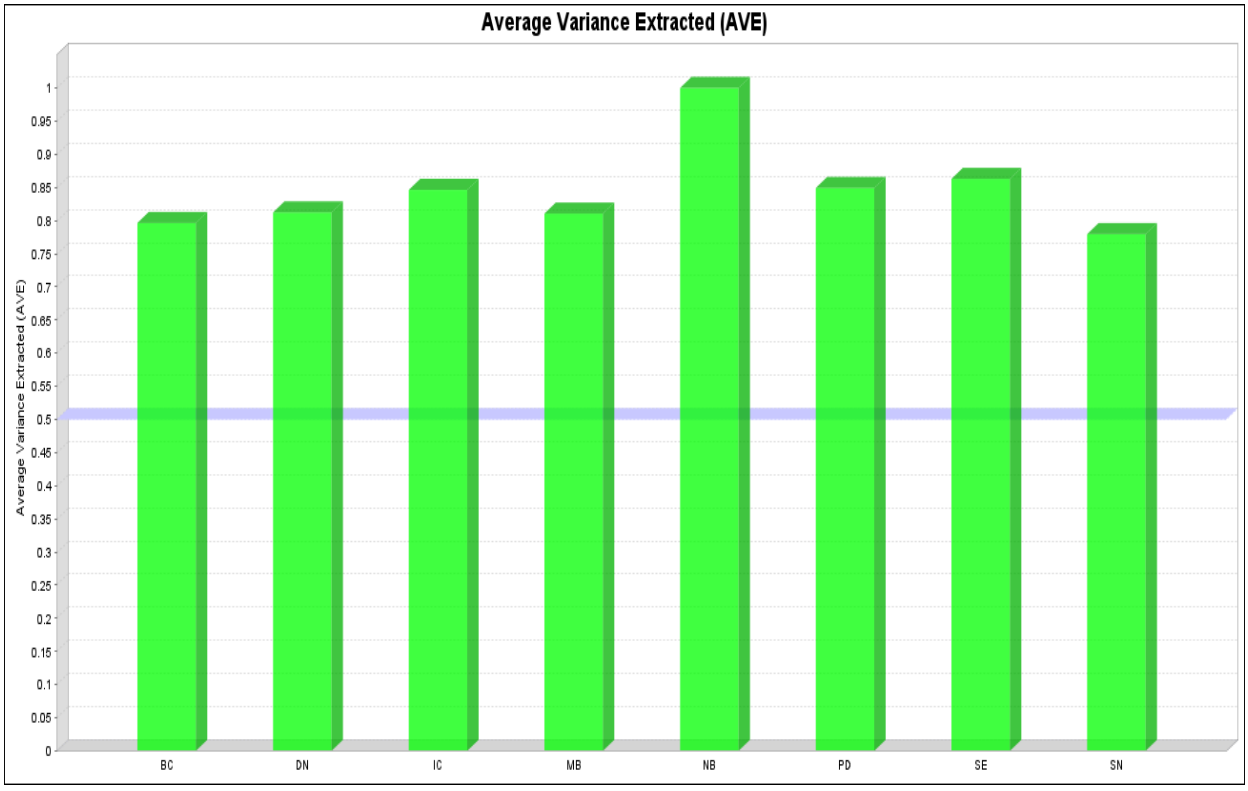


Figure 4.5 Average Variance Extracted (AVE) from SmartPLS

Discriminant Validity

Constructs should be unique and distinct from one another, and this is how to establish discriminant validity (Hair et al., 2017: p. 115). Earlier methods relied on cross-loadings and Fornell-Larcker criterion to assess discriminant validity (Hair et al., 2017: pp. 115 - 116). The Fornell-Larcker criterion states that each construct's AVE's square root should be greater than its highest correlation with other constructs

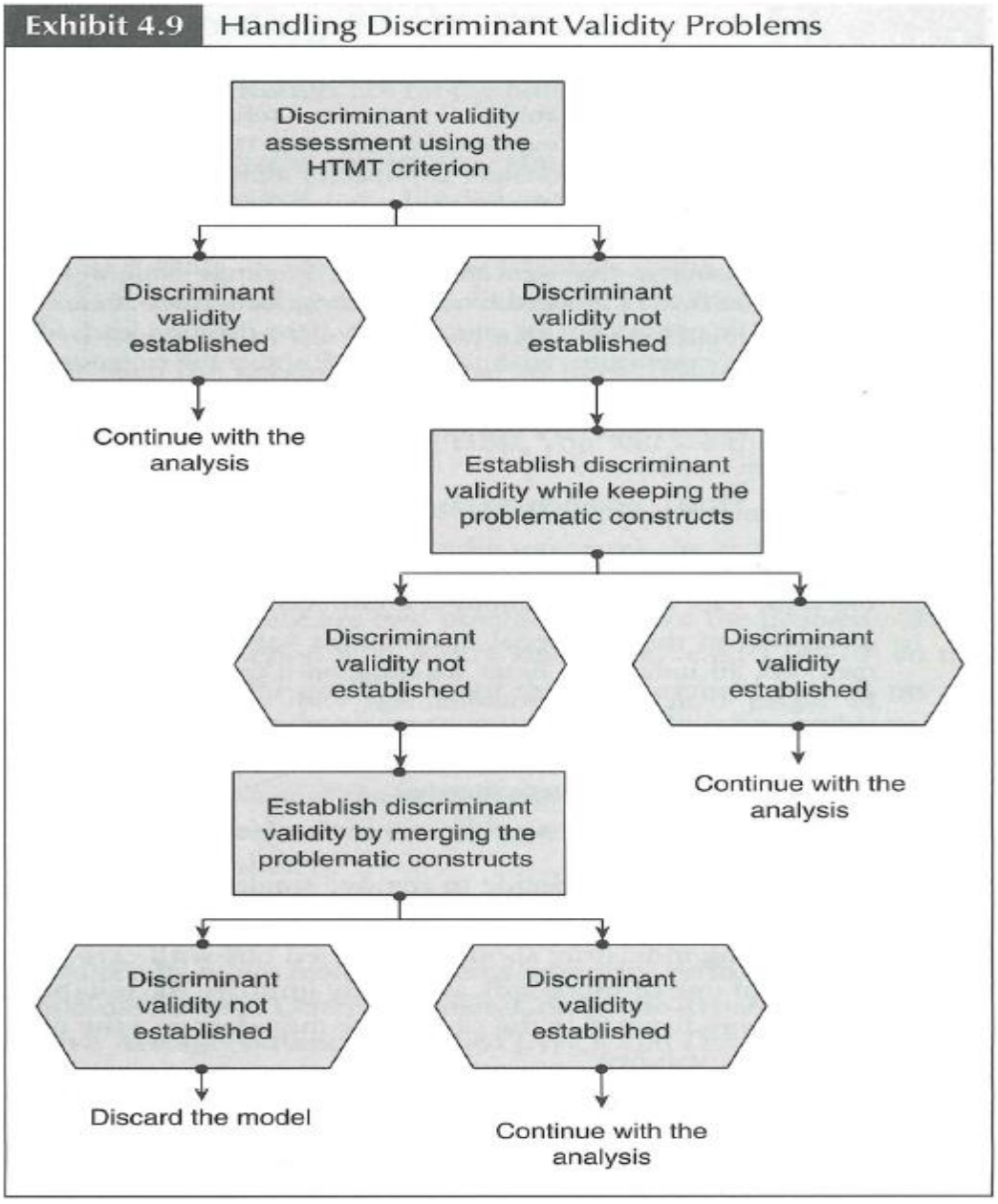


Figure 4.6 (Hair et al., 2017: p. 121)

(Fornell & Larcker, 1981; Hair et al., 2017: p. 116). In addition, the rule requires that a latent construct shares more variance with its indicators than with another latent construct (Hair et al., 2011). The data in table 4.5 conform to the Fornell-Larcker criterion. The second method of determining discriminant validity is loading. The rule is that an indicator loading with its associated latent construct should be higher than its loading with other constructs (cross-loading) (Hair et al., 2011). Indicators' outer loadings are shown in table 4.3.

Table 4.5. Fornell-Larcker Criterion

	BC	DN	IC	MB	NB	PD	SE	SN
BC	**0.892**							
DN	0.529	**0.901**						
IC	0.695	0.568	**0.920**					
MB	0.664	0.520	0.598	**0.900**				
NB	0.622	0.592	0.565	0.657	**1.000**			
PD	0.685	0.556	0.704	0.641	0.759	**0.921**		
SE	0.479	0.628	0.553	0.472	0.434	0.506	**0.929**	
SN	0.457	0.594	0.502	0.518	0.475	0.441	0.639	**0.883**

Henseler, Ringle, and Sarstedt (2015) were not satisfied with the efficacy of the Fornell-Larcker criterion and cross-loading for the assessment of discriminant validity, which success rates were at 14.59 % and 8.78%, respectively, in a variance-based SEM. The way to correct the low sensitivity of the Fornell-Larcker and cross-loading to discriminant validity in variance-based SEM was the proposal of Heterotrait-Monotrait Ratio of Correlation (HTMT). A Multitrait-Multimethod (MTMM) was developed to systematically assess discriminant validity (Campbell & Fiske, 1959). The idea for HTMT took off from there. The new method, estimated to be more accurate than the previous two HTMTs, yields the ratio of

between and within-traits correlations (Hair et al., 2017: p. 118). One way to resolve discriminant validity problems when first discovered is illustrated in figure 4.6, which

Table 4.6. Heterotrait-Monotrait Ratio of Correlation for Discriminant Validity

	BC	DN	IC	MB	NB	PD	SE	SN
BC								
DN	0.603							
IC	0.779	0.631						
MB	0.758	0.591	0.665					
NB	0.666	0.629	0.588	0.700				
PD	0.769	0.620	0.767	0.717	0.799			
SE	0.535	0.695	0.603	0.525	0.453	0.551		
SN	0.525	0.680	0.564	0.591	0.508	0.496	0.716	

Shows the results of a systematic assessment and elimination. The required HTMT value should be (< 0.850) (Wong, 2019: pp. 118 - 119). The highest value in table 4.6 is 0.799, which is below the threshold of (0.850) and is also represented in figure 4.7. The HTMT values should also be tested to show that they are significantly different from 1 (Hair et al., 2017: p. 130). The bootstrapping samples from 5,000 results are shown in table 4.7. The values between the 2.5% and 97.5% (bias corrected) confidence interval are significantly different from 1. Therefore, discriminant validity is established.

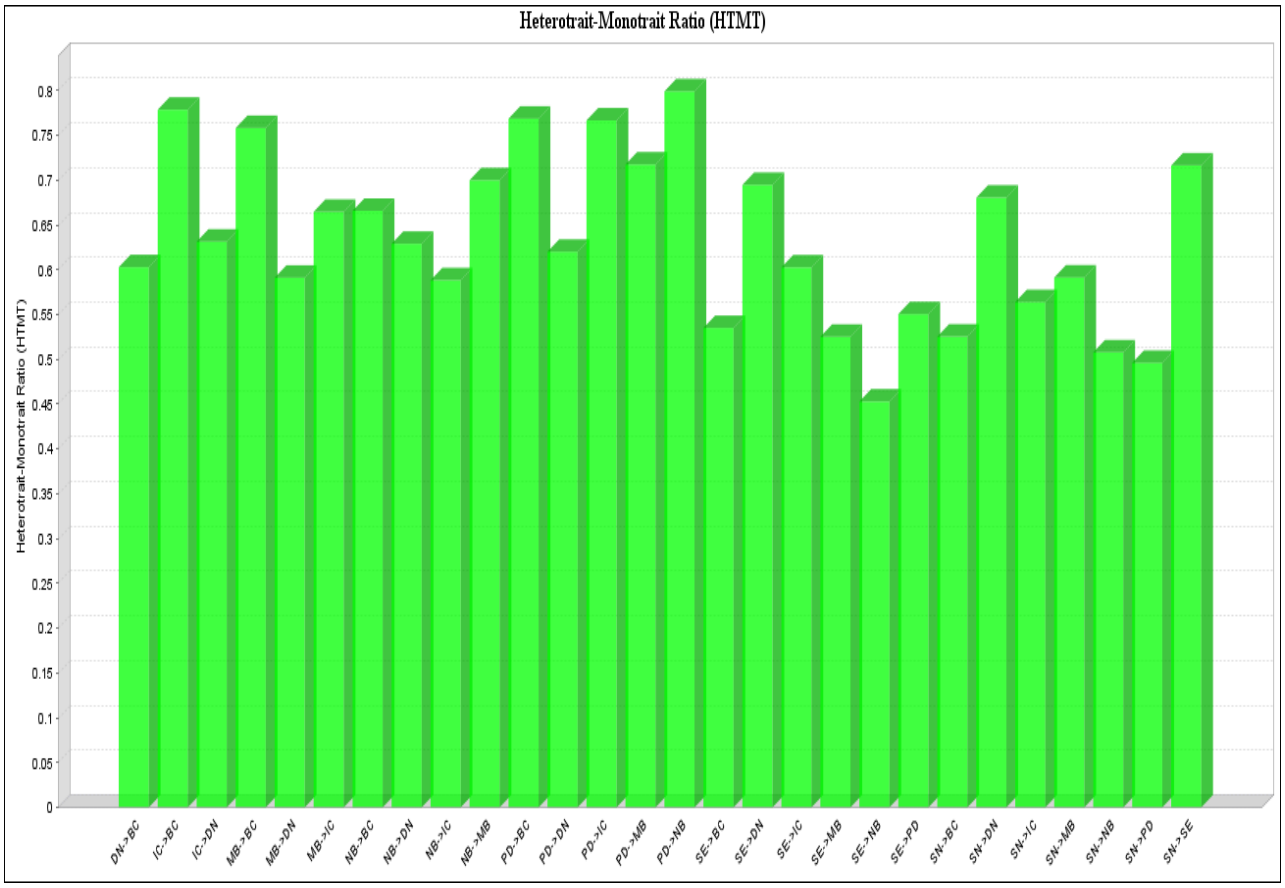


Figure 4.7 HTMT calculated by SmartPLS algorithm

Table 4.7 Confidence Interval for for Hetorotrait-Monotrait Ratio (HTMT)				
	Confidence Intervals Bias Corrected			
	Original Sample (O)	Sample Mean (M)	2.50%	97.50%
DN -> BC	0.603	0.602	0.507	0.689
IC -> BC	0.779	0.778	0.705	0.843
IC -> DN	0.631	0.631	0.539	0.716
MB -> BC	0.758	0.758	0.664	0.842
MB -> DN	0.591	0.590	0.490	0.686
MB -> IC	0.665	0.664	0.567	0.755
NB -> BC	0.666	0.665	0.585	0.735
NB -> DN	0.629	0.628	0.548	0.701
NB -> IC	0.588	0.588	0.505	0.666
NB -> MB	0.700	0.700	0.616	0.775
PD -> BC	0.769	0.768	0.685	0.842
PD -> DN	0.620	0.619	0.526	0.700
PD -> IC	0.767	0.766	0.691	0.832
PD -> MB	0.717	0.718	0.620	0.809
PD -> NB	0.799	0.800	0.746	0.846
SE -> BC	0.535	0.534	0.433	0.630
SE -> DN	0.695	0.695	0.614	0.768
SE -> IC	0.603	0.603	0.519	0.682
SE -> MB	0.525	0.525	0.429	0.615
SE -> NB	0.453	0.453	0.361	0.539
SE -> PD	0.551	0.550	0.452	0.641
SN -> BC	0.525	0.526	0.428	0.618
SN -> DN	0.680	0.681	0.596	0.757
SN -> IC	0.564	0.566	0.479	0.646
SN -> MB	0.591	0.592	0.494	0.682
SN -> NB	0.508	0.508	0.432	0.581
SN -> PD	0.496	0.497	0.400	0.588
SN -> SE	0.716	0.716	0.640	0.785

The summary of the results of the reflective measurement model assessment is shown in table 4.8. Upon examining the results, it becomes evident that all the criteria are met, so measurement model reliability and validity are established.

Table 4.8. Results Summary of Reflective Measurement Models							
Latent variables	Indicators	Convergent Validity			Internal Consistency Reliability		Discriminant Validity
		Loadings	Indicator Reliability	AVE	Composite Reliability	Cronbach's Alpha	
		>0.70	>0.50	>0.50	0.60-0.90	0.60-0.90	HTMT confidence interval does not include 1
BC	*BC1*	0.881	0.776	0.796	0.921	0.872	Yes
	BC2	0.907	0.823				
	BC3	0.889	0.790				
DN	*DN1*	0.880	0.774	0.812	0.928	0.884	Yes
	DN2	0.918	0.843				
	DN3	0.905	0.819				
IC	*IC1*	0.913	0.834	0.846	0.943	0.909	Yes
	IC2	0.919	0.885				
	IC3	0.927	0.845				
MB	*MB1*	0.899	0.767	0.811	0.928	0.882	Yes
	MB2	0.941	0.808				
	MB3	0.858	0.736				
NB	*NB1*	1.000	1.000	1.000	1.000	1.000	Yes
PD	*PD1*	0.889	0.790	0.849	0.944	0.911	Yes
	PD2	0.932	0.869				
	PD3	0.942	0.887				
SE	*SE1*	0.910	0.828	0.863	0.950	0.920	Yes
	SE2	0.939	0.882				
	SE3	0.937	0.878				
SN	*SN1*	0.865	0.748	0.779	0.914	0.859	Yes
	SN2	0.904	0.817				
	SN3	0.879	0.773				

Assessment of Structural Model

Structural model assessment includes:

- Checking for issues with collinearity
- Coefficient of determination (R^2)
- Predictive relevance (Q^2)
- Size and significance of path coefficient
- Effect size f^2
- Effect size q^2
- The standardized root mean square residual (SRMR)
- The procedure is shown in figure 4.8 from step 1 to step 5, step 6 is effect size q^2

calculated manually.

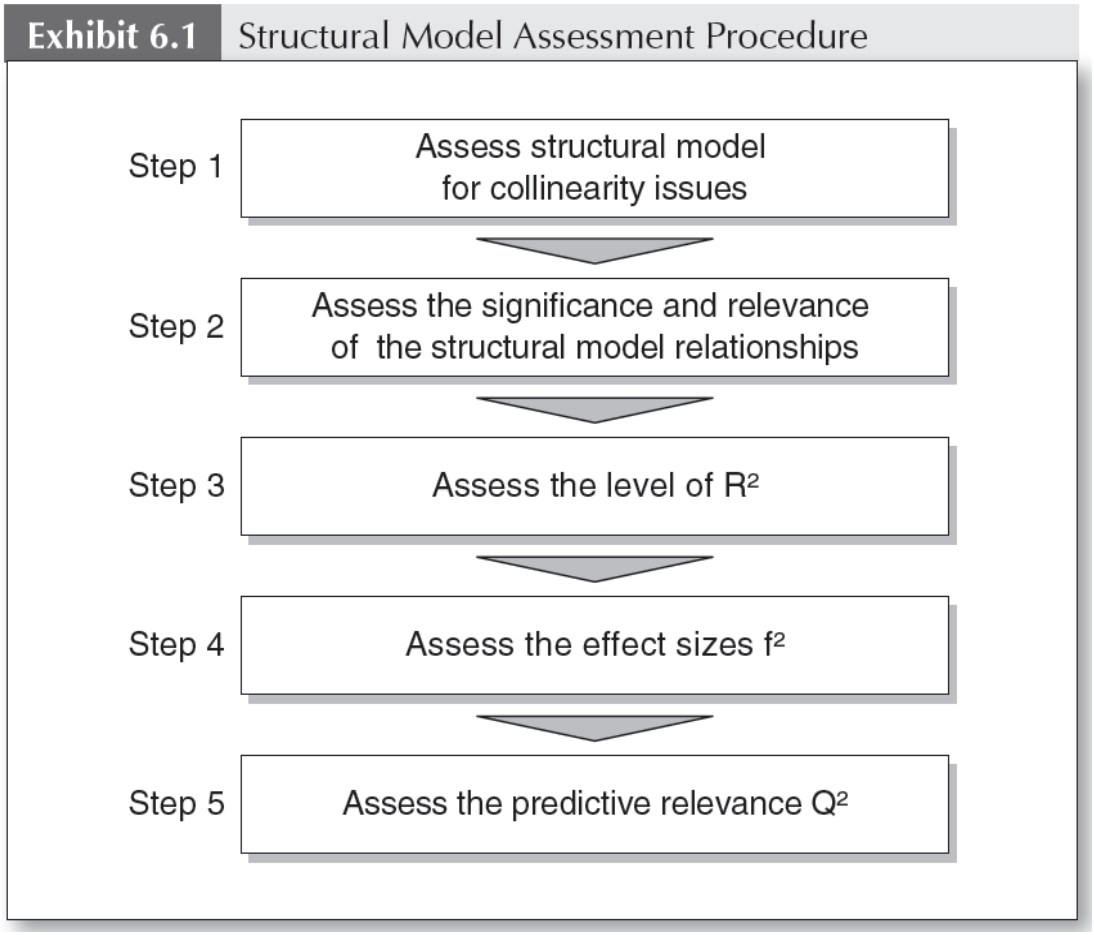


Figure 4.8 (Hair et al., 2017: p. 191)

Collinearity Issues

Collinearity is a condition where two independent variables in a model are so highly correlated that they fail to independently predict the value of the response variable and become insignificant; variance inflation factor (VIF), a good measure of collinearity (VIF value < 5), is required (Hair et al., 2017: pp. 192 - 194). The VIF is computed as the reciprocal of tolerance and tolerance is (1- R^2), as represented below (Hair et al., 2017: p. 143; Robinson & Schumacker, 2009).

$$VIF = \frac{1}{1-R^2}$$

Multicollinearity occurs when two or more predictor variables in a multiple regression model relate to each other and the response variable (Akinwande, Dikko, & Samson, 2015). Multicollinearity inflates standard errors of the coefficient unnecessarily which makes some

variables statistically insignificant when they should be significant (Akinwande et al., 2015). The values of variance inflation factor (VIF) in table 4.9 are substantially below the threshold (value of 5). Therefore, there is no collinearity issue.

Table 4.9. Collinearity Statistics (Inner VIF)

	BC	DN	IC	MB	NB	PD	SE	SN
BC			2.328					
DN			2.221					
IC								
MB			2.336					
NB			2.917					
PD			3.040					
SE			2.143					
SN			2.021					

Coefficient of Determination (R^2 Value)

One of the measures used to evaluate the structural equation model is the coefficient of determination (R^2), which represents the model's predictive power, how well the data fit the model, or how much endogenous variance is explained by the exogenous variables linked to it (Hair et al., 2017: p. 198; Hair et al., 2011). The R^2 value represents the overall effects of all the exogenous variables on the endogenous variable connected to them (Hair et al., 2017: p. 198). The R^2 values range between 0 and 1; the higher the value, the higher the predictive accuracy (Hair et al., 2017: p. 199). There is no rule of thumb for setting acceptable R^2 values. It depends on how complex a model is and the research discipline (Hair et al., 2017: p. 199). The values expected for scholarly research in marketing are usually, 0.75, 0.50, and 0.25 for endogenous variables, referred to as substantial, moderate, and weak, respectively (Hair et al., 2017: p. 199). Based on the R^2 value of 0.624 obtained, as shown in figure 4.9, the effect is substantial.

Structural Model Path Coefficients

Path coefficients represent hypothesized relationships between constructs, and their standardized values are between -1 and +1 (Hair et al., 2017: p.195). The value of +1

indicates a strong positive relationship, and the value of -1 indicates a strong negative relationship; the closer the coefficients are to 0, the weaker their relationships (Hair et al., 2017: p. 195). Standard error plays a critical role in determining if a coefficient obtained is significant or not, and the standard error is obtained by bootstrapping (Hair et al., 2017: p.195). The computation of the standard error by bootstrapping helps assess each exogenous variable's significant contribution to the endogenous variable (Hair et al., 2017: p. 195; Hair et al., 2011). Empirical t- values and p-values are obtained from bootstrapping computations; for a coefficient to be significant the empirical t value must be greater than the critical value. In two-tailed tests the following are the assessment levels: 1.65 (Significance level = 10%), 1.96 (significance level = 5%) and 2.57 (significance level = 1%) (Hair et al., 2017: p. 195). Table 4.10 shows path coefficient, t statistics, *p*-value, and significance in a sample of 5,000, at 0.05 level of significance two-tailed bootstrapping and confidence intervals, bias corrected. The sample size of 5,000 was tested at a .01 significance level; BC -> IC, and PD -> were significant at that level with a *p*-value of (0.000) each. In exploratory studies, researchers often assume a significance level of 10% (Hair et al., 2017: p. 196).

Table 4.10. Path Coefficient and Confidence Intervals Bootstrapping Results

	Original Sample (O) (β)	T Statistics (|O/STDEV|)	P Values	Significant at (0.05)	2.50%	97.50%
BC -> IC	0.312	5.065	0.000	Yes	0.185	0.429
DN ->IC	0.107	1.962	0.049	Yes	0.002	0.217
MB ->IC	0.076	1.241	0.215	No	-0.038	0.207
NB -> IC	-0.113	1.760	0.079	No	-0.234	0.020
PD -> IC	0.380	5.361	0.000	Yes	0.248	0.525
SE -> IC	0.112	2.185	0.029	Yes	0.011	0.212
SN -> IC	0.071	1.504	0.133	No	-0.025	0.116

Significant relationships are necessary to assess how significant each exogenous' path coefficient is related to the endogenous variable. The relationship of PD to IC was very significant (β = 0.380**),** BC to IC and SE to IC made significant contributions at (β = 0.312**)** and (β = 0.112) respectively. The path coefficients of DN to IC made small contributions at (β = 0.107). They were all significant at a 0.05 level of significance. The path MB to IC was not significant at any level and had a path coefficient of (β = 0.076). NB to IC had a negative path coefficient (β = -0.113), indicating a negative relationship, opposite to the hypothesized relationship between constructs. SN to IC with a path coefficient (β = 0.071) was not significant.

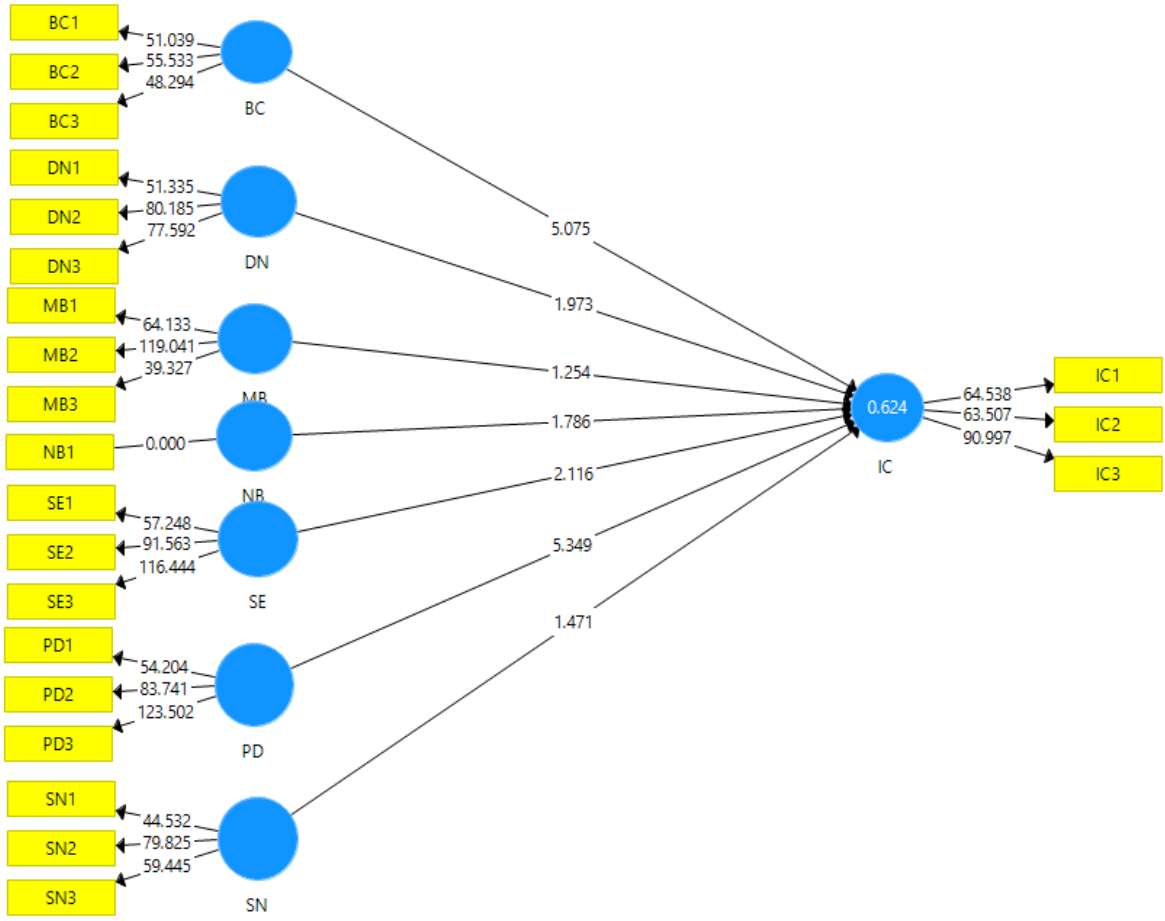


Figure 4.9 Results from Bootstrapping in SmartPLS T-Statistics and R^2 value

Effect Size f^2

The act of omitting a specific exogenous variable and the calculation of a new R^2 to determine its impact on the endogenous construct is called effect size f^2; the value of the newly calculated R^2 determines how substantial the effect of the variable is in the model (Hair et al., 2017: p. 201). The calculation of effect size is shown below

$$f^2 = \frac{R_i^2 - R_e^2}{1 - R_i^2}$$

Where {subscripts *i* means included and *e* means excluded}.

The guidelines are that the values 0.02, 0.15, and 0.35 represent small, medium and large respectively (Cohen, 1988: pp.413 - 414; Hair et al., 2017: p. 201). All constructs linked to intent to comply (IC) except benefits of compliance (BC) and power distance (PD) had a small effect; BC → IC and PD → IC had a medium effect, (see table 4.11).

Table 4.11. Effect Size f^2

	Original Sample (O)	Effect Size
BC -> IC	0.111	Medium
DN -> IC	0.014	Small
MB -> IC	0.007	Small
NB -> IC	0.012	Small
PD -> IC	0.127	Medium
SE -> IC	0.016	Small
SN -> IC	0.007	Small

Blindfolding and Predictive Relevance Q^2

The Q^2 value, also known as Stone-Geisser's Q^2 value (Geisser, 1974; Stone, 1974) measures the predictive relevance of a model, which means it accurately predicts data not used for model estimations, which is also referred to as out-of-sample data. A value larger than zero is needed for accurate predictive relevance (Hair et al., 2017: p. 202). A blindfolding calculation is performed using a specified omission distance, D, to obtain Q^2 values. The process omits the d^{th} data point and uses the obtained estimate to predict the

omitted data (Hair et al., 2011). The rule in choosing distance D, which is between 5 and 10, is that when the number of observations is divided by D, the result should not be an integer (Hair et al., 2011). The blindfolding procedure applies to endogenous constructs with reflective measurement models (Hair et al., 2011). For this calculation the omission distance used was (D = 7) and the Q^2 value obtained was (0.516), which is larger than zero confirming the predictive relevance of the model.

Effect Size q^2

The calculation of q^2 is similar to f^2, but it uses the Q^2 value to obtain the effect on the model of removing Q^2 value of a particular exogenous variable. The values of 0.02, 0.15, and 0.35, respectively represent small, medium, or large (Hair et al., 2017: pp. 207 - 208). The values were calculated manually. The formula and example calculation are shown below.

$$q^2 = \frac{Q_i^2 - Q_e^2}{1 - Q_i^2}$$

The (subscripts *i* and *e* are included and excluded respectively).

For BC excluded, $q^2 = \frac{0.516-0.481}{1-0.516}$ = 0.072

The summary of the calculations is shown in table 4.12 and all the results indicate that the effect sizes in all cases except MB and PD are small. MB has no effect and PD has medium effect.

Table 4.12. q^2 Effect Sizes

	IC	Effect Size
BC	0.072	Small
DN	0.006	Small
MB	0.000	No Effect
NB	0.006	Small
PD	0.082	Medium
SE	0.008	Small
SN	0.002	Small

Standardized Root Mean Square Residual (SRMR)

Goodness of fit (GoF) measures how well the model of observed values fits the model of expected values based on the random sampling of normally distributed data. It is used to obtain a good fit to the value of SRMR, which is (< 0.080) (Benitez, Henseler, Castillo, & Schuberth, 2019; Wong, 2019: pp. 123 - 125). According to Wong (2019), for a perfect fit, SRMR should be zero, but any value (<0.080) is acceptable. As seen in table 4.13, The value obtained was 0.044 below the recommended value, and therefore acceptable.

Table 4.13. Model Fit

	Saturated Model	Estimated Model
SRMR	0.044	0.044
d_ULS	0.499	0.499
d_G	0.433	0.433
Chi-Square	1120.313	1120.313
NFI	0.857	0.857

Hypothesis Testing

Table 4.14. Results of Hypotheses H1 – H7			
Hypotheses	Path Coefficient	Significance	P Values
H1: Self-efficacy will positively impact employees' attitudes toward ISP compliance.	0.112	*	0.033
H2: Benefits of compliance will positively impact employees' attitudes toward ISP compliance.	0.312	*	0.000
H3: Descriptive norms will positively impact employees' attitudes toward ISP compliance.	0.107	*	0.049
H4: Sanctions will positively impact employees' attitudes toward ISP compliance.	0.071	NS	0.140
H5: Moral beliefs will positively impact employees' attitudes toward ISP compliance.	0.077	NS	0.218
H6: Normative beliefs will positively impact employees' attitudes toward ISP compliance.	-0.113	NS	0.075
H7: High power distance positively impacts employees' attitudes toward ISP compliance.	0.380	*	0.000

*p<0.05. NS=not significant

Five hypotheses were significant. Four were significant at (p<0.05), two also at (p<0.01) and one at (p<0.10), as summarized in table 4.14. In exploratory studies, a 10% level of significance is permitted (Bartlett, Kotrlik, & Higgins, 2001; Hair et al., 2017: p.

153), but in this study we restrict the results to (p<0.05). In results H7, high power distance had the largest influence on intent to comply with information security policy, followed by H2, benefits of compliance, and H1, self-efficacy. The results are presented in figures 4.10 – 4.12.

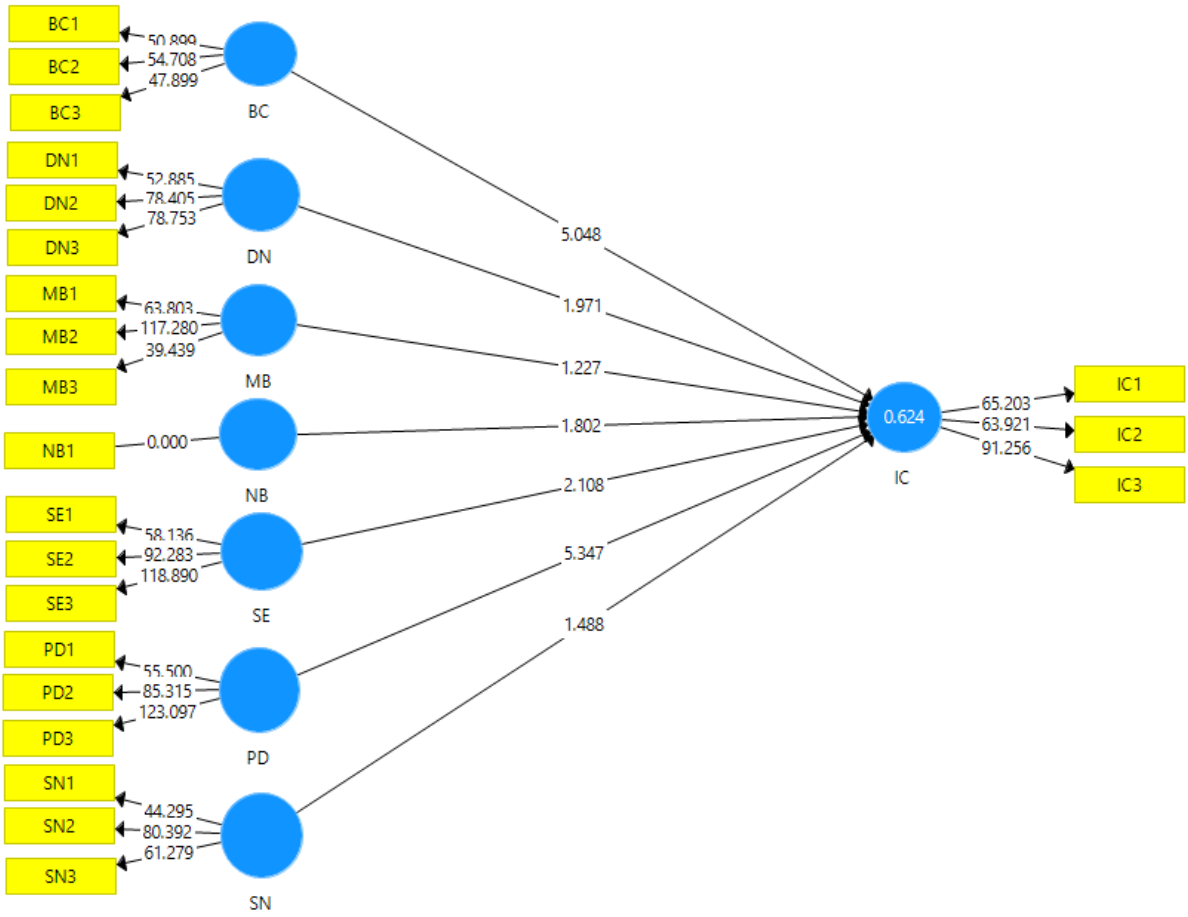


Figure 4.10 Research Model Showing R^2 Value, and T-Statistics at (P<0.05)

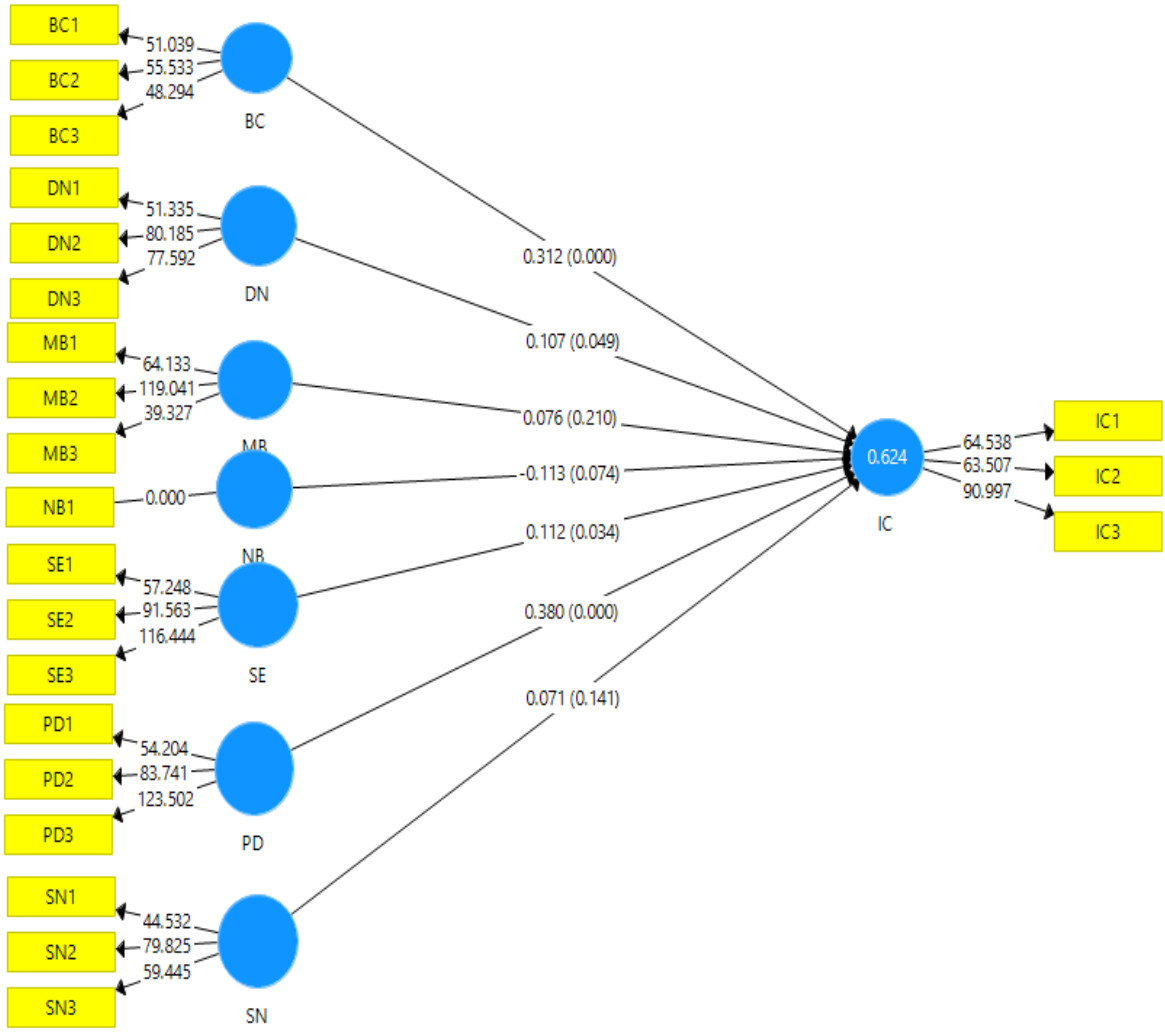


Figure 4.11 Research Model Showing R^2 Value, Path Coefficient and P-Values at (*P*<0.05)

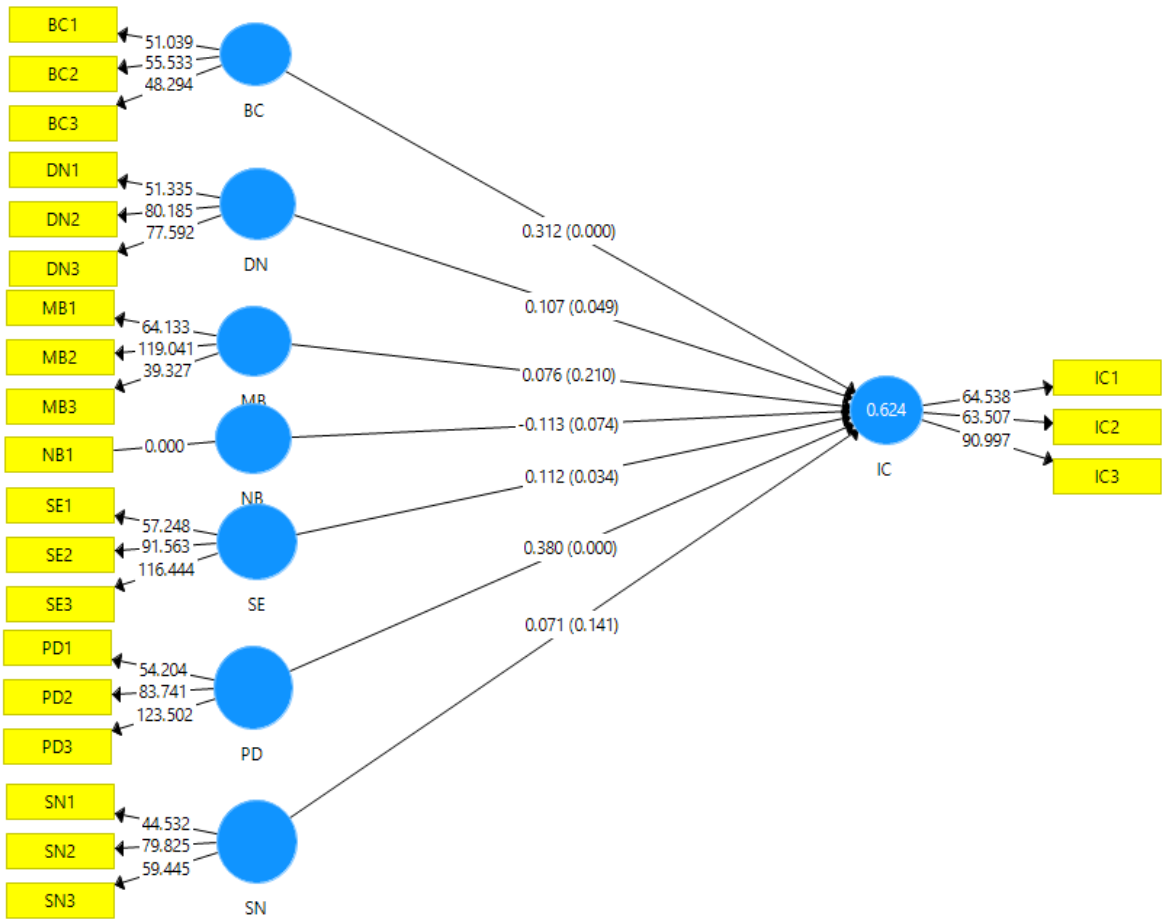


Figure 4.12 Research Model Showing R^2 Value, Path Coefficient and P-Values at (*P*<0.01)

Individual hypotheses were analyzed based on their relationship with intention to comply with ISP.

H1: Self-efficacy will positively impact employees' attitudes toward ISP compliance. The hypothesis was supported and significant at (p<0.05). It shows that employees can perform the necessary functions needed to protect organizations' information.

H2: Benefits of compliance will positively impact employees' attitudes toward ISP compliance. The hypothesis was supported and significant at (p<0.01), employees like to feel

accomplished for doing the right thing, but the benefits of compliance are not their ultimate desire.

H3: Descriptive norms will positively impact employees' attitudes toward ISP compliance. The hypothesis was supported and significant at (p<0.05). Employees naturally like to imitate one another but according to the research outcome, that feeling is secondary to the main reason for the intention to comply with ISP.

H4: Sanctions will positively impact employees' attitudes toward ISP compliance. The hypothesis was not supported, and therefore not significant. However, the result indicates that sanctions do not overtly influence employees who have set their minds on doing right.

H5: Moral beliefs will positively impact employees' attitudes toward ISP compliance. The hypothesis was not supported at any level.

H6: Normative beliefs will positively impact employees' attitudes toward ISP compliance. The hypothesis was not significant at (p<0.05), though applying the guideline that (p<0.10) is allowed for exploratory research (Hair et al. 2017), it was not supported based on prior restriction. The path indicated that as normative beliefs increased the intention to comply with ISP decreased. The violation of the stated positive influence of the hypothesis renders it unacceptable (Ifinedo, 2012).

H7: High power distance positively impacts employees' attitudes toward ISP compliance. The hypothesis was supported and significant at (p<0.01). PD was the largest contributor to intention to comply with ISP.

Answers to Research Questions

The results obtained from the hypotheses analysis will provide insight into how effective the research was in answering the following research questions.

- RQ1 - What effect does power distance have on employees' behavior toward ISP compliance intention?
- RQ2 - How significant are the data on power distance?
- RQ3 - How do the data on power distance compare with the data on other constructs in the survey?

RQ1 answer

As shown in table 4.14 it is clear from the path coefficient that PD is the largest contributor to intention to comply with ISP. Compared to other constructs, PD had the most impact on the intention to comply with ISP.

RQ2 answer

The result showed that PD was very significant and would play a crucial role in the intention to comply with ISP.

RQ3 answer

The other constructs are common in research of this type, and they may be expected to get a better response from respondents. The data obtained, however, showed that high PD outperformed all of them.

Summary

Chapter 4 started with data collection by distributing and collecting survey questionnaires. The surveys were sorted by eliminating those whose organizations did not have an ISP. Further action on the surveys was to examine the responses that had a suspicious pattern. The number used for analysis was 410 out of 597 collected from 1,000 distributed. The process continued with demographic analysis using Microsoft Xcel to complete descriptive statistics. Finally, inferential statistics began with the assessment of measurement models and a structural model for validity and reliability using SmartPLS.

Hypotheses were tested using SmartPLS and the results were explained and summarized. Finally, the research questions were answered after the hypothesis analysis.

In Chapter 5, concluding assessment is made of the success or the failure of the research. It includes a summary of the results, a discussion of the results, limitations, implications, and further research recommendations.

CHAPTER 5

DISCUSSIONS, RECOMMENDATIONS, AND CONCLUSIONS

Introduction

The last chapter was on model assessments, validation, data analysis and hypothesis testing. The results of the hypotheses were explained. In this chapter, the results obtained in the previous chapter will be examined and discussed with suggestions on the issues encountered. In addition, it provides a discussion on this study's contributions to theory and practice. The limitations of the research will also be addressed, recommendations for further research made, and the conclusions summarized.

Discussion

The assessment of measurement model revealed problems of cross-loading and high correlations between constructs that led to the removal of some factors. The assessment was completed successfully. Likewise, the assessment of the structural model was successful. Both assessments proved the validity and reliability of the model.

The assessment of measurement model required a Cronbach's alpha value of 0.70 for composite reliability to prove internal consistency, and the values in table 4.2 are well above the required threshold. The proof of convergent validity requires a value of 0.708 for each indicator's outer loading, and the values in table 4.3 show that the conditions were met. The final step needed to complete the measurement model assessment was to test for discriminant validity using the Fornell-Larcker criterion and Heterotrait-Monotrait Ratio of Correlations (HTMT). The Fornell-Larcker criterion requirement is that each construct's AVE's square root should be greater than its highest correlation with the other constructs, and table 4.5 shows that the requirement is satisfied. HTMT is more accurate than Fornell-Larcker and it is the recommended test for discriminate validity. For the test to be valid the results should be (<0.850); table 4.6 shows that the value of 0.799 is below the threshold.

The next step was Structural model assessment which required tests for collinearity, coefficient of determination, predictive relevance, size and significance of path coefficient, effect sizes, and the standardized root mean square residual (SRMS). The recommended test for collinearity is the variance inflation factor (VIF) test, and a value below

5 is acceptable. The values in table 4.9 are below the recommended threshold; therefore, no collinearity issues were found. The coefficient of determination R^2 measures the model's predictive power. Values of 0.25, 0.50, and 0.75 are weak, moderate, and substantial, respectively. The tested R^2 value was 0.624, which was slightly was substantial. The Q^2 value is the measure of the predictive relevance of a model. The Q^2 value obtained was (0.516), and any value greater than zero would indicate accurate predictive relevance. The size and significance of each path coefficient, at (p<0.05) is shown in table 4.10; the path BC → IC (β = 0.312), DN → IC (β = 0.107), PD → IC (β = 0.380), and SE → IC (β = 0.112) were significant; the path MB → IC (β = 0.076), NB → IC (β = -0.113) and SN → IC (β = 071) were not significant.

The effect size, f^2 represents the change in R^2 when an exogenous variable is removed. The results in table 4.11 show the effect sizes, f^2 for BC → IC (0.111), medium, DN → IC (0.014), small, MB → IC (0.007), small, NB → IC (0.012), small, PD → IC (0.127), medium, SE → IC (0.016), small and SN → IC (0.007), small. The effect size, q^2, is the relative impact on predictive relevance when a path from an exogenous variable to an endogenous variable is removed, and it uses Q^2 for calculations. The results as shown in table 4.12 are: BC → IC (0.072), small, DN → IC (0.006), small, MB → IC (0.000), no effect, NB → IC (0.006), small, PD → IC (0.082), medium, SE → IC (0.008), small and SN → IC (0.002), small. The standardized root mean square residual is used to ascertain the goodness of fit (GoF) of a model. The upper threshold of SRMS is (0.080) and any value less than the threshold shows a good fit. The obtained value was 0.044, below the threshold (see table 4.13).

Table 4.14 shows the results of hypotheses H1 – H7 tested at significance levels (p<0.05). A p-value of 0.10 is permitted for exploratory studies (Hair et al., 2017: p. 153), but not used since the study is restricted to(p<0.05).

- H1: Self-efficacy will positively impact employees' attitudes toward ISP compliance. The hypothesis was supported and significant at (p<0.05); the respondents were confident in their knowledge and skills to comply with whatever the ISP required.
- H2: Benefits of compliance will positively impact employees' attitudes toward ISP compliance. The hypothesis was supported and significant at (p<0.05); participants

indicated that they would feel accomplished and satisfied that they acted appropriately when complying with ISP.

- H3: Descriptive norms will positively impact employees' attitudes toward ISP compliance. The hypothesis was supported and significant at (p<0.05); respondents knew that other employees responded positively to ISP and that was a source of encouragement to them to do the same (Smith et al., 2012; White et al., 2009).
- H4: Sanctions will positively impact employees' attitudes toward ISP compliance. The hypothesis was not significant at (p<0.05), and therefore, not supported; employees who respect rules and follow instructions do not need sanctions to effect compliance with ISP (E. E. Etim, 2021; Vance & Siponen, 2012a).
- H5: Moral beliefs will positively impact employees' attitudes toward ISP compliance. The hypothesis was not supported at (p<0.05). Following instruction is a national phenomenon, based on power distance, while moral beliefs are personal.
- H6: Normative beliefs will positively impact employees' attitudes toward ISP compliance. The hypothesis was only significant at (p<0.10); the negative path coefficient and a T-statistics of 1.760 (table 4.8) indicate that there is another independent variable that dominates the model. This relationship is inverse: as normative beliefs decrease, the response to ISP compliance increases. Therefore, this hypothesis is not accepted.
- H7: High power distance positively impacts employees' attitudes toward ISP compliance. As the path coefficient proved, the hypothesis was supported and significant at (p<0.01); power distance was a dominating predictor variable.

Research question 1 answer: The effect of PD on employees' intention to comply with ISP is captured by the path coefficient, as it had the most considerable influence on the intention to comply. The responses to PD questions in the survey exposed the underlying principle the respondents cherish most, which is living according to their culture (E. Etim, Streff, Park, & Rowland, 2021) (see figure 4.11).

Research question 2 answer: The data on PD was significant based on the analysis and very substantial, at (p<0.01) (see table 4.12).

Research question 3 answer: Compared to other variables in the model, PD was very substantial, outperforming the other variables. The only inference that could be drawn from this finding is that respondents are serious about their cultures.

The interpretation of hypotheses brings up another issue that resulted from the analysis of data. It is appropriate to provide recommendations for both factor cross-loadings and negative path coefficient of normative beliefs. Factor cross-loadings revealed that some of the factors loaded very high on their own variables and others'. On further examination of the correlation matrix, the same indicators were highly correlated, preventing meaningful discriminant validity assessment. The cross-loading factors were dropped. Three questions were assigned to each construct to facilitate questionnaires completion, which could have contributed to the cross-loading problems. The remedies could be an expansion of questions assigned to each construct and selecting constructs that can function together without correlating factors. One selection of constructs would not interfere with another, as demonstrated by the negative path coefficient in H6. The dominance of power distance may have contributed to the experience, which means not having both in the same model. Finally, testing questions on potential respondents before settling on the right questions to use in the survey would be helpful.

Contribution to Theory

Rational Choice Theory is directed toward social rather than individual outcomes (Hechter & Kanazawa, 1997)**.** Embedded in RCT is a social structure that guides individual action (Hechter & Kanazawa, 1997). The title of the research, **Exploring High-Power Distance among other Variables in Information Security Policy Compliance,** is about the social construct power distance, which is interpreted as respect for authority in high PDI countries. There are different religions or affiliations in Nigeria, and there may be different beliefs, but respect for elders and authority are not compromised (Falola, 2001). The research results show the impact of power distance in its contribution to intention to comply with ISP. This shift is social, meaning that respondents have an underlying reason to choose this action over others. Although some have described RCT as a theory of individual choice and others have defined it as a social phenomenon (Lovett, 2006), in this research, it is a social phenomenon that influences individual choice. Conforming to societal norms is

unavoidable since this also constitutes people's daily lives (Idang, 2015). This research is the first to introduce power distance as a part of RCT when investigating ISP compliance.

This construct is about choice in the RCT sense and understanding that a person's actions can protect organizational assets because of the cultural characteristic of power distance. One of the antecedents of intention is beliefs about consequences (Fishbein & Ajzen, 1975). It takes strength to stand against what is popular; that is the choice that a principled person must make in the present age, when defying authority is acceptable. Drawing from the premise that power distance should be considered an antecedent to attitudinal behavior, belief strength is an antecedent to attitudinal behavior (Sideridis et al., 1998). An employee could evaluate his/her action as taking a stand to do something good by complying with ISP. It could be said that power distance also contributes to TRA, and this study is the first to draw that conclusion.

Contribution to Practice

The study of ISP compliance is essential to any organization, especially when there seems to be no protection against information theft. Technology alone cannot offer the protection needed in any organization; therefore, dependency on the human is necessary. This study used data obtained from a high PDI country, and the contribution will be of practical use in such a country. The Nigerian government has commissioned the National Information Technology Development Agency (NITDA) to prepare an information security policy that protects government information systems.

- Promoting self-efficacy is important in every organization, as employees are a line of defense against potential information security problems. In the study, self-efficacy contributed substantially to the intention to comply with ISP. That finding should serve as a notice to management in any organization that technical and information security training are important components for business survival. Employees will perform their best if they are knowledgeable and confident, so training should not be limited to technical personnel since every employee has to work with some form of technology (Compeau & Higgins, 1995; Jaafar & Ajis, 2013).
- Employers should encourage every employee on the benefits of compliance. In this study's findings, employees derive a certain amount of gratification from knowing that they have done what is required (Bulgurcu et al., 2010). Employers should see this

sense of accomplishment as a sign that employees are invested in the organization's goals and leverage that by providing an incentive to encourage more such actions.

- Descriptive norms are what social beings do (they copy what others do). They also provide an excellent way to learn, as demonstrated by the result of the analysis (Merhi & Ahluwalia, 2019). Descriptive norms were significant in the results obtained, an indication that employees learn from each other, and management should take advantage of this fact by encouraging employees to share how they perform tasks. Information security training should involve hands-on sessions when employees work in groups, and rotations of group members should be encouraged.
- Sanctions are a necessary evil that did not show effects on ISP compliance intention. Therefore, it could only be applied in extreme cases to discourage negative response to ISP, but not to be used as a primary form of control. Sanctions should be applied when repeated warnings do not curb repeated security violations.
- Moral beliefs do not mean the same thing to every person. They do not have uniform applications; what people hear and how they translate them are different. Therefore, moral beliefs had no impact on ISP compliance. Management may pay attention to moral beliefs by inviting public speakers to encourage employees' moral principles without making it a religious event.
- Normative beliefs was significant, but its path coefficient was negative. The contribution is that management should not exert excessive pressure on employees to comply with ISP; instead, it should do other practical things discussed in this section. The intention is not to drive bad actors underground but bring change by encouraging good practices.
- Power distance was significant with a large path coefficient. The practical point to its significance is that it is a social construct that affects every employee in a high PDI country. Management can take advantage of this result and have employees with the cultural characteristic to be influencers in the organization. Training should incorporate power distance characteristics. Management could leverage PD by developing a profile of each employee for job assignments.

Limitations of the Study

There are several limitations in this study, and they are listed here.

- The study is not generalizable outside of Nigeria, because of differences in national culture.
- The survey was administered during a global lockdown, with only a few people allowed to work outside their homes; therefore, access was limited.
- Each construct was limited to three questions in the survey to encourage many people to complete it.
- There were 1,000 surveys distributed, 597 responded, but only 410 were useable because the study only used responses from businesses with ISP programs.
- In a self-reporting survey, there is the problem of reliability, and this study did not escape it. People understand questions differently and the responses to such questions may be dubious.
- There are possibilities that some respondents might have answered some questions without reading them.
- The cross-loading problems and correlations between factors across construct could also be sources of limitations.
- Time constraints and resources could be limitations.
- Answering questions on survey forms does not allow the respondents to explain the reasons for their answers.
- Over 40 percent of the people did not respond

There is overall satisfaction despite these limitations. In addition, the introduction of power distance as a variable contributes to the available body of knowledge, making it possible to include the construct in future studies.

Recommendation for Future Research

This research was to prove if power distance had a role in information security policy compliance. The results from analyses demonstrated that the desired goal was met. The study was exploratory, and not much could be done to explore other possible interactions; the hope is that further research would pick up from what has been done so far.

Generalizability is not guaranteed, but the same constructs and model could be used to obtain the desired results. The study done in one country may not produce the same results in another (Cheng, Li, Li, Holm, & Zhai, 2013). The model and the variables are developed for high PDI countries, so performing similar research would require expanding the question base for each variable to control for cross-loadings and correlations between factors and constructs.

This research was not developed to test for moderation and mediation between variables. Future research should test the mediating and moderating effects of age and gender on the relationship between power distance and intention to comply with ISP. The survey distribution should be expanded to include all the states in Nigeria, for example. The data collection process should consist of in-person and on-location interviews, with observations used for triangulation. Future research should also go above the intent to comply with ISP to explore actual acts of compliance.

Conclusions

The problem of information security will be here if there is technology. Researchers have done great studies to make available to organizations factors that may contribute to ISP compliance. Research findings based on various combinations of constructs and theories have proven to help businesses monitor and protect their assets, but those of different cultures cannot avail themselves of these findings because of cultural barriers. Technology is expanding so rapidly in other regions of the world that it seems overwhelming, and calls are out for research applicable in these regions based on their national cultures; this research is one of the answers to that call. This research set out to determine if PD had a role in information security policy compliance. The empirical results showed that power distance in combination with normative beliefs, moral beliefs, descriptive norms, benefits of compliance, self-efficacy, and sanctions based on available theories could support ISP compliance. One size fit all does not work in information security, so there is a need to base research on the organization's environment; this research has joined others in doing that.

Other researchers will see this as an opportunity to build on this foundation and bring protection to those in need. Organizations should be able to use the findings to improve their lots in the fight to address their ISP compliance problems. To encapsulate this,

it would be that the gap that existed at the start of this study has now been closed with the hope that it will help chip away at the ISP compliance problem.

REFERENCES

(NITDA), N. I. T. D. A. (2019). Nigeria Data Protection Regulation, 1–20. Retrieved from https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf

Acedo, F. J., & Jones, M. V. (2007). Speed of internationalization and entrepreneurial cognition: Insights and a comparison between international new ventures, exporters and domestic firms. *Journal of World Business*, *42*(3), 236–252. https://doi.org/10.1016/j.jwb.2007.04.012

Aigbomian, S. E., & Oboro, O. G. (2015). The Impact of Culture on Business Organizations. *Journal of Poverty, Investment and Development*, *16*(June), 404–411. https://doi.org/10.1080/10400410802391835

Ainuddin, R. A., Beamish, P. W., Hulland, J. S., & Rouse, M. J. (2007). Resource attributes and firm performance in international joint ventures. *Journal of World Business*, *42*(1), 47–60. https://doi.org/10.1016/j.jwb.2006.11.001

Ajzen, I. (1991). The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, *50*, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1980). Theory of Reasoned Action / Theory of Planned Behavior.

Akers, R. L. (1990). Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken. *Journal of Criminal Law and Criminology*, *81*(3), 653–676. Retrieved from https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=http://scholar.google.co.uk/&httpsredir=1&article=6670&context=jclc

Akinwande, M. O., Dikko, H. G., & Samson, A. (2015). Variance Inflation Factor: As a Condition for the Inclusion of Suppressor Variable(s) in Regression Analysis. *Open Journal of Statistics*, *05*(07), 754–767. https://doi.org/10.4236/ojs.2015.57075

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). Information security policy compliance: An empirical study of ethical ideology. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3018–3027. https://doi.org/10.1109/HICSS.2013.272

Albers-Miller, N. D., & Gelb, B. D. (1996). Business Advertising Appeals as a Mirror of Cultural Dimensions: A Study of Eleven Countries. *Journal of Advertising*,

XXV(Number 4).

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behaviour compliance conceptual framework. *Conferences in Research and Practice in Information Technology Series*, *105*, 47–55.

Aluko, M. A. O. (2003). The Impact of Culture on Organizational Performance in Selected Textile Firms in Nigeria. *Nordic Journal of African Studies*, *12*(2), 164–179. https://doi.org/10.4314/gjss.v4i1.22779

Ariff, M. S. M., Yeow, S. M., Zakuan, N., Jusoh, A., & Bahari, A. Z. (2012). The Effects of Computer Self-Efficacy and Technology Acceptance Model on Behavioral Intention in Internet Banking Systems. *Procedia - Social and Behavioral Sciences*, *57*, 448–452. https://doi.org/10.1016/j.sbspro.2012.09.1210

Awofala, A. O. A., Olabiyi, O. S., Awofala, A. A., Arigbabu, A. A., Fatade, A. O., & Udeani, U. N. (2019). Attitudes toward computer, computer anxiety and gender as determinants of pre-service science, technology, and mathematics teachers' computer self-efficacy. *Digital Education Review*, (36), 51–67. https://doi.org/10.1344/der.2019.36.51-67

Aytes, K., & Connolly, T. (2011). Computer Security and Risky Computing Practices. *Journal of Organizational and End User Computing*, *16*(3), 22–40. https://doi.org/10.4018/joeuc.2004070102

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *Proceedings of the International Conference on Cyber Security for Sustainable Society*, (July), 118–131.

Bagozzi, R. P., Yi, Y. (1988). On_the_Evaluation_of_Structure_Equation_Models.pdf. *Journal of the Academy of Marketing Science*, *16*(1), 74–94.

Bailey, W. C., & Smith, R. W. (1972). Punishment: Its Severity and Certainty. *The Journal of Criminal Law, Criminology, and Police Science*, *63*(4), 530. https://doi.org/10.2307/1141807

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*. https://doi.org/10.1037/0033-295X.84.2.191

Bandura, A. (1997). *Self-Efficacy The Exercise of Control*. W. H. Freeman and Company, New York.

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 Information Systems*, *19*(8), 689–715. https://doi.org/10.17705/1jais.00506

Bartlett, J. E. I., Kotrlik, J. W. ., & Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, *19*(1), 43.

Becker, G. S. (1974). *Crime and Punishment: An Economic Approach. In: Essays in the economics of crime and punishment.* (B. G.S. & L. W.M., Eds.) (Vol. I). Cambridge, MA: National Bereau of Economic Research, Cambridge (MA): NBER. Retrieved from http://www.nber.org/chapters/c3625

Benitez, J., Henseler, J., Castillo, A., & Schuberth, F. (2019). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. *Information and Management*, (October 2017). https://doi.org/10.1016/j.im.2019.05.003

Birkinshaw, J., Morrison, A., & Hulland, J. (1995). Structural and competitive determinants of a global integration strategy. *Strategic Management Journal*, *16*(8), 637–655. https://doi.org/10.1002/smj.4250160805

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 103–122.

Borena, B. ., & Bélanger, F. . (2013). Religiosity and information security policy compliance. *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, *4*(November), 2848–2855. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84893234119&partnerID=40&md5=c905534fca7da61e4491ead314406ae4

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164. https://doi.org/10.1057/ejis.2009.8

Brock, D. M., Shenkar, O., Shoham, A., & Siscovick, I. C. (2008). National culture and

expatriate deployment. *Journal of International Business Studies*, *39*(8), 1293–1309. https://doi.org/10.1057/palgrave.jibs.8400361

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. https://doi.org/10.1093/bja/aeq366

Burns, T., & Roszkowska, E. (2016). Rational Choice Theory: Toward a Psychological, Social, and Material Contextualization of Human Choice Behavior. *Theoretical Economics Letters*, *06*(02), 195–207. https://doi.org/10.4236/tel.2016.62022

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, *56*(2), 81–105. https://doi.org/10.1037/h0046016

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior Mark Chan National University of Singapore Irene Woon School of Computing , National University of Singapore Atreyi Kankanhalli School of Com. *Journal of Information Privacy and Security*, *1*(3), 18–41. https://doi.org/10.2307/3151312

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 and Security*, *39*(PART B). https://doi.org/10.1016/j.cose.2013.09.009

Cheolho Yoon1, carlyoon@empal. co., Jae-Won Hwang2, hjw504@Kunsan. ac. k., & Kim rhkim@ucr.edu, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, *23*(4), 407–415. Retrieved from https://proxy.library.mcgill.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eft&AN=89084300&site=ehost-live&scope=site

Chin, W. W., & Dibbern, J. (2010). An Introduction to a Permutation Based Procedure for Multi-Group PLS Analysis: Results of Tests of Differences on Simulated Data and a Cross Cultural Analysis of the Sourcing of Information System Services Between Germany and the USA. *Handbook of Partial Least Squares*, (June 2015). https://doi.org/10.1007/978-3-540-32827-8

Chinwuba, N. N. (2015). Human Identity: Child Rights and the Legal Framework for Marriage in Nigeria. *Marriage and Family Review*, *51*(4), 305–336. https://doi.org/10.1080/01494929.2014.938286

Choi, M., Levy, Y., & Anat, H. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC - Workshop on Information Security and Privacy (WISP) 2013*, (December), 1–19. Retrieved from https://nsuworks.nova.edu/gscis_facpres/98

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, *35*(6), 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005

Cialdini, R. B. (2007). DESCRIPTIVE SOCIAL NORMS AS UNDERAPPRECIATED SOURCES OF SOCIAL CONTROL. *Psychometrika*, *72*(2), 263–268. https://doi.org/10.1007/s11336-006-1560-6

Claudia, I. (2012). Modeling the impact of normative beliefs in the context of online buying: Direct and moderating effects. *The Romanian Economic Journal*, *15*(44), 243–262.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (Second). Mahwah, NJ: Lawrence Erlbaum Associates, Mahwah, NJ.

Cohen, J. (1992). A Power Primer. *Psychological Bulletin*, *112*(1), 155–159. https://doi.org/10.1038/141613a0

Coleman, J. (1992). Rational Choice Theory Advocacy And Critique - James S. Coleman.pdf. *Philosophical Psychology*. https://doi.org/10.1080/095150899105783

Collins, C. S., & Stockton, C. M. (2018). The Central Role of Theory in Qualitative Research. *International Journal of Qualitative Methods*, *17*(1), 1–10. https://doi.org/10.1177/1609406918797475

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/249688

Cronan, T. P., & Al-Rafee, S. (2008). Factors that influence the intention to pirate software and media. *Journal of Business Ethics*, *78*(4), 527–545. https://doi.org/10.1007/s10551-

007-9366-8

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, *29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Deloitte. (2019). Nigeria Cyber Security Outlook 2019. Retrieved from https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2019.html

Derouet, E. (2015). 13 Email Fraud Stats Every Security Professional Should Know, 11–12.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, *19*(4), 391–412. https://doi.org/10.1111/j.1365-2575.2007.00289.x

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resource Management Journal*, *18*(4), 21–39.

Dols, T., & Silvius, A. J. G. (2010). Exploring the Influence of National Cultures on Non-Compliance Behavior. *Communications of the IIMA*, *10*(3), 11–32.

Doran, R., & Larsen, S. (2016). The Relative Importance of Social and Personal Norms in Explaining Intentions to Choose Eco-Friendly Travel Options. *International Journal of Tourism Research*, *18*(2), 159–166. https://doi.org/10.1002/jtr.2042

Eri, Y., Aminul Islam, M., & Ku Daud, K. A. (2011). Factors that Influence Customers' Buying Intention on Shopping Online. *International Journal of Marketing Studies*, *3*(1), 128–139. https://doi.org/10.5539/ijms.v3n1p128

Expert Panel, Y. E. C. (2019). 10 Exciting Technological Innovations This Year And Their Implications. *Forbes.Com*. Retrieved from https://www.forbes.com/sites/theyec/2019/11/18/10-exciting-technological-innovations-

this-year-and-their-implications/#5fb70790730b

Falola, T. (2001). *Culture and Customs of Nigeria*. Westport, Connecticut: Greenwood Press.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitute, intention and behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Fock, H., Hui, M. K., Au, K., & Bond, M. H. (2013). Moderation Effects of Power Distance on the Relationship Between Types of Empowerment and Employee Satisfaction. *Journal of Cross-Cultural Psychology*, *44*(2), 281–298. https://doi.org/10.1177/0022022112443415

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39. https://doi.org/10.2307/3151312

Forward, S. E. (2009). The theory of planned behaviour: The role of descriptive norms and past behaviour in the prediction of drivers' intentions to violate. *Transportation Research Part F: Traffic Psychology and Behaviour*, *12*(3), 198–207. https://doi.org/10.1016/j.trf.2008.12.002

Garson, G. D. (2016). *Partial Least Squares: Regression & Structural Equation Models*. *G. David Garson and Statistical Associates Publishing*.

Gastil, R. D. (1961). Behavior The Determinants of Human. *American Anthropologist*, *63*(6), 1281–1291.

Gefen, D., & Straub, D. W. (1997). Gender Differences in the Perception and Use of E-Mail: An Extension to the Technology Acceptance Model. *MIS Quarterly*, *21*(4), 389. https://doi.org/10.2307/249720

Geisser, S. (1974). A Predictive Approach to the Random Effect Model. *Biometrika*, *61*(1), 101–107. https://doi.org/10.2307/2334290

George, J. F. (2004). The theory of planned behavior and Internet purchasing. *Internet Research*, *14*(3), 198–212. https://doi.org/10.1108/10662240410542634

Goldsmith, R. E., Montford, W. J., & Goldsmith, R. E. (2014). Digital Commons @ Georgia Southern The Influence of Descriptive Norms on Investment Risk The Influence of Descriptive Norms on Investment Risk.

Goldstein, J. R., & Kenney, C. T. (2001). Marriage Delayed or Marriage. *American Sociological Review*, *66*, 506–519.

Goodhue, D. L., Lewis, W., & Thompson, R. (2012). DOES PLS HAVE ADVANTAGES FOR SMALL SAMPLE SIZE OR NON-NORMAL DATA? *MIS Quarterly*, *36*(3), 1335–1345.

Hair, J. F. J., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (Pls-Sem)* (2nd ed.). Los Angeles: SAGE Publications Inc.

Hair, Joe F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hair, Joseph F., Black, W. C., Babin, B. J., & Anderson, R. E. (2015). *Multivariate Data Analysis* (Seventh). Tamil Nadu: Pearson India Education Services Pvt Ltd.

Hale, J. L., Householder, B. J., & Greene, K. L. (2003). The Theory of Reasoned Action. *The Persuasion Handbook: Developments in Theory and Practice*. https://doi.org/10.1016/S0002-8223(99)00012-7

Hameed, M. A., & Asanka Gamagedara Arachchilage, N. (2018). Understanding the influence of individual's self-efficacy for information systems security innovation adoption: A systematic literature review. *ArXiv*.

Hechter, M., & Kanazawa, S. (1997). Sociological Rational Choice Theory. *Annual Review of Sociology*, *23*(1), 191–214. https://doi.org/10.1146/annurev.soc.23.1.191

Henseler, J. (2018). Partial least squares path modeling: Quo vadis? *Quality and Quantity*, *52*(1), 1–8. https://doi.org/10.1007/s11135-018-0689-6

Henseler, J., Ringle, C. M., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing*, *20*(2009), 277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in

organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hofstede, G. (1994). The business of international business is culture. *International Business Review*, *3*(1), 1–14. https://doi.org/10.1016/0969-5931(94)90011-6

Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, *2*(1), 1–26. https://doi.org/10.9707/2307-0919.1014

Hofstede, G. (2017). Country Comparison. *Hofstede Insights*. https://doi.org/10.1039/c3ee42101e

Hofstede, G., Jan Hofstede, G., & Minkov, M. (2010). *Cultures and Organizations*. *Cultures and Organizations* (3rd ed.). McGraw Hill Companies. https://doi.org/10.1007/s11569-007-0005-8

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

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. https://doi.org/10.1145/1953122.1953142

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic Management Journal*, *20*(2), 195–204. https://doi.org/10.1002/(sici)1097-0266(199902)20:2<195::aid-smj13>3.3.co;2-z

Icek, A. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. Retrieved from http://www.sciencedirect.com/science/article/pii/074959789190020T

Idang, G. E. (2015). African Culture and Values. *Phronimon*, *16*(2), 97–111. Retrieved from http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1561-40182015000200006&lng=en&nrm=iso&tlng=en

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1). https://doi.org/10.1016/j.im.2013.10.001

Ifinedo, P., & Idemudia, E. C. (2017). Factors influencing employees' participation in non-malicious, information systems security deviant behavior: Focus on formal control mechanisms and sanctions. *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, *2017-Augus*, 1–10.

Jaafar, N. I., & Ajis, A. (2013). Organizational Climate and Individual Factors Effects on Information Security Faculty of Business and Accountancy. *International Journal of Business and Social Science*, *4*(10), 118–131.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3). https://doi.org/10.1057/ejis.2015.15

Johnston, B. A. C., & Warkentin, M. (2010). F EAR A PPEALS AND I NFORMATION S ECURITY B EHAVIORS : A N E MPIRICAL S TUDY 1, *34*(1), 1–20.

Jones, M., & Alony, I. (2007). The cultural impact of information systems – through the eyes of Hofstede – a critical journey what is culture? *Issues in Informing Science and Information Technology*, *4*, 408–419. Retrieved from http://books.google.com/books?hl=en&lr=&id=2t9INNWbB_QC&oi=fnd&pg=PA407&dq=The+Cultural+Impact+of+Information+Systems+?+Through+the+Eyes+of+Hofstede+?+A+Critical+Journey&ots=kygzRg9qWr&sig=beuXtEkwehV07Y7WrSo0KJHNwXU

Jung, J. M., Polyorat, K., & Kellaris, J. J. (2009). A cultural paradox in authority-based advertising. *International Marketing Review*, *26*(6), 601–632. https://doi.org/10.1108/02651330911001314

Kadir, M. R. A., Norman, S. N. S., Rahman, S. A., Ahmad, A. R., Bunawan, A.-A., & Bunawan, A. (2017). Information Security Policies Compliance among Employees in Cybersecurity Khalid S . Soliman International Business Information Management

Association (IBIMA). *Proceedings of the 28th International Business Information Management Association Conference*, (November 2016).

Kawulich, B. (2009). *The Role of Theory in Research*. inbook.

Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *The Scientific World Journal*, *2014*, 1–12. https://doi.org/10.1155/2014/463870

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, *28*(1), 227–261. https://doi.org/10.1111/isj.12131

Koloseni, D., Lee, C. Y., & Lee, G. M. (2018). Journal of Applied Structural Equation Modeling Security Compliance in Public Institutions: An Integrative Approach. *Journal of Applied Structural Equation Modeling*.

Krebs, B. (2014). Email Attack on Vendor Set Up Breach at Target. *KrebsonSecurity*. Retrieved from http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

Kruger, H. A., Drevin, L., Flowerday, S., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *2011 Information Security for South Africa*, 1–7. https://doi.org/10.1109/ISSA.2011.6027505

Lawan, L. A., & Zanna, R. (2013). Evaluation of Socio - Cultural Factors Influencing Consumer Buying Behaviour of Clothes in Borno State , Nigeria. *International Journal of Basic and Applied Science*, *1*(3), 519–529.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management*, *41*(6), 707–718. https://doi.org/10.1016/j.im.2003.08.008

Leidner, D. E., Carlsson, S., & Elam, J. J. (1995). A cross-cultural study of executive information systems. *Vol. III. Proceedings of the Twenty-Eighth Hawaii International Conference On*, *3*, 91–100.

Lekhanya, L. (2013). Cultural Influence On The Diffusion And Adoption Of Social Media Technologies By Entrepreneurs In Rural South Africa. *... Business & Economics Research Journal (IBER)*, *12*(12), 1563–1575. Retrieved from http://www.cluteonline.com/journals/index.php/IBER/article/view/8250

Levin, J., & Milgrom, P. (2004). Introduction to Choice Theory. *Microeconomics*, (September), 1–25. https://doi.org/10.1006/obhd.2000.2941

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://doi.org/10.1016/j.dss.2009.12.005

Lim, T. Y. ., & Lau, J. L. (2017). THE ROLE OF EMPLOYEE EMPOWERMENT IN HIGH POWER-DISTANCE ORGANISATIONS. *International Journal of Accounting, Finance and Business*, *2*(6), 1–17.

Lovett, F. (2006). Rational choice theory and explanation. *Rationality and Society*, *18*(2), 237–272. https://doi.org/10.1177/1043463106060155

Lowry, P. B., & Moody, G. D. (2015). Proposing the controlreactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal 25, 5*.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Mathew, S., & Perreault, C. (2016). Cultural history, not ecological environment, is the main determinant of human behaviour. *Proc. R. Soc. B 283 : 20160177.*, 2–4. https://doi.org/http://dx.doi.org/10.1098/rspb.2016.0177

Mccrum-gardner, E. (2010). Calculations made simple. *International Journal of Therapy and Rehabilitation*, *17*(1), 10–14.

Merhi, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, *92*(October 2018), 37–46. https://doi.org/10.1016/j.chb.2018.10.031

Merriam-Webster. (n.d.). Theory. Retrieved April 6, 2021, from https://www.merriam-webster.com/dictionary/theory

Mintu-Wimsatt, A., & Graham, J. L. (2004). Testing a negotiation model on Canadian anglophone and Mexican exporters. *Journal of the Academy of Marketing Science*, *32*(3), 345–356. https://doi.org/10.1177/0092070304266123

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311.

https://doi.org/10.25300/MISQ/2018/13853

Mooij, M. De, & Hofstede, G. (2007). The Hofstede model: Applications to global branding and advertising stratgey and research. *International Journal of Advertising*, *29*(1), 85–110. https://doi.org/10.2501/S026504870920104X

Moran, R. F. (2004). How Second-Wave Feminism Forgot the Single Woman. *Hofstra L. Rev.*, *33*(1), 223.

Mykytyn, P. P., & Harrison, D. A. (1993). The Application of the Theory of Reasoned Action to Senior Management and Strategic Information Systems. *Information Resources Management Journal (IRMJ)*, *6*(2), 15–26. https://doi.org/10.4018/irmj.1993040102

Myyry, L., Siponen, M., Pahnila, 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 Information Systems*, *18*(2), 126–139. https://doi.org/10.1057/ejis.2009.10

Nath, R., & Murthy, N. R. V. (2004). A study of the relationship between Internet diffusion and culture. *Journal of International Technology and Information*, *13*(1994), 123–132. Retrieved from http://www.iima.org/JITIM/JITIM 13 Downloads/P11-Nath.pdf

Norman, P., Clark, T., & Walker, G. (2005). The theory of planned behavior, descriptive norms, and the moderating role of group identification. *Journal of Applied Social Psychology*, *35*(5), 1008–1029. https://doi.org/10.1111/j.1559-1816.2005.tb02157.x

Oghojafor, B., George, O., & Owoyemi, O. (2012). Corporate governance and National culture are siamese twins: The case of cadbury(Nigeria) Plc. *International Journal of Busuness and Social Science*, *3*(15), 269–278.

Olavsrud, T. (2014). 11 Steps Attackers Took to Crack Target | CIO. Retrieved from http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. *Pacis 2007 Proceedings*, (April), 438–439. https://doi.org/10.1007/978-0-387-72367-9_12

Pahnila, S., Siponen, M., Mahmood, A., Box, P. O., Oulun, F.-, Siponen, E. M., & Pahnila, S. (2007). Employees ' Behavior towar ds IS Secur ity Policy Compliance University of Oulu , Department of Information Processing Department of Information and Decision

Sciences , University of Texas at El Paso. *Proceedings of the 40th Hawaii International Conference on System Sciences*, 1–10.

Pahnila, S., Siponen, M. T., Mahmood, A., IMONIANA, J. O., Boudreau, M.-C., Gefen, D., … Rao, H. R. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *MIS Quarterly*, *1*(3), 1–12. https://doi.org/10.1155/2014/463870

Paternoster, R., & Simpson, S. (1996). Sanction Threats and Appeals to Morality : Testing a Rational Choice Model of Corporate Crime. *Law & Society Review*, *30*(3), 549–583.

Peltier, T. R. (2004). *Information security policies, procedures, and standards: A Practitioner's Reference* (Second Edi). Boca Raton, FL: Auerbach.

Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of Operations Management*, *30*(6), 467–480. https://doi.org/10.1016/j.jom.2012.06.002

Pham, H. C., Brennan, L., & Furnell, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications*, *46*, 96–107. https://doi.org/10.1016/j.jisa.2019.03.012

Ringle, C. M., Wende, S., & Becker, J. M. (2015). "SmartPLS 3.0." BoenningStedt: SmartPLS GmbH. Retrieved from http://www.smartpls.com

Rivis, A., & Sheeran, P. (2017). Descriptive norms as an additional predictor in the theory of planned behavior: A meta-analysis. *Planned Behavior: The Relationship between Human Thought and Action*, *22*(3), 43–62. https://doi.org/10.4324/9781315126449-4

Robinson, C., & Schumacker, R. (2009). Interaction effects: centering, variance inflation factor, and interpretation issues. *Multiple Linear Regression Viewpoints*, *35*(1), 6–11.

Roehling, P. V., Roehling, M. V., & Moen, P. (2001). The relationship between work-life policies and practices and employee loyalty: A life course perspective. *Journal of Family and Economic Issues*, *22*(2), 141–170. https://doi.org/10.1023/A:1016630229628

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. *In J.Cacioppo & R. Petty (Eds.) Social Psychophysiology* (Vol. 19). New York: Guilford Press. https://doi.org/10.1016/0022-1031(83)90023-9

Rogers, Ronald W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude

Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosenbloom, B., & Larsen, T. (2003). Communication in international business-to-business marketing channels. Does culture matter? *Industrial Marketing Management*, *32*(4), 309–315. https://doi.org/10.1016/S0019-8501(01)00202-4

Rousseau, D. M. (1990). Normative Beliefs in Fund-Raising Organizations: Linking culture to organizational performance and individual responses. *Group & Organization Management*, *15*(4), 448–460. https://doi.org/10.1177/105960119001500408

Sawaya, Y., Sharif, M., Christin, N., & Kubota, A. (2017). Self-confidence trumps knowledge: A cross-cultural study of security behavior. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2202–2214. https://doi.org/10.1145/3025453.3025926

Sideridis, G. D., Kaissidis, A., & Padeliadu, S. (1998). Comparison of the theories of reasoned action and planned behaviour. *British Journal of Educational Psychology*, *68*(4), 563–580. https://doi.org/10.1111/j.2044-8279.1998.tb01312.x

Siponen, M. T. (2000). Conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information and Management*, *49*(7–8), 334–341. https://doi.org/10.1016/j.im.2012.06.004

Škerlavaj, M., Su, C., & Huang, M. (2013). The moderating effects of national culture on the development of organizational learning culture: A multilevel study across seven countries. *Journal for East European Management Studies*, *18*(1), 97–134.

Smith, J. R., & Louis, W. R. (2009). Do As We Say and As We Do: The Interplay of Descriptive and Injunctive Group Norms in the Attitude-Behaviour Relationship. *British Journal of Social Psychology*, *26*(3), 201–231.

Smith, J. R., Louis, W. R., Terry, D. J., Greenaway, K. H., Clarke, M. R., & Cheng, X. (2012). Congruent or conflicted? The impact of injunctive and descriptive norms on environmental intentions. *Journal of Environmental Psychology*, *32*(4), 353–361. https://doi.org/10.1016/j.jenvp.2012.06.001

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management and Computer Security*, *22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Stone, M. (1974). Cross-Validatory Choice and Assessment of Statistical Predictions. *Journal of the Royal Statistical Society: Series B (Methodological)*, *36*(2), 111–133. https://doi.org/10.1111/j.2517-6161.1974.tb00994.x

Straub, D. W., & Weike, R. J. (1998). Coping with systems Risk: Security Planning Models for Management Decision Making. *MIS Quaterly*, *December*(December), 441–469.

Straub, Detmar, Boudreau, M.-C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems*, *13*, *Articl*(March), 380–427. https://doi.org/10.17705/1cais.01324

Straub, DW, & Welke, R. (1998). Coping with systems risk: security planning models for management decision making. *Mis Quarterly*, *22*(4), 441–469. Retrieved from http://www.jstor.org/stable/249551

Vance, A., Siponen, M., & Pahnila, S. (2012a). Motivating IS security compliance: Insight from Habit and Protection Motivation Theory. *Information & Management*, *49*(49), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vance, A., Siponen, M., & Pahnila, S. (2012b). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vance, A., & Siponen, M. T. (2012). IS Security Policy Violations. *Journal of Organizational and End User Computing*, *24*(1), 21–41. https://doi.org/10.4018/joeuc.2012010102

Verizon Business. (2018). 2018 Data breach investigations report. *Trends*, 1–62. Retrieved from rp_data-breach-investigations-report-2013_en_xg.pdf

Westland, C. J. (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications*, *9*(6), 476–487. https://doi.org/10.1016/j.elerap.2010.07.003

White, K. M., Smith, J. R., Terry, D. J., Greenslade, J. H., & Blake, M. (2009). QUT Digital Repository : Running head : SOCIAL INFLUENCE IN THE TPB Social influence in the theory of planned behaviour : The role of descriptive , injunctive , and Queensland

University of Technology University of Exeter University of Queensland. *Society*, *48*, 135–158.

Winick, E., Regalado, A., Woyke, E., Snow, J., Condliffe, J., Metz, R., … Rotman, D. (2018, February). 10 Breakthrough Technologies 2018. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/lists/technologies/2018/

Wittek, R. (2013). Rational Choice. *Rational Choice*, (January 2013), 2013–2016. https://doi.org/10.1007/978-1-137-42744-1

Wong, K. K.-K. (2013). 28/05 - Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS. *Marketing Bulletin*, *24*(1), 1–32. Retrieved from http://marketing-bulletin.massey.ac.nz/v24/mb_v24_t1_wong.pdf%5Cnhttp://www.researchgate.net/profile/Ken_Wong10/publication/268449353_Partial_Least_Squares_Structural_Equation_Modeling_(PLS-SEM)_Techniques_Using_SmartPLS/links/54773b1b0cf293e2da25e3f3.pdf

Wong, K. K. (2019). *Mastering Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS in 38 Hours*. Bloomington: iUniverse.

Woon, I. M. Y., Tan, G. . W., & Low, R. . T. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In *Twenty-Sixth International Conference on Information Systems* (Vol. 5, pp. 367–380).

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Zhang, Y., & Begley, T. M. (2011). Power distance and its moderating impact on empowerment and team participation. *International Journal of Human Resource Management*, *22*(17), 3601–3617. https://doi.org/10.1080/09585192.2011.560877

APPENDICES

APPENDIX A: LETTER OF CONSENT

Title of Research Project: **Exploring High-Power Distance Among Other Variables in Information Security Policy Compliance**

Principal Investigator: Dr. Kevin Streff, Chair, kevin.steff@dsu.edu, 605-270-4427

Co-Investigators: Erasmus Etim, PhD student, Erasmus.etim@trojans.dsu.edu

Invitation to be Part of a Research Study

You are invited to participate in a research study. In order to participate, you must be 18 years or older. Taking part in this research project is voluntary. Please take time to read this entire form and ask questions before deciding whether to take part in this research project.

What is the study about and why are we doing it?

The purpose of the study is to determine the role of high-power distance in complying with information security policy. About 500 people will take part in this research.

What will happen if you take part in this study?

If you agree to take part in this study, you will be asked to complete anonymous survey questionnaires which will take approximately 15 minutes.

How could you benefit from this study?

Although you will not directly benefit from being in this study, businesses and other organizations will be able to apply the results of this study to help their employees comply with information security policies.

How will we protect your information?

The records of this study have no identifiers as the questionnaires are distributed and completed anonymous.

Your Participation in this Study is Voluntary

It is totally up to you to decide to be in this research study. Participating in this study is voluntary. Even if you decide to be part of the study now, you may change your mind and stop at any time. You do not have to answer any questions you do not want to answer.

Contact Information for the Study Team and Questions about the Research

The researchers conducting this study are Dr. Kevin Streff, and Erasmus Etim. You may contact us to ask any questions you have now, or if you have questions, concerns, or complaints about the research later, please contact Dr. Kevin Streff at 605-270-4427 during the day.

If you have any questions, concerns or complaints now or later, you may contact us at the number below. If you have any questions about your rights as a human subject, complaints, concerns or wish to talk to someone who is independent of the research, contact the Dakota State Institutional Review Board staff at 605-256-5038. Thank you for your time.

Your Consent

Before agreeing to be part of the research, please be sure that you understand what the study is about. We will give you a copy of this document for your records [or you can print a copy of the document for your records]. If you have any questions about the study later, you can contact the study team using the information provided above.>

APPENDIX B: IRB APPROVAL LETTER

Institutional Review Board

DAKOTA STATE UNIVERSITY

820 N, Washington Ave
Madison, SD 57042

Expedited Review Determination

Date: February 11, 2021

To: Kevin Streff & Erasmus Etim

Project Title: Exploring High-Power Distance Among Other Variables in Information Security Policy Compliance

Approval #: 20210211

Dear Dr. Streff & Mr. Etim:

The Dakota State University IRB has conducted expedited review, in accordance with federal requirements under 45 CFR 46.110, of your project and approved it on February 11, 2021. This approval was based on your project's meeting the condition of:

Research that only includes no more than minimal risk to participants.

To maintain its approved status, your research must be conducted according to the most recent plan reviewed by the IRB. You must notify the IRB in writing within four days of:

- Any changes to your research plan or departure from its description as stated in your application and/or other documents submitted;
- Any unexpected or adverse event that occurs in relation to your research project.

Within 364 days of the date of this letter, you must submit:

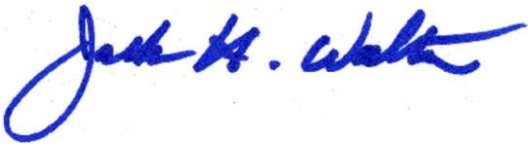
- A notice of closure once all project activities have concluded;

-- or --

- An application for extension of time to complete your research.

If you have any questions regarding this determination or during the course of your study, please contact us at 605-256-5100 or irb@dsu.edu. Best wishes to you and your research.

Yours truly,



Jack H. Walters, Chair

APPENDIX C: SURVEY QUESTIONNAIRE

Dakota State University

Erasmus Etim

Survey Questions

---

1. Does your organization have Information Security Policy (ISP)?

☐ Yes ☐ No

Please answer the following questions by circling one of the numbers: 1-Strongly Disagree, 2-Disagree, 3-Somewhat Disagree, 4- Neither Agree or Disagree, 5-Somewhat Agree, 6-Agree and 7-Strongly Agree.

Sanctions

2.	I will be demoted if I do not comply with information security policy.	1 2 3 4 5 6 7
3.	I will be reprimanded if I do not comply with information security policy.	1 2 3 4 5 6 7
4.	I will incur financial loss if I do not comply with information security policy.	1 2 3 4 5 6 7

Moral Beliefs

5.	It is morally right to comply with information security policy.	1 2 3 4 5 6 7
6.	I feel that it is my moral obligation to comply with information security policy.	1 2 3 4 5 6 7
7.	My morality compels me to comply with information security policy.	1 2 3 4 5 6 7

Benefits of Compliance

8.	I will feel satisfied if I comply with information security policy.	1 2 3 4 5 6 7
9.	I will feel accomplished if I comply with information security policy.	1 2 3 4 5 6 7
10.	I will feel content if I comply with information security policy.	1 2 3 4 5 6 7

Self-efficacy

11.	I have the required knowledge to comply with information security policy.	1 2 3 4 5 6 7
12.	I have the required skills to comply with information security policy.	1 2 3 4 5 6 7
13.	I have the required competencies to comply with information security policy.	1 2 3 4 5 6 7

Descriptive Norms

14.	I believe that other employees comply with information security policy.	1 2 3 4 5 6 7
15.	I know that other employees comply with information security policy.	1 2 3 4 5 6 7
16.	I have a strong opinion that majority of employees comply with information security policy.	1 2 3 4 5 6 7

Normative Beliefs

17.	Upper management believes that I should comply with information security policy.	1 2 3 4 5 6 7
18.	My immediate superiors believe that I should comply with information security policy.	1 2 3 4 5 6 7
19.	My colleagues believe that I should comply with information security policy.	1 2 3 4 5 6 7

Power Distance

20.	Organization's rules should not be broken, therefore I have to comply with information security policy.	1 2 3 4 5 6 7
21.	I respect management decisions, therefore I have to comply with information security policy.	1 2 3 4 5 6 7
22.	Management has the right to expect complete obedience in work related matters, therefore I have to comply with information security policy.	1 2 3 4 5 6 7

Intention to Comply

23.	I intend to comply with information security policy.	1 2 3 4 5 6 7
24.	I intend to help others comply with information security policy.	1 2 3 4 5 6 7
25.	I encourage others to comply with information security policy.	1 2 3 4 5 6 7

Information About you and Your Organization

---

26. Gender

☐ Male ☐ Female

27. Age

☐ 18-29

☐ 30-39 ☐ 40-49

☐ 50-59 ☐ 60 and above

28. Education

☐ Less than secondary school ☐ Bachelor's degree

☐ Completed secondary school ☐ Graduate degree

☐ Some university credits ☐ Other

29. Job role

☐ Information technology ☐ Other

30. Time on the job in the present organization

☐ Less than 1 year ☐ 10 – 15 years

☐ 1 – 5 years ☐ More than 15 years

☐ 5 – 10 years

31. Time in the present position

☐ Less than 1 year ☐ 10 – 15 years

☐ 1 – 5 years ☐ More than 15 years

☐ 5 – 10 years

32. Number of employees in your organization

☐ Less than 100 ☐ 501 – 1000

☐ 100 – 500 ☐ More than 1000

33. Organization's sector

☐ Education ☐ Government

☐ Financial Services ☐ Health Care

☐ Information Technology ☐ Telecommunications

☐ Manufacturing ☐ Nonprofit

☐ Other, please specify_____

Thank you for taking time to participate