Power Distance as a Variable in Assessing Employees’ Behavior towards Information Security Policy Compliance in a High-Power Distance Society: An Exploratory Study

Erasmus E. Etim1 | Kevin Streff2 | Insu Park3 | Pam Rowland4

1Doctoral Student, Dakota State University
2Professor, Dakota State University
3Professor, Dakota State University
4Professor, Dakota State University

Abstract

Information security is a concern of every business, therefore the need for employees to comply with a policy that would protect the organization’s assets. The model developed for this research was based on Protection Motivation Theory, Theory of Planned Behavior, and Rational Choice Theory. There were 129 responses from Nigeria used to validate the model. The data analysis using PLS-SEM resulted in these findings: self-efficacy, normative beliefs, and power distance were significant, therefore impacting. Therefore, not significant descriptive norms did not positively impact intention to comply with information security policy. Power distance was impactful on employees’ intention to comply with information system policy and contributed to theory and practice; respondents chose to do right by their intention to comply with information security policy. Training and managerial oversight in policy compliance are significant since those actions would help protect the organization’s information. The analysis showed the adverse effect of a high correlation between indicators of different constructs.

Keywords: Information security compliance, Phishing, Self-efficacy, Descriptive norms, Normative beliefs, Power distance

1 INTRODUCTION

Information security policy (ISP) is crafted for an organization’s employees to guide in what to do to protect the organization’s assets and resources (1); current events do not support the intended outcome. According to Myyry, Siponen, Pahnila, Vartiainen, and Vance (2), 90% of organizations have at least one information security occurrence in a year. The 2006 Computer Security Institute / Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey indicates that organizations are exposed to thirteen categories of attacks, ranging from viruses, laptop/mobile theft to unautho-
rized access to information (3). There are concerns about phishing, weak and unprotected passwords that would allow information security breaches.

Phishing is a way criminal represents himself as trusted entities using social engineering to obtain information for exploitation (4). Phishing attacks do not show signs of slowing down, mainly by email, and one reason for the increase is that they are effortless to create, and email filters are not very successful as detecting agents (5, 6). In 2014 28.8% of phishing attacks were to steal financial data, and the business segment that suffered the worst episode was the mail service (7). Between October 2013 and January 2015 FBI saw a 270 percent increase in victims of fake email crime referred to as the CEO emails, which resulted in a $2.3 billion loss to businesses (7).

The past 50 years have witnessed different evolutions of an imperfect security system we know as password. Against all proposed alternative forms of ways to secure systems and data, it has survived and gained widespread use (8). Weak passwords are subject to guessing attacks and the leakage of password hash database makes them vulnerable, as pointed out by Chatterjee, Athayle, Akawhe, Juels, and Ristenpart [(9, 10). The success of the first form of attack depends on the complexity of the password. Password complexity depends on the user, and the user must have the knowledge and desire to provide such a complex password.

Statistics based on over one hundred forty-three million data records collected by Verizon and the United States Secret Service, after analysis, show that out of one hundred forty-one confirmed breaches, insider attacks were responsible for 46% of them (11). Criminals seek access to enterprise systems by exploiting connections to the organization, as employees or supply chain partners, for example, the breach at Target retail company (12). Information security researchers are constantly investigating factors that would help increase ISP compliance and reduce data breaches, but power distance is not one of the factors investigated.

Power distance (PD), as defined by Hofstede, Jan Hofstede, and Minkov (13), is "the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally." In a high-power distance index (PDI) society, subordinates must obey their superiors and carry out their instructions without questions. In a low PDI society, the opposite is true (14, 15). The environment’s culture shapes a person’s behavior he/she grows up in (15, 16).

ISP is a crucial tool to guide employees on managing incidents they may face, such as those stated above. Still, the responsibility is left to the employees to implement the instructions outlined in such policy. Behavior subsequently determines the response exhibited by each employee. This research aims to introduce power distance as one of the factors to research in assessing the behavior of employees in a high PDI society toward ISP, which would address the question (17):

1. How would PD influence employees in a high PDI society to respond to ISP compliance in their organizations?

The theoretical background for the model in this research is Protection Motivation Theory (PMT) (18), which leads to the concept that possessing the right skills and knowledge will facilitate compliance with ISP, self-efficacy. Theory of Planned Behavior (TPB) (19), subjective norms will encourage ISP compliance. Cultural attributes will influence intention to comply with ISP stemming from Rational Choice Theory (RCT) (20). The research adds to the available body of knowledge in information security by introducing the concept of power distance as one of the constructs that need investigation. It provides practical insight to businesses that may expand into high PDI countries.

The rest of the paper is as follows: Literature review, Theoretical Background, Research Model and
2 | LITERATURE REVIEW

Early research on ISP was based on sanctions and fear appeals (21, 22). Focus has shifted to behavior-based research recently to highlight variables responsible for ISP violations (23) Building psychological profiles and behavior models to predict the potential for ISP compliance or violations have proven partially successful (23–25). The following literature shows employees’ behaviors considering ISP compliance.

In an attempt to find why employees may go rogue and violate ISP, Hu, Xu, Dinev, and Ling (26) investigated deterrence effectiveness. The authors discovered that comprehensive ISP and extensive awareness training did not deter employees from ISP violations. The prime reason for their finding was that violators derived benefits from violation of ISP than compliance. The concept of Neutralization Theory (NT), violators rationalizing their actions, was introduced by Siponen and Vance (27) as an alternative to deterrence in the study of ISP violations. The research was designed based on Sykes and Matza’s (28) neutralization techniques; denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, and the appeal to higher loyalties. The collected data analysis pointed to neutralization as a predictor of intention to violate ISP (26).

A study conducted by Bulgurcu et al. (21) included normative beliefs as one of the constructs that affected employees’ ISP compliance. Normative beliefs are social pressures centered around employment, based on what colleagues, managers, and executives think (21). Based on data analysis from 464 participants, the finding supported their hypothesis that normative beliefs positively influenced employees’ intention to comply with ISP.

Cheng, Li, Li, Holm, and Zhai (29) investigated the effect of subjective norms and co-worker behavior, both grouped as social pressure, on employee’s intention to comply or violate ISP. Their proposed hypotheses were that the immediate supervisor’s opinion weighed negatively on employees’ intent to violate ISP, and co-worker’s behavior would positively impact employees’ intention to violate ISP. The data supported the two hypotheses on the evaluation of 185 completed surveys returned (29).

Self-efficacy is an essential aspect of information security; it involves assessing individual skills, knowledge, and confidence in performing required tasks (18, 30). Rhee, Kim, and Ryu (31) investigated the influence of self-efficacy on the end users’ information security behavior; they postulated that those with higher self-efficacy in information security use more security software and are more security conscious and dedicated to information security. Analysis of the survey data returned by 415 graduate students provided significant results supporting the stated hypotheses (31).

Power distance as a construct in ISP compliance deserves investigation. The study of PD in another discipline makes it possible to understand its effect on ISP compliance. Albers-Miller and Gelb (32) wanted to answer whether business advertisement had to mirror cultural dimension, including power distance. In a study conducted in eleven countries, five out of eight appeals coded for power distance showed significant support leading the authors to conclude that general advertisement across culture was not advisable. Target the market’s culture when advertising to specific people (32). Ahmed, Mouratidis, and Preston (33) observed that website design was one-dimensional, excluding high power distance and high-context culture contents. Based on several websites, they developed guidelines for websites that incorporated components that would appeal to high power distance and high context cultures.

Another area that depends on behavior is the detection and response to phishing emails. Employees must examine phishing emails that escape filters visually to determine their authenticity, therefore the following research outcome. One of the signs that shows an email to be fake is an IP address in the link, but more sophisticated ones do not have such links (5). Paypal.com, PayPal-update are examples of slight changes made to domain names to entice users’ clicks. Spelling errors should be a giveaway
of a phishing email (5, 34). Users should be cautious of email with instructions like "click here to restore your account" as it is a red flag indicating a problem link (5). Users are the primary target for phishing email attacks, and proper training is the only way to prevent users from becoming victims (4). Public education efforts by the news media, government agencies, and corporations have not been very successful because users frequently do not update their software to either the latest versions or patches (35). Policies should be straightforward and easy to understand by all users (3). Users are known to be tired of learning and have even ignored policies, license agreements, and help pages (3). Users have to examine URLs to identify a phishing email using a mouse-over (34).

The use of passwords for access has been another area generating problems for information protection. Several studies concerning secure passwords and proper usage have resulted in some of the findings expressed here. Unique passwords with sufficient complexity repeated several times depending on the number of accounts a user sets up is not reality, Bonneau et al. (9) argued. It is impossible to expect any person to set up a complex password comprising a mix of symbols, letters, at least eight characters long, no personal information, not written down, and unique on every account set up and remembered (8). The results of research conducted for the United Kingdom’s MI5 security service exposed some of the prevailing password practices (25). Password policy – mandating complex and frequently changed passwords do not solve insider attacks since remembering such passwords becomes a problem for the employees who may have to write them down to be easily assessable by others (25). Security experts’ advice to users on secure passwords only causes irritation and annoyance to users who would conveniently ignore such advice (9).

### 3 | THEORETICAL BACKGROUND

Protection Motivation Theory (PMT) consists of fear appeals and coping appraisal (18, 36). Fear appeals result from a threat that leaves a person vulnerable, followed by assessing the threat severity (36). The next logical step in the process is an analysis of the possibility of an event taking place and ascertaining the recommended remedy’s efficacy (36). Rogers (37) revised original postulates to include the coping process, mediating process, and modes of coping. The coping strategy triggers an adaptive response to assess response efficacy followed by self-efficacy. Self-efficacy is needed to perform the necessary action to protect the information system from threats. This type of protection is not a planned action since an employee does not know the danger beforehand. Self-efficacy is to be armed with the right knowledge and be confident to apply it when needed to protect (36, 37).

Rational Choice Theory (RCT): this theory explains that a person chooses based on his/her moral or cultural beliefs and acts on those beliefs that could be wrong or right (38). It links selection to preference, which indicates that people should behave purposefully according to their values. The theory’s extension includes a positive spectrum of moral or cultural obligation, doing right instead of wrong (38, 39). One of the Criticism of RCT by researchers is unfalsifiability, but Lovett (40) explains that RCT is one of the tools employed to make sense of causal social phenomena.

Theory of Planned Behavior (TPB): this is an extension to the Theory of Reasoned Action (TRA) (19). TPB relates to a person’s behavioral intention, and the choice results from a person’s attitude toward the behavior (41). Fishbein and Ajzen (42) postulate that behavior results from purpose, and philosophy and subjective norms makeup that intention. Ajzen (19), as an extension to TRA, added perceived control, consisting of time, money, right skills, and other people’s help. Moody, Siponen, and Pahnila (43) agree that self-efficacy provides a positive attitude toward behavior.

### 4 | RESEARCH MODEL AND HYPOTHESES

There are five constructs in the model, four independent variables: self-efficacy, descriptive norms, normative beliefs, and power distance, and one dependent variable, the intention to comply, as shown in Figure 1. The subjects under research make the
model unique; studies have not used a similar model with power distance as a construct before. ISP compliance issues are new concepts not yet explored by any research connected with this group, and power distance is a new construct.

Fear is a powerful motivator that invokes a defensive posture or sometimes confrontation avoidance (36). Fear appeals are the underpinnings of PMT (18, 43–46). PMT originally was proposed for health research (37), but it applies to information security. The fear invokes the cognitive process, leading to the threat severity appraisal; the coping strategy drives the solution, culminating in self-efficacy (18, 43). As an extension to TRA, TPB states that there is a need for self-efficacy in combination to perform a behavior (37, 43). The proliferation of technology into this society requires strategies to defend against the impending danger of data breaches. Knowledge and confidence in handling such tasks are among the methods. Hence, we hypothesize that,

1. H1: Self-efficacy will encourage ISP compliance by employees.

Working in an organization where employees tend to respond favorably to instructions will weigh on every person in such an environment to adapt. Complying with ISP by other employees is designated a social factor that would encourage every person to do the same; a positive environment would generate a positive response (19, 44). Instead, the research subjects would do what others do without understanding the implications, not to be left out. Hence, we hypothesize that,

1. H2: Descriptive norms will encourage ISP compliance by employees.

There are pressures on an employee from co-workers and management when they follow protocols, as they respond positively to them; this is the primary outcome of normative beliefs (19, 21, 41). In an environment where following instructions is the norm, employees will not disregard pressure from management. Hence, we hypothesize that,

1. H3: Normative beliefs will encourage ISP compliance by employees.

Dinev, Goo, Hu, and Nam (47) agree that cultural factors should be a part of the ISP program to make it successful. The antecedent of behavior is culture, shaping a person’s everyday life event (48). Employees in high PDI society would obey instructions without questions (14–16). When exposed to choices, to follow or not, the option would be to perform the required instructions. Hence, we hypothesize that,

1. H4: Power distance will encourage ISP compliance by employees.

TABLE 1: Construct and Related Theory

| Construct          | Related Theory |
|--------------------|----------------|
| Self-efficacy      | TPB, PMT       |
| Descriptive Norms  | TPB            |
| Normative Beliefs  | TPB            |
| Power Distance     | RCT            |
| Intention to Comply| TPB            |

5 | RESEARCH METHODOLOGY

The study is quantitative research that empirically validates the hypotheses derived from the research model. The model is exploratory as power distance has not been tested before for ISP compliance.
Data Collection

A trusted representative distributed and collected the survey in a southern state in Nigeria; there is a high concentration of most ethnic groups. The population was the Nigerian working class, and the population sampling was by random survey questionnaire distribution in different organizations. There were 219 returned questionnaires out of 510 distributed. There were 129 useable, 25% completion rate.

Operationalization of construct

Measurement items are adopted from extant literature to maximize validity, reliability, and minimize bias, on the recommendation of Straub, Boudreau, and Gefen (49). There are no easy means of measuring latent variables except by indicators (50). The constructs from the research model turn into measurement items with a 7-point Likert scale. Table 2 describes the measurement items.

6 | RESULTS

We used SmartPLS software version 3.3.3 (52) partial least square (PLS) to test the measurement model’s reliability and validity and the significance and relevance of the structural model relationship. SmartPLS provides an integrated environment for combining the calculations for measurement and structural models. It is suitable for small sample analysis, and Hair et al. (50), Wong (53) provided standard guidelines. We used Microsoft Excel to perform demographic calculations.

Table 3 shows demographic details. The respondents were 55.81 percent male and 44.19 percent female. One of the table items is the respondents’ job functions; 15.50 percent work as information technology personnel, while 84.50 percent have other job functions.

Assessment of Measurement Model

The indicators used in the model are reflective. The measurement model’s assessment included evaluating internal consistency, each indicator’s reliability, convergent reliability, and discriminant validity. We removed indicators DN3, NB1, NB2, PD3, and SE3; they loaded high on more than one variable (50, 54); the empirical correlation value between NB1 and PD1 was very high. Reflective constructs must exceed the required threshold of 0.7 to be reliable (50, 55). Outer loading has to exceed 0.708 to be considered statistically significant, and 0.4 is acceptable for exploratory research (50, 56). Table 4 shows individual indicator reliability exceeds the required minimum. The assessment of convergent validity requires the average variance extracted (AVE) of each latent variable to be (≥ 0.50) (50, 53). The values in Table 4 are (> 0.5) confirm that the measure of all reflective constructs has met the requirements of convergent validity.

Discriminant validity, the traditional method of testing for this distinction, is the Fornell-Larcker criterion, which states that each construct’s AVE’s square root should be greater than the AVE of other correlated constructs (50, 57, 58). The data in Table 5 comply, satisfying the requirement. Heterotrait-Monotrait Ratio of Correlation is another means of assessing discriminant validity; the required value should be (< 0.850) (the more conservative value) (57). The highest value in Table 6 is 0.776; therefore, discriminant validity is established. The criteria for the measurement model are satisfied.

Assessment of Structural Model

Structural model measurement represents the relationship between constructs [50]. The evaluation of the following criteria must be satisfied for an assessment to be valid: collinearity issues, the significance and relevance of structural model relationships, coefficient of determination R², the effect sizes F², and the predictive relevance Q² effect sizes [50], [59]. Variance Inflation Factor of 5 or greater means problem with collinearity [50]. The values of predictor variables in Table 7 are < 5; therefore, no collinearity issues.
### TABLE 2: Measurement Item Sources

| Construct          | Item   | Item Description                                                                 | Source                                      |
|--------------------|--------|----------------------------------------------------------------------------------|---------------------------------------------|
| **Self-efficacy**  | SE1    | I have the required knowledge to comply with ISP                                 |                                             |
|                    | SE2    | I have the required skills to comply with information security policy.           | Al-Omari, Deokar, El-Gayar, Walters, & Aleasa [31] |
|                    | 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.           |                                             |
|                    | DN2    | I know that other employees comply with information security policy.              | Herath & Rao 2009a [22]                     |
|                    | DN3    | I have a strong opinion that the majority of employees comply with information security policy. |                                             |
| **Normative Beliefs** | NB1  | Upper management believes that I should comply with information security policy.  |                                             |
|                    | NB2    | My immediate superiors believe that I should comply with information security policy. | Bulgurcu et al. 2010 [21]                  |
|                    | 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 [20]                    |
|                    | 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 the information security policy.                          | Bulgurcu et al. 2010 [21]                  |
|                    | IC2    | I intend to help others comply with information security policy.                  |                                             |
|                    | IC3    | I encourage others to comply with information security policy.                    |                                             |

The critical t-values are 1.65 for a 10% significant level, 1.96 for 5% significant level and 2.5% for 1% significant level. Alternatively, a $p$-value less than 0.10 for a 10% significant level, less than 0.05 for a 5% significant level, and less than 0.01 for a 1% significant level. The path coefficient value should be between +1 and -1; a value close to 1 represents a strong relationship between the predictor and outcome variables. A value close to 0 represents a weak relationship [50]. Figure 2 shows the research model with path coefficient and $R^2$ value. Table 8 shows path coefficient, T statistics, and $p$-values. Table 8 shows the relationships between each exogenous construct and the endogenous construct. Descriptive Norms (DN), path coefficient ($\beta = 0.101$), and Power Distance (PD) path coefficient ($\beta = 0.231$) have weakest relationships with Intention to Comply (IC). Normative Beliefs (NB) path coefficient ($\beta = 0.293$) has the largest path coefficient, Self-efficacy (SE), path coefficient ($\beta = 0.289$) is next.
| Demographic                  | Frequency | Percentage |
|-----------------------------|-----------|------------|
| Gender                      |           |            |
| Male                        | 72        | 55.81      |
| Female                      | 57        | 44.19      |
| Age                         |           |            |
| 18 - 29                     | 40        | 31.01      |
| 30 - 39                     | 50        | 38.76      |
| 40 - 49                     | 21        | 16.28      |
| 50 - 59                     | 12        | 9.30       |
| More than 60                | 6         | 4.65       |
| Education                   |           |            |
| Less than HS.               | 0         | 0.00       |
| Completed HS.               | 14        | 10.85      |
| Some College Credits        | 8         | 6.20       |
| Bachelor's Degree           | 58        | 44.96      |
| Graduate Degree             | 41        | 31.78      |
| Other                       | 8         | 6.20       |
| Job Role                    |           |            |
| Information Tech.           | 20        | 15.50      |
| Other                       | 109       | 84.50      |
| Time in the present organization |     |            |
| Less than 1 year            | 30        | 23.26      |
| 1 - 5 years                 | 40        | 31.01      |
| 6 - 10 years                | 21        | 16.28      |
| 11 - 15 years               | 14        | 10.85      |
| Greater than 15 years       | 24        | 18.60      |
| Time in the present position |           |            |
| Less than 1 year            | 35        | 27.13      |
| 1 - 5 years                 | 63        | 48.84      |
| 6 - 10 years                | 18        | 13.93      |
| 11 - 15 years               | 10        | 7.75       |
| More than 15 years          | 3         | 2.33       |
| Number of employees in your organization | |            |
| Less than 100               | 30        | 23.26      |
| 100 - 500                   | 44        | 34.11      |
| 501 - 1000                  | 19        | 14.73      |
| More than 1000              | 36        | 27.91      |
| Organization's sector       |           |            |
| Education                   | 33        | 25.58      |
| Government                  | 30        | 23.26      |
| Financial Services          | 39        | 30.23      |
| Health Care                 | 7         | 5.43       |
| Information Tech.           | 4         | 3.10       |
| Telecommunications           | 2         | 1.55       |
| Manufacturing               | 6         | 4.65       |
| Nonprofit                   | 3         | 2.33       |
| Other                       | 5         | 3.88       |
| Total                       | 129       | 100        |
The table below shows the loadings, reliability, and validity measures for the constructs in the study.

**Table 4: Loadings, Reliability, and Validity**

| Construct | Loading | Cronbach’s Alpha | Composite Reliability | AVE |
|-----------|---------|------------------|------------------------|-----|
| DN1       | 0.910   | 0.800            | 0.909                  | 0.833 |
| DN2       | 0.916   |                  |                        |     |
| IC1       | 0.930   | 0.927            | 0.954                  | 0.872 |
| IC2       | 0.940   |                  |                        |     |
| IC3       | 0.932   |                  |                        |     |
| NB3       | 1.000   | 1.000            | 1.000                  | 1.000 |
| PD1       | 0.920   | 0.830            | 0.921                  | 0.854 |
| PD2       | 0.929   |                  |                        |     |
| SE1       | 0.939   | 0.877            | 0.942                  | 0.890 |
| SE2       | 0.949   |                  |                        |     |

The $R^2$ value is a measure of a model predictive power. The $R^2$ values of 0.75, 0.50, or 0.25 for the endogenous construct are substantial, moderate, and weak, respectively [50]. The $R^2$ value for this research is 0.603, as represented in Table 8, which means that 60.3% variation in the intention to comply is the combined effect of all the independent variables. Based on the predictive accuracy power guidelines, we observed that the model has moderate explanatory power.

Using Standard Root Mean Square Residual (SRMR), we assessed Goodness of Fit (GoF), a good fit is ($< 0.080$) [60]. Our value was 0.057, below the required threshold. Predictive Relevance $Q^2$ is known as Stone-Geisser’s $Q^2$ value, a measure of how well the path model predicts the observed values. The rule of thumb requires the $Q^2$ value must be larger than 0 to show that the exogenous constructs have predictive relevance for the endogenous linked to them [50]. The parameter for the blindfolding process used was omission Distance (D) value = 7. The value of $Q^2$ observed was (>0), as seen in Table 8, indicating a high predictive relevance. Effect Size $f^2$ is a recalculation of $R^2$ after eliminating a specified exogenous construct to determine how much impact such elimination has on the $R^2$ value of the remaining endogenous constructs [50]. The guideline points out three values for assessing $f^2$ effect size, 0.02, 0.15, and 0.35; small, medium, and large effects, respectively [61]. The effect size of all the constructs was small ($< 0.15$), as shown in table 8. The structural model assessment is satisfactory.

**Hypothesis Testing**

The findings were as follows: the path from self-efficacy to intention to comply with information security policy ($\beta = 0.289$), normative beliefs to intention to comply with information security policy ($\beta = 0.293$), and power distance to intention to comply with information security policy ($\beta = 0.231$) were significant at 0.05 level, therefore supported. The path from descriptive norms ($\beta = 0.101$) was not
### TABLE 5: Fornell-Larcker Criterion

|                         | DN | IC | NB | PD | SE  |
|-------------------------|----|----|----|----|-----|
| Descriptive Norms (DN)  | 0.913 | | | | |
| Intention to Comply (IC)| 0.557 | 0.934 | | | |
| Normative Beliefs (NB)  | 0.577 | 0.702 | 1.000 | | |
| Power Distance (PD)     | 0.623 | 0.658 | 0.706 | 0.924 | |
| Self-efficacy (SE)      | 0.496 | 0.655 | 0.654 | 0.545 | 0.944 |

Note: Values in bold are the Square-root of AVE

### TABLE 6: HTMT Ratio

|     | DN | IC | NB | PD | SE  |
|-----|----|----|----|----|-----|
| DN  |    |    |    |    |     |
| IC  | 0.645 |    |    |    |     |
| NB  | 0.645 | 0.728 |    |    |     |
| PD  | 0.762 | 0.747 | 0.776 |    |     |
| SE  | 0.592 | 0.725 | 0.694 | 0.636 |     |

### TABLE 7: Variance Inflation Factor (InnerVIFs)

| Variance Inflation Factor (InnerVIFs) | IC |
|---------------------------------------|----|
| DN                                   | 1.780 |
| IC                                   |    |
| NB                                   | 2.563 |
| PD                                   | 2.334 |
| SE                                   | 1.821 |

### TABLE 8: Significance and Relevance of Path Coefficient

|                         | β  | STDEV | T Statistics | P values | f    | 2.50% | 97.50% |
|-------------------------|----|-------|--------------|----------|------|-------|--------|
| DN → IC                 | 0.101 | 0.087 | 1.153       | 0.249    | 0.014 | 0.000 | 0.108  |
| NB → IC                 | 0.293 | 0.135 | 2.167       | 0.030    | 0.084 | 0.001 | 0.336  |
| PD → IC                 | 0.231 | 0.113 | 2.050       | 0.040    | 0.057 | 0.001 | 0.255  |
| SE → IC                 | 0.259 | 0.108 | 2.673       | 0.004    | 0.115 | 0.012 | 0.376  |
|                         | R² | Q²    |              |          |      |       |        |
| DN                     |    |       |              |          |      |       |        |
| IC                     | 0.603 | 0.497 |              |          |      |       |        |
| NB                     |    |       |              |          |      |       |        |
| PD                     |    |       |              |          |      |       |        |
| SE                     |    |       |              |          |      |       |        |
significant at 0.05 level, therefore not supported (see Table 9).

7 | DISCUSSION

We showed that normative beliefs, power distance, and self-efficacy influenced employees’ intention to comply with information security policy. The $p$-value for descriptive norms exceeded the required threshold of 0.05 and did not influence intention to comply with information security policy. We dropped some of the factors because they loaded high on more than one variable. Investigation revealed that the correlation between the factors of one variable and other variables also were high.

Though our findings supported the hypotheses that self-efficacy, normative beliefs, and power distance would positively impact employees’ intention to comply with information security, there is a need to choose the correct grouping of variables for better survey results. The respondents were 219 out of 510; useable responses constituted a completion rate of 25 percent (129). Limiting the number of indicators to three for each construct was to improve the completion rate. Expansion of questions on each construct may have yielded better results.

8 | LIMITATIONS

There were several limitations to this study.

First, taking the survey was during the pandemic limiting access to employees.

Second, the questions related to each construct may have invoked the same response type since they were highly correlated, which showed up on the questionnaire prompting rejection.

Third, the reliability of the responses was not ascertainable.

Fourth, people understand questions differently, which could lead to wrong responses.

Fifth, people could respond to questions without reading them.

Sixth, over 50 percent did not respond, and a small percent of responses were useable.

9 | PRACTICAL IMPLICATIONS

The point that normative beliefs, self-efficacy, and power distance have produced positive results should encourage management to be directly involved in information security programs. Build trust between management and employees in information security to promote its importance. Information security training should be the same for all; the employees who lack technical knowledge should be brought up to the required technical level to participate comfortably. Hands-on participation should be a requirement for every employee, including management, to increase confidence. Job assignments should consider power distance as an influencing factor to encourage a positive response to information security policy. An information security policy should be written in plain and concise language to avoid misinterpretation. Give the policy to every employee; every few months, there should be a short refresher training to stress its importance.
TABLE 9: Hypothesis Testing Results H1 to H4

| Hypotheses                                      | $\beta$ | P Values    | Outcome       |
|------------------------------------------------|---------|-------------|---------------|
| H1: Self-efficacy will encourage ISP compliance by employees | 0.289   | 0.004       | Supported     |
| H2: Descriptive norms will encourage ISP compliance by employees | 0.101   | 0.249       | not supported |
| H3: Normative beliefs will encourage ISP compliance by employees | 0.293   | 0.030       | Supported     |
| H4: Power distance will encourage ISP compliance by employees | 0.231   | 0.040       | Supported     |

10 | CONCLUSIONS

This study was theory-based research combining Protection Motivation Theory, Theory of Planned Behavior, and Rational Choice Theory to empirically validate a model that introduced a new construct, power distance in information security policy compliance. Nigeria was a random survey location because it is a high-power distance country. The findings demonstrated that employees in a high-power distance society would respond favorably to the concept of information security policy compliance; the newly introduced construct power distance played a major role in the favorable response to ISP compliance. The results showed that normative beliefs, power distance, and self-efficacy had significant impacts on intention to comply with information security policy. On the contrary descriptive norms, did not positively affect the intention to comply with information security policy.

REFERENCES

[1] T. R. Peltier, Information security policies, procedures, and standards: A Practitioner’s Reference, Second Edi. Boca Raton, FL: Auerbach, 2004, p. 47.
[2] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance, "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," Eur. J. Inf. Syst., vol. 18, no. 2, pp. 126–139, 2009.
[3] J. S. Griffin and M. Grimalia, "Insider threats to information systems," Proc. South. Assoc. Inf. Syst. Conf., no. 2004, pp. 1–6, 2008.
[4] PhishTank, "What is phishing?," www.PhishTank.Com, 2009.
[5] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," 16th Int. World Wide Web Conf. WWW2007, vol. 0389, no. June, pp. 649–656, 2007.
[6] L. Werner and J. Courte, "Analysis of an anti-phishing lab activity," Inf. Syst. Educ. J., vol. 8, no. April 19, 2010, 2010.
[7] Kaspersky Lab, "Over a quarter of phishing attacks in 2014 targeted users financial data Kaspersky Lab," www.Kaspersky.Com, pp. 5–8, 2015.
[8] B. L. Tung, "FBI: Beware fake CEO emails that have cost," 2016.
[9] J. Bonneau, P. C. Van Oorschot, and F. Stajano, "Passwords and the Evolution of Imperfect Authentication," Commun. ACM, vol. 58, no. 7, pp. 78–87, 2015.
[10] R. Chatterjee, A. Athayle, D. Akawhe, A. Juels, and T. Ristenpart, "PASSWORD tYPOS and How to Correct Them Securely," 37th IEEE Symp. Secur. Priv., pp. 799–818, 2016.
[11] F. L. Greitzer and R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," J. Strateg. Secur., vol. 4, no. 2, pp. 25–48, 2011.
[12] N. Gagliardi, "The Target breach, two years later DNet," DNet, 2016, [Online]. Available: https://www.zdnet.com/article/the-target-breach-two-years-later/.
[13] G. Hofstede, G. Jan Hofstede, and M. Minkov, Cultures and Organizations, 3rd ed. McGraw Hill Companies, 2010.
[14] G. Hofstede, "The business of international business is culture," Int. Bus. Rev., vol. 3, no. 1, pp. 1–14, 1994.
[15] G. Hofstede, “Dimensionalizing Cultures: The Hofstede Model in Context,” Online Readings Psychol. Cult., vol. 2, no. 1, pp. 1–26, 2011.
[16] S. S. Glenn, "Individual behavior, culture, and social change," Behav. Anal., vol. 27, no. 2, pp. 133–151, 2004.
[17] D. E. Leidner and T. Kayworth, "Review: a review of culture in information systems research: toward a theory of information technology culture conflict," MIS Q., vol. 30, no. 2, pp. 357–399, 2006.
[18] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," J. Exp. Soc. Psychol., vol. 19, no. 5, pp. 469–479, 1983.
[19] I. Ajzen, "The theory of planned behavior," Organizational Behav. Hum. Decis. Process., vol. 50, pp. 179–211, 1991.
[20] Y. hang and T. M. Begley, "Power distance and its moderating impact on empowerment and team participation," Int. J. Hum. Resour. Manag., vol. 22, no. 17, pp. 3601–3617, 2011.
[21] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," MIS Q., vol. 34, no. 3, pp. 523–548, 2010.

[22] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," Decis. Support Syst., vol. 47, no. 2, pp. 154–165, 2009.

[23] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," Comput. Secur., vol. 29, no. 2, pp. 196–207, 2010.

[24] A. McCormac, K. Parsons, and M. Butavicius, "Preventing and Profiling Malicious Insider Attacks," pp. 1–22, 2012.

[25] J. R. C. Nurse et al., "Understanding Insider Threat: A Framework for Characterising Attacks," 2014.

[26] Q. Hu, T. Dinev, and H. Ling, "Does deterrence work in reducing information security policy abuse by employees?," Commun. ACM, vol. 54, no. 6, p. 54, 2011.

[27] M. Siponen and A. Vance, "NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS," MIS Quarterly, vol. 34, no. 3, pp. 487–502, 2010.

[28] G. M. Sykes and D. Matza, "Techniques of Neutralization," Am. Sociol. Rev., vol. 22, no. 6, pp. 664–670, 1957.

[29] L. Cheng, Y. Li, W. Li, E. Holm, and Q. hai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," Comput. Secur., vol. 39, no. PART B, 2013.

[30] A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," Psychological Review, vol. 84, no. 2. pp. 191–215, 1977.

[31] H. S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users information security practice behavior," Comput. Secur., vol. 28, no. 8, pp. 816–826, 2009.

[32] N. D. Albers-Miller and B. D. Gelb, "Business Advertising Appeals as a Mirror of Cultural Dimensions: A Study of Eleven Countries," J. Advert., vol. XXV, no. Number 4, 1996.

[33] T. Ahmed, H. Mouratidis, and D. Preston, "Website Design Guidelines: High Power Distance and High Context Culture," Int. J. Cyber Soc. Educ., vol. 2, no. 1, pp. 47–69, 2009.

[34] M. Jakobsson, "The Human Factor in Phishing," Priv. Secur. Consum. Inf., vol. 7, pp. 1–19, 2007.

[35] E. Bekkering, D. Hutchison, and L. Werner, "A Follow-up Study of Detecting Phishing Emails," in CONISAR, 2009, vol. 2, no. Washington DC, pp. 1–6.

[36] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," J. Psychol., vol. 91, no. 1, pp. 93–114, 1975.

[37] R. W. Rogers, Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation, vol. 19, no. 5. New York: Guilford Press, 1983.

[38] A. Vance and M. T. Siponen, "IS Security Policy Violations," J. Organ. End User Comput., vol. 24, no. 1, pp. 21–41, 2012.

[39] R. L. Akers, "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," J. Crim. Law Criminol., vol. 81, no. 3, pp. 653–676, 1990.

[40] F. Lovett, "Rational choice theory and explanation," Ration. Soc., vol. 18, no. 2, pp. 237–272, 2006.

[41] I. Ajzen and M. Fishbein, "Theory of Reasoned Action / Theory of Planned Behavior," 1980.

[42] M. Fishbein and I. Ajzen, Belief, attitude, intention and behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley, 1975.

[43] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a Unified Model of Information Security Policy Compliance," MIS Q., vol. 42, no. 1, pp. 285–311, 2018.

[44] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," Eur. J. Inf. Syst., vol. 18, no. 2, pp. 106–125, 2009.

[45] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," Inf. Manag., vol. 49, no. 3–4, pp. 190–198, 2012.
[46] I. M. Y. Woon, G. W. Tan, and R. T. Low, "A Protection Motivation Theory Approach to Home Wireless Security," in Twenty-Sixth International Conference on Information Systems, 2005, vol. 5, pp. 367–380.

[47] T. Dinev, J. Goo, Q. Hu, and K. Nam, "User behaviour towards protective information technologies: The role of national cultural differences," Inf. Syst. J., vol. 19, no. 4, pp. 391–412, 2009.

[48] M. Jones and I. Alony, "The cultural impact of information systems – through the eyes of Hofstede – a critical journey what is culture?," Issues Informing Sci. Inf. Technol., vol. 4, pp. 408–419, 2007.

[49] D. Straub, M.-C. Boudreau, and D. Gefen, “Validation Guidelines for IS Positivist Research,” Commun. Assoc. Inf. Syst., vol. 13, Articl, no. March, pp. 380–427, 2004.

[50] J. F. J. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, A primer on partial least squares structural equation modeling (Pls-Sem), 2nd ed. Los Angeles: SAGE Publications Inc, 2017, pp. 6, 13, 104 - 223.

[51] A. Al-Omari, A. Deokar, O. El-Gayar, J. Walters, and H. Aleassa, "Information security policy compliance: An empirical study of ethical ideology," Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 3018–3027, 2013.

[52] C. M. Ringle, S. Wende, and J. M. Becker, "SmartPLS 3.0." SmartPLS GmbH, BoenningStedt, 2015.

[53] K. K.-K. Wong, "28/05 - Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS," Mark. Bull., vol. 24, no. 1, pp. 1–32, 2013.

[54] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, Multivariate Data Analysis, Seventh. Tamil Nadu: Pearson India Education Services Pvt Ltd, 2015, pp. 116 - 118.

[55] Y. Bagozzi, R. P., Yi, “On the Evaluation of Structural Equation Models.pdf,” J. Acad. Mark. Sci., vol. 16, no. 1, pp. 74–94, 1988.

[56] J. Hulland, "Use of partial least squares (PLS) in strategic management research: a review of four recent studies," Strateg. Manag. J., vol. 20, no. 2, pp. 195–204, 1999.

[57] K. K. Wong, Mastering Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS in 38 Hours, no. March. Bloomington: iUniverse, 2019, pp. 30 - 124.

[58] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," J. Mark. Res., vol. 18, no. 1, p. 39, 1981.

[59] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a silver bullet," J. Mark. Theory Pract., vol. 19, no. 2, pp. 139–152, 2011.

[60] J. Benitez, J. Henseler, A. Castillo, and F. Schuberth, "How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and exploratory IS research," Inf. Manag., no. October 2017, 2019.

How to cite this article: Etim E.E., Streff K., Park I., Rowland P. Power Distance as a Variable in Assessing Employees’ Behavior towards Information Security Policy Compliance in a High-Power Distance Society: An Exploratory Study. International Journal of Contemporary Research and Review. 2021;20361–20375. https://doi.org/10.15520/ijcrr.v12i04.895
Dakota State University  
Erasmus Etim

Survey Questions

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.

| Self-efficacy | 1 2 3 4 5 6 7 |
|---------------|---------------|
| I have the required knowledge to comply with information security policy. | 1 2 3 4 5 6 7 |
| I have the required skills to comply with information security policy. | 1 2 3 4 5 6 7 |
| I have the required competencies to comply with information security policy. | 1 2 3 4 5 6 7 |

| Descriptive Norms | 1 2 3 4 5 6 7 |
|-------------------|---------------|
| I believe that other employees comply with information security policy. | 1 2 3 4 5 6 7 |
| I know that other employees comply with information security policy. | 1 2 3 4 5 6 7 |
| I have a strong opinion that majority of employees comply with information security policy. | 1 2 3 4 5 6 7 |

| Normative Beliefs | 1 2 3 4 5 6 7 |
|-------------------|---------------|
| Upper management believes that I should comply with information security policy. | 1 2 3 4 5 6 7 |
| My immediate superiors believe that I should comply with information security policy. | 1 2 3 4 5 6 7 |
| My colleagues believe that I should comply with information security policy. | 1 2 3 4 5 6 7 |

| Power Distance | 1 2 3 4 5 6 7 |
|----------------|---------------|
| Organization's rules should not be broken, therefore I have to comply with information security policy. | 1 2 3 4 5 6 7 |
| I respect management decisions, therefore I have to comply with information security policy. | 1 2 3 4 5 6 7 |
| 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 | 1 2 3 4 5 6 7 |
|---------------------|---------------|
| I intend to comply with information security policy. | 1 2 3 4 5 6 7 |
| I intend to help others comply with information security policy. | 1 2 3 4 5 6 7 |
| I encourage others to comply with information security policy. | 1 2 3 4 5 6 7 |

Information About you and Your Organization

Gender

☐ Male  ☐ Female
| Age       | 18-29 | 30-39 | 40-49 | 60 and above |
|-----------|-------|-------|-------|--------------|
| Education | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
| Job role  | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
| Time on the job in the present organization | ☐ | ☐ | ☐ | ☐ |
| Time in the present position | ☐ | ☐ | ☐ | ☐ |
| Number of employees in your organization | ☐ | ☐ | ☐ | ☐ |
| Organization's sector | ☐ | ☐ | ☐ | ☐ |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
|          | ☐     | ☐     | ☐     | ☐            |
| Thank you for taking time to participate |