

Neutralization Tendencies in Information Systems Security Violations

Frank King
Howard University
fking@law.howard.edu

Souren Paul
Northern Kentucky
Souren.paul@gmail.com

Abstract

It is estimated that over half of all information systems security breaches are due directly or indirectly to employee’s poor security practices in organizations. This problem is considered the biggest threat to an organization because employees are trusted with the knowledge and privilege of organization’s resources. Previous research has shown neutralization techniques as having influence on the intent to violate information security policy. What has not been determined from extant information security research is an explanation that addresses why employees drift into a neutralization state in the first place. We propose an expansion of the neutralization model by including the effects of business orientation and ethical orientation of individuals on their tendencies to neutralize and compromise with information security policy.

1. Introduction

Studies on the violation of information security policy have been reviewed from the perspective of deterrence theory, by both practitioners and Information Security (IS) scholars (Kankanhalli et al., 2003; Straub Jr, D. W., & Nance, W. D, 1990). Previous research recognized that all information systems (IS) violations may not be best explained through the lens of Deterrence Theory by fear of sanctions because employees typically fall into neutralization techniques (Siponen, M., & Vance, A. (2010). Prior research demonstrates that neutralization techniques influence employee’s intentions to violate IS security policies. However, these studies did not explain why employees drift into a neutralization state in the first place. The term “drift” can be defined as “a temporary period of irresponsibility or an episodic relief from moral constraint” (Maruna, S., & Copes, H. (2005). Sykes and Matza suggested people psychologically enable themselves to commit rule-breaking or any anti-social actions by applying techniques of neutralization that render existing norms inoperative by justifying behavior, and in this context, violating information security policies. This research proposes two relevant antecedents’ business and ethical orientation on neutralization, and it is inspired by the belief that

moral beliefs or different ethical doctrines affect people’s thinking (Vance, A., Siponen, M. T., & Straub, D. W. 2020). Siponen and Vance (2010) created a multidimensional second order construct with moral beliefs or different ethical doctrines affect people’s thinking (Vance, A., Siponen, M. T., & Straub, D. W. 2020). Siponen and Vance (2010) created a multidimensional second order construct with several distinct dimensions that exist within the construct Neutralization. This research is inspired by a better understanding of cognitive rationalization of employees as they make decisions from both a business and ethical orientation.

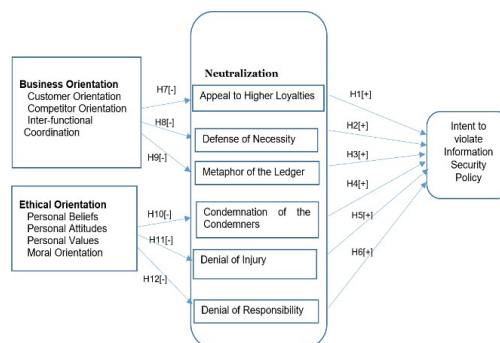
Due to employees being a key factor in information security (IS) breaches, research in this area continues to be relevant (D’Arcy et al., 2019; Siponen & Vance 2010; Furnell & Clarke, 2015).

The primary research question in this study is:

RQ1: What factors influence employees to accept neutralization techniques?

2. Conceptual Background

In this section, we develop the research model of our study. We suggest that the business orientation and ethical orientation of an individual influence his/her tendency to rationalize their behavior to violate information security policy. First, we define and discuss prior literature on the key constructs of our study. Next, we develop the relationship among the constructs and develop our



research model which is shown in figure1.
Figure 1. Research Model: Expansion of Neutralization Model

3. Neutralization

The study of Neutralization Theory is associated with the idea that people psychologically enable themselves to commit to the idea of breaking rules or any anti-social actions Skyes G, Matza D. (1957).

Matza showed that offenders who might otherwise feel guilt and shame were able to neutralize their feelings by justifying their behaviors before committing the deviant act. The term neutralization can be defined as the act of rationalizing or justifying an immoral or illegal act (Silic, M., Barlow, J. B., & Back, A. 2017). Barlow, Warkentin, Ormond, and Dennis (2018) defined neutralization as the use of rationalization when violating a policy. Neutralization theory explains the justification of human behavior that is considered wrong under most circumstances but allows an individual to justify his or her self-concept while committing an act that is wrong (Costello, B. J. (2000).

Previous research of Neutralization suggests theories of criminal behavior ascribe the importance of one's individual belief system in the context of whether their beliefs are in line with societal standards of conventional behavior. Silic et al., (2017). expanded the perspective on neutralization in the context of IT usage. They suggested that those who commit illegal or illegitimate actions may use neutralization, while certain values may prohibit them from committing these same actions. Trinkle, Warkentin, and Raddaz (2021) found neutralization processes can enable potential IS security policy violators to justify their behavior and overcome the deterrence effect of sanctions to engage in unethical behaviors. From an organizational context, Silic et al., (2017) point out that employees may use one or more neutralization techniques to persuade himself or herself that policy violation does not represent a problem. Thus, neutralization protects the violator from feeling self-blame and enabling him or her from deviant acts.

Siponen and Vance (2010) developed a multi-dimensional second order construct research model that illustrated the bearing that Deterrence Theory constructs –formal sanctions, informal sanctions, and shame had on the intentions to violate IS security policy. Likewise, their research model also illustrated the causal effect the first order constructs –Appeal to Higher Loyalties, Defense of Necessity, Metaphor of the Ledger, Condemnation of the Condemners, Denial of Injury, and Denial of Responsibility have on the intent to violate information security policy. Six types of Neutralization techniques, suggested by Siponen and Vance (2010) are

presented in table 1. These constructs were initially proposed by Sykes and Matza who formed the original formulation of Neutralization Theory. Minor, W. W. (1981). added the Defense of Necessity, in which an offender attempts to justify their actions based on the perceived necessity to commit the act. D'Arcy, J., & Teh, P. L. (2019) observed whether security-related stress (SRS) engenders frustration and fatigue from security requirements and whether the emotional reaction invokes neutralization of ISP violations. Their study provided evidence that Neutralization is not a completely stable phenomenon. In other words, neutralization can vary within individuals from any point and time. Teh et al. [70] studied the relationships among job satisfaction, organizational commitment, role conflict, role ambiguity, and neutralization. They found a positive relationship between role conflict and neutralization of ISP violations and a negative relationship between organizational commitment and neutralization.

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

Table 1 Neutralization Techniques -Siponen, M., A.,& Willison, R. (2012)

Siponen and Vance (2010) found neutralization had a positive effect on the intention to violate IS security policy. Siponen, M., Vance, A., & Willison, R. (2012). examined educational training interventions aimed at de-neutralizing techniques. Although their research found that individuals who received their educational training used neutralization techniques substantially less, some individuals still used neutralization techniques, nonetheless. Hence:

H1: Appeal to Higher Loyalties will positively affect the intent to violate information security policy.

H2: Defense of Necessity will positively affect the intent to violate information security policy.

H3: Metaphor of the Ledger will positively affect the intent to violate information security policy.

H4: Condemnation of the Condemners will positively affect the intent to violate information security policy.

H5: Denial of Injury will positively affect the intent to violate information security policy.

H6: Denial of Responsibility will positively affect the intent to violate information security policy.

4. Business Orientation

In this research, we rely on prior studies on market orientation to explain our conceptualization of Business Orientation Narver and Slater (1990). Business Orientation can be defined as an organization wide market of intelligence pertaining to current and future needs of customers, dissemination of intelligence horizontally and vertically within the organization, and organization-wide action or responsiveness to market intelligence Kohli, A. K., Jaworski, B. J., & Kumar, A. (1993). Customer Orientation, Competitor Orientation, Inter-Functional Coordination are three components of Market Orientation Narver and Slater (1990). We suggest that these components explain some of the neutralization techniques used in the violation of IS security policies. Customer Orientation can include various elements, which include measuring customer satisfaction, creating customer value, understanding customer needs and customer commitment. Sin, L. Y., Tse, A. C., Yau, O. H., Chow, R. P., & Lee, J. S. (2005) examined the economic ideology and industry type which moderated the impacts of market orientation and the relationship market orientation on business performance. Hooley, Cox, Fahy, Beracs, Fonfara, and Snoj (2000) reviewed the transition of economies of Central Europe in testing Narver and Slater Market Orientation scales. Their research focused on the transition economies that other business orientations may coexist with Market Orientation. Diamantopoulos and Hart (1993) focused on linking customer orientation, competitor orientation and inter-functional coordination to company performance.

Competitor Orientation, a component of Business Orientation, suggests highly involved employees in the organization work hard and become highly involved in accomplishing the organizational goals (Arthur, J. B. 1994; Wood, S., & de Menezes, L. 1998). Thus, employees that are highly involved are less likely to break the rules or policy Sims, R. L. (2002). Competitor Orientation can be defined as the means that a seller understands the short-term strengths and weaknesses and the long-term capabilities and strategies of both the current and the key potential competitors Chandler, D., & Werther Jr, W. B. (2013). Narver and Slater (1990) researched and examined whether the competitive environment might have an impact on the effectiveness of different corporate objectives. We suggest employee's involvement in the workplace will influence

the effectiveness of organizational objectives and thus impact neutralization.

Inter-functional Coordination can be defined as the mechanism that facilitates the coordination between the various organizational units' functionality (Gatignon, H., & Xuereb, J. M. 1997). Yang, Wang, Zhu, and Wu [80] defined Inter-Functional Coordination in the context of an organization as the utilizations of company resources in creating superior value for target customers. Rogerson and Sallnas (2017) defined Inter-functional Coordination as working together across functions to achieve common company goals. Rapp, Beitelspacher, Schillewaert, and Baker (2012) studied the outcomes of different workplace structures. Their study reviewed sales organization's structure, e-learning and technological tools to determine the influence coordination and the level of customer orientation within an organization. Their results suggest that organization structure type, coupled with e-learning, and technological tools, lead to greater positive outcomes. Jebarajakirthy, Thaichon, and Yoganathan (2016) study found that inter-functional coordination significantly and positively influenced corporate social responsibility. The authors study found that inter-functional coordination significantly and positively influenced corporate social responsibility involvement.

Previous studies show that employees who are more enthusiastic about work will be more responsible in avoiding mistakes, and thus, more likely to safeguard the organization's interests Cheng, L., Li, Li, W., Holm, E., & Zhai, Q. (2013). Thus, employees with more involvement in the organizational activities will be less likely to violate IS policy.

Siponen and Vance (2010) found neutralization to be a strong indicator in predicting information security policy violations. However, they did not examine the factors that influenced employees to accept neutralization techniques. We believe business orientation will influence neutralization techniques that are more organizational oriented. Hence:

H7: Business Orientation will negatively influence the acceptance of *appeal to higher loyalties*.

H8: Business Orientation will negatively influence the acceptance of *defense of necessity*.

H9: Business Orientation will negatively influence the acceptance of *metaphor of the ledger*.

5. Ethical Orientation

The business community continues to struggle with issues surrounding ethical behavior. Studies have concluded that ethical judgements in situations of high

moral intensity are affected by personal values Douglas, P.C., Davidson, R.A., & Schwartz, B.N. (2001). Ethical orientation can be defined as a variable of study that refers to the approach an individual take in making ethical judgment through ethical perceptions and sensitivity with the ability to recognize the ethical nature of a situation in a profession (Clikeman, P. M., Geiger, M. A., & O'Connell, B. T., 2001). Beekun and Westerman (2012) recognized the rise in unethical business conduct and researched the need to better understand the antecedents to ethical decision-making with the influence of internal factors needing the most focus. Beekun and Westerman (2012) examined three sources of influence on ethical decision-making: personal spirituality, peer pressure, and national culture. The authors study examined the relationship between ethical decision-making and behavioral norms. They used the social identity theory, which suggests a person's knowledge that he or she belongs to a social group. Fok et al. (2012) researched for a deeper understanding of the process in which cultural values influence ethical decisions.

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

Ethics is the foundation in which self-inquiries of morality, moral judgement, standards and rules of conduct of a person. Other words, ethics are the guidelines of human behavior one distinguishes between good and bad, right, and wrong (Phatak, A. V., Bhagat, R. S., & Kashlak, R. J. 2005). Business ethics similarly concentrates on the moral standards as they apply to business, policies, organizations, and behaviors. In this context, ethical orientation is a decision justification that leads to the decision maker to consider different criteria and alternatives. Past research showed that individual's ethical orientation is directly associated with ethical judgement (Payne, D., Corey, C. M., & Fok, L. Y. 2016).

Individual factors, such as personal values, affect the ethical decision-making process and are the guidelines for doing ethical behavior (Turk, Z., & Avcilar, M. Y. 2018). The most popular definitions used in the business literature for personal value are (1) value can be defined as a specific conduct or end-state that is personally and socially the preferred mode of conduct or end-state of

one's existence (Rokeach, 1973) and (2) personal values are the beliefs or standards that individuals use to evaluate and define actions and events throughout the multiple domains in their lives Hyde, R. E., & Weathington, B. L. (2006). The importance of personal values on ethical decision-making has been studied in other disciplines like accounting and business literature for several years (Fritzsche, D., & Oz, E., 2007; Mingzhi, L., 2008). Researchers found ethical decision making and behavior to be potentially influenced by personal values in both the social psychology and organizational behavior literature [58, Hunt, S. D., & Vitell, S. (1986). Moreover, empirical studies have shown a positive link between personal values and ethical sensitivity and judgement decisions (Fritzsche, D., & Oz, E., 2007; Mingzhi, L., 2008). Forsyth (1980) and Ferrell and Gresham (1985) suggest that theoretical models and theory of ethical decision-making demonstrate that personal values provide the basis for ethical judgement.

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

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

derived attitude, normal belief, and self-efficacy, based on the theory of Reasoned Action with seven factors of neutralization, and the response from the Protection Motivation Theory.

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

Fok et al., 2016) argued that values affect ethical decision making in a business context. Alteer, Yahya, and Haron (2013) also found ethical decisions are a result of personal values. The authors noted that these values are ideals that are abstract in one's mind and represent happiness and impacts behavioral decisions. As a result, we believe Ethical Orientation will influence neutralization. Hence:

H10: Ethical Orientation will negatively influence the acceptance of *condemnation of the condemners*.

H11: Ethical Orientation will negatively influence the acceptance of *denial of injury*.

H12: Ethical Orientation will negatively influence the acceptance of *denial of responsibility*.

6. Research Methods

A web-based survey was conducted to examine our research model. The overall approach for this research was based on survey and scenario methodology for data collection. The participants were identified from the

three targeted groups: employees from academic institutions, employees from corporate organizations, and employees from information technology professional. In designing a hypothetical scenario for this research, we wanted to ensure that the situation was not uncommon to respondents. The scenario methodology was used to reflect real-world problems that are important and relevant to IS security practice. The scenario provided a situation on a common IS violation, in which employees violate log off procedures to circumvent signing on and signing off their computers. This method was followed by Piquero and Hickman (2005) and Limayem and Hirt (2005). Siponen and Vance (2010) used this methodology and solicited security experts and information security managers for their most common violations. They found the most common and significant information security policy violations through an open-ended questionnaire that resulted in the response from 54 information security experts that identified the top four IS security policy compliance problems. This research borrowed from the work of Siponen and Vance (2010) as it ensured a scenario that reflected real-world problems that are important and relevant to IS security practice. Secondly, in keeping with Siponen and Vance, the scenario-based design ensures findings are generalizable across different IS security violation policies. Smart PLS software was used to further analyze the data for model fit, convergent validity, discriminant validity, construct reliability and validity, and factor loading. After running the PLS algorithm, with all initial loadings, the model fit SRMR was at 0.060, which is considered an acceptable level. Any level less than 0.08 is considered a good fit (Hooley et al., 2000). A quantitative survey approach was used to analyze the independent variables business orientation, ethical orientation, and neutralization. A stratified random sampling was conducted, and descriptive statistics were used to provide the mean, median, and mode. A pilot study was conducted with 40 participants to validate data. A final collection of data was conducted and based on results of the analyses, evidence either supported or rejected the hypotheses.

6.1 Sample Design

To decide the minimum sample size, we relied on the Statistical Power Analysis which is based on pre-determined factors of the significance level, effect size, power, and estimated variance (Cohen, 1992). The statistical level of significance was set at .05. Effect size indices for small, medium, and large sizes are .02, .15, and .35, respectively. Cohen (1992) proposed that a medium effect size is desirable as it would be able to

approximate the average size of the observed effects in various fields. For this study, the maximum number of independent variables is eight. Following the recommendations of Cohen (1992), the sample sizes for small, medium, and large samples are 50, 107, and 757, respectively. This study aimed for a medium effect size, and therefore, the sample size for this study is 107, based on the recommendations of Cohen (1992). For this study, we exceeded the minimum sample size of 107 to ensure a more accurate mean values that may identify outliers that could skew the data in a smaller sample. The unit of analysis for this study was at the individual level. Invitations were sent to over 800 individuals, of which 240 responded, resulting in a response rate of 30%.

6.1.1 Operational Variables

As mentioned by Devellis (2012) the key in selecting the most appropriate instrument for a research study is the type of data called upon, based on the research questions and the hypotheses. This research was inspired by prior studies conducted in the field of Information Systems Security and utilized vetted survey instruments as well as questions from those studies. This was necessary to guarantee the validity and reliability of the study. This study included items to measure Neutralization, Business Orientation, and Ethical Orientation. Neutralization construct explains the justification of human behavior that is considered wrong under most circumstances but allows an individual to justify his or her self-concept while committing an act that is considered wrong. Business Orientation construct explains the business culture in which all employees are committed to the continuous creation of super value for customers. Ethical construct explains the approach an individual may take in making ethical judgment through ethical perceptions and sensitivity with the ability to recognize the ethical nature of a situation in a profession. Table 2 illustrates the model constructs and instrument source.

Construct	Source
<i>Intent to Violate Information Security Policy</i>	(Siponen & Vance, 2010)
<i>Business Orientation</i>	(Hooley et al., 2000), (Sin et al., 2005)
<i>Ethical Orientation</i>	(Allmon et al., 2000), (Douglas et al., 2001)
<i>Neutralization</i>	(Siponen & Vance, 2010)

Table 2. Constructs and Instrument Source

7. Pilot Study

We conducted a pilot study to work through any issues

that might arise before the actual study is presented to the participants. The pilot study helped flush out the following: questions that were misleading, any confusion to the participants, and a pre-test of the survey instrument. The pilot study sampled around 10% of the overall target audience.

This method allowed the ability to focus on the details as a final quality assurance check before commitment to the full study.

8. Data Collection

All To closely match the population, stratified random sampling was used to represent the population as much as possible. Descriptive statistical information on gender had an even split with male respondents numbering 103 (50%) and female respondents numbering 103 (50%), totaling 206 respondents. The response rate for information technology professionals reports a frequency of 34, with a cumulative percent of 16.5 % of the population, corporate organizations report a frequency of 63, with a cumulative percent of 30.6% of the population, and Academic Institutions reports a frequency of 109, with a cumulative percent of 52.9%. This method is unbiased and the most efficient of the probability sampling techniques. This guarantees the sample chosen is representative of the population in an unbiased way. Data was collected over 3 months from June 2020, July 2020, and August 2020.

9. Reliability and Validity

A reliability analysis was conducted on each of the items within the study. Cronbach alpha values of .70 and above indicate acceptable reliability (Piquero, A. R., & Hickman, M., 1999). With the exception of Ethical Orientation, Cronbach alphas for the measures for all other constructs were found to exceed 0.70. Cronbach alpha for Ethical Orientation was .684 which is borderline to the acceptable range. To evaluate for convergent validity of each construct, a factor analysis was conducted for items that correspond with each construct with a principal component analysis method of extraction and a varimax rotation. Another factor analysis was conducted using the items measuring all constructs to establish the discriminant validity. Convergent and discriminant validities of constructs were found satisfactory. Table 3 illustrates reliability and convergent validity and table 4 illustrate discriminant validity.

Constructs	Cronbach Alpha	Rho_A	Composite Reliability	Average Variance Extracted	Number of Items	Factor Loading
Business Orientation	.815	0.834	.874	.635	4	.736 - .831
Ethical Orientation	.684	0.710	.864	.862	2	.838 - .902
Appeal to Higher Loyalties	1.000	1.000	1.000	1.000	1	1.000
Defense of Necessity	0.734	.756	.882	.788	2	.863 - .912
Metaphor of the Ledger	.884	.884	.945	.896	2	.946 - .947
Condemnation of the Condemners	.800	.833	.908	.832	2	.890 - .934
Denial of Injury	.950	.951	.976	.952	2	.975 - .977
Denial of Responsibility	.838	.864	.924	.859	2	.912 - .942

Table 3. Statistics and Reliability

Construct	Business Orientation	Ethical Orientation	Appeal to Higher Loyalties	Defense of Necessity	Metaphor of the Ledger	Condemnation of the Condemners	Denial of Injury	Denial of Responsibility	Intent to Violate
B01	0.736	0.180	-0.083	-0.080	-0.093	-0.068	-0.41	-0.135	-0.091
B02	0.787	0.209	-0.143	-0.194	-0.217	-0.139	-0.169	-0.195	-0.134
B04	0.830	0.218	-0.146	-0.186	-0.216	-0.128	-0.132	-0.207	-0.047
B06	0.831	0.206	-0.173	-0.231	-0.207	-0.175	-0.182	-0.240	-0.115
E02	0.190	0.838	-0.247	-0.327	-0.338	-0.213	-0.171	-0.153	-0.250
E03	0.252	0.902	-0.227	-0.225	-0.348	-0.217	-0.243	-0.223	-0.088
N1	-0.181	-0.270	1.000	0.782	0.629	0.601	0.687	0.512	0.342
N2	-0.272	-0.326	0.724	0.912	0.635	0.624	0.674	0.621	0.429
N3	-0.131	-0.212	0.660	0.883	0.554	0.600	0.652	0.410	0.394
N4	-0.237	-0.347	0.641	0.655	0.946	0.564	0.609	0.587	0.417
N5	-0.228	-0.397	0.550	0.619	0.947	0.496	0.592	0.490	0.425
N6	-0.227	-0.269	0.563	0.657	0.611	0.934	0.637	0.467	0.343
N7	-0.067	-0.169	0.531	0.596	0.386	0.890	0.574	0.376	0.299
N8	-0.195	-0.255	0.675	0.712	0.603	0.655	0.975	0.579	0.336
N9	-0.159	-0.210	0.665	0.743	0.634	0.645	0.977	0.609	0.382
N10	-0.285	-0.200	0.430	0.541	0.485	0.408	0.515	0.912	0.238
N11	-0.196	-0.208	0.512	0.556	0.563	0.455	0.606	0.942	0.238
Intent to Violate ISP	-0.122	-0.193	0.342	0.464	0.4444	0.354	0.368	0.305	1.000

Table 4. Discriminant Validity & Cross Loadings

10. Hypotheses Tests

This study used SmartPLS to test the proposed hypotheses and the significance of all paths in the research model. The PLS algorithm was run to produce the standardized regression weights, factor loadings, and R^2 (i.e., the percent of variance explained by the explanatory variables). To assess if regression weights were significant, a bootstrapping algorithm created t statistics to show significance. Business Orientation, and Ethical Orientation increased the variance in the intent to violate IS policy with 25.4% explained (see Figure 2).

From a data analysis perspective, intent to violate IS policy was positively influenced by four out of six neutralization techniques but was only influenced significantly by two of the neutralization techniques defenses of necessity ($\beta=0.375, t=2.156, p=0.032$), and Metaphor of the ledger ($\beta=0.265, t=2.463, p=0.014$). The remaining techniques appeal to higher loyalties ($\beta=-0.126, t=0.967, p=0.397$), Condemnation of the condemners ($\beta=0.036, t=0.375, p=0.708$), denial of injury ($\beta=-0.008, t=0.060, p=0.952$), and denial of responsibility ($\beta=-0.014, t=0.165, p=0.869$) did not significantly impact the intent to violate information

security policy. Therefore, for this research model, **H1** was not supported. Results show employees, when faced with a dilemma, did not feel it was worth breaking policy at the cost of getting the job done. **H2** is supported. As hypothesized, Defense of Necessity had a positive influence on intent to violate information systems security policy (ISSP). The analysis shows that employees feel that they are in a dilemma and their task must be resolved at the cost of violating security policy. **H3** is also supported. Results show employees are willing to break the information security policy because they believe they have done a surplus of good, and an occasional bad action is okay. **H4, H5, H6** are not supported. Results show that employees take some level of responsibility as it relates to minimizing any harm that may affect the organization and others. Results also show that employees take ownership in their actions. As predicted, **H7** is supported. Business Orientation had a negative influence on employees accepting neutralization technique appeal to higher loyalties ($\beta = 0.181, t = 2.775, p = 0.006$). Results show that employees cognitive thinking allowed them to rationalize or contemplate accepting appeal to higher loyalties technique. However, employees were not willing to use the justification to violate information security policy. **H8** is supported ($\beta = -0.234, t = 3.780, p = 0.000$). Results show employees believe that some security policies are unreasonable and rationalize their action, as necessary. **H9** is supported ($\beta = -0.245, t = 3.869, p = 0.000$). Results show employees often compensate good action with bad action and as a result, rationalizes that it is okay to break ISSP policy. **H10** is supported ($\beta = -0.247, t = 3.117, p = 0.002$). Results show that employees believe that ISSP is unreasonable and focuses the blame on those that are the target of the action. **H11** is supported ($\beta = -0.241, t = 2.957, p = 0.003$). Results show that employees believe their action by minimizing the harm it causes. **H12** is supported ($\beta = -0.220, t = 3.123, p = 0.002$). Results show employees lacking responsibility for herself/himself in committing the act. Employees justify their action of not knowing the policy or blaming someone else.

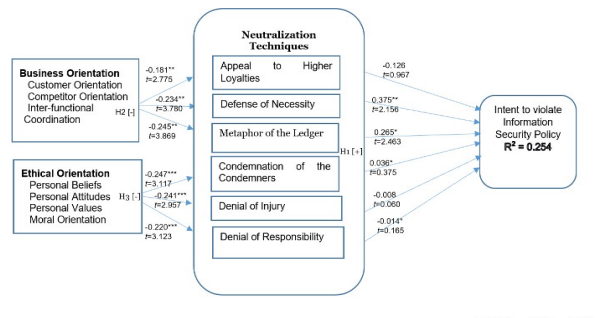


Figure 2. Results of Hypothesis Test

11. Discussion

We presented a research model that suggested the influences of Business Orientation and Ethical Orientation of individuals in shaping their tendencies to pursue different neutralization techniques in the context of IS security policy violation. Our analysis revealed a negative influence of business orientation and ethical orientation on the techniques of neutralization.

As hypothesized, we found that business and ethical orientation had a negative influence on the neutralization techniques. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010) noted that it is important to connect end user's behavior with an organization's security policy in evaluating difficult choices by employees. Our research suggest employees were willing to cross the line and violate ISSP for two reasons: (1) if policy is considered and viewed unreasonable, and (2) if an employee believes they have a surplus of good behavior and rationalizes that one bad action is excusable. This model evaluated neutralization techniques independently focusing on the intent to violate information security policy and found an impact of 25.4% on the intent to violate in ISSP. Our analysis suggests employees believe that certain IS policies to be unreasonable and therefore willing to break them as they feel it is necessary to accomplish their task. Our research further revealed that employees believe that a surplus of good behavior condones bad behavior when it comes to ISSP compliance. Our main research questions this

12. Limitation of Study

One of the important limitations of this study is the use of web-based surveys. To reach more participants, a web-based survey was selected. However, could create some bias as paper-based survey was not an option. To ensure success with a web-based survey, invitations were sent via e-mail to participants asking for their voluntary participation. Secondly, this research was limited to data collection in the United States. It is suggested that future studies focus on data collection from different populations outside the states. Additionally, this study did not consider government organizations or U.S. military, as these organizations manage information security differently. It is hoped that future studies expand to different countries and diverse groups. Lastly, this research focused on Neutralization Techniques, Appeal to Higher Loyalties, Defense of Necessity, and Metaphor of the Ledger to regress on Business Orientation. We also limited Neutralization Techniques Condemnation of the Condemners, Denial on Injury, and Denial of Responsibility to only regress on Ethical Orientation.

research addressed is: Do employees knowingly make business or ethical decisions when accepting one of the six neutralization techniques with the intent to violate ISSP. Previous research from Siponen and Vance (2010)] also found neutralization to be an indicator of employee's information security behavior. Neutralization techniques showed some positive and negative impact on the intent to violate information security behavior. More specifically, Metaphor of the Ledger and Defense of Necessity showed significant impact on the intent to violate ISSP, while Appeal to Higher Loyalties, Condemnation of the Condemners, Denial of Injury and Denial of Responsibility showed an insignificant impact.

13. Implications

This study showed the intent to violate information security policy was explained by 25.4 percent of variance from neutralization techniques. This leads us to two research implications. First, the study confirmed that findings on the impact of neutralization techniques in the intent to violate ISSP. As suggested by Siponen and Vance (2010), we reiterate the importance of neutralization in the development and implementation of information systems security policies. Second, we found that breaking out neutralization techniques separately provided insight in employees decisions to rationalize and adopt certain behaviors in intent to violate ISSP through specific techniques.

14. Conclusion

While there is no denying of the importance of neutralization techniques in shaping the intention to violate information security policy, our study highlights business orientation and ethical orientation as inhibitors of tendencies to pursue neutralization techniques. Our study also revealed that employees gravitate toward rationalizing and adopting some neutralization techniques more than others.

15. References

- Alteer, A. M., Yahya, S. B., & Haron, M. H. (2013). Auditors' Personal Values and Ethical Judgement at Different Levels of Ethical Climate: A Conceptual Link. *Journal of Asian Scientific Research*, 3(8), 862.
- Allport, G. (1967). Attitudes. In M. Fishbein (Ed.), *Readings in attitude theory and measurement*. New York: *John Wiley & Sons*, pp. 1-13.
- Arthur, J. B. (1994). Effects of human resource systems on manufacturing performance and turnover. *Academy of Management Journal*, 37, 670-687.

- Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & security, 39*, 145-159.
- Beekun, R. I., & Westerman, J. W. (2012). Spirituality and national culture as antecedents to ethical decision-making: a comparison between the United States and Norway. *Journal of business ethics, 110*(1), 33-44.
- Bugurcu, 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.
- Chandler, D., & Werther Jr, W. B. (2013). *Strategic corporate social responsibility: Stakeholders, globalization, and sustainable value creation*. Sage Publications.
- Cheng, L., Li, W., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*, 447-459.
- Clikeman, P. M., Geiger, M. A., & O'Connell, B. T. (2001). Student perceptions of earnings management: the effects of national origin and gender. *Teaching Business Ethics, 5*(4), 389-410.
- Cohen, J. (1992). A power primer. *Psychological bulletin, 112*(1), 155.
- Costello, B. J. (2000). Techniques of neutralization and self-esteem: a critical test of social control and neutralization theory. *Deviant Behavior, 21*(4), 307-329.
- D'Arcy, J., & Teh, P. L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management, 56*(7), 103151.
- DeVellis, R. F. (2012). *Scale development: Theory and applications*. Thousand Oaks, CA: Sage.
- Diamantopoulos, A., & Hart, S. (1993). Linking market orientation and company performance: preliminary evidence on Kohli and Jaworski's framework. *Journal of strategic marketing, 1*(2), 93-121.
- Douglas, P.C., Davidson, R.A., & Schwartz, B.N. (2001). The effect of organizational culture and ethical orientation on accountant's ethical judgements. *Journal of Business Ethics, 34*(2), 101-121.
- Fok, L. Y., Payne, D. M., & Corey, C. M. (2016). Cultural values, utilitarian orientation, and ethical decision making: A comparison of US and Puerto Rican professionals. *Journal of Business Ethics, 134*(2), 263-279.
- Forsyth, D. R. (1980). A taxonomy of ethical ideologies. *Journal of Personality and Social Psychology, 39*(1), 175.
- Fritzsche, D., & Oz, E. (2007). Personal values' influence on the ethical dimension of decision making. *Journal of Business Ethics, 75*(4), 335-343.
- Gatignon, H., & Xuereb, J. M. (1997). Strategic orientation of the firm and new product performance. *Journal of Marketing Research, 34*(1), 77-90.
- Gatignon, H., & Xuereb, J. M. (1997). Strategic orientation of the firm and new product performance. *Journal of marketing research, 34*(1), 77-90.
- Hirschi, T. (1969). *Causes of delinquency*. University of California Press, Berkeley.
- Hooley, G., Cox, T., Fahy, J., Shipley, D., Beracs, J., Fonfara, K., & Snoj, B. (2000). Market orientation in the transition economies of central Europe: tests of the Narver and Slater market orientation scales. *Journal of Business research, 50*(3), 273-285.
- Hunt, S. D., & Vitell, S. (1986). A general theory of marketing ethics. *Journal of Macromarketing, 6*(1), 5-16.
- Hyde, R. E., & Weathington, B. L. (2006). The congruence of personal life values and work attitudes. *Genetic, social, and general psychology monographs, 132*(2), 151-190.
- Jebbarajakirthy, C., Thaichon, P., & Yoganathan, D. (2016). Enhancing corporate social responsibility through market orientation practices in bottom of pyramid markets: with special reference to microcredit institutions. *Journal of Strategic Marketing, 24*(5), 398-417.
- Kaitazi, M., Cavusoglu, H., Benbasat, I., & Haftor, D. (2018). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information & Computer Security, 26*(2), 171-193.
- Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.
- Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal, 2014*.
- Kohli, A. K., Jaworski, B. J., & Kumar, A. (1993). MARKOR: a measure of market orientation. *Journal of Marketing research, 30*(4), 467-477.
- Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems, 4*(1), 3.
- Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research? *Crime and Justice, 32*, 221-320.
- Myrsky, L., Siponen, M., Pahlila, 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.

- Mingzhi, L. (2008). The effect of personal values on individuals' ethical behavioral intentions: evidence from professional auditors in people's republic of China. *Canadian Academic Accounting Association*.
- Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency, 18*(2), 295-318.
- Molina, C. M., Moreno, R. R., & Moreno, M. R. (2013). Previous beliefs and continuance intention. *International Entrepreneurship and Management Journal, 9*(2), 199-216.
- Morris, R. G., & Higgins, G. E. (2009). Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review, 34*(2), 173-195.
- Narver, J.C., Slater, S.F. (1990). The effect of a market orientation on business profitability. *Journal of Marketing, 54*(4), pp. 20-35.
- Payne, D., Corey, C. M., & Fok, L. Y. (2016). The Indirect Effects of Cultural Values on Ethical Decision Making via Utilitarian Ethical Orientation. *American Journal of Management, 16*(1), 19.
- Phatak, A. V., Bhagat, R. S., & Kashlak, R. J. (2005). *International management: Managing in a diverse and dynamic global environment*. New York, NY: McGraw-Hill Irwin.
- Piquero, A. R., & Hickman, M. (1999). An empirical test of Tittle's control balance theory. *Criminology, 37*(2), 319-342.
- Rapp, A., Beitelspacher, L. S., Schillewaert, N., & Baker, T. L. (2012). The differing effects of technology on inside vs. outside sales forces to facilitate enhanced customer orientation and interfunctional coordination. *Journal of Business Research, 65*(7), 929-936.
- Richardson, V. (1996). *The role of attitudes and beliefs in learning to teach*. In J. Sikula, Ed. *Handbook of Research on Teacher Education* (2nd ed.), pp. 102-119. New York: Simon & Schuster Macmillan.
- Rokeach, M. (1973). *The nature of human values*. Free press.
- Rogerson, S., & Sallnäs, U. (2017). Internal coordination to enable high load factor. *The International Journal of Logistics Management, 28*(4), 1142-1167.
- Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management*, (in press), 1-15.
- Sims, R. L. (2002). Ethical rule breaking by employees: A test of social bonding theory. *Journal of business ethics, 40*(2), 101-109.
- Sin, L. Y., Tse, A. C., Yau, O. H., Chow, R. P., & Lee, J. S. (2005). Market orientation, relationship marketing orientation, and business performance: The moderating effects of economic ideology and industry type. *Journal of International Marketing, 13*(1), 36-57.
- Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly, 48*7-502.
- Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management, 49*(7-8), 334-341.
- Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers & Security, 88*, 101617.
- Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly, 45*-60.
- Sykes G, Matza D. (1957). Techniques of neutralization: a theory of delinquency. *American Sociological Review, 22*(6):664-70
- Teh, P. L., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees? :insights from neutralization and social exchange theory. *Journal of Global Information Management (JGIM), 23*(1), 44-64.
- Trinkle, B. S., Warkentin, M., Malimage, K., & Raddatz, N. (2021). High-Risk Deviant Decisions: Does Neutralization Still Play a Role?. *Journal of the Association for Information Systems, 22*(3), 3.
- Turk, Z., & Avcilar, M. Y. (2018). An Investigation of the Effect of Personal Values on the Students' Ethical Decision-Making Process. In *Eurasian Business Perspectives* (pp. 245-262). Springer, Cham.
- Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management, 57*(4), 103212.
- Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and organization, 16*(4), 304-324.
- Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal, 28*(2), 266-293.
- Wood, S., & de Menezes, L. (1998). High commitment management in the U.K.: evidence from the Workplace Industrial Relations Survey and Employers' Manpower and Skills Practices Survey. *Human Relations, 51*, 485-515.
- Wooten, K. G., Wortley, P. M., Singleton, J. A., & Euler, G. L., (2012). Perceptions matter: beliefs about influenza vaccine and vaccination behavior among elderly white, black, and Hispanic Americans. *Vaccine, 30*(48), 6927-6934.