A Study of the Effect of Types of Organizational Culture on Information Security Procedural Countermeasures

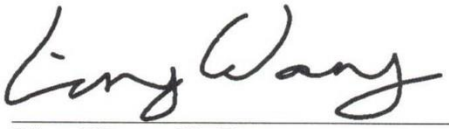
By

Sheri R James

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

College of Computing and Engineering
Nova Southeastern University
2023

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



Ling Wang, Ph.D.
Chairperson of Dissertation Committee

4/24/23
Date

Junping Sun, Ph.D.
Dissertation Committee Member

4/24/23
Date

Gregory Simco, Ph.D.
Dissertation Committee Member

4/24/23
Date

Approved:

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

4 /24/23
Date

College of Computing and Engineering
Nova Southeastern University

2023

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

A Study of the Effect of Types of Organizational Culture on Information Security Procedural Countermeasures

by
Sheri R James

This study examined the impact of specific organizational cultures on information security procedural countermeasures (ISPC). With increasing security incidents and data breaches, organizations acknowledge that people are their greatest asset as well as a vulnerability. Previous research into information security procedural controls has centered on behavioral, cognitive, and social theories; some literature incorporates general notions of organization culture yet there is still an absence in socio-organizational studies dedicated to elucidating how information security policy (ISP) compliance can be augmented by implementing comprehensive security education, training, and awareness (SETA) programs focusing on education, training, and awareness initiatives.

A theoretical model was developed to examine the effect of types of organizational culture on ISPC. The types of organizational culture were bureaucratic, competitive, participative, and learning culture.

To evaluate the reliability of the model, a survey was conducted by Centiment utilizing responses from its panel. The types of organizational culture and ISPC were from well-known scales derived from the literature. Data were collected from the subjects using an online survey form with a Likert scale and demographic data such as age, gender, education, industry, and size of organization.

Data analysis showed bureaucratic organizational culture significantly influenced both ISP and SETA, but the effect was positive instead of negative as hypothesized. Learning organizational culture had a significant positive effect on SETA. Both competitive organizational culture and participative culture did not have a significant effect on ISP or SETA. Learning organizational culture did not have a significant effect on ISP. This study added to the body of knowledge by adding a socio-organization aspect to understanding employees' non-compliance and adherence to ISP and SETA. The study revealed a correlation between socio-organizational understanding and compliance to ISP and SETA. As such, better policies and training can be produced with less detrimental influence for organizations looking to follow regulations efficiently.

Acknowledgements

I'm so grateful for everyone who helped me complete this important milestone! My dissertation chair, Dr. Ling Wang was an invaluable source of insight and guidance throughout the process. Similarly, thanks to Dr. Gregory Simco and Dr. Junping Sun for their insights into my research quality which enabled it reach its full potential. Moreover, NSU resources provided access to essential databases that were necessary in finishing up all remaining steps along the way. Additionally, Laura Macias at Graduate Academic Advising services that kept me right on track with timely registration throughout grad school life.

And lastly: no amount words could ever express how grateful am I for the unconditional guidance & strength shown by mother Cheryl Kappes plus aunt Marilyn Prince & uncle Robert Bakken and my two sons Edgardo Rivera II and Nicholaus Rivera throughout entire journey – your kind encouragement has carried me through many dark times yet whose unwavering belief was an incredible source of strength during the journey ahead.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

A strategy used to combat information system (IS) misuse is the combination of procedural and technical countermeasures (Alabdulatif, Liu, & Alrawais, 2020; Albrechtsen & Hovden, 2019; Asghar, Raza, & Khan, 2021; D'Arcy & Hovav, 2009; D'Arcy, Hovav, & Galletta, 2009; Gao, Liang, Zhang, & Wang, 2019; Hovav & Galletta, 2009; Vintila & Iancu, 2021). Recent studies have delved into the use of multi-feature analysis, factors affecting employee compliance with security policies, technical and non-technical approaches to preventing insider threats and enhancing information security as well as adaptive architectures for enhanced protection. In particular, Alabdulatif et al. (2020), Albrechtsen & Hovden (2019), Asghar et al., (2021) Gao et al.,(2019), and Vintila & Iancu's study in 2021 focus on combining both technological tools along with behavioral measures to secure critical data infrastructure against malicious insiders. Information security policy (ISP) and security education, training, and awareness (SETA) are procedural countermeasures for combating IS misuse. Monitoring software, authentication, or filtering applications and technologies are examples of technical countermeasures (Alabdulatif, Liu, & Alrawais, 2020; Albrechtsen & Hovden, 2019; Asghar, Raza, & Khan, 2021; D'Arcy & Hovav, 2009; D'Arcy et al., 2009, Gao et al., 2019; Hovav & Galletta, 2009; Vintila & Iancu, 2021). Straub (1990) referred to the combination of procedural and technical countermeasures as security countermeasures (Alabdulatif, Liu, & Alrawais, 2020; Albrechtsen & Hovden, 2019; Asghar, Raza, &

Khan, 2021; D'Arcy & Hovav, 2009; D'Arcy et al., 2009; Gao et al., 2019; Hovav & Galletta, 2009; Vintila & Iancu, 2021). Organizations continue to strive for new ways to ensure ISP compliance and adherence to the SETA program.

Research has investigated behavioral (Herath & Rao, 2009) and cognitive theories (Bhattacharya, & Zhang, 2020; Bulgurcu, Cavusoglu & Benbasat, 2010; Choi, Jung, & Kim, 2021; Flores, Antonsen, & Ekstedt, 2014; Hu, & Dinev, 2020; Kankanhalli, Tan, & Wei, 2020; Shu, Teo, Wei, & Chen, 2021; Yuryna Connolly, Lang, Gathegi, & Tygar, 2017) of employee behavior to instill more compliance and adherence. Recent research has sought to identify ways of increasing employees' adherence to information security policies. Studies such as Bhattacharya and Zhang (2020), which explored the influence of social norms on compliance behavior in a Chinese online company, or Choi et al. (2021) who examined how cognitive load theory impacts training effectiveness, have shown promise from varying angles. Hu & Dinev's (2020) self-determination perspective aims at understanding employee motivation for greater compliance too - all providing valuable insights into effective strategies for encouraging desirable behaviors among staff members regarding data protection practices. In Kankanhalli, Tan and Wei's (2020) model of employee compliance behavior, cognitive and emotional reactions to information security policies were linked with positive outcomes in policy adherence. This work was furthered the following year by Shu et al. (2021) who proposed a dual-process conceptualization which blends together both mind-based rationales alongside affective components for proactive behavioral efficacy. Recent studies underscore the value of comprehending employee behavior and motivation to bolster information security compliance. By building effective strategies that consider employees' cognitive,

affective, and motivational patterns, organizations can better protect against potential breaches as well as reinforce their overall data safety posture. Research has also tied organization culture (Bulgurcu et al., 2010; Da Veiga & Martins, 2015; Dhillon & Backhouse, 2001; Ifinedo, 2014) or applying information security culture (Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015; Da Veiga & Martins, 2017; Lim, Chang, Maynard, & Ahmad, 2009; Ruighaver, Maynard, & Chang, 2007). Psychological research on organizational behavior calls for more research to understand "strong influence on an individual and a group's behavior within an organization" (Mowday & Sutton, 1993). Behavioral InfoSec calls for more research from an organizational behavior perspective on information security procedural countermeasures (ISPC) (Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville, 2013). Lebek, Uffen, Neumann, Hohler, and Breitner (2014) called for research connecting the social factors of organizations and employees. For extending ISPC compliance/adherence theory, this research tested types of organizational culture (OC) effects on ISPC.

The rest of the chapter is divided into nine sections. The first section discusses the scope and nature of the problem statement. The second section addresses the goal of the dissertation in what the research has accomplished. The third section prompts the investigation of solutions to our identified problem by offering targeted research questions. The fourth section provides the relevance and significance of the problem statement and the goal of the dissertation. The fifth section provides barriers and issues that impact the problem statement and goal of the dissertation. The sixth section provides a brief literature review encompassing organizational culture and information security countermeasures. The seventh section provides an approach to the research problem and

the goal of the dissertation. The eighth section provides milestones of the process used to accomplish the research problem. The concluding section provides a detail of the resources needed to address the research problem and goal of the dissertation.

Problem Statement

Organizations seek to minimize and altogether eliminate data breaches and security incidents. Security reports like Verizon's annual release of Data Breach Investigations Report (DBIR) have shown people are the most susceptible to causing these data breaches and security incidents organizations implement ISPC in the desire to gain compliance and adherence by their employees. However, ISPC implementation is not always successful for an organization. What may work for one organization is unsuccessful in other organizations. Limiting companies from evaluating the lone wolf that caused the breach (Paine, 1994) does not adequately account for external factors like the type of organizational culture that may impact the employee. Without a clear understanding of all the factors that affect ISPC, which limits IS misuse, the damages that occurred by organizations continue to persist. Thus, there is a need to examine the effect of the types of organizational culture on ISPC.

Dissertation Goal

This study explored the repercussions of varying organizational cultures on ISPC. The researcher referenced Hellriegel and Slocum's (1994) well–established research model to examine four distinct culture types: bureaucratic, competitive, participative, and learning – to determine their respective impacts on ISPC. ISPC harnesses two sophisticated constructs to evaluate individual perceptions of ISP and SETA initiatives, adapted from Ifinedo (2014) and D'Arcy et al. (2009), respectively. Table 2 provides an

overview for each construct to capture a comprehensive picture regarding ISP and SETA effectiveness.

Research Questions

The existing literature on organizational cultures was explored in this research, focusing specifically on the impact of four distinct topologies (bureaucratic, competitive, participative and learning culture) proposed by Hellriegel & Slocum (1994). These four distinct topologies were analyzed to assess their influence of negative or positive impact on the two ISPCs for compliance of ISP or adherence of SETA. Figure 1 shows the four types of organizational culture used in this research. Figure 2 shows the conceptual framework used in this research. The objective of this study was to answer the following research questions:

1. Do distinct types of organizational culture affect Information Security Policy?
2. Do distinct types of organizational culture affect the SETA program (or adherence to the SETA program)?

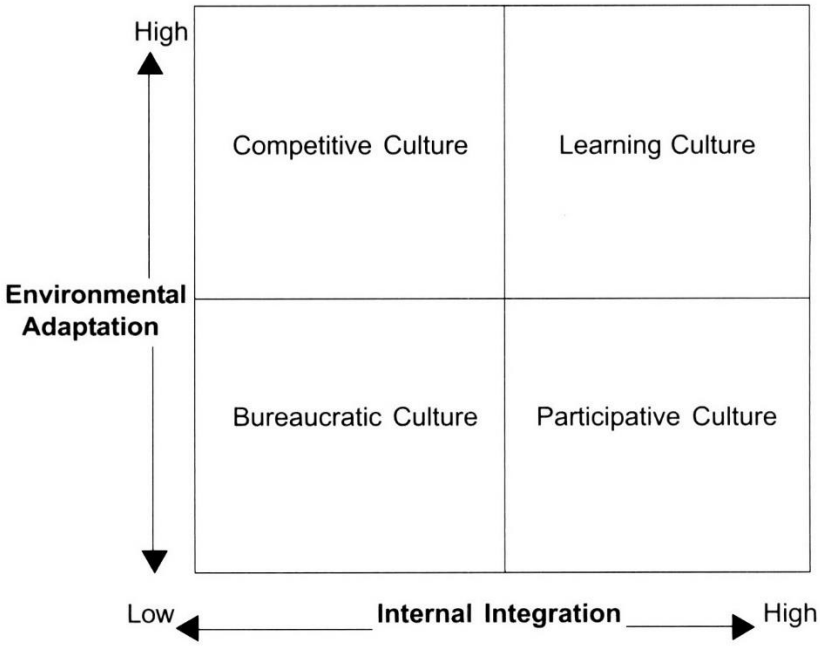


Figure 1: Four Types of Organizational Culture

Note: Four Types of Organizational Culture. Reprinted from Management, 6e. by Hellriegel and Slocum, 1994, New York: Addison Wesley. Copyright 1994 by New York: Addison Wesley. Reprinted with permission.

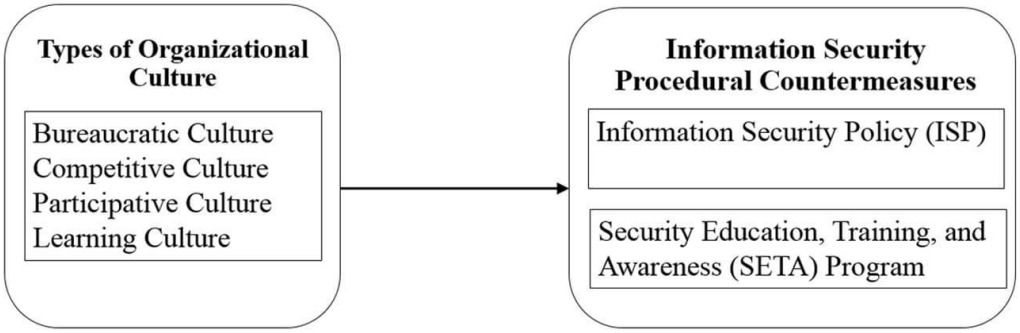


Figure 2: The Conceptual Framework

The research by Fard, Rostamy, and Taghiloo (2009), who examined the relationships between organizational types and shaping learning organizations, is the basis for the four types of organizational culture used in this study. ISPC consists of two individuals constructs to measure ISP and SETA. The four measures (see Table 2) used in this study

for ISP were adapted from Ifinedo (2014). The five measures (see Table 2) used in this study for SETA were adapted from D'Arcy et al. (2009). By utilizing a conceptual framework (referenced in Figure 2) and conducting an extensive literature review, several hypotheses could be formulated.

H_1. Bureaucratic organizational culture will have a negative influence on ISP.

H_2. Competitive organizational culture will have a negative influence on ISP.

H_3. Participative organizational culture will have a positive influence on ISP.

H_4. Learning organizational culture will have a positive influence on ISP.

H_5. Bureaucratic organizational culture will have a negative influence on SETA.

H_6. Competitive organizational culture will have a negative influence on SETA.

H_7. Participative organizational culture will have a positive influence on SETA.

H_8. Learning organizational culture will have a positive influence on SETA.

Relevance and Significance

Information security system management (ISM) has three pillars' people, processes, and technology. Any failure in one of the three can lead to a security breach of information systems. People remain the weakest link of the three ISM pillars (Bulgurcu et al., 2010; Crossler et al., 2013; Guo, Yuan, Archer, & Connelly, 2011; Ifinedo, 2014; Johnston, Warkentin, McBride, & Carter, 2016; Sasse, Brostoff, Weirich, 2001; Stanton, Stam, Mastrangelo, & Jolton, 2005; Veiga & Marins, 2015; Vroom & Von Solms, 2004).

> Rarely do the character flaws of a lone actor fully explain corporate misconduct. More typically, the unethical business practice involves the tacit, if not explicit, the cooperation of others and reflects the values, attitudes, beliefs, language, and

> behavioral patterns that define an organization's operating culture (Paine, 1994, p. 106).

Another point of the quote is that while people engage in the behavior, other cultural forces like organizational culture can be detrimental to ISC compliance. Organizational culture impacts the implementation of ISP (Bulgurcu et al., 2010; Da Veiga & Martins, 2015; Guo et al., 2011; Hu, Dinev, Hart, & Cooke, 2012). An understanding of socio-organizational resources can help organizations with the importance of creating an organizational culture that adheres to policy and regulatory requirements, which in turn instills ISP compliance (Bulgurcu et al., 2010; Da Veiga & Martins, 2015; Dhillon & Backhouse, 2001; Ifinedo, 2014) and SETA programs. In 2017 the tenth year running, Verizon released the annual Data Breach Investigations Report (DBIR) that compiles their security team and other leading security practitioners globally that reported more than 42,000 security incidents and almost 200 breaches (Biscoe, 2017). An incident is "a security event that compromises the integrity, confidentiality, or availability of an information asset" (Verizon, 2018). A breach is "an incident that results in the confirmed disclosure—not just potential exposure — of data to an unauthorized party" (Verizon, 2018). The takeaway from the report showed the following: 1. 61% of data breach victims were from smaller companies, 2. 1 in 14 users was susceptible to phishing frauds, with 25% being repeatable offenders. 3. 51% of breaches involved ransomware. 4. 80% of hacking-related breaches involved stolen and weak passwords. 5. Organizations are not proactive in updating defenses (Biscoe, 2017). In 2018 the eleventh year running, Verizon released the annual DBIR. The incidents increased to 53,000+ and 2,216 confirmed data breaches (Verizon, 2018). The findings' highlights showed that 28%

involved internal actors (Verizon, 2018). The victims of breaches were 14% public sector, 15% for accommodation, and food services, 24% for healthcare organizations, and 58% for small businesses (Verizon, 2018). The tactics utilized still showed 48% hacking as the highest, 30% malware, 17% social attacks, 12% privilege misuse, and 11% involved physical actions (Verizon, 2018). A review of these two consecutive reports shows the problem continues to persist and increase among organizations globally. Langevoort (2015) stated, "Sociologists, in turn, urge that we look outside the individual mind for what drives compliance or noncompliance with the law, to various cultural forces." ISP is a set of guidelines and rules for security behavior in an organization's context. SETA is a set of directives to be adhered to in ensuring an understanding of security behavior. While ISP and SETA are not explicitly law, they are both procedural countermeasures for combating IS misuse (D'Arcy & Hovav, 2009; D'Arcy et al., 2009). Monitoring software, authentication, or filtering applications and technologies are examples of technical countermeasures (D'Arcy & Hovav, 2009; D'Arcy et al., 2009). Straub (1990) referred to the combination of procedural and technical countermeasures as security countermeasures (D'Arcy & Hovav, 2009; D'Arcy et al., 2009). This research focused on the two controls within procedural countermeasures, ISP, and SETA. ISPC seeks employee compliance over non-compliance within an organization.

Understanding socio-organizational resources can help organizations create an organizational culture that adheres to policy and regulatory requirements, instilling ISP compliance (Bulgurcu et al., 2010; Dhillon & Backhouse, 2001; Ifinedo, 2014; Veiga & Martins, 2015). A domain of Information Security research dealing with behaviors of individuals regarding the protection of information and information system assets

throughout the organization is known as behavioral InfoSec (Crossler et al., 2013; Fagnot, 2008; Flores et al., 2014; Han, Kim, Y., & Kim, H, 2017; Stanton, Stam, Mastrangelo, & Jolton, 2006; Yuryna Connolly et al., 2017). The Behavioral Information Security research domain draws more attention to the human element of ISM. ISM is the attitudes, beliefs, norms, behavioral patterns, leadership, culture, security awareness, etc. (Albrechtsen & Hovden, 2010; Dhillon & Blackhouse, 2001; Siponen, 2005) that, in turn, influence information security behaviors. Two broad categories exist in these approaches 1). Users' cognitive processes affect information security behavior (Bulgurcu et al., 2010; Flores et al., 2014; Yuryna Connolly et al., 2017). 2). Organizational culture affects information security behavior (Flores et al., 2014; Flores & Ekstedt, 2016; Yuryna Connolly et al., 2017). Organizational culture impacts the implementation of ISP (Bulgurcu et al., 2010; Da Veiga & Martins, 2015; Guo et al., 2011; Hu et al., 2012). Through an analysis of the effect organizational culture has on information security behaviour (Flores et al., 2014; Flores & Ekstedt, 2016; Yuryna Connolly et al., 2017), it is possible to create more effective and tailored ISPCs that specifically address particular cultures with regards to protecting against misuse. The Behavioral InfoSec research domain has expanded, showing the need to look at ISM from a socio-organizational perspective. Herath and Rao (2009) review of literature listed three areas of behavioral InfoSec 1). Conceptual papers, 2) Empirical papers, and 3). Security compliance papers. This review showed an emphasis on socio-organizational perspectives using theories: theory of anomie, general deterrence theory (GDT), theory of reasoned action (TRA), theory of planned behavior (TPB), theory of technology acceptance model (TAM), intrinsic, motivation, protection motivation theory (PMT), organizational behavior (OB),

organizational climate (OC), Hofstede's cultural dimensions, and game theory. Anderson and Agarwal (2010) review of literature in behavioral InfoSec also showed an emphasis on socio-organizational perspectives that included other theories: rational choice theory, fear appeal theory, neutralization theory, GDT, control theory, decomposed TPB, PMT expanded to include social influence and situation-specific factors, theory of cognitive moral development, theory of motivational types of values, social cognitive theory, information systems success and Triandis' behavioral framework and rewards, Schien's 3-level of organizational culture. Lebek et al. (2014) performed a meta-analysis on ISP compliance that found four primary theories TPB, GDT, PMT, and TAM. As such, these theories have a solid foundation in the literature supporting relationships of the constructs to which future research should focus on factors influencing employee behaviors and connections to their organizations (Han et al., 2017).

Organizational culture has research on the impact of different organizational settings. Using TPB results, Hu et al. (2012) show top management influences on organizational culture that impacted employees' ISP compliance. Similarly, Barton, Tejay, Lane, & Terrell (2016) used neo-institutional theory to examine senior management's external influences on information security system commitment. Results showed that mimetics significantly influence senior management, which is an aspect of organizational culture. Chang and Lin (2007) examined organizational culture effectiveness in implementing ISM, finding that control-oriented organizational cultures affect ISM principles. In contrast, flexibility-oriented organizational cultures are not significantly related to ISM principles. Yuryna Connolly et al. (2017), using GDT found procedural security countermeasures and organizational culture to impact employee security behaviors.

Da Veiga and Eloff (2010) proposed an information security culture framework based on current approaches to employee security behavior that does not consider the type of culture of the organization and employee behavior which they suggest for future research. The study aimed to shed light on employee security behavior within an organization and how the type of organizational culture affects ISPC compliance. This study provided insight into why one organization may be more successful in implementing ISPC while others fail. Prior research has shown the following gaps in the literature exist. Researchers are calling for more research in behavioral InfoSec regarding improving ISP compliance (Crossler et al., 2013; Lebek et al., 2014) and organizational behavioral perspective on factors in ISP compliance (Flores & Ekstedt, 2016; Han et al., 2017). Additionally, more research effects of organizational culture that shapes employee compliance behavior (Lebek et al., 2014; Flores & Ekstedt, 2016; Hu et al., 2012; Yuryna Connolly et al., 2017).

This research seeks to address previous literature gaps by examining types of organizational culture effects on ISPC. The theoretical model could help organizations to understand the type of organizational culture and how it affects information security measures. This understanding could lead to better-developed ISP and SETA programs for employee compliance in understanding organizational culture strengths and weaknesses. The potential for generalization is high for results to show organizations how to construct ISPC better and for researchers to apply organizational culture types to previous studies that did not account for external factors' impact on ISPC. To the best of my knowledge, this is among the first studies to discuss how types of organizational culture affect ISPC,

which can lead to better compliance and adherence in creating ISP and SETA programs in line with the type of organizational culture.

Barriers and Issues

Navigating the complexities of organizational culture's influence on IS and associated SETA program efforts can be difficult due to various issues, such as:

1. Multifaceted constructs: Understanding the nature of how organizational culture and ISP and SETA program which multifaceted constructs interaction are a complex task, one which requires careful examination to elicit out both their individual facets as well as the causality between them. To answer a given research question, it is essential to assess the aspects of both constructs that are most important; however, due to the complexity of their relationship finding causal relationships between these components can be difficult.
2. Measurement: Gauging the nuances of an organization's culture and assessing ISP and SETA program posture is a daunting task. Traditional self-reported metrics for these domains may be skewed due to respondent bias, complicating accurate measurements even further.
3. Data collection: Collecting reliable data for both constructs can be a challenging task, especially in large organizations that require the collaboration of multiple departments and personnel. Alternatively engaging the services of an experienced survey panel provider may offer valuable insights and access to essential information.

4. Limited generalizability: Analyzing how organizational culture influences ISP and SETA initiatives can vary depending on the context of a particular organization. Thus, results may not be applicable across all beliefs or cultures.
5. Complex causal mechanisms: The method by which different organizational cultures shape the implementation of effective ISP and SETA initiatives is intricate, requiring careful consideration of various intermediate variables.
6. Limited research: Despite the increasing importance of security in organizations, there remains a dearth of research exploring its relationship to organizational culture—specifically how it impacts policy and educational initiatives.

Overall, these barriers and issues made it challenging to fully understand the effect of distinct types of organizational culture on ISP and SETA initiatives. The researcher employed rigorous methodology in designing the study, using known constructs such as organizational culture types, ISP, and SETA initiatives to precisely measure results. The researcher collected reliable data for both constructs by purchasing from an organization that specializes in survey panels. The researcher conducted statistical analysis using Smart PLS for discussion and reporting of results. While there is a deficiency of research concerning the influence various organizational cultures have on ISP and SETA, these are promising fields to explore, as what this study managed to explore and achieved.

Assumption, Limitations, and Delimitations

Assumptions

The primary assumption in this study was that participants were actively working or had worked for an organization. Another assumption is that ISPC is implemented,

adhered to, and enforced within the organization where the participants worked, and they answered each question in the survey from such perspective.

Limitations

Limitations provide a list of factors uncontrollable by the researcher that may influence the study. The limitations of the study are as follows:

1. Prior research does not consider the effect of organizational culture types on ISPC.
2. The sample size used within the study is not a large sample despite using PLS-SEM, which does not require a large dataset to determine results.
3. The results of this study are limited by the measures used for types of organizational culture and ISPC.

Delimitations

Delimitations of the study are those imposed by the researcher to constrain the scope to a manageable depth. The delimitations of the study are as follows:

1. The study was delimited to participants 18 and older residing in the United States.
2. The study was delimited to participants actively working or who had worked for an organization.
3. The study was delimited to the Centiment survey panel.

Definition of Terms

Information Security Policy (ISP) – A procedural countermeasure for combating information security (IS) misuse that contains guidelines for organizational IS resources about proper and improper usage (D'Arcy & Hovav, 2009; D'Arcy, Hovav & Galletta, 2009).

Information Security Procedural Countermeasures (ISPC) – The combination of two information security procedural controls, ISP, and SETA programs (D'Arcy & Hovav, 2009; D'Arcy et al., 2009).

Security Education, Training, and Awareness (SETA) – A procedural countermeasure for combating information security (IS) misuse which provides ongoing reinforcement of acceptable usage of organizational IS resources (D'Arcy & Hovav, 2009; D'Arcy et al., 2009).

List of Acronyms

ISPC: Information Security Procedural Countermeasures

ISP: Information Security Policy

NIST: National Institute of Standards and Technology

SEM: Structured Equation Modeling

TPB: Theory of Planned Behavior

TAM: Technology Acceptance Model

GDT: General Deterrence Theory

CET: Cognitive Evaluation Theory

TRA: Theory of Reasoned Action

OB: Organizational Behavior

OC: Organizational Climate

SETA: Security Education, Training, and Awareness

Summary

Recent research has explored various strategies to mitigate insider threats and strengthen information security, such as multi-feature analysis (Alabdulatif et al., 2020),

examining the drivers of employee compliance with IT policies (Albrechtsen & Hovden, 2019), using both technical and non-technical approaches for fortification (Asghar et al., 2021), adaptive cybersecurity architectures (Gao et al. ,2019) ;and combining technical and non-technical measures in a unified system (Vintila & Iancu, 2021). Recent years have seen researchers invest significant effort into discovering unique strategies for encouraging employees to follow information security policies. Bhattacharya and Zhang (2020) considered the effects of social norms and moral obligation on employee compliance within a Chinese online company, Choi et al. (2021) applied cognitive load theory in their exploration of improved training as an avenue for higher adherence, while Hu and Dinev (2020) approached this topic from a self-determination perspective by researching how motivation affects behavior. Kankanhalli et al. (2020) explored the correlation between employee cognitive and emotional reactions to ISP compliance; discovering that perceived ease of use, usefulness, and attachment were all linked with higher levels of adherence. Shu et al.'s (2021) work was an extension on this idea; proposing a dual-process model which assesses both cognitive and affective factors in driving compliance behavior. Research has determined that ISPC is efficient way to reduce IS misuse when combined with GDT, a model deriving its efficacy from user-perceived severity and certainty (D'Arcy & Hovav, 2009; D'Arcy et al., 2009). However, evidence also showed that the user's level of morality affected the perception (D'Arcy et al., 2009, Hovav, & Galletta, 2009). A multi-level theory of PMT, TRA, and cognitive evaluation theory (CET) also showed the perception of severity and perception of vulnerability and employees' attitudes e a positive effect on IS misuse (Siponen, Mahmood, & Pahnila, 2014). In addition, social norms have a significant and positive

effect on compliance with ISP, impacting organizational culture (Siponen, Mahmood, & Pahnila, 2014). Lastly, considering that leadership style can influence organizational culture (Ogbonna & Harris, 2000), this research suggests the type of organizational culture affects ISPC. The research's main goal is to show that distinct types of organizational culture would have a positive or negative effect based on the type.

Chapter 2

Review of Literature

Overview

Organizational culture types have been linked to employees' attitudes and actions (Chen, & Yang, 2021; Hwang, Cheng, & Wu, 2020; Martins & Martins, 2016; Kaba, & Lyra, 2021; Liu, S., Guo, Li, Q., & Wei, 2020; Zhang, Feng, Chen, H., & Chen, Y., 2021). Figure 3 illustrates the broader theoretical model that explores the relationship between organizational cultures and information security procedural countermeasures (ISPC) (Von Solms, R., & Von Solms, B., 2004). Several recent studies provide further insights into this relationship. For instance, Albrechtsen and Hovden (2019) identified factors influencing employees' compliance with information security policies in organizations, while Bhattacharya and Zhang (2020) conducted an empirical study of employee information security behavior in a Chinese online company. Asghar et al. (2021) proposed technical and non-technical approaches to prevent insider threats, which could also have implications for enhancing ISPC. Additionally, Kankanhalli et al. (2020) and Shu et al. (2021) investigated the cognitive and emotional mechanisms underlying employee information security policy (ISP) compliance, while Hu and Dinev (2020) and Choi et al. (2021) proposed strategies to enhance employees' information security compliance. Other studies have also examined the impact of organizational culture on employees' knowledge sharing (Chen & Yang, 2021; Hwang et al., 2020; Kaba & Lyra, 2021; Liu et al., 2020) and phishing vulnerability (Chun et al., 2019), as well as the moderating role of innovation type on the relationship between organizational culture and

innovation performance (Zhang et al., 2021). Finally, Marinagi et al. (2021) conducted an empirical study to understand employee information security behavior. This examination delves into the intricate interactions between various organizational cultures and their relation to ISPC. By analyzing relevant literature, hypotheses regarding these associations were postulated: an explorative review of existing research further solidified this theoretical foundation by elucidating current understanding in the field of information security behavior. With a comprehensive grasp on prior knowledge, new insights can be added towards advancing progress within this area.

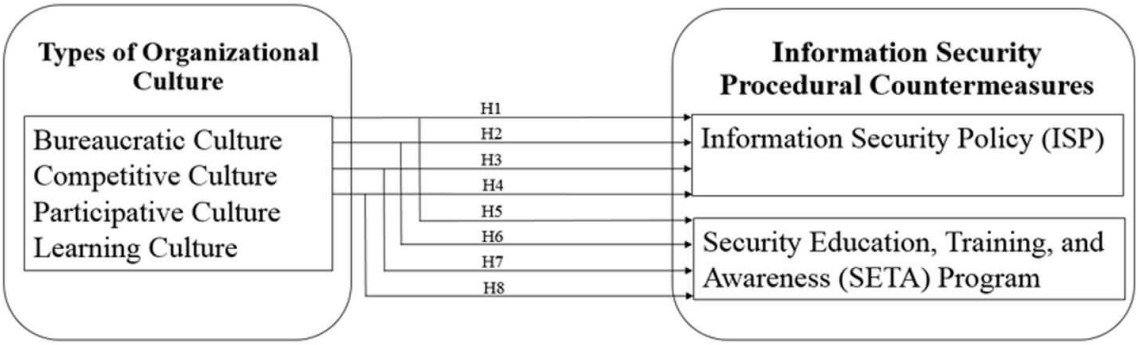


Figure 3. Theoretical Model

Information Security Policy

The National Institute of Technical Standards (NIST) provides a comprehensive security controls catalog labeled NIST Special Publication 800-53; revision 4 is the latest version published in 2013 since its inception in 2005. Security controls are the safeguards/countermeasures suggested for information systems and organizations to use for information security management principles: confidentiality, integrity, and availability. These principles protect information processed, stored, and transmitted within information systems and organizations along with a pre-defined set of security requirements. Several definitions in the IS research domain have been used in literature to define information policy (Baskerville & Siponen 2002). Regarding information security,

a comprehensive definition is “guiding statements of goals to be achieved” (Gaston 1996, p. 175). Han et al. (2017) used a more descriptive definition of ISP as derived from the works of Bulgurcu et al. (2010) and D’Arcy et al. (2009), which this study adopts their definition. Therefore, the definition of ISP as standards applied to employees’ roles and responsibilities for compliance with information and technology resources used in an organization. Organizational culture has been found to have a significant influence on the implementation of Information Security Policies (ISP) (Bulgurcu et al., 2010; Da Veiga & Martins, 2017; Guo et al., 2011; Hu et al., 2012; Albrechtsen & Hovden, 2019; Chun et al., 2019; Hwang et al., 2020; Kaba & Lyra, 2021; Liu et al., 2020; Zhang et al., 2021; D'Arcy & Greene, 2014; D'Arcy et al., 2009a; D'Arcy & Hovav, 2009; Bhattacharya & Zhang, 2020; Choi et al., 2021; Kankanhalli et al., 2020; Shu et al., 2021). The impact of organizational culture on employee knowledge sharing behavior and information security compliance has been investigated in many studies. For instance, Albrechtsen and Hovden (2019) found that factors such as leadership commitment, communication, and training influenced employees' compliance with information security policies. Chun et al. (2019) investigated the effect of cognitive reflection and security motivation on phishing vulnerability. Hwang et al. (2020) conducted a multi-group analysis to explore how organizational culture influences knowledge sharing in information systems development projects. Kaba and Lyra (2021) investigated the impact of organizational culture on employee knowledge-sharing behavior in developing countries. Liu et al. (2020) investigated the mediating roles of trust and knowledge sharing self-efficacy in linking organizational culture types to knowledge sharing behaviors. Bhattacharya and Zhang (2020) examined the relationship between organizational culture and employee

information security behavior in a Chinese online company. Choi et al. (2021) investigated the impact of information security training on employees' compliance behavior from a cognitive load theory perspective. Hu and Dinev (2020) proposed a self-determination perspective to enhance employees' information security compliance. Kankanhalli et al. (2020) studied the role of employee cognitive and emotional reactions in ISP compliance. Shu et al. (2021) proposed a dual-process model to unpack the cognitive mechanisms underlying employee ISP compliance. Overall, these studies highlight the importance of organizational culture in promoting employees' compliance with ISP and improving information security behavior in organizations. Normative beliefs, which are an important aspect of organizational culture, have a significant influence on employee compliance with Information Security Policies (ISPs) (Bulgurcu et al., 2010). Albrechtsen and Hovden (2019) found that employees' compliance with information security policies was influenced by their perceptions of the importance of security and the norms and values of their organization. Similarly, Bhattacharya and Zhang (2020) demonstrated that organizational culture plays a crucial role in shaping employees' information security behavior. Furthermore, Hu and Dinev (2020) emphasized the importance of self-determination theory in understanding employees' information security compliance, stating that organizational culture should create an environment that supports employees' basic psychological needs. Additionally, Kankanhalli et al. (2020) suggested that employee cognitive and emotional reactions play a vital role in ISP compliance. D'Arcy and Greene (2014) found that security culture and the employment relationship are significant drivers of employees' security compliance. Similarly, D'Arcy and Hovav (2009) argued that security countermeasures should be

tailored to the individual's perceptions and attitudes towards security. In contrast, D'Arcy and Hovav (2009) noted that the effectiveness of security countermeasures may vary depending on the individual. Choi et al. (2021) investigated the impact of information security training on employee compliance behavior and found that cognitive load theory can provide insights into the effectiveness of training programs. Furthermore, Chun et al. (2019) demonstrated that cognitive reflection and security motivation can impact employees' vulnerability to phishing attacks. The research found that employees' feelings of job satisfaction influence ISP (D'Arcy, & Greene, 2014); however, position, tenure, and industry are contingent factors to job satisfaction, which links to the type of organizational culture. In conclusion, organizational culture, cognitive and emotional reactions, training programs, and individual perceptions and attitudes all play crucial roles in employee compliance with ISP. This study examined the effects of types of organizational culture and ISP.

Security Education, Training, and Awareness (SETA) Program

A SETA program provides a combination of processes to ensure the security of information systems and technology resources within an organization. Security education and communications, like training and awareness, provide rules and guidelines for employees to adhere to within an organization that is paramount for compliant behavior (Von Solms, R., & Von Solms, B., 2004). The SETA program provides knowledge, usage, and skills to protect an organization's information systems and technology resources (Han et al., 2017). The SETA program provides a holistic view of compliance and noncompliance in a security environment (Han et al., 2017). The various traits found in different organizational cultures are more predisposed to comply with the SETA

program. Therefore, a SETA program may exist within the organization, but without a type of organizational culture conducive to security compliance, it is ineffective (Da Veiga & Martins, 2015). Karjalainen and Siponen (2011) set out to posit a new theory of IS security training (SETA) programs. IS security training having unique characteristics apart from other types of training and defined four pedagogical requirements for designing and evaluating IS security training. The pedagogical requirements are (1) psychological context having a basis in a group-oriented approach to teaching and learning, (2) content having a basis on the collective experiences and meanings of the learners, (3) teaching method having a basis on revealing and producing collective knowledge through collaborative learning, (4) evaluation of learning having a basis on the experiential and communicative method found in the learning community. The study concluded with studies that meet one or more pedagogical requirements and advancing training provided. The theory posited by Karjalainen and Siponen (2011) is akin to an organizational culture in that a group shares assumptions and beliefs and teaches new members what it has learned to solve, whether internal or external, problems. This group-orientated, collective, knowledge sharing, collaboration, and experiences lead to a more vital type of organizational culture that fosters the pedagogical requirements posited by Karjalainen and Siponen (2011) present which in turn shows an organizational culture more likely predisposed to adhering to a SETA program. Norms and job satisfaction studies link SETA and organizational culture. Individuals feeling alienated and angry can result in negative work-related behaviors within their group membership (Ensher, Grant-Vallone, & Donaldson, 2001). Job satisfaction leads to a lower turnover rate, and the learners' collective knowledge and experience continue to contribute to the culture of

solving problems and reinforcing learning. This study examines the effects of types of organizational culture and the SETA program.

Organizational Culture

Organizational behavior literature defines organizational culture as the group norms, values, beliefs, and assumptions practiced in an organization. In the most regarded and highly cited management book Organizational Culture and Leadership, organizational culture definition:

> A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way you perceive, think, and feel in relation to those problems (Schein, 2004, p. 17).

Schein (1990) states two critical elements of organizational culture: visible and invisible. Visible elements that are visible in the outer world. Invisibles are elements that people inside the group can only see—examples, values, norms, assumptions, etc. Examples are buildings, attire, and modes of behavior, stories, myths, language, and rites. The works of Deal and Kennedy (1982) and Peters and Waterman (1982) helped to show how culture could be used strategically by organizations to foster a way to control and shape the beliefs, norms, and values to help organizations succeed. This paper uses the four types of organizational culture as posited by Hellriegel and Slocam's (1994) topology: bureaucratic, competitive, participative, and learning cultures. With evidence-based literature and hypothesis to back it up, the researcher explored the distinct definitions of cultures and how they relate to information security countermeasures are discussed next.

Bureaucratic Culture

A bureaucratic culture exhibits trait of inflexibility, rigid regulations & rules, an elevated level of centralism, and an affirmative leadership style (Fard et al., 2009; Hellriegel & Slocum, 1994; Karyda, Kiountouzis & Kouklakis, 2005). Military and government sectors will exhibit this type of culture. D'Arcy et al. (2009) demonstrated through their study that security policies, SETA programs and computer monitoring are effective countermeasures to information systems misuse as supported by the General Deterrence Theory. While that has a positive effect, the company studied included computer users. The culture of the military and government is different from what type of culture may have existed in the companies tested. The military and government sectors are well known for their plethora of outdated policies, rules, and regulations, i.e., government – red-tape to get anything done and military – hurry up and wait for mentality with both has an exceptionally long historical culture. Deal and Kennedy (1982) label it as a culture of process. This organizational culture type is limited in innovative processes, repetition, and centralized decision-making, slow and reluctant to change with a high degree of conformity. The use of perceived threat of punishment becomes less the further you are away from the flagpole (headquarters). The literature review by D'Arcy et al. (2009) also showed mixed results of security policies or SETA programs not affecting compliance with security and did not consider the organizational culture type. Karyda, Kiountouzis, and Kokolakis (2005) case study explored the formulation, implementation, and adoption of ISP within two organizations. The study clearly illustrated contextual factors, with the historical data being two decades worth for one non-government and the other government in which neither had an ISP in place as

having a role in the application of ISP. The Social Security Institute (SSI) is a government organization that, despite 300 regional offices dispersed geographically having autonomy, operates as a bureaucratic and highly centralized management (Karyda, Kiountouzis, & Kouklakis, 2005).

The study also annotated that previous major IT projects progressed very slowly, and results were significantly different from their initial specifications (Karyda, Kiountouzis, & Kouklakis, 2005). The study showed that the government organization's bureaucratic culture negatively affected adherence to ISP and SETA. The study's key findings showed that the bureaucratic nature of SSI hindered the creation or assignment of personnel to address SETA due to management's lack of flexibility to employ qualified personnel or alter the organizational structure. Both contributed to low user awareness of ISP and SETA out of fear, lack of understanding, and distrust of the technology (Karyda, Kiountouzis, & Kouklakis, 2005). In addition, security control implementation was slow due to many bureaucratic procedures to be adhered to and incorporated (Karyda, Kiountouzis, & Kouklakis, 2005). Silverthorne (2004) study showed bureaucratic culture had the lowest levels of job satisfaction and organizational commitment. When you take in the factors of each study by Silverthorne (2004) and Karyda, Kiountouzis, & Kouklakis (2005), the predisposition of ISPC compliance is likely to be below. Therefore, companies with or exhibit bureaucratic culture are not likely predisposed to engage proactively in ISP compliance and adherence to SETA programs collectively defined as ISPC.

Competitive Culture

A competitive culture exhibits high flexibility, low integration, contract relations between employees and the organization, low loyalty, low cultural identity, and achieving quantitative objectives (Fard et al., 2009; Hellriegel & Slocum, 1994). Financial and corporate sectors will exhibit this type of culture. A study by Han et al. (2017) results showed psychological contract fulfillment could mitigate adverse effects on ISP compliance in supervisor groups. Also, employees comply if they recognize the benefits of ISP compliance. The theory was used as a rational choice theory as the literature review showed explanatory power in corporate crimes against ISP compliance in assessing the cost and benefits. The literature review by Han et al. (2017) also showed mixed results were obtained previously and did not consider the organizational culture type in the study or those found in the literature review. Dhillon and Torkzadeh (2006) study provide a value-focused assessment of the overall objective of maximizing information security in an organization. Here are three listed as shown in Table 1. a. Create an environment that promotes organizational loyalty. b. Enhance individual/group pride in the organization. c. Stress individuals treat others as they would like to be treated (Dhillon & Torkzadeh, 2006, p. 306). Employees' “psychological contract” is about producing results that lead to better pay and incentives (Tollefson, 2000). They believe their skills are marketable to other employers and are not likely to stay lifelong with an employer, which is a trait of low loyalty and low cultural identity. With this belief, they perform when rewarded and stop performing when not rewarded (Tollefson, 2000). Therefore, if the employee feels they are not an asset to the company nor rewarded, they do not comply with or adhere to ISPC. The traits of the competitive culture of low

integration, low loyalty, and low cultural identity are counterproductive to maximize security, as shown by Dhillon and Torkzadeh (2006). Therefore, companies with or exhibit competitive culture are not likely predisposed to engage proactively in ISP compliance and adherence to SETA programs collectively defined as ISPC.

Participative Culture

A participative culture exhibits low flexibility, high integration, loyalty, personal commitment, teamwork, high social acceptance, and a tendency to stability (Fard et al., 2009; Hellriegel & Slocum, 1994). Non-profit organizations and healthcare sectors will exhibit this type of culture. Participative cultures include groups in decision-making. The theory of groupthink is linked to this type of organizational culture (Janis, 1972, 1982, 1989), in which the leader or more influential members of the group drive the decision-making process. The rationale is based on the entire group as a single collective, stereotypes of outgroups, lack of understanding of alternatives, limited risk assessment of selected solution, and selective information processing (Turner, & Pratkanis, 1998). Jones, Jimmieson, and Griffiths (2005) study showed an organizational culture that places high prominence on human relations values through (training and development, open communication, and participative decision-making) fosters employee cohesion and morale. The fostering of cohesion, teamwork, and personal commitment strive to meet new challenges for the organization's benefit, which ISPC helps the organization's performance (Zhou, David, & Li, 2006). Albrechtsen and Hovden (2010) result on information security awareness and behavior that employee participation, collective reflection, and group processes are positively related. The decision-making groups within a participative culture share knowledge and experiences that add to the benefit of

compliance and adherence to ISPC (Albrechtsen & Hovden, 2010). A participative culture does not question or go against a group decision concerning ISP and SETA program initiatives for the organization's betterment. Silverthorne (2004) study showed a participative culture akin to supportive culture had the highest levels of job satisfaction and organizational commitment. So, it makes sense that a participative culture would be more indicative of engaging in ISPC. Therefore, companies with or exhibit participative culture are predisposed to proactively engage in ISP compliance and adherence to SETA programs collectively defined as ISPC.

Learning Culture

A learning culture exhibits traits of the trend to change, knowledge expansion, sensitivity and responsive to external changes, complex environment, competitive advantage, informed about the environment, gathering environmental information and process, service development, encouraging innovation, creativity, and learning, and organizational commitment (Fard et al., 2009; Hellriegel & Slocum, 1994). Education and public sectors (startups, entrepreneurship, and innovative companies) will exhibit this culture. A study by Bates and Khasawneh (2005) results showed organizational learning culture was a predictor of learning transfer climate, and both influenced organizational innovation. Bates and Khasawneh (2005) literature review showed members of the learning culture value learning as it, in turn, enhanced the drive for excellence and increased performance for innovation and progression. Rebelo and Duarte Gomes (2011) study showed organic structure, an approach to total quality principles and highly educated employees were factors that instill organizational learning. Learning in organizations is promoted through the flexible, decentralized, and organic organizational

structure (Rebelo & Duarte Gomes, 2011). An organic structure (culture) conducive to collaboration and continual learning is predisposed to seeking understanding to comply and adhere to ISPC. The approach to total quality principles instills the characteristic of ISPC. Highly educated employees like organic structure led to a predisposition to learning which leads to understanding and compliance, and adherence to ISPC. Egan, Yang, & Bartlett (2004) study showed that a learning culture is associated with job satisfaction and motivation to transfer learning. Silverthorne (2004) study showed an innovative culture akin to a learning culture was the second-highest level of job satisfaction and organizational commitment. So, it makes sense that a learning culture would be more indicative of ISPC as job satisfaction relates to learning organizational culture. Employees with high job satisfaction are motivated to share knowledge of ISPC (Egan et al., 2004). Therefore, companies with or exhibit a learning culture are predisposed to proactively engage in ISP compliance and adherence to SETA programs collectively defined as ISPC.

Summary

Studies have shown organizational culture impacts behavior and compliance with ISP (Chen, & Yang, 2021; Hwang et al., 2020; Martins & Martins, 2016; Kaba, & Lyra, 2021; Liu et al., 2020; Zhang et al., 2021; Von Solms, R., & Von Solms, B., 2004). This chapter reviewed relevant literature for each construct used in this study. In the literature review, I discussed the construct ISP and SETA labeled as ISPC, organizational culture, and types of organizational culture: bureaucratic, competitive, participative, and learning to explore the relationships of ISPC and types of organizational culture. ISP is the standards applied to employees' roles and responsibilities for compliance with

information and technology resources used in an organization, and how I examined the relationship of types of organizational culture with ISP. SETA is a program that provides a combination of processes to ensure the security of information systems and technology resources within an organization and how. I examined the relationship between types of organizational culture with SETA. This academic discussion of organizational culture was prefaced by Schein's (2004) definition, which provided a basis for exploring the nuances between each type to ensure their distinct cultural identities. I hypothesized that these different patterns and beliefs foster the organizational culture to adhere and comply with ISPC and the more restrictive and limited organizational culture to disregard adherence and compliance to ISPC.

Chapter 3

Methodology

Overview

This chapter presents the research methodology to understand the effects of types of organizational culture on ISPC. The first section provided a general overview of the research method employed for this study. The following section outlines the data collection procedures and operationalization of the constructs in the study. Subsequent sections include participants, data analysis, the format of results, and resource requirements concluding with a chapter summary.

Research Method

The effects of types of organizational culture on ISPC are difficult to observe without input from the individual's perspective. This study used a quantitative survey research method. A survey provides a reasonable objective measure of the evaluated constructs to examine the effects by answering the research questions and testing hypotheses. The subsequent data collection procedures section provides more detail on the use of previously validated constructs.

The study consisted of six primary constructs adapted from previously validated research. Each construct for this study is within acceptable levels for internal consistency, convergent validity, and discriminant validity.

Data Collection Procedures

The research model used a survey to collect data for the tested constructs. Centiment received a form with survey items to collect data from a survey panel of 18-year-old and older in the U.S. who were employed. I provided Centiment a brief introduction to why I

was conducting the study and asked them to provide one at the beginning of the study for each participant in the research panel used for the study. Centiment participants received a disclaimer notice clause before they began the study. Once Centiment had collected the data, the raw data was cleaned and prepared for analysis using SmartPLS 3.0. The unit of analysis is an individual who has/is working for an organization/company.

Operationalization of the Constructs

The study consisted of six primary constructs taken from previously validated research. Types of organizational culture consist of four constructs: bureaucratic, competitive, participative, and learning culture, identified by Fard et al. (2009). The labels adopted for the study correspond (respectively) to bureaucratic, competitive, community, and innovative those used by Ogbonna and Harris (2000), which came from Deshpandé, Farley, and Webster Jr. (1993). The first four items designated as bureaucratic culture in Table 1 (p. 775) of the study by Ogbonna and Harris (2000) are mapped to the bureaucratic culture of the types of organizational culture, as shown in Table 1. The four items starting at the fifth through eighth designated as competitive culture in Table 1 (p. 775) of the study by Ogbonna and Harris (2000) are mapped to the competitive culture of the types of organizational culture, as shown in Table 1. The four items from the ninth through twelfth designated as community culture in Table 1 (p. 775) of the study by Ogbonna and Harris (2000) are mapped to the participative culture of the types of organizational culture, as shown in Table 1. The four items from the thirteenth through sixteenth as innovative culture in Table 1 (p. 775) of the study by Ogbonna and Harris (2000) to learning culture of the types of organizational culture as shown in Table 1.

Table 1. Survey Items for Types of Organizational Cultures

Types of Organizational Culture	Indicators	Measures	Source
Bureaucratic	BUR 1	Formal rules and policies. Maintaining a smooth-running company is important here.[c]	Ogbonna & Harris, 2000
	BUR 2	The company is very formalized and structured. Established procedures generally govern what people do.[b]	Ogbonna & Harris, 2000
	BUR 3	Coordinators, organizers or administrators.[d]	Ogbonna & Harris, 2000
	BUR 4	Permanence and stability. Efficient, smooth operations are important.[a]	Ogbonna & Harris, 2000
Competitive	COM 1	An emphasis on tasks and goal accomplishment. A production orientation is shared.[c]	Ogbonna & Harris, 2000
	COM 2	Producers, technicians or hard-drivers.[d]	Ogbonna & Harris, 2000
	COM 3	Competitive actions and achievement. Measurable goals are important.[a]	Ogbonna & Harris, 2000
	COM 4	This company is production oriented. The major concern is with getting the job done. People aren't very personally involved.[b]	Ogbonna & Harris, 2000
Participative	PAR 1	Commitment to this firm runs high. Loyalty and tradition are important here.[c]	Ogbonna & Harris, 2000
	PAR 2	This company is personal. It's like an extended family.[b]	Ogbonna & Harris, 2000
	PAR 3	Human resources. High cohesion and morale in the firm are important.[a]	Ogbonna & Harris, 2000

Types of Organizational Culture	Indicators	Measures	Source
	PAR 4	Mentors, sages or father/mother figures.[d]	Ogbonna & Harris, 2000
Learning	LEA 1	Growth and acquiring new resources. Readiness to meet new challenges is important[a]	Ogbonna & Harris, 2000
	LEA 2	This company is dynamic and entrepreneurial. People are willing to take risks.[b]	Ogbonna & Harris, 2000
	LEA 3	A commitment to innovation and development. There is an emphasis on being first.[c]	Ogbonna & Harris, 2000
	LEA 4	Entrepreneurs, innovators or risk takers.[d]	Ogbonna & Harris, 2000

Notes

[a] Question wording was 'This company emphasizes:' measured on a 5-point Likert-type scale respectively anchored by (1) Strongly Agree and (7) Strongly Disagree.

[b] Question wording was 'To what extent does your company place a high priority on the following?' measured on a 5-point Likert-type scale respectively anchored by (1) Strongly Agree and (7) Strongly Disagree.

[c] Question wording was 'The glue which holds this company together is' measured on a 5-point Likert-type scale respectively anchored by (1) Strongly Agree and (7) Strongly Disagree.

[d] Question wording was 'In this company the best managers are considered to be:' measured on a 5-point Likert-type scale respectively anchored by (1) Strongly Agree and (7) Strongly Disagree.

Note. Adapted from "Leadership style, organizational culture, and performance: empirical evidence from UK companies," by E. Ogbonna, & L. C. Harris, 2000, *International Journal of Human Resource Management*, *11*(4), p. 766-788. Copyright 2000 by Taylor & Francis Ltd.

ISPC harnesses two sophisticated constructs to evaluate individual perceptions of ISP and SETA initiatives, adapted from Ifinedo (2014) and D'Arcy et al. (2009), respectively.

Table 2 provides an overview for each construct to capture a comprehensive picture regarding ISP and SETA effectiveness.

Table 2. Survey Items for Information Security Procedural Controls

Information Security Procedural Countermeasures	**Indicators**	**Measures**	**Source**
Information Security Policy	ISP 1	It is my intention to continue to comply with the organization's ISP	Ifinedo, 2014
	ISP 2	I am certain I will adhere to my organization's ISP	Ifinedo, 2014
	ISP 3	I am likely to follow the organization's ISP in the future	Ifinedo, 2014
	ISP 4	I would follow the organization's security policy whenever possible	Ifinedo, 2014
Security Education, Training, and Awareness Program	SETA 1	My organization provides training to help employees improve their awareness of computer and information security issues.	D'Arcy et al., 2009
	SETA 2	My organization provides employees with education on computer software copyright laws.	D'Arcy et al., 2009
	SETA 3	In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	D'Arcy et al., 2009
	SETA 4	My organization educates employees on their computer security responsibilities.	D'Arcy et al., 2009
	SETA 5	In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	D'Arcy et al., 2009

The ISPC measurement items on a seven-point Likert-type scale range from “strongly disagree” to “strongly agree,” in which participants indicate appropriate responses. Appendices list questionnaire items, descriptive statistics, construct definitions, and additional relevant information and metrics for the study.

The survey collected demographic information: gender contains four options: male, female, non-binary/third gender, and prefer not to say, age contains eight options: Under 18, 18 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64, 65 to 99, 100 or older, education level contains seven options: Less than high school, High school graduate, Some college, 2-year degrees, 4-year degree, Professional degree, Doctorate, type of industry contains three options: Primary industry (The primary industry examples include mining, fishing, mountain engineering industries. The economic activities in a primary industry revolve around the usage of the planet's natural resources like vegetation, water, minerals, earth, etc. The people engaged in working in the primary industry identified as red-collar workers.), Secondary industry (The significant examples of secondary industry are the plastic industry, the food industry, the home appliances industry, the textile and leather industry, the entertainment and gardening industry, the personal care and beauty products industry, storage, and cleaning industry. Economic activities revolve around adding value to natural resources by transforming the various raw materials into usable and valuable products. Workers in this industry are referred to as blue-collar workers.) and Tertiary industry (The tertiary industry examples include professional services like auditors, architects, lawyers, engineers, doctors, consulting, information technology/computer science, dentists, administrators, nurses, pharmacists, and surgeons. The significant economic activities include exchange and production. The

workers in this sector are referred to as white-collar professionals), and the company size (no. of employees) contains three options: Small Less than 100, Medium 101-500, and Large 501+. Appendices I, J, K, L, and M indicate the survey measures and the reporting view.

Participants

The target population for this study is adults 18 years and older in the United States who have formal ISP and SETA programs implemented within the organization and those who do not. Sample size considerations are the background of the model, data characteristics distribution, psychometric properties of the variables, and magnitude of their relationships (Wong, 2013). Hair et al. (2013) lists the following factors when determining structural equation model design:

1. The significance level
2. The statistical power
3. The minimum coefficient of determination (*R*2 values) used in the model
4. The maximum number of arrows pointing at a latent variable (Wong, 2013).

Typical marketing research uses a significance level of 5%, a statistical power of 80%, and R^2 values of at least 0.25 (Wong, 2013). This study's minimum sample size is 84, with a maximum of 8 arrows pointing at a latent variable in the model (Wong, 2013) (see Table 3).

Table 3. Suggested Sample Size in a Typical Marketing Research

The minimum sample size required	Maximum # of arrows pointing at a latent variable in the model
52	2
59	3
65	4
70	5
75	6
80	7
84	8
88	9
91	10

Note. Reprinted from "Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS," by K.K. K.Wong, 2013, *Marketing Bulletin*, *24*(1), 1-32. Copyright 2013 by The Marketing Bulletin.

Cappelleri, Darlington, and Trochim (1994) calculate sampling size in behavioral sciences using the most popular approach Cohen Statistical Power Analysis. According to Cohen (1988), performing a statistical power analysis is like Hair et al. (2013) first two factors of the significance of level and statistical power but differs in two distinct factors and has one additional factor. The five factors of Cohen (1988) for performing a statistical power analysis:

1. significance level or criterion
2. effect size
3. desired power
4. estimated variance
5. sample size

Cohen (1988) factors consider that each is related and interconnected and a function of the other factors. The other four factors are estimated by determining the sample size

and maximizing the sample while not exceeding resources to obtain the study's results. Most studies set the significance level at alpha = 0.5. Setting the alpha at .05 is most widely used to avoid Type I error in the probability of rejecting the null hypothesis. The second factor of effect size is the degree to which the null hypothesis is false (Cohen, 1988). Each statistical test has its effect size index continuously ranging from zero upwards (Cohen, 1992). Cohen's (1992) definition of effect size states that it is the ratio of the difference between the means of the treatment and control groups to the standard deviation of the scores on which the difference is based, and not a statistical test for the null hypothesis.

Significance of product-moment that tests a sample for significance in which the index r and H_0 posit that $r = 0$. The product-moment correlation coefficient, r, is .10 for small, .30 for medium, and .50 for large. Cohen (1992) suggested that a medium effect size does provide a more desirable result and be more observable to the researcher. The third factor is statistical power, the probability of testing the rejection of the null hypothesis for a specified value of the alternate hypothesis (Cohen, 1992). Statistical power is identified as $1-\beta$, where β is the probability of wrongly accepting the null hypothesis when it fails to reject the null hypothesis when it is false, resulting in Type II error. The value of the power can range from zero to one. Cohen (1992) suggests using the power of .80 ($\beta = .20$), which is the most used but notes it can be adjusted per type of test, sample size, and effect size of the sample. The fourth and final factor in determining the standard deviation for estimating the variance. Prior studies or pilot studies can be used to obtain this value, but it is not that variance is already implied in the sampling and, therefore, not a requirement. For a product-moment correlation using an effect size of $r =$

.30 (medium), a significant level alpha = .05, and statistical power of .08, the desired sample size is 84 for four independent variables, as shown in Table 2 of Cohen (1992). This size of 84 is the same sample size suggested by Wong (2013). High (2000) denotes sample size is critical in providing meaningful results. While both Cohen (1992) and Wong (2013) are similar in sample size 84, it is also noted other researchers like Hoyle (1995) suggest a good starting point for path modeling would be more advantageous in ranges of 100 – 200 participants for sample size. PLS is well known for smaller sample sizes; therefore, the proposed sample size is 100 participants.

The researcher purchased a survey panel from Centiment for participants in this study (https://quote.centiment.co/lander/default/lp1/). Centiment is an online survey platform providing survey respondents for market researchers and everyday business surveys. Centiment compensates participation in the survey with a reward upon completion of quality data provided for the study. Centiment does not compensate participants that do not complete the survey. Centiment provides a fraud score feature to ensure the accuracy of responses, and participants who fail the score cannot be part of the panel. All data collected from the participants was anonymous. Personally, identifiable information was not provided to the researcher.

Data Analysis

The Structural Equation Model (SEM) is a second-generation method used for multivariate data analysis (Fornell, 1985; Wong, 2013). Covariance-based SEM (CB-SEM) is the most widely used in research using software packages like AMOS, EQS, LISREL, and MPlus (Wong, 2013). Another emerging statistical modeling is Partial Least Squares (PLS). PLS is a technique that uses component-based software packages

PLS-Graph, VisualPLS, SmartPLS, and WarpPLS (Wong, 2013). The study used the PLS technique. While LISREL would be more applicable for theory confirmation, this study is still exploring a theory of the existence of the effect of types of organizations on ISPC (Fornell & Bookstein, 1982). Using a small sample size in validating predictive models is better suited to using PLS (Chin, 1998). This study used the tool SmartPLS 3.0 created by Ringle, Wende, and Will (2005). There are three reasons for using PLS for data analysis. First, as noted sample size can be smaller (Chin, 1998). Second, you do not need normalized data before use (D'Arcy et al., 2009), and third, PLS has reflective and formative scales (D'Arcy et al., 2009). Formative scales can represent more than one dimension of a construct, whereas reflective scales can only represent one single dimension (D'Arcy et al., 2009). D'Arcy et al. (2009) used the constructs for SETA, which are formative scales, but SETA can also fall under the reflective construct. PLS supports two assessment measurements: the measurement model and the structural model. PLS-SEM better understands inter-relationships by assessing the measurement model within the structural model's context. While smaller sample sizes often compromise the power of SEM models, Smart PLS and PLS-SEM offer viable solutions. Of these two platforms, many have found that when samples consist of 100 or fewer respondents, Smart PLS may be a more effective approach to structural equation modeling than conventional PLS-based techniques. Here are three reasons why Smart PLS is a better choice than PLS-SEM used in this study: 1. Computational efficiency: Smart PLS offers a major advantage in terms of computational efficiency over PLS-SEM, allowing users to save time and reduce the use of computing resources. This is especially beneficial when analyzing data from small sample sizes; Smart PLS can prevent issues

such as oversampling while simultaneously promoting model stability and accuracy within results. 2. User-friendly interface: Smart PLS is a powerful SEM tool that offers great usability, making it ideal for those with limited experience in the field. Its user-friendly interface makes working with smaller samples easy; users can quickly interpret results and identify any modeling issues. 3. Robustness: Smart PLS offers a clear advantage in analyzing complex models with non-normal data or small sample sizes, providing increased robustness compared to PLS-SEM. These capabilities make it an invaluable tool for dealing with difficult and unpredictable datasets. With Smart PLS and PLS-SEM both offering distinct advantages, the ultimate decision between them should be based on your research objectives, data characteristics, and model complexity. If a sample size of 100 is applicable to your situation though, you may find that its computationally efficient features combined with an intuitive interface make for a robust solution – giving Smart PLS greater appeal than its counterpart in such cases. Therefore, the sample size coupled with the three reasons stated previously the researcher chose to use Smart PLS for this study. By utilizing Smart PLS testing, our hypothesis was rigorously evaluated, and the data analyzed. After examining results, a thorough discussion ensued whereby meaningful representation of findings as presented in table format were explored to arrive at conclusions based on evidence provided by empirical examination.

Assessment of the Measurement Model

The model's psychometric properties used the following conventional tests: indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. The following table shows what to check for reporting PLS-SEM (see Table 4).

Table 4. Checking Reliability and Validity

What to check?	What to look for in SmartPLS?	Where is it in the report?	Is it OK?
Reliability			
Indicator Reliability	"Outer loadings" numbers	PLS->Calculation Results->Outer Loadings	Square each of the outer loadings to find the indicator reliability value. 0.70 or higher is preferred. If it is an exploratory research, 0.4 or higher is acceptable. (Hair, Ringle, & Sarstedt, 2011; Hulland, 1999)
Internal Consistency Reliability	"Reliability" numbers	PLS->Quality Criteria->Overview	Composite reliability should be **0.7 or higher**. If it is an exploratory research, 0.6 or higher is acceptable. (Bagozzi and Yi, 1988; Hair et al., 2011)
Validity			
Convergent validity	"AVE" numbers	PLS->Quality Criteria->Overview	It should be **0.5 or higher** (Bagozzi and Yi, 1988) It should be **0.7 or higher** (Fornell and Larcker 1981, Gefen and Straub 2005; Hair et al., 2011)
Discriminant validity	"AVE" numbers and Latent Variable Correlations	PLS->Quality Criteria->Overview (for the AVE number as shown above) PLS->Quality Criteria->Latent Variable Correlations	Fornell and Larcker (1981) suggest that the "**square root**" of AVE of each latent variable (Hair et al., 2011) should be greater than the correlations among the latent variables

Note. Reprinted from "Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS," by K.K. K.Wong, 2013, *Marketing Bulletin*, *24*(1), 1-32. Copyright 2013 by The Marketing Bulletin.

The researcher used a table of the results for the reflective outer models to show the results of the reliability and validity of the measurement model. The researcher checked

indicator reliability for values of 0.4 for minimum acceptance and the preferable level above 0.7. The researcher checked internal consistency reliability by composite reliability provided by the PLS output for all constructs to have values above 0.70, which is the recommended threshold (Baggozi & Yi, 1988; Fornell & Larcker, 1981). Convergent validity was checked by evaluating each latent variable's Average Variance Extracted (AVE), which Baggozi and Yi (1988) state as being above 0.5 and Fornell and Larcker (1981) state to be above 0.70 to confirm meeting the acceptable threshold for convergent validity. The researcher considered discriminant validity if the square root of AVE of each construct is larger than the inter-construct correlations, in which they should load more strongly on their corresponding construct than other constructs (Fornell & Larcker, 1981; Gefen & Straub, 2005).

Assessment of the Structural Model

The hypotheses were tested by examining the structural model. The test includes estimating the path coefficient to indicate the strength of relationships between independent and dependent variables and the R^2 value (the variance explained by the independent variables) (Chin, 1998). The *t*-statistics are significant if larger than 1.96 for a two-tailed *t*-test with a significance level of 5% for both the inner and outer models (Hair et al., 2011; Wong, 2013). The model's f^2 effect size shows how much exogenous latent variables contribute to endogenous latent variables' R^2 value (Hair et al., 2011; Wong, 2013). This measure helps to show the magnitude or strength of the relationship between latent variables (Hair et al., 2011; Wong, 2013). The researcher assessed the Stone-Geisser's (Q^2) values for the inner model to determine if all values are more significant than zero to contribute to the predictive power (Hair et al., 2011; Hair, Risher,

Sarstedt, & Ringle, 2019). The research concluded with conclusions, implications, recommendations, and a summary.

Format for Presentation of Results

The researcher presented data in figures and tables in the results section of the final dissertation report. The data in the tables and figures provided conclusions about the hypotheses presented in the dissertation report.

Resource Requirements

The following resources are required to complete the study.

Literature Research

Literature review retrieved from Internet catalog of Nova Southeastern University library.

Survey Instrument Approval

Submit approval Institutional Review Board (IRB) at Nova Southeastern University approval of the survey instrument as human participants used for the study.

Survey Instrument Administration

The survey developed was administered by a survey vendor, and I purchased responses for participants within the U.S. population 18 years and older who have worked.

Data Analysis Software

The researcher used SmartPLS3.0 software (www.smartpls.com/) to analyze data gathered from the survey.

Summary

This chapter discussed in detail the methodology used in the study. Data collection procedures cover the operationalization of the six primary constructs from previously validated research. Types of organizational culture consisted of four

constructs and two constructs for ISPC represented in tables—the overview section as discussed by the researcher of the participants in the study. The data analysis section briefly discussed how the researcher analyzed the data. The remaining two sections covered the format of results and the resource requirements used for the study.

Chapter 4

Results

Overview

The objectives of this quantitative study were to examine the extent to which types of organizational culture (bureaucratic, competitive, participative, and learning culture) affect ISPC. To obtain this objective, Smart PLS was employed to determine the relationship between organizational culture and ISPC.

This chapter is organized as follows: First, pre-analysis data screening is conducted, and descriptive statistics of the final data used for analysis are presented in written and table format. Second, the measurement model analysis of types of organizational culture and ISPC was conducted and presented. Finally, the proposed structural model, including organizational culture and ISPC, is analyzed, and the results are summarized.

Pre-Analysis Data Screening

The researcher collected data from participants by purchasing a survey panel from Centiment (https://quote.centiment.co/lander/default/lp1/). Centiment is an online survey platform providing survey respondents for market researchers and everyday business surveys. The total number of participants 228, as shown in Appendix B who opted to take the survey. Centiment compensated the participant as being part of their survey panel. The average time, as anticipated, was 5 minutes per participant. The soft launch to test the survey setup collected 17 responses when it was found the items to collect the industry were not working as anticipated. Since each section of the online survey required the participant to supply a response to go to the next question, there was no missing data. Participants in the survey responded attentively and accurately to a prompt halfway

through, indicating understanding of instructions after reading. The question required "none of the above" as an answer for verification that all were paying attention throughout. The survey instrument by Centiment could not list all the different industries in one question, so the researcher created several questions. However, as the participant skipped the question if the industry were not listed, they could not go back and mark a previous question. Therefore, the industry question was changed to three main groups: primary (red-collar), secondary (blue-collar), and tertiary (white-collar). The researcher removed the first 17 responses from the dataset. The researcher reviewed the next 100 of the 211 remaining participants for any missing data points. The researcher found no missing data points in the 100 participants' responses. The responses were placed into a CSV file to import into SmartPLS 3.0 by changing the data into numeric values instead of strings supplied by Centiment to be used by the SmartPLS software for analysis.

Descriptive Analysis

Each survey response included gender, age, education, industry, and size of company demographic data. Mostly females (58%) compared to males (40%) and (1%) to non-binary/third gender and prefer not to say participated in the study. They ranged from 18 to 99, with most participants aged 24-34 (40%) and 35-44 (36%). The education level stated for most participants was some college (27%) and bachelor's degree (26%). The industry type was 1/3 for each respective category: tertiary (white-collar professionals) was (35%), next was the primary (red-collar workers) was (29%), and the last was secondary (blue-collar workers) at (26%). The size of the company was Large 501+ (43%), next was Medium 101-500 (29%), and last was Small, less than 100 (28%) with only a 1% difference from the medium.

Table 5. Frequencies and Percentage of Demographic Data (N=100)

Item	*Frequency*	*Percentage*
Gender		
Female	37	58%
Male	43	40%
Non-binary/ third gender	1	1%
I prefer not to say	1	1%
Age Range		
18-24	4	4%
24-34	40	40%
35-44	36	36%
45-54	14	14%
55-64	5	5%
65-99	1	1%
Education Level		
Less Than High School	1	1%
High School	21	21%
Some College	27	27%
Associate degree	18	18%
Bachelor's degree	26	26%
Graduate Level +	5	5%
Doctorate	2	2%
Industry Type		
Primary	29	29%
Secondary	36	26%
Tertiary	35	35%
Item	*Frequency*	*Percentage*
Size of Company		
Small Less than a 100	28	28%
Medium 101-500	29	29%
Large 501+	43	43%

Measurement Model Analysis

This study measures organizational culture (OC) and ISPC as reflective constructs based on previous research (D'Arcy et al., 2009; Ogbonna & Harris, 2000). The effectiveness of an instrument is measured through the evaluation of validity and reliability. If these qualities are not present, it can be concluded that any structural relationships found in analysis would lack meaningfulness (Hair et al., 2011; Hair et al.,

2014; Lowry & Gaskin, 2014; Leedy & Ormrod, 2005). The reflective measurement model of bureaucratic (BUR), competitive (COM), participative (PAR), and learning culture (LEA) ISP, and SETA (see Figure 4) is evaluated using the following criterion that includes internal consistency, reliability, convergent validity, and discriminant validity (Hair et al., 2011; Hair et al., 2014; Wong, 2013).

The first criterion evaluated is internal consistency reliability. Reliability in research refers to the scale's ability to measure constructs consistently even with time decay and relates to reflective indicators (Hair et al., 2011; Hair et al., 2014; Lowry & Gaskin, 2014; Sekran, 2003; Wong, 2013). Traditionally, Cronbach alpha's measures internal consistency reliability, but the measurement tends to be conservative. Instead, it is more appropriate to apply composite reliability (Hair et al., 2011; Hair et al., 2014; and Wong, 2013). Composite reliability is interpreted similarly as Cronbach's alpha with values greater than .70 (Hair et al., 2011; Hair et al., 2014; Lowry & Gaskin, 2014; and Wong, 2013). All constructs demonstrated a level of composite reliability well above the recommended threshold of .70 (Hair et al., 2011; Hair et al., 2014; Lowry & Gaskin, 2014; and Wong, 2013), as shown in Table 6.

Outer loadings of the indicators and average variance extracted (AVE) establish convergent validity (Hair et al., 2011; Hair et al., 2014; Lowry & Gaskin, 2014; and Wong, 2013). Convergent validity is when highly correlated scores from two different instruments measure the same concept (Lowry & Gaskin, 2014; Sekaran, 2003; Wong, 2013). SmartPLS was employed to identify values above .708 to determine if the factor outer loadings were significant (Hair et al., 2014). All BUR, COM, PAR, LEA, ISP, and SETA constructs had loadings above .708, showing sufficient indicator reliability except

for COM_4 (0.581) and PAR_1 (0.647), which is below the acceptable value. The AVE value was above.50, so removing the COM_4 or PAR_1 would result in higher AVE, but as it is within the acceptable range for AVE, both items are retained. Finally, convergent validity on the construct level is determined by AVE. An AVE value of .50 or higher indicates that the construct explains more than half the variance of its indicators (Hair et al., 2011; Hair et al., 2014; Lowry & Gaskin, 2014; and Wong, 2013). All BUR, COM, PAR, LEA, ISP, and SETA constructs had AVE above .50, as shown in Table 6.

Discriminant validity implies that the constructs within the model are unique and uncorrelated to other constructs (Hair et al., 2011; Hair et al., 2014; Lowry & Gaskin, 2014; Sekaran, 2003; and Wong, 2013). Discriminant validity was established for all constructs (see Table 6 below). One method of determining discriminant validity was identifying the -cross-loadings. "Discriminant validity is adequate if the cross-loadings are more than the absolute value of .100 distant from the loading of the primary latent variable (Lowry & Gaskin, 2014, p. 2)." The second method uses the Fornell and Larcker (1981) criterion that suggests the square root of the AVE of each latent variable can be used to test for discriminant validity if the value is larger than other correlation values among the latent variables (Hair et al., 2011; Hair et al., 2014; and Wong, 2013). The SQRT of each construct AVE exceeded the highest correlation between the two constructs, thus confirming the discriminant validity.

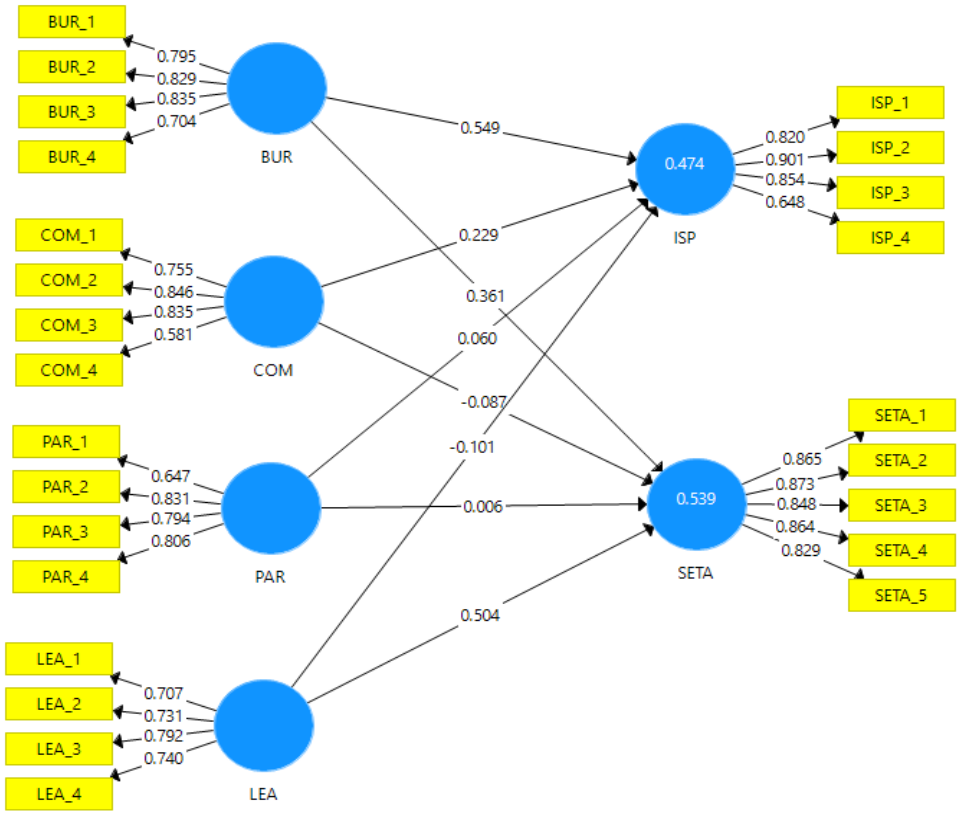


Figure 4: Measurement Model of BUR, COM, PAR, LEA, ISP, and SETA

Table 6. Reflective Measurement Model Results of Constructs

1st Order Variables	Indicators	Loadings	Indicator Reliability	Composite Reliability	Ave	Discriminant Validity
BUR	BUR _1	0.796	0.796	0.870	0.628	Yes
	BUR _2	0.829	0.829			
	BUR _3	0.835	0.835			
	BUR _4	0.704	0.704			
COM	COM_1	0.755	0.755	0.844	0.580	Yes
	COM_2	0.846	0.846			
	COM_3	0.835	0.835			
	COM_4	0.580	0.580			
LEA	LEA_1	0.707	0.707	0.831	0.552	Yes
	LEA_2	0.731	0.731			
	LEA_3	0.792	0.792			
	LEA_4	0.740	0.740			
PAR	PAR_1	0.648	0.648	0.855	0.597	Yes
	PAR_2	0.831	0.831			
	PAR_3	0.794	0.794			
	PAR_4	0.805	0.805			
ISP	ISP_1	0.807	0.807	0.885	0.660	Yes
	ISP_2	0.901	0.901			
	ISP_3	0.853	0.853			
	ISP_4	0.671	0.671			
SETA	SETA_1	0.863	0.863	0.932	0.733	Yes
	SETA_2	0.872	0.872			
	SETA_3	0.851	0.851			
	SETA_4	0.862	0.862			
	SETA_5	0.830	0.830			

Structural Model Analysis

The structural model analysis assesses the impact that BUR, COM, LEA, and PAR have on ISP and SETA using the eight-hypothesis testing of each type of OC on each of the respective ISPC (ISP and SETA) testing if the constructs have a significant effect of proving or disproving the hypothesis. This part of the analysis uses the reflective

measurement of ISP and SETA and the formative measure of BUR, COM, LEA, and PAR to confirm the nomological link between the constructs (Lowry & Gaskin, 2014).

The path coefficient for the relationship between BUR -> ISP was ($\beta = 0.555$, $t = 4.202$, $p < 0.001$) showed positive beta coefficient and significant. The path coefficient for the relationship between COM -> ISP was ($\beta = 0.225$, $t = 1.706$, $p = 0.088$) showed positive beta coefficient and not significant. The path coefficient for the relationship between PAR -> ISP was ($\beta = 0.050$, $t = 0.406$, $p = 0.685$) showed positive beta coefficient and not significant. The path coefficient for the relationship between LEA -> ISP ($\beta = -0.101$, $t = 0.699$, $p = 0.485$) showed negative beta coefficient and not significant. The path coefficient for the relationship between BUR -> SETA was ($\beta = 0.361$, $t = 2.990$, $p < 0.01$) showed positive beta coefficient and significant. The path coefficient for the relationship between COM -> SETA ($\beta = -0.090$, $t = 0.620$, $p = 0.535$) showed negative beta coefficient and not significant. The path coefficient for the relationship between PAR -> SETA was ($\beta = 0.006$, $t = 0.036$, $p = 0.971$) showed positive beta coefficient and not significant. The path coefficient for the relationship between LEA -> SETA was ($\beta = 0.506$, $t = 2.886$, $p < 0.01$) showed positive beta coefficient and significant. The confidence intervals at 25% and 97.5% confirmed the *t*-statistics and *p*-values of the path coefficient being statistically significant or not statistically significant (see Table 7, Table 8, and Figure 5).

Therefore, only LEA has influenced SETA but not ISP; all other hypotheses were not supported (see Table 7 and Figure 5).

Table 7. Path Coefficients, *t*-Statistic, *p*-Values, and Significance of BUR, COM, LEA, PAR, ISP, and SETA Constructs

Path	Path Coefficient(ρ)	*t*- Statistic	*p* Value	Significance Level
BUR -> ISP	0.555	4.202	0.000	***
BUR -> SETA	0.361	2.990	0.003	**
COM -> ISP	0.225	1.706	0.088	NS
COM -> SETA	-0.090	0.620	0.535	NS
LEA -> ISP	-0.101	0.699	0.485	NS
LEA -> SETA	0.506	2.886	0.004	**
PAR -> ISP	0.050	0.406	0.685	NS
PAR -> SETA	0.006	0.036	0.971	NS

***p* < .05, ***p* < .01, ****p* < .001,** t-statistic > 1.96 Note: NS – not significant

Table 8. Path Coefficients, *p*-Values, and Confidence Intervals of BUR, COM, LEA, PAR ISP, and SETA Constructs

Path	Path Coefficient(ρ)	*p* Value	Confidence Intervals (2.5%)	Confidence Intervals (97.5%)
BUR -> ISP	0.555	0.000	0.293	0.817
BUR -> SETA	0.361	0.003	0.133	0.603
COM -> ISP	0.225	0.088	-0.064	0.455
COM -> SETA	-0.090	0.535	-0.356	0.209
LEA -> ISP	-0.101	0.485	-0410	0.163
LEA -> SETA	0.506	0.004	0.149	0.835
PAR -> ISP	0.050	0.685	-0.184	0.293
PAR -> SETA	0.006	0.971	-0.369	0.281

***p* < .05, **p* < .01, ****p* < .001**

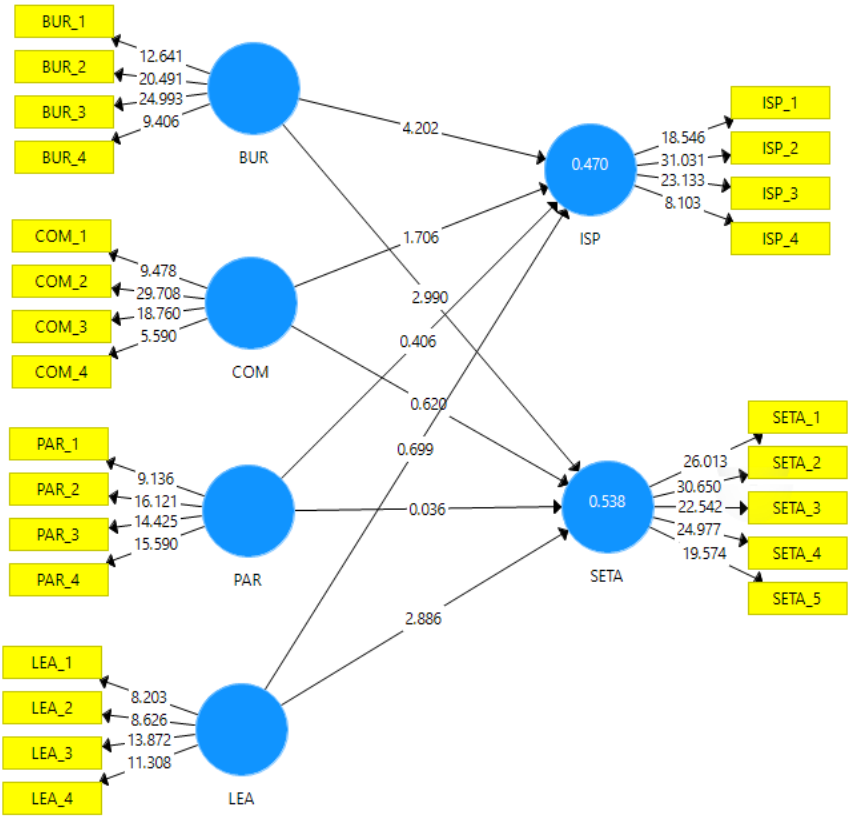


Figure 5: Structural Model of BUR, COM, PAR, LEA, ISP, and SETA

The R^2 coefficient of determination most commonly assesses the structural model's predictive accuracy. R^2 determines how much change the dependent variable is on the independent variable. Cohen (1988) suggested R^2 values for endogenous latent variables to be assessed as follows: 0.26 (substantial), 0.13 (moderate), and 0.02 (weak). Chin (1988) suggested a slightly higher of 0.67 (substantial), 0.33 (moderate), and 0.19 (weak). Later research with a focus on marketing from Hair et al. (2011) & Hair et al. (2013) suggested 0.75 (substantial), 0.50 (moderate), and 0.25 (weak). In this structural model, the ISP R^2 coefficient values for BUR → ISP, COM → ISP, PAR → ISP, LEA → ISP link is considered substantial at 0.470 (47% variance) as suggested by Cohen (1988), moderate link at 0.470 (47% variance) as suggested by Chin (1988) and weak link at

0.470 (47% variance) as suggested by Hair et al. (2011) & Hair et al. (2013). In this structural model, the SETA R^2 coefficient values for BUR → SETA, COM → SETA, PAR → SETA, LEA → SETA link is considered substantial at 0.538 (53.8% variance) as suggested by Cohen (1988), moderate link at 0.538 (53.8% variance) as suggested by Chin (1988) and moderate link at 0.538 (53.8% variance) as suggested by Hair et al. (2011) & Hair et al. (2013). The structural model's predictive relevance is most assessed by $Q^{2,}$ which measures whether a model has predictive relevance or not (>0 is good). In addition to establishing the predictive relevance of the endogenous constructs. When Q^2 values are above zero, the values are well reconstructed, and the model has predictive relevance. Q^2 in Smart-PLS is found running the Blindfolding procedure. The Q^2 predictive relevance for ISP was 0.286, a medium predictive relevancy for BUR, COM, PAR, and LEA effect on ISP. The Q^2 predictive relevance for SETA was 0.371, with medium predictive relevancy for BUR, COM, PAR, and LEA effects on SETA (see Table 9 below).

Table 9. Coefficient of Determination and Relevance of BUR, COM, LEA, PAR Constructs on ISP AND SETA Constructs

Endogenous Latent Variable	R^2	Q^2
ISP	0.470	0.286
SETA	0.538	0.371

The structural model's variable may be affected or influenced by several different variables in the model. Removal of an exogenous variable can affect the dependent

variable. The f^2 effect size is the change in R^2 when removing an exogenous variable from the model. Cohen (1988) states effect size (>=0.02 is small; >= 0.15 is medium; >= 0.35 is large (see Table 8 below). In this structural model, BUR has a medium effect on ISP, and BUR has a small effect on SETA; COM has a small effect on ISP, and COM has no effect on SETA; LEA has no effect on ISP, and LEA has a medium effect on SETA; PAR does not affect ISP and does not affect SETA as shown in Table 10.

Table 10. Effect Size f^2 of ISP and SETA

	ISP	SETA
	f^2	f^2
BUR	0.263	0.128
COM	0.040	0.007
LEA	0.005	0.155
PAR	0.002	0.000

*** f^2 >=0.02 small; ** f^2 >=0.15 medium; *** f^2 >=0.35 large**

Summary of Results

Hypothesis H_1, which states bureaucratic organizational culture will negatively influence ISP, was not substantiated as shown in Tables 7-10 because the result was significant positive relationship, so hypothesis H_1 is not supported. Hypothesis H_5, which states bureaucratic organizational culture will negatively influence SETA, was not substantiated as shown in Tables 7-10 because the result showed significant positive relationship, so Hypothesis H_5 is not supported. Hypothesis H_8 states that learning organizational culture will positively influence SETA, was substantiated as shown in Tables 7-10 because the result showed significant positive relationship, so hypothesis H_8

is supported. H_2, H_3, H_4, H_6 and H_7 were not supported. Table 11 below summarizes the findings.

The most restrictive organizational culture is bureaucratic, as shown in ISP and SETA. The nature of the organization of so many policies, rigid regulations & rules, and prominent level of centralism and affirmative leadership was shown that does have an impact of positive and not negative on ISPC that leads employees to more non-compliance (Fard et al., 2009; Hellriegel & Slocum, 1994; Karyda, Kiountouzis, & Kouklakis, 2005). The only culture shown to be supported was learning culture positively influencing SETA. Therefore, employees would want to ensure ISPC adds to the traits of knowledge expansion, trends to change, responsiveness to external changes, and encourage innovation. Surprisingly, those traits did not show hypothesis H_4 was supported (Fard et al., 2009; Hellriegel & Slocum, 1994). Results from five hypotheses (H_2, H_3, H_4, H_6 and H_7) indicated that organizational culture can have a salient impact on employee performance with either positive or negative influence. This was seen through employees' reactions to the opposing influences of ISP and SETA. In hypotheses, H_2 and H_6 competitive organizational culture was hypothesized to be a negative influence on ISP and also a negative influence on SETA based on the literature of the type of traits of high flexibility, low loyalty, low cultural identity, and low integration in this organizational culture, but the results showed positive influence so neither hypothesis was supported (Fard et al., 2009; Hellriegel & Slocum, 1994). In hypotheses, H_3 and H_7, participative organizational culture were hypothesized to influence ISP and SETA, respectively, positively. The traits of the participative culture of low flexibility, high integration, loyalty, personal commitment, teamwork, prominent level of social acceptance, and

tendency to stability (Fard et al., 2009; Hellriegel & Slocum, 1994) would seem to lend themselves to have employees to be more in compliance to help this organizational culture, but the results showed otherwise.

Table 11. Summary of Findings for Research Hypotheses

Hypothesis	Hypothesis Description	Results
Hypothesis H_1	Bureaucratic organizational culture will have a negative influence on ISP.	Not Supported
Hypothesis H_2	Competitive organizational culture will have a negative influence on ISP.	Not Supported
Hypothesis H_3	Participative organizational culture will have a positive influence on ISP.	Not Supported
Hypothesis H_4	Learning organizational culture will have a positive influence on ISP.	Not Supported
Hypothesis H_5	Bureaucratic organizational culture will have a negative influence on SETA.	Not Supported
Hypothesis H_6	Competitive organizational culture will have a negative influence on SETA.	Not Supported
Hypothesis H_7	Participative organizational culture will have a positive influence on SETA.	Not Supported
Hypothesis H_8	Learning organizational culture will have a positive influence on SETA.	Supported

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

The chapter offers an in-depth examination of research questions through the application of quantitative methods. To begin, conclusions are presented which lead into discussion regarding primary objectives and questions to be addressed by this study. An overview is then provided on relevant literature and details on techniques used to measure and structure data while validating hypotheses, such as Smart PLS software analysis. Moreover, limitations and implications for current academic knowledge are discussed followed by proposal recommendations for future studies – culminating with a comprehensive summary outlining results from this work.

Conclusions

This study aimed to examine the effect of types of organizational culture (bureaucratic, competitive, participative, and learning culture) on ISPC. The research's main goal is to show that distinct types of organizational culture have a positive or negative effect on ISP and SETA based on the organizational culture.

These two research questions guided the study:

1. Do distinct types of organizational culture affect Information Security Policy?
2. Do distinct types of organizational culture affect the SETA program (or adherence to the SETA program)?

Both research questions were answered based on the findings showing that distinct types of organizational culture affect compliance and adherence to ISP and SETA.

Research based on existing literature supports that different organizational culture types can have a range of impacts - from positive to negative – when it comes to ISP and SETA. Hypotheses were created in order to determine the degree of such influence. H^1 and H_5 for bureaucratic organizational influence on ISP and SETA were not supported in this study and backed by previous research by Karyda, Kiountouzis, and Kouklakis, 2005. The study showed bureaucratic organizational culture had a negative effect on adherence. H_8 for learning organizational culture influence on SETA was supported and backed by previous Bates and Khasawneh 2005 in which learning was valued in this organizational culture. H_2, H_3, H_4, H_6 and H_7 were not supported.

A comprehensive review of existing literature highlighted the strong connection between an organization's success and its own culture. This collective atmosphere, comprised of shared norms, values, and beliefs among all members within the company, is a key factor in achieving results. Organizational culture studies have shown an impact on behavior and compliance with ISP (Chun, Park, & Lee, 2019; Chen, & Yang, 2021; Hwang et al., 2020; Marinagi, Kitsios, Papanikolaou, & Katsikas, 2021; Martins & Martins, 2016; Kaba, & Lyra, 2021; Liu et al., 2020; Zhang et al., 2021; Von Solms, R., & Von Solms, B., 2004). Han et al. 2017, showed psychological contract fulfillment effectively mitigated negative ISP. In turn, that psychological contract can be tied back to the organizational culture type conducive to compliance through the norms and beliefs of loyalty to the organization. Dhillon and Torkzadeh (2006) pointed out that organizational loyalty, pride in the organization, and treating others as they would like to be treated reaffirm if employees do not have these traits in the organization, the likelihood of compliance and adherence to ISP and SETA is affected. This study's results indicated

that one of the eight proposed hypotheses were supported, while the remainder showed insufficient evidence.

A quantitative study was used to answer research questions, and the model proposed was developed from a literature review from prior research. The types of organizational culture were taken from research by Fard, Rostamy, and Taghiloo (2009), who examined the relationships between organizational types and shaping learning organizations. The organizational culture type items measurements for this study were taken from previous research by Ogbonna and Harris 2000. ISPC harnesses two sophisticated constructs to evaluate individual perceptions of ISP and SETA initiatives, adapted from Ifinedo (2014) and D'Arcy et al. (2009), respectively. Table 2 provides an overview for each construct to capture a comprehensive picture regarding ISP and SETA effectiveness.

Smart PLS was used to assess the measurement and structural models and validate the hypothesis. The hypothesis of the negative relationship between BUR and ISP was not supported because the results indicated a significant positive relationship. The hypothesis of the negative relationship between BUR and SETA was not supported because the results indicated a significant positive relationship. The hypothesis of the positive relationship between LEA and SETA was supported because the results indicated a significant positive relationship. The hypotheses for competitive and participative organizational culture did not have a significant effect on ISP or SETA. Furthermore, learning organizational culture was found to have no significant effect on ISP. The ISP construct value of 0.470 demonstrated moderate predictive accuracy, and the Q^2 predictive relevance of 0.286 was acceptable at medium. The SETA construct value of 0.538 demonstrated moderate predictive accuracy, and the Q^2 predictive relevance of

0.371 was acceptable at medium. The summary of the hypothesis testing results is presented in Table 11.

Limitations

The study used a third party to collect the data for the measurement items, so participants only received a screener at the beginning of the study to which they could opt out or proceed. The study was conducted online for the participant to mark each question until completion. The researcher mailed out no physical study. Selection bias can impact the accuracy of research findings, as samples that are not representative may lead to conclusions which do not accurately reflect reality. To ensure objectivity in results, it is essential to carefully consider recruitment methods and examine sample composition for any potential issues such as self-selecting participants or an unbalanced population representation. The criteria were US 18-year-old that had worked; therefore, a participant may not work for an organization that had ISP and SETA in one of their organizations. With any research sample, it is important to consider its representativeness of the population being studied. If a certain group is underrepresented in relation to their actual rate within society and industry, results may not apply beyond that limited scope – raising questions about implications for other workplaces or sectors with distinct levels of usage when it comes to ISP and SETA programs. Limited statistical power can be a hindrance to accurately determining the differences between two or more groups. In this case, however, Smart PLS proved effective despite limited resources; surprisingly suitable for such an ambitious endeavor with just 100 participants in the sample population (Hair et al., 2014). ISP and SETA programs' efficacy remains unknown without the use of a control group, rendering any possible casual inferences imprecise at best. The lack of

control in this study serves as an impediment to developing insight into such causality. The study's results may have limited applicability outside the tested sample, as it is not guaranteed to be a representative example of all relevant populations.

Implications

This study has the following implications for the existing body of knowledge in the Information Security field. This study revealed that certain socio-organizational factors have a direct impact on compliance and adherence to ISPs and SETA. One of the eight hypotheses demonstrated this correlation, suggesting organizations with fewer rules often hold themselves more accountable for adhering to standards. The research also provided evidence that strict regulations may not be effective in incentivizing individuals within an organization; such findings could prove useful when designing appropriate policies or training materials. Contrary to expectation, those companies with stricter rules had less compliance in comparison; this insight has opened opportunities for crafting improved policies or training programs untainted by such negative influences. While prior studies on organizational culture have not tested their effects upon ISPs/SETAs specifically, this research explored individual (or group) traits potentially impacting said conformity.

Recommendations for Future Research

Further study may be conducted to explore the influence of organizational cultures on effective ISP and SETA initiatives (Chen, & Yang, 2021; Chun et al., 2019; Hwang et al., 2020; Marinagi et al., 2021; Martins & Martins, 2016; Kaba, & Lyra, 2021; Liu et al., 2020; Zhang et al., 2021). A combination of technical and non-technical measures, including insider threat detection and adaptive security architecture, could help organizations optimize their programmatic approaches for safeguarding digital assets in a

constantly evolving risk landscape (Alabdulatif et al., 2020; Gao et al., 2019; Vintila & Iancu, 2021). By taking into account the factors influencing employees' compliance with information security policies, such as security culture and awareness, organizations can better prevent insider threats and improve their overall security posture (D'Arcy & Greene, 2014; D'Arcy & Hovav, 2009). A thorough analysis of the intricate correlations between organizational culture, data security regulations and information education programs is essential in developing effective strategies for digital asset protection facing an unpredictable risk environment. Research indicates that variables such as cognitive/emotional reactions, self-determination, trust building and knowledge sharing confidence can all be influenced by corporate climate; additionally studies have unveiled a link between staff compliance with info security policies (Chen & Yang 2021; Hu & Dinev 2020; Kaba & Lyra 2021; Liu et al., 2020), thus confirming the importance of understanding these elements to optimize results. Research has shown the importance of understanding employee perspectives, executive leadership practices, and corporate structure in relation to information security policies (ISP) and security education, training, and awareness (SETA) programs (Wu et al., 2019; Liang et al., 2018). However, further exploration of organizational culture is necessary to deepen our understanding about the connection between corporate cultures, ISP, and SETA. By studying different varieties such as clan, adhocracy, or hybrid structures in greater depth, researchers can gain a more holistic view on how education programs impact organizations’ safety protocols (Wu et al., 2019; Liang et al., 2018; McLaughlin et al., 2017). Several studies have investigated the impact of organizational culture on employees' compliance with information security policies, including Albrechtsen and Hovden (2019), Bhattacharya

and Zhang (2020), D'Arcy and Greene (2014), D'Arcy and Hovav (2009), and Liu et al. (2020). Meanwhile, Choi et al. (2021), Hu and Dinev (2020), Kankanhalli et al. (2020), and Shu et al. (2021) have explored various factors influencing employees' ISP compliance behavior. Asghar et al. (2021), Vintila and Iancu (2021), and Alabdulatif et al. (2020) have also studied approaches for preventing insider threats in information systems, which can be linked to ISP compliance. Maroofi et al. (2019) found that organizational culture significantly affects ISP compliance, but Singh and Mitchell (2017) argue that effective information security awareness training programs can counteract negative influences of organizational culture. Odeyemi and Yusuf (2017) suggest that organizations could create effective policies and training programs to ensure compliance with regulations without compromising performance. Further research should explore the impacts of various policy types and program designs on staff compliance with information security initiatives and educational efforts, taking into account the insights provided by the aforementioned studies. This cross-sectional study suggests that organizational culture may play a role in the success of ISPs and SETAs, as evidenced by several research efforts which have sought to examine this relationship. Albrechtsen and Hovden (2019), Bhattacharya & Zhang (2020); D'Arcy & Greene (2014) et al., all point to varying impacts on employee compliance with information security policies caused by underlying cultural shifts within organizations. Numerous studies have recently investigated the factors driving employee behavior in terms of complying with information security policies (Choi et al., 2021; Hu & Dinev, 2020; Kankanhalli et al., 2020; Shu et al., 2021). In addition, approaches for preventing insider threats and their potential association to compliance requirements have been examined by Asghar at el.

(2021), Vintila and Iancu (2021) as well as Alabdulatif et al. (2020). To better comprehend how these variables evolve together over time and evaluate such changes' effects on employees' conduct future research should adopt a longitudinal methodical approach. Further investigation of the influence distinct types of organizational culture can have on ISP and SETA is required to gain a more comprehensive insight into this domain.

Summary

Prior research continues to focus on the individual applying behavior or cognitive theories to address the issue of non-compliance or adherence, with little research emphasizing the environment the individuals are in each day. Based on previous research calling for more behavioral information security and socio-organizational studies, this study combined both aspects to derive a new study that would answer both calls to add more to this discipline.

This dissertation studied the effect of types of organizational culture on information security procedural countermeasures and why more research was needed to understand the socio-organizational of employee behaviors regarding compliance and adherence to ISP and SETA within the organizational culture.

The primary goal of the research was to understand the types of organizational culture (bureaucratic, competitive, participative, and learning culture) that affect ISPC. The four types of organizational culture were drawn from Hellriegel and Slocum (1994), and ISP and SETA were drawn from previous research-validated instruments. The objective of this study is to answer the following research questions:

1. Do distinct types of organizational culture affect Information Security Policy?

2. Do distinct types of organizational culture affect the SETA program (or adherence to the SETA program)?

A literature review was used to determine if the organizational culture type would have a negative or positive influence. It was hypothesized that two organizational cultures would positively influence both ISP and SETA and the other two would have a negative influence based on the traits established in the literature. With an understanding from the literature of the organizational culture type coupled with the research of the ISP and SETA (see Figure 2) and a literature review, the following hypotheses were developed:

H_1. Bureaucratic organizational culture will have a negative influence on ISP.

H_2. Competitive organizational culture will have a negative influence on ISP.

H_3. Participative organizational culture will have a positive influence on ISP.

H_4. Learning organizational culture will have a positive influence on ISP.

H_5. Bureaucratic organizational culture will have a negative influence on SETA.

H_6. Competitive organizational culture will have a negative influence on SETA.

H_7. Participative organizational culture will have a positive influence on SETA.

H_8. Learning organizational culture will have a positive influence on SETA.

The structural model was developed to analyze the relationship between organizational culture types and ISP and SETA. A survey instrument was created from the measures and submitted to Centiment, which used its survey panel to collect 228 responses, and of those, the first 100 responses were used to assess the data. Smart PLS was used to assess the measurement model for internal consistency, reliability, convergent validity, and discriminant validity (Hair et al., 2011; Hair et al.,

2014; Wong, 2013). The researcher assessed the structural model's predictive accuracy *R*2 and predictive relevancy *Q*2.

The findings show that bureaucratic organizational culture does not have a negative influence on ISP and SETA instead it is positive influence. In addition, learning organizational culture does have a positive influence on SETA but not on ISP. The result of the bureaucratic organizational culture was not in line with previous research that also showed bureaucratic organizational culture affecting ISP. The results showed there is a relationship between the effect of organizational culture types on ISP and SETA, but as noted, only one of the eight proposed hypotheses showed support and were statistically significant.

Some limitations in this study that may have impacted the results of having only one hypothesis showing supported in that the participants were selected from a general US populace; therefore, assumptions were made that the participant's workplace had some security policies and training programs when answering the measures for each of ISP and SETA measures. The measures used for each item came from validated research, and the measures did show they measured what they were measuring per the assessment of the measurement model. However, there still could be a misunderstanding of the items by the participants for each statement provided for each measure. Using Smart PLS can provide the same depth of insights as a larger dataset, by allowing multiple interactions to be bootstrapped and analyzed. This makes it an effective alternative for data analysis without requiring the availability or processing power associated with increased sample sizes. Still, it would be amiss not to point out that a more extensive data set could provide additional insight to analyze

and validate if the study would prove more hypothesis-supported or remain with just one of the eight.

The study added to the existing knowledge body in Information Security with additional implications and contributions to the field. One implication is that the researcher made the call by other researchers and studies to include another aspect of the Information Security field by adding socio-organization to the study to add more knowledge beyond individual behavioral theories. Prior studies missing the socio-organization aspect are another factor of why non-compliance and policy adherence could be tied more directly to the organizational culture—trying to justify a "lone wolf" individual employees' behavior not following information security policies, and training is limiting the research in IS field. Research indicates that organizational culture has the potential to impede ISP compliance. However, effective awareness-raising initiatives can help offset this effect and foster adherence among staff members (Maroofi et al., 2019; Singh & Mitchell, 2017). Odeyemi and Yusuf's (2017) research suggests policies and training programs of varied designs could ensure regulatory compliance without sacrificing performance outcomes. Moving forward, further studies should evaluate the impact different types of protocols have on workers' behavior related to cybersecurity practices as well as educational endeavors regarding these topics. Further research could separate into one individual type of organizational culture, like bureaucratic, to determine why the positive influence exists for ISP and SETA. Additional research could take the opposite stance for the hypothesis that was not supported to validate if the opposite holds in having some influence on ISP and SETA.

Appendix A

IRB Approval Letter from Nova Southeastern University

NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: Sheri R James, Master of Science
College of Engineering and Computing

From: Ling Wang, Ph.D.
College Representative, College of Engineering and Computing

Date: December 15, 2021

Subject: IRB Exempt Initial Approval Memo

TITLE: A Study of the Effect of Types of Organizational Culture on Information Security Procedural Countermeasures– NSU IRB Protocol Number 2021-532

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **December 15, 2021**. You may proceed with your study.

Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Annual Status of Research Update: You are required to notify the IRB Office annually if your research study is still ongoing via the *Exempt Research Status Update xForm.*

Final Report: You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm.*

Translated Documents: No

Please retain this document in your IRB correspondence file.

CC: Ling Wang, Ph.D.

Souren Paul

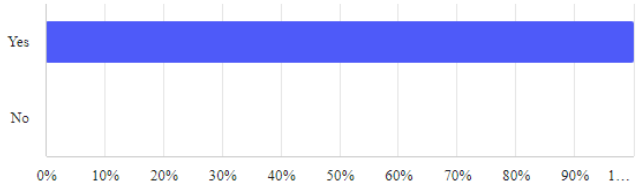
3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-5369 • 866-499-0790 • Fax: (954) 262-3977 • Email: *irb@nova.edu* • Web site: *www.nova.edu/irb*

Appendix B

Notice to participants purpose of study accept to participate

1 228 of 228 answered

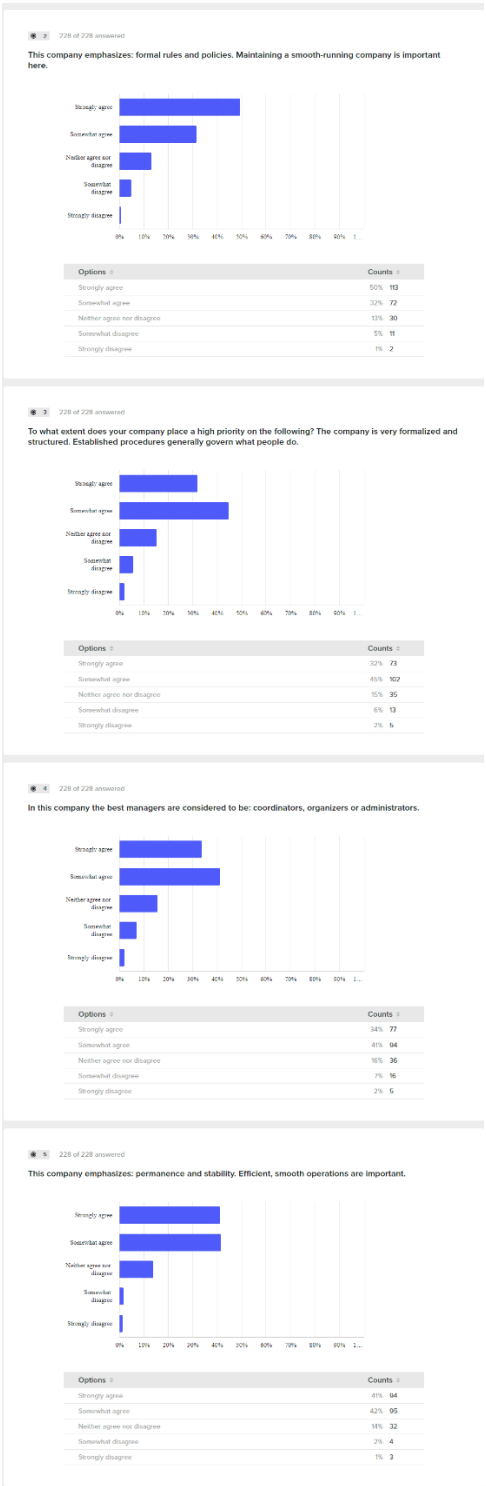
The purpose of this study is to find out if there is a relationship between types of organizational culture and information security procedural countermeasures. You will be taking a one-time, anonymous survey. The survey will take approximately 5-6 minutes to complete. You will be answering questions about your company's organizational culture and information security procedural countermeasures (security policies). You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time. If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll-free at 1-866-499-0790 or email at IRB@nova.edu. Do you agree to participate?



Options	Counts
Yes	100% 228
No	0% 0

Appendix C

Organizational Culture Survey (Bureaucratic)



7 228 of 228 answered

This company emphasizes: formal rules and policies. Maintaining a smooth-running company is important here.

Options	Counts
Strongly agree	50% 113
Somewhat agree	32% 72
Neither agree nor disagree	13% 30
Somewhat disagree	5% 11
Strongly disagree	1% 2

3 228 of 228 answered

To what extent does your company place a high priority on the following? The company is very formalized and structured. Established procedures generally govern what people do.

Options	Counts
Strongly agree	32% 73
Somewhat agree	45% 102
Neither agree nor disagree	15% 35
Somewhat disagree	6% 13
Strongly disagree	2% 5

4 228 of 228 answered

In this company the best managers are considered to be: coordinators, organizers or administrators.

Options	Counts
Strongly agree	34% 77
Somewhat agree	41% 94
Neither agree nor disagree	16% 36
Somewhat disagree	7% 16
Strongly disagree	2% 5

5 228 of 228 answered

This company emphasizes: permanence and stability. Efficient, smooth operations are important.

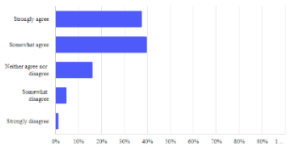
Options	Counts
Strongly agree	41% 94
Somewhat agree	42% 95
Neither agree nor disagree	14% 32
Somewhat disagree	2% 4
Strongly disagree	1% 3

Appendix D

Organizational Culture Survey (Competitive)

6 228 of 228 answered

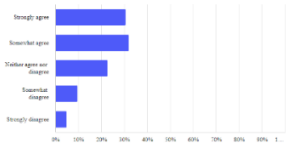
The glue which holds this company together is an emphasis on tasks and goal accomplishment. A production orientation is shared.



Options	Counts
Strongly agree	38% 86
Somewhat agree	40% 91
Neither agree nor disagree	16% 37
Somewhat disagree	5% 11
Strongly disagree	1% 3

7 228 of 228 answered

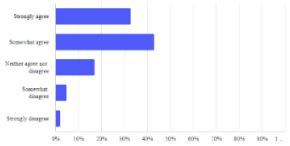
In this company the best managers are considered to be: producers, technicians or hard-drivers.



Options	Counts
Strongly agree	31% 70
Somewhat agree	32% 73
Neither agree nor disagree	23% 52
Somewhat disagree	10% 22
Strongly disagree	5% 11

8 228 of 228 answered

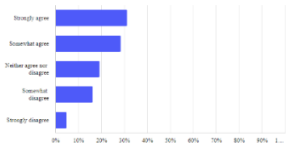
This company emphasizes: competitive actions and achievement. Measurable goals are important.



Options	Counts
Strongly agree	33% 75
Somewhat agree	43% 98
Neither agree nor disagree	17% 39
Somewhat disagree	5% 11
Strongly disagree	2% 5

9 228 of 228 answered

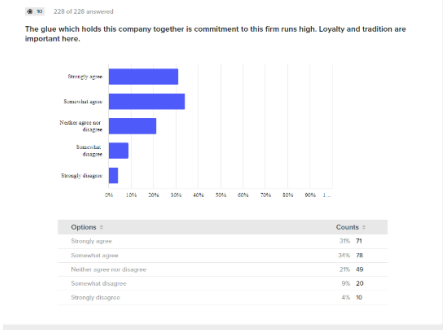
To what extent does your company place a high priority on the following? This company emphasizes: This company is production oriented. The major concern is with getting the job done. People aren't very personally involved.

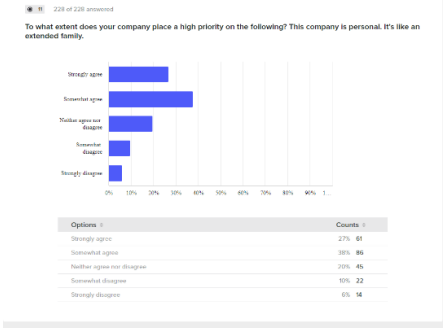


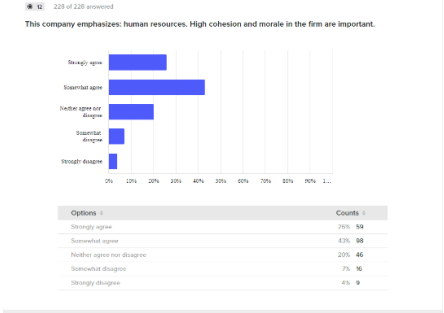
Options	Counts
Strongly agree	31% 71
Somewhat agree	29% 65
Neither agree nor disagree	19% 44
Somewhat disagree	16% 37
Strongly disagree	5% 11

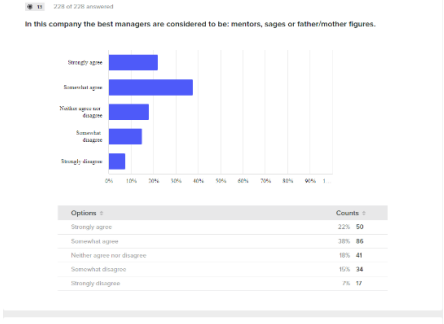
Appendix E

Organizational Culture Survey (Participative)







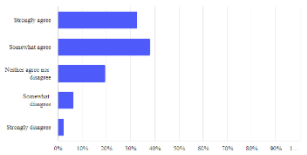


Appendix F

Organizational Culture Survey (Learning)

14 228 of 228 answered

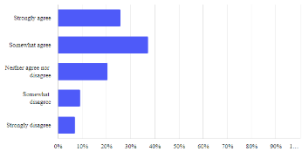
This company emphasizes: growth and acquiring new resources. Readiness to meet new challenges is important.



Options	Counts
Strongly agree	33% 75
Somewhat agree	38% 87
Neither agree nor disagree	20% 45
Somewhat disagree	7% 15
Strongly disagree	3% 6

15 228 of 228 answered

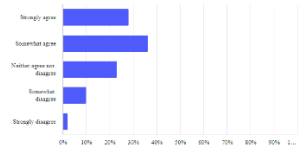
To what extent does your company place a high priority on the following? This company is dynamic and entrepreneurial. People are willing to take risks.



Options	Counts
Strongly agree	26% 59
Somewhat agree	37% 85
Neither agree nor disagree	21% 47
Somewhat disagree	9% 21
Strongly disagree	7% 16

17 228 of 228 answered

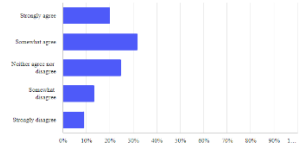
The glue which holds this company together is a commitment to innovation and development. There is an emphasis on being first.



Options	Counts
Strongly agree	28% 64
Somewhat agree	36% 83
Neither agree nor disagree	23% 53
Somewhat disagree	10% 23
Strongly disagree	2% 5

18 228 of 228 answered

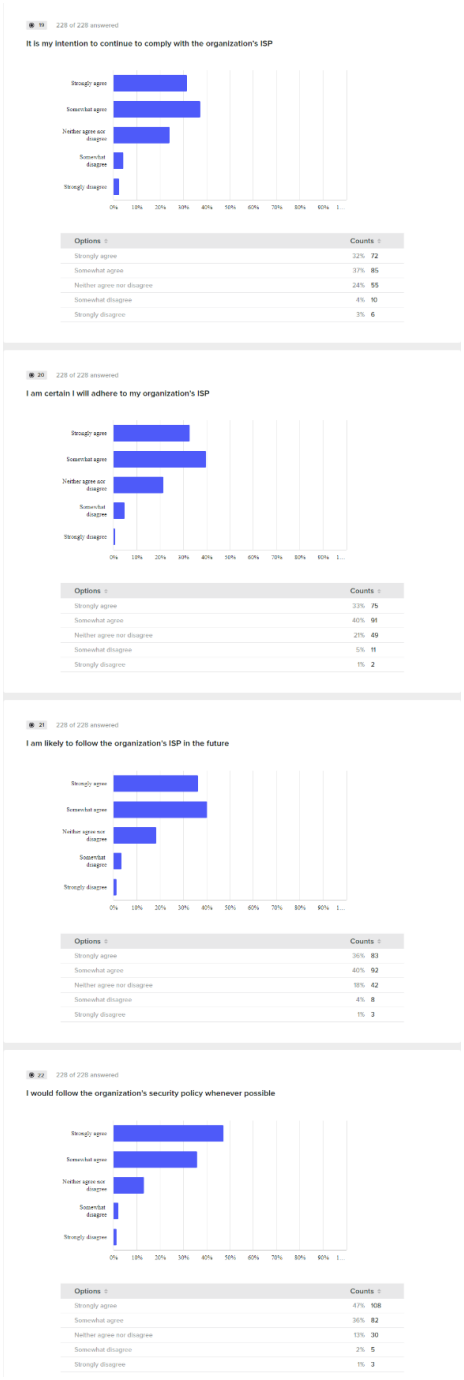
In this company the best managers are considered to be: entrepreneurs, innovators or risk takers.



Options	Counts
Strongly agree	20% 46
Somewhat agree	32% 73
Neither agree nor disagree	25% 57
Somewhat disagree	14% 31
Strongly disagree	9% 21

Appendix G

Information Security Procedural Countermeasures Survey (Information Security Policy)



Appendix H

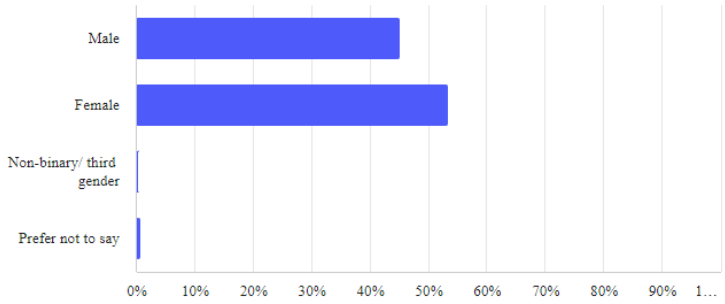
Information Security Procedural Countermeasures Survey (Information Security Policy)

Appendix I

Demographics Survey (Gender)

28 228 of 228 answered

What is your gender?



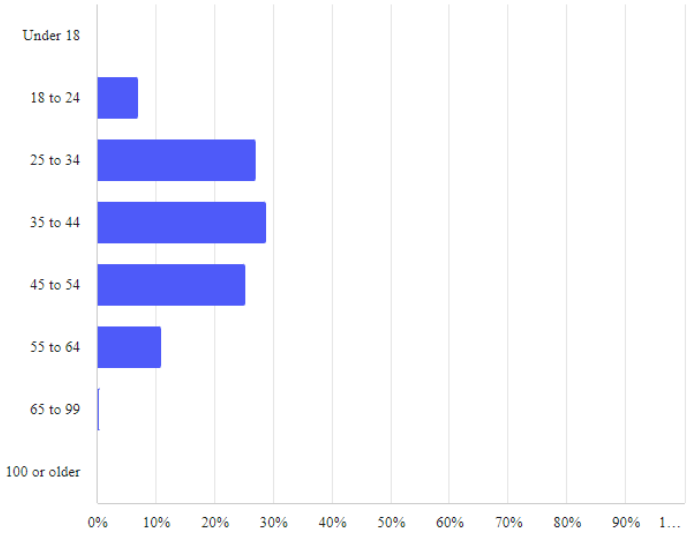
Options	Counts
Male	45% 103
Female	54% 122
Non-binary/ third gender	0% 1
Prefer not to say	1% 2

Appendix J

Demographics Survey (Age)

29 228 of 228 answered

What is your age?



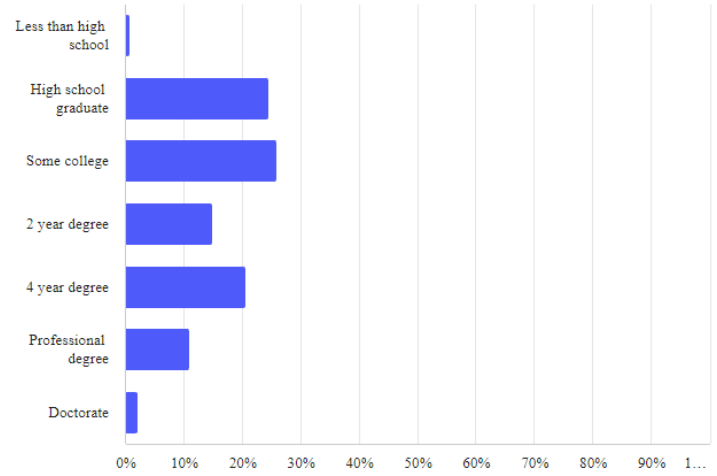
Options	Counts
Under 18	0% 0
18 to 24	7% 16
25 to 34	27% 62
35 to 44	29% 66
45 to 54	25% 58
55 to 64	11% 25
65 to 99	0% 1
100 or older	0% 0

Appendix K

Demographics Survey (Education)

30 228 of 228 answered

What is your education?



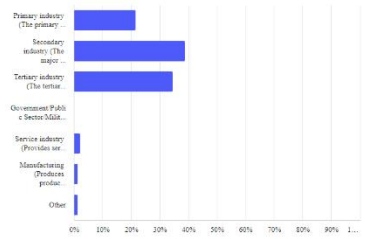
Options	Counts
Less than high school	1% 2
High school graduate	25% 56
Some college	26% 59
2 year degree	15% 34
4 year degree	21% 47
Professional degree	11% 25
Doctorate	2% 5

Appendix L

Demographics Survey (Industry)

32 226 of 228 answered

What is the type of industry you are employed?



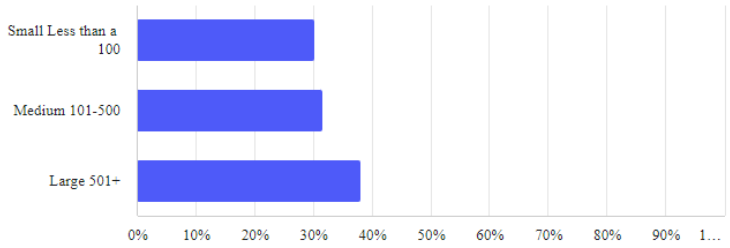
Options	Counts
Primary industry (The primary industry examples include mining, fishing, mountain engineering industries. The economic activities in a primary industry revolve around the usage of the natural resources of the planet like vegetation, water, minerals, earth, etc. The people engaged in working in the primary industry are generally referred to as red-collar workers.)	22% 49
Secondary industry (The major examples of secondary industry are the plastic industry, the food industry, home appliances industry, the textile and leather industry, entertainment and gardening industry, personal care and beauty products industry, storage and cleaning industry. The economic activities revolve around adding value to the natural resources by transforming the various raw materials into usable and valuable products. The workers belonging to this industry are generally referred to as blue-collar workers.)	39% 88
Tertiary industry (The tertiary industry examples include professional services like auditors, architects, lawyers, engineers, doctors, consulting, information technology/computer science, dentists, administrators, nurses, pharmacists and surgeon. The major economic activities include exchange and production. The workers belonging to this sector are generally referred to as white-collar professionals.)	35% 78
Government/Public Sector/Military	0% 0
Service industry (Provides service to customers)	2% 5
Manufacturing (Produces products)	1% 3
Other	1% 3

Appendix M

Demographics Survey (Size of Company)

31 228 of 228 answered

What is size (no. of employees) of your company?



Options	Counts
Small Less than a 100	30% 69
Medium 101-500	32% 72
Large 501+	38% 87

Appendix N

Overview, Loadings, and Weights of BUR, COM, PAR, LEA, ISP, and SETA

Overview

	Cronbach's Alpha	Rho_A	Composite Reliability	AVE	R Square
BUR	0.801	0.812	0.870	0.628	
COM	0.755	0.803	0.844	0.580	
PAR	0.771	0.770	0.855	0.597	
LEA	0.729	0.730	0.831	0.552	
ISP	0.827	0.853	0.885	0.660	0.470
SETA	0.909	0.910	0.932	0.733	0.538

Outer Loadings

	BUR	COM	ISP	LEA	PAR	SETA
BUR_1	0.796					
BUR_2	0.829					
BUR_3	0.835					
BUR_4	0.704					
COM_1		0.755				
COM_2		0.846				
COM_3		0.835				
COM_4		0.580				
ISP_1			0.807			
ISP_2			0.901			
ISP_3			0.853			
ISP_4			0.671			
LEA_1				0.707		
LEA_2				0.731		
LEA_3				0.792		
LEA_4				0.740		
PAR_1					0.648	
PAR_2					0.831	
PAR_3					0.794	
PAR_4					0.805	
SETA_1						0.863
SETA_2						0.872
SETA_3						0.851
SETA_4						0.862
SETA_5						0.830

Outer Weights

	BUR	COM	ISP	LEA	PAR	SETA
BUR_1	0.301					
BUR_2	0.349					
BUR_3	0.338					
BUR_4	0.268					
COM_1		0.312				
COM_2		0.419				
COM_3		0.348				
COM_4		0.205				
ISP_1			0.330			
ISP_2			0.334			
ISP_3			0.343			
ISP_4			0.209			
LEA_1				0.344		
LEA_2				0.310		
LEA_3				0.352		
LEA_4				0.339		
PAR_1					0.341	
PAR_2					0.344	
PAR_3					0.319	
PAR_4					0.299	
SETA_1						0.229
SETA_2						0.252
SETA_3						0.218
SETA_4						0.235
SETA_5						0.234

Appendix O

Fornell-Larcker Discriminant Validity for BUR, COM, PAR, LEA, ISP, and SETA

	BUR	COM	ISP	LEA	PAR	SETA
BUR	***0.792***					
COM	0.656	***0.762***				
ISP	0.668	0.546	***0.813***			
LEA	0.674	0.733	0.477	***0.743***		
PAR	0.663	0.619	0.478	0.783	***0.773***	
SETA	0.647	0.522	0.533	0.688	0.586	***0.856***

Appendix P

Model Fit

	Saturated Model	Estimated Model
SRMR	*0.087*	0.089
d_ULS	2.459	*2.548*
d_G	1.015	1.024
Chi-Square	533.914	536.785
NFI	0.682	0.680

References

Alabdulatif, A., Liu, D., & Alrawais, A. (2020). Detecting insider threats in information systems using multi-feature analysis. *Information Systems Frontiers, 22*(6), 1397-1413.

Albrechtsen, E., & Hovden, J. (2019). Factors influencing employees' compliance with information security policies in organizations. *Information & Management*, 56(6), 103144.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Asghar, M. Z., Raza, A., & Khan, I. A. (2021). Preventing insider threats using technical and non-technical approaches. *Information Systems Management*, 38(1), 43-56.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74-94.

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, *59*, 9-25.

Bates, R., & Khasawneh, S. (2005). Organizational learning culture, learning transfer climate and perceived innovation in Jordanian organizations. *International Journal of Training and Development, 9*(2), 96-109.

Baskerville, R., M. Siponen. (2002). An information security metapolicy for emergent organizations. *Logistics Information Management*, 15(5/6), 337–346.

Bhattacharya, S., & Zhang, N. (2020). Understanding employee information security behavior: An empirical study of a Chinese online company. *Information Technology & People*, 33(1), 89-117.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Cappelleri, J. C., Darlington, R. B., & Trochim, W. M. (1994). Power analysis of cutoff-based randomized clinical trials. *Evaluation Review*, *18*(2), 141-152.

Chandrasekaran, A., & Radhakrishnan, S. (2017). Organizational culture and effectiveness: A study of values, attitudes, and organizational outcomes. *Journal of Business Research*, 70, 263-276.

Chen, C. C., & Yang, C. Y. (2021). The impact of organizational culture on employees' knowledge sharing: A case study of a high-tech company in Taiwan. *Journal of Knowledge Management*, 25(1), 106-125.

Choi, J., Jung, S. G., & Kim, H. W. (2021). Investigating the impact of information security training on employees' compliance behavior: A cognitive load theory perspective. *Computers & Security*, 105, 102231.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling.

Chun, S. A., Park, J. H., & Lee, K. H. (2019). The effect of cognitive reflection and security motivation on phishing vulnerability. *Information & Management*, 56(6), 103150.

Cohen, J. (1988). Statistical power analysis for the behavioural sciences. Hillsdale, NJ: Laurence Erlbaum Associates.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. C*omputers & Security*, *32*, 90-101.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162-176.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72-94.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474-489.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79-98.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, *89*(1), 59.

Deal, T. and Kennedy, A. (1982), *Corporate Cultures: The Rites and Rituals of Corporate Life*, Addison-Wesley, Reading, MA.

Deshpandé, R., Farley, J. U., & Webster Jr, F. E. (1993). Corporate culture, customer orientation, and innovativeness in Japanese firms: a quadrad analysis. *The Journal of Marketing*, 23-37.Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127-153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293-314.

Egan, T. M., Yang, B., & Bartlett, K. R. (2004). The effects of organizational learning culture and job satisfaction on motivation to transfer learning and turnover intention. *Human Resource Development Quarterly*, *15*(3), 279-301.

Ensher, E. A., Grant-Vallone, E. J., & Donaldson, S. I. (2001). Effects of perceived discrimination on job satisfaction, organizational commitment, organizational citizenship behavior, and grievances. *Human Resource Development Quarterly*, *12*(1), 53-72.

Fakhraddin Maroofi, et al. (2019). The impact of organizational culture on information security policy compliance: An empirical study in Iran. *Computers & Security*, 87, 101590

Fard, H. D., Rostamy, A. A. A., & Taghiloo, H. (2009). How types of organisational cultures contribute in shaping learning organisations. *Singapore Management Review*, *31*(1), 49.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90-110.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26-44.

Fornell, C. (1985). A second generation of multivariate analysis: Classification of methods and implications for marketing research.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing research*, *19*(4), 440-452.

Gao, S., Liang, X., Zhang, Y., & Wang, Y. (2019). An adaptive security architecture based on the integration of technical and procedural security measures. *Journal of Network and Computer Applications*, 126, 130-139.

Gaston, S. J. (1996). Information Security: Strategies for Successful Management. CICA Publishing, Toronto.

Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, *4*(1), 7.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(1), 5.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52-65.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2013). *Multivariate data analysis: Pearson new international edition*. Pearson Higher Ed.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–151.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Hellriegel, D., & Slocum Jr, J. W. (1994). Management. Philipines.

High, R. (2000). Important factors in designing statistical power analysis studies. *Computing News*, Summer issue, 14-15.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660.

Hu, Q., & Dinev, T. (2020). Enhancing employees' information security compliance: A self-determination perspective. *Information & Management*, 57(5), 103256.

Hwang, T., Cheng, Y., & Wu, T. (2020). How organizational culture influences knowledge sharing in information systems development projects: A multi-group analysis. *International Journal of Information Management*, 50, 268-282.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79.

Janis, I. L. (1972). Victims of groupthink. Boston: Houghton Mifflin.

Janis, I. L. (1982). Groupthink: Psychological studies of policy decisions and fiascoes (2nd Ed.). Boston: Houghton Mifflin.

Janis, I. L. (1989). Crucial decisions: Leadership in policymaking and crisis management. New York: The Free Press.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231-251.

Jones, R. A., Jimmieson, N. L., & Griffiths, A. (2005). The impact of organizational culture and reshaping capabilities on change implementation success: The mediating role of readiness for change. *Journal of Management Studies*, *42*(2), 361-386.

Kaba, A., & Lyra, M. (2021). The impact of organizational culture on employee knowledge-sharing behavior in developing countries. *Journal of Business Research*, 129, 478-486.

Kankanhalli, A., Tan, B. C., & Wei, K. K. (2020). The role of employee cognitive and emotional reactions in information security policy compliance. *Information Systems Journal*, 30(3), 525-559.

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

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

Langevoort, D. C. (2015). Behavioral Ethics, Behavioral Compliance. *Research Handbook on Corporate Crime and Financial Misdealing, Jennifer Arlen, ed., Edward Elgar Publishing, Forthcoming*.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review, 37*(12), 1049-1092.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2018). Understanding the impact of organizational culture on the success of information security management. *Information & Management*, 55(6), 704-719. doi: 10.1016/j.im.2017.10.008

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. In *7th Australian Information Security Management Conference* (p. 88). Retrieved 24th April, 2021, from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.189.313&rep=rep1&type=pdf#page=93

Liu, S., Guo, Y., Li, Q., & Wei, J. (2020). Linking organizational culture types to knowledge sharing behaviors: The mediating roles of trust and knowledge sharing self-efficacy. *Journal of Knowledge Management*, 24(5), 1175-1196.

Marinagi, C., Kitsios, F., Papanikolaou, V., & Katsikas, S. K. (2021). Understanding employee information security behavior: An empirical study. *Information & Management*, 58(1), 103402.

Martins E, Martins N. (2016). Organisational culture. In: Robbins SP, Odendaal A, Roodt G, editors. Organisational behaviour. 3rd ed. Cape Town: Pearson Education; p. 606–41.

McLaughlin, J., Anderson, A., & Fisher, J. (2017). Information security education: Awareness and behavior of undergraduate students. *Journal of Education for Business*, 92(4), 169-178. doi: 10.1080/08832323.2017.1305289

National Institute of Technical Standards (NIST). NIST SP 800-53, revision 4. Security and privacy controls for federal information systems and organization. NIST Special Publication; 2013.

Odeyemi, A. O., & Yusuf, A. T. (2017). Organisational culture and information security awareness: Evidence from Nigerian universities. *International Journal of Information Management*, 37(3), 252-261.

Ogbonna, E., & Harris, L. C. (2000). Leadership style, organizational culture and performance: empirical evidence from UK companies. *International Journal of Human Resource Management*, *11*(4), 766-788.

Paine, L. S. (1994). Managing for organizational integrity. *Harvard Business Review*, *72*(2), 106-117.

Peters, T. J., Waterman, R. H., & Jones, I. (1982). In search of excellence: Lessons from America's best-run companies.

Ringle, C.M. Wende, S., Will, A. (2005). SmartPLS 3.0 (M3) beta, Hamburg, http:// www.smartpls.com

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1), 56-62.

Rebelo, T. M., & Duarte Gomes, A. (2011). Conditioning factors of an organizational learning culture. *Journal of Workplace Learning*, *23*(3), 173-194.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122-131.

Schein, E. 1985. *Organizational Culture and Leadership*. Jossey-Bass, San Francisco, CA.

Schein, E. 1992. *Organizational Culture and Leadership* (2nd ed.). Jossey-Bass, San Francisco, CA.

Schein, E. 2004 *Organizational Culture and Leadership (3rd ed.).* Jossey-Bass, San Francisco, CA.

Schein, E. 1990. Organizational Culture. *Amer. Psychologist* 45, 109–119.

Shu, F., Teo, H. H., Wei, K. K., & Chen, L. (2021). Unpacking the cognitive mechanisms underlying employee information security policy compliance: A dual-process model. *Journal of Management Information Systems*, *38*(1), 181-218.

Singh, J., & Mitchell, R. (2017). Organisational culture and information security awareness: A review and research agenda. *Computers & Security*, *68*, 177-189.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224.

Silverthorne, C. (2004). The impact of organizational culture and person-organization fit on organizational commitment and job satisfaction in Taiwan. *Leadership & Organization Development Journal*, *25*(7), 592-599.

Smart, J. C., & St. John, E. P. (1996). Organizational culture and effectiveness in higher education: A test of the "culture type" and "strong culture" hypotheses. *Educational Evaluation and Policy Analysis*, *18*(3), 219-241.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2006). Behavioral information security. *Human-Computer Interaction and Management Information Systems: Foundations, 262*.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information. Systems Research. 1*(3), 255–276.

Tollefson, P. (2000, May 29). Utilities altering culture to compete. *The Gazette* Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/docview/268188708?accountid=6579

Turner, M. E., & Pratkanis, A. R. (1998). Twenty-five years of groupthink theory and research: Lessons from the evaluation of a theory. *Organizational Behavior and Human Decision Processes, 73*(2-3), 105-115.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Vintila, C., & Iancu, E. A. (2021). Combining technical and non-technical measures to address insider threats in information systems. *Journal of Information Security and Applications*, 61, 102846.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275-279.

Wong, K. K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, *24*(1), 1-32.

Wu, Y., Hu, Q., Liang, H., & Xue, Y. (2019). A meta-analysis of the impact of organizational culture on the success of information security management. *Information & Management*, 56(3), 103141. doi: 10.1016/j.im.2018.12.003

Yang, B., Watkins, K. E., & Marsick, V. J. (2004). The construct of the learning organization: Dimensions, measurement, and validation. *Human Resource Development Quarterly*, *15*(1), 31-55.

Yuryna Connolly, L., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security*, *25*(2), 118-136.

Zhang, W., Feng, J., Chen, H., & Chen, Y. (2021). Organizational culture and innovation performance: The moderating role of innovation type. *Journal of Business Research*, 129, 731-743.

Zhou, K. Z., David, K. T., & Li, J. J. (2006). Organizational changes in emerging economies: Drivers and consequences. *Journal of International Business Studies*, *37*(2), 248-263.