A STUDY OF THE EFFECT OF MIDDLE MANAGEMENT PARTICIPATION AND ORGANIZATIONAL CULTURE ON EMPLOYEE SECURITY POLICY COMPLIANCE INTENTIONS

by

Justin Bree

SHAWON RAHMAN, PhD, Faculty Mentor and Chair

SHERRI BRAXTON, ScD, Program Committee Member

WILLIAM J. McKIBBIN, PhD, School Committee Member

Todd C. Wilson, PhD, Dean

School of Business, Technology, and Health Care Administration

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

June 2021

Abstract

This quantitative, nonexperimental study utilized the theory of planned behavior and elements of the competing values framework to examine how middle management participation and organization culture may influence employees' security policy compliance intentions. The theory of planned behavior has been widely used to measure behavioral intentions. The competing values framework supports measuring relevant elements of organizational culture. A previously validated survey instrument was used to gather the required data. Qualtrics recruited study participants following defined parameters. Participants could not have management or supervisory responsibilities, and they could not be part of the organization's technology or information security groups. All study participants were in the United States and were over 18 years, and the participants' organizations all had more than 1,000 employees. This study used partial least squares structural equation modeling to examine the relationships between middle management participation, goal-orientation, rule-orientation, and employees' security policy compliance intentions. The findings indicated that middle management participation has a significant effect on policy compliance intentions. Organizational culture played a less significant role. The perceived goal and rule orientation elements of the competing values frameworks did not significantly affect compliance intentions. Perceived goal orientation did indicate employees were more likely to respond to a value-based approach to compliance than a strict compliance enforcement regime. From a practical application perspective, organizations should be mindful of the role played by an employee's immediate manager or supervisors in influencing security policy compliance outcomes. The study identified several opportunities for future research. All participants were from the United States, creating an opportunity for national

cross-cultural influences to be studied further. The study did not include an experimental element, and reported intentions can differ from actual behaviors. Future studies could be conducted on a longitudinal basis and examine actual employee behaviors. With the influence of the management relationship, there is also an opportunity to explore further the development, presence, and effect of microcultures on information security policy compliance.

Dedication

My overall academic journey has spanned more than a decade. I appreciate the assistance and support I have received from so many people as I worked towards achieving my educational goals. I would like to thank my mother and father for their support over these many years. Your encouragement made a difference during those times when contemplating the difficulties that accompany the pursuit of advanced studies. It is something for which I am so very thankful. I would also like to thank my sisters for being a constant source of support and good humour. It really did make a difference during the more difficult periods.

I would like to dedicate this dissertation to Claire, my beautiful wife, and partner of more than two decades. The pursuit of a PhD requires dedication and commitment from the student and those closest to us. The hours, weeks, and years dedicated to the work needed to achieve the goal is time not spent with loved ones. It is a sacrifice they willingly make with us in support of our aim to achieve. Words will never adequately express the depths of my gratitude for all you have given to support my academic pursuits. Your unwavering support and belief that I could get to the end made the greatest difference in the most challenging moments. It would not have been possible without you.

Acknowledgments

I would like to acknowledge the tremendous support I have received from the faculty and staff at Capella University. It is difficult to overstate the contribution made by my dissertation mentor and committee Chair, Dr. Shawon Rahman. I consider myself incredibly fortunate to have had the benefit of his guidance and support over the journey. I would also like to extend my sincere thanks and gratitude to my committee members, Dr. Sherri Braxton, and Dr. William J. McKibbin. Your comments and insights have made an invaluable contribution and lifted the quality of the final product in a way that would not otherwise have been possible. I would also like to thank the many staff at Capella, particularly the Doctoral Success Program team. What you do to support learners navigating the trials of higher studies does make a difference.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Today, it is difficult to imagine a world that is not digitally enabled. Instantaneous access to information and the ubiquitous presence of connectivity-enabled devices such as smartphones, coupled with real-time information services, online commerce, and social media, is almost taken for granted due to the pervasiveness of their presence. Businesses and organizations are now more dependent than ever on the information economy and the Internet to connect companies and public sector entities with their respective customer bases.

The dimensions and rate of expansion are evident when looking at how rapidly the information economy has grown over a relatively short period. A 2017 report by the United Nations on the information economy brings into sharp focus the exponential growth experienced in this market sector. For example, in 2015, information technology-related goods and services equated to 6.5% of global gross domestic product (United Nations Conference on Trade and Development, 2017). The worldwide trade of information technology-related goods exceeded $2 trillion, and between 2015 and 2019, a 66-fold increase in Internet traffic was forecast (United Nations Conference on Trade and Development, 2017). However, the expansion of the information economy has been accompanied by a proportional increase in cyber incidents and cybercrime.

Accenture’s 2019 report on the global cost of cybercrime highlights the substantial nature of the costs associated with cyber incidents and cybercrime. The report estimates between 2019 and 2023, losses related to direct and indirect cybercrime attacks could approximate $5.2 trillion in lost value. The report also observed the number, cost, and impact of attacks are increasing (Accenture, 2019). Also notable in the report is the observation that malicious software, such as ransomware, and insider attacks, were the fastest areas of cyberattack growth (Accenture, 2019). The size and development of the information economy is too great an opportunity for many organizations to ignore if they wish to remain competitive in a digitally enabled world. Still, there is also a need to ensure their information assets are protected from information security threats and risks.

Employees have the potential to be an information security threat or a security asset. Employees can pose a threat to an organization's information due to apathy towards information security, security policy noncompliance, and operational negligence (Safa et al., 2016). In response to information security threats, organizations implement a range of countermeasures designed to detect and mitigate threats (Nazareth & Choi, 2015). However, a security approach based entirely on technological countermeasures cannot adequately protect an organization's information (Safa et al., 2016). Effective information security requires a culture that encourages individuals to make a positive contribution through compliance with measures set out in security policies (D'Arcy & Teh, 2019). Policy compliance is important because there is almost no technical countermeasure that an appropriately authorized user cannot deliberately or inadvertently undo.

This research considers the relationship between organizational culture, the employee's manager/supervisor's participation, and the employee's behavioral intentions towards being compliant with an organization's information security policy. Information security policies are an essential element of an organization's information security approach as they provide clear guidance regarding acceptable behaviors (Höne & Eloff, 2002). However, policies only make a valuable security contribution if employees are compliant. This research's intended outcome is an improved understanding of how the interrelationships between these elements influence an individual's security policy compliance intentions.

Background of the Problem

We live in a data and information-driven environment. Individuals and organizations are more dependent on information systems than ever before, with technology and information systems permeating almost every aspect of everyday life. Organizations are now more dependent on information systems for their ability to service their customers than ever. Information systems are critical to enabling organizations to meet customer expectations regarding ease of purchase, speed of delivery, and lower costs in an almost borderless marketplace. Information systems also play a particular role in supporting an organization's efforts to differentiate themselves from their competitors by creating opportunities to establish a consumer value proposition through the use of information and information sharing services (Wu et al., 2018).

Because of this increase in, and in some instances, total dependence on information systems, consideration needs to be given to the risks posed by cybersecurity threats. Organizations should carefully evaluate the potential damage from adverse cybersecurity events when considering their current and future viability. The recent example of a severe security breach suffered by the retailer Target is one example of such a breach's potential consequences. In this case, the breach resulted in the disclosure of credit card details for approximately 40 million customers and had estimated consequential losses exceeding $100 million (Pigni et al., 2018). Other notable examples include the breach of approximately 50 million Facebook user accounts, the ransomware attack that affected the United States city of Atlanta, the Equifax data breach that affected approximately 148 million consumers, the U.S. Internal Revenue Service's breach that affected approximately 100,000 taxpayer records, and the breaches of Yahoo's security, involving over 1 billion user accounts (Zhang et al., 2018). These cases bring into sharp focus the seriousness of the threats to information systems and the potentially dire economic and reputational consequences associated with such information system breaches.

Organizations are not oblivious to the risks posed to their information security systems. The U.S. State of Cybercrime survey (as cited in Zhang et al., 2018), conducted in 2016, noted that of the 400 survey respondents, 79% had experienced a security incident, and 76% were more concerned about threats and risks to their information systems than they were in the previous year. In response to their systems' perceived threats, organizations are making significant investments in information security measures. For example, in 2017, the United States Government invested approximately $19 billion in cybersecurity (Aggarwal & Reddie, 2018) and Gartner estimated that global investment in information security would increase from approximately $80 billion to $93 billion in the period between 2016 to 2018 (Zhang et al., 2018). While the level of investment in information security measures is significant, the question of how organizations can ensure these investments deliver the desired results arises.

Numerous research papers argue that while technical countermeasures are essential, individual users are a critical element of an organization's security structure (Stewart & Jürjens, 2017). Numerous research papers also state that users can represent a significant security risk (Heartfield & Loukas, 2018; Warkentin, Johnston, Shropshire, et al., 2016), primarily because it is difficult to prevent an authorized user from performing permitted actions. In this context, the challenge becomes how the various aspects of organizational culture and behaviors, individual behaviors, and technical controls interact to provide the desired level of protection. The challenge is considerable as eliminating the end-user's role in an information security management structure is not practically achievable.

To address this issue, organizations have developed and put in place comprehensive information security policies and process structures to govern user behaviors. Information security policies are the instrument used by an organization's leadership to describe the set of acceptable and unacceptable behaviors and the consequential actions in the event inappropriate behaviors (behaviors contrary to the policy) occur (Flowerday & Tuyikeze, 2016).

Reflecting on the importance of the individual's role in securing an organization's information, information security policies and their effectiveness are often cited as being a critical cornerstone of an information security management system (Bulgurcu et al., 2010; Ifinedo, 2014; Mbowe et al., 2014; Safa, Von Solms, & Furnell, 2016). However, policies are only effective as a security measure if individual users are compliant. Despite the supposed importance of such policies, employees will, in some cases, deliberately attempt to ignore or circumvent policy controls (D'Arcy & Lowry, 2019) despite the potentially negative consequences for the individual and the organization. Questions arise regarding what factors may positively or negatively contribute to an employee's compliance intentions.

The extensive body of published literature that examines the reasons and motivations for employee compliance (or noncompliance) with security policies leverages established theoretical models to explain employee behaviors. A significant proportion of the published literature utilizes cognitive-behavioral models (Lebek et al., 2013). One of the theories often cited in the published literature is the theory of planned behavior (Lebek et al., 2013). This theory suggests an individual’s behavioral intentions are the product of their attitudes towards a behavior, the perceived social pressure to perform or not perform a behavior, and perceived effort associated with the behavior (Ajzen, 1985, 1991). Seminal research by Bulgurcu et al. (2010) uses this theory as the basis for their research, as do many other information security papers. Its use in information security research is based on broad empirical support (Lebek et al., 2013; Safa & Von Solms, 2016), establishing its relevance through its use in published research. Another cognitive-behavioral theory widely used in information security research is the general deterrence theory (Straub & Welke, 1998), positing the severity of sanctions for noncompliance can shape an individual’s behavior. Protection motivation theory shares some of what could be considered similar characteristics to general deterrence theory. An individual’s behaviors are shaped by their response to a fear-arousing suggestion (X. Chen et al., 2018; Rogers, 1975). While the empirical value of these and other cognitive models and their applicability to information security are well established in the published literature, other influencing factors have been identified as warranting further investigation.

A contributing factor to an organization’s security posture is the role played by senior management (Soomro et al., 2016). Top management plays a pivotal role in shaping an organization’s culture, assuming its culture is influenced by top management and subsequently driven down through the organization (O’Reilly et al., 2014). A logical extension of this position is that if information security is vital to an organization, this will be reflected by top management in their behaviors and attitudes towards information security (D’Arcy & Greene, 2014). This observation highlights the importance of top management participation in shaping the organization’s overall culture, including the information security culture.

In many instances, there is an assumption that an organization's culture cascades down from top management and is mainly homogeneous (D'Arcy & Greene, 2014). However, there is an alternative view of how organizational cultures can form and how this may influence an organization's security culture. Rather than being cascading and homogenous, some research suggests that larger organizations' culture may be more organic and generated within individual groups (Boss et al., 2009; D'Arcy & Greene, 2014). In larger organizations with a stratified management structure, and where employees may be several layers removed from top management, a question arises of whether top management's influence dissipates relatively to the degree of hierarchical distance (Hu et al., 2012). Consequentially, the possibility that an individual's manager or supervisor's attitudes and beliefs may play a more prominent role in shaping an individual's attitudes and behaviors towards compliance needs to be considered.

Hu et al. (2012) examined how employee security policy compliance intentions, organizational culture, and top management participation were expected to be a primary contributor; the research results did not support this. Hu et al. (2012) stated this was potentially due to the hierarchical distance between the executive and employees. Later studies by D'Arcy and Greene (2014) and Barton et al. (2016) also considered senior management's role and the connection to organizational and security culture. It noted the importance of management participation; it also pointed out that further to the research by Hu et al. (2012), more research was needed to understand the interrelationships between the respective elements. Other observations included considering management participation on a more holistic basis (Soomro et al., 2016) and organizational culture's social aspects (Kayworth & Whitten, 2010). The cited research illustrates a relationship between management participation, organizational culture, and employee compliance that are still to be explored. While the role of top management participation has been examined in the published literature, the role of an employee's immediate manager or supervisor as it relates to information security is less well understood.

Supervisors play an integral role in influencing an employee's behaviors through the intrapersonal relationship shared due to proximity. A relationship between perceived supervisor support and employee ethical behaviors is suggested in the research (Sguera et al., 2018). Other published studies found a similar link to employees' supervisory support and unethical behaviors (Jacobs et al., 2014). This dynamic can be partially explained by the interdependent nature of the employee and supervisor relationship. Leaders are considered role models whose behaviors are to be emulated; essentially, culture is taught by role modeling and mentoring (Bass & Avolio, 1993; Jacobs et al., 2014). While there are potential positives associated with the supervisor and employee relationship, if viewed through a negative lens where the supervisor operates contrary to broader organizational values to accomplish specific tasks or outcomes, this can have a bearing on an employee's perceptions and behaviors (Bonner et al., 2017). The implications are potentially broader if security management is more bottom-up than top-down (Barton et al., 2016). D'Arcy and Greene (2014) mentioned that organizational culture is more organic and local than uniform and homogeneous. In these circumstances, the potential ramifications for an organization's information security management position could be material.

The published literature that considers employee information security policy compliance intentions using cognitive-behavioral models is considerable. It has been empirically established that employee behaviors are influenced by several factors, including self-efficacy, subjective norms, and an individual's attitudes towards compliance behaviors (Bulgurcu et al., 2010;

Ifinedo, 2012; Sommestad et al., 2014; Tsohou et al., 2015). However, what is not clear is the relationship between organizational culture, the attitudes, and behaviors of an employee's supervisor/manager, and how these elements may interact and influence an individual's policy compliance intentions (Hu et al., 2012; Karlsson et al., 2015; Sommestad et al., 2014; Tang et al., 2016).

This study extends previous research by Hu et al. (2012), D'Arcy and Greene (2014), and Barton et al. (2016). It differs by examining the manager/supervisor's role in influencing an employee's security policy compliance intentions. Hu et al. (2012) and D'Arcy and Greene (2014) noted in their research that management's contribution at different hierarchical levels within an organization is poorly understood. This position was indirectly supported by Sguera et al. (2018), who noted that there is only a limited number of studies investigating the role of first-line supervisors and the influence exerted on ethical employee behaviors.

With organizations increasingly dependent on information systems for their very livelihood and with an evolving threat and risk environment, there is a need to understand better how the human element in an information security management framework can positively contribute. This study seeks to contribute to the published body of knowledge by exploring the relationships between organizational culture, manager/supervisor participation, and an employee's information security policy compliance intentions. This study will add to the knowledge base that will potentially make information security frameworks more effective in mitigating the numerous threats and risks confronting organizations and their information assets.

Statement of the Problem

The problem is the relationship between organizational culture, manager/supervisor participation and how they may affect employee behavioral intentions is unclear. The information security threat and risk environment are constantly changing. Risks once thought to be marginal, such as those posed by state actors (Lemay et al., 2018), are now a constant presence. Because of this changing landscape, organizations need to understand the factors that can positively or negatively influence information security outcomes. The literature identifies organizational culture, employee cognitive behaviors, and manager/supervisory relationships as factors that influence security policy compliance intentions.

The published literature that examines employee information security compliance intentions shows that intentions are influenced by several factors, including self-efficacy, subjective norms, and attitudes towards compliance behaviors (Bulgurcu et al., 2010; Ifinedo, 2012; Sommestad et al., 2014; Tsohou et al., 2015). The established body of literature has also examined the importance of management practices, including the contribution made by top management participation towards influencing information security outcomes (Ezingeard & Bowen-Schrire, 2007; Kayworth & Whitten, 2010; Phillips, 2013; Singh et al., 2013; Whitman & Mattord, 2012). The influential nature of the relationship between a supervisor and an employee has also been established in the extant literature (Bernerth et al., 2016; Whitener et al., 1998; Yadav & Rangnekar, 2015), but the literature does not explicitly explore the effect of the manager/supervisor relationship on an employee’s security policy compliance intentions.

Organizational culture is sometimes assumed to be primarily influenced by the chief executive officer (O’Reilly et al., 2014) and driven down through the organization by top management. An alternative perspective is that an organization's culture is not necessarily the result of a cascading effect, but it is more organic and generated within individual groups (Boss et al., 2009; D'Arcy & Greene, 2014). Because of a relative lack of clarity regarding the role of organizational culture and its influence on security policy compliance, it has been suggested that further research is needed (Crossler et al., 2013) to understand better its role in the broader security policy compliance discussion. Previous studies have examined the potential connection between organizational culture and information security policy compliance (AlHogail & Mirza, 2014) however the precise nature of the relationship between these elements would benefit from further research (Tang et al., 2016).

A substantial body of published literature supports organizational culture, employee cognitive behaviors as they relate to information security policy compliance, and the influential nature of the relationship between a manager/supervisor. Hu et al. (2012) noted in their study that further research was needed to understand better the combined effects of these respective elements on security policy compliance outcomes. The interrelationship between supervisory participation and organizational culture, and the effect on behavioral intentions, is also unclear.

An organization's ability to adequately protect its information assets could directly impact an organization's market position, competitive advantage, or overall viability. The increasing breadth of the risks posed to organizations shows no signs of abating. With a need to ensure security investments are targeted and effective, understanding the various contributing elements that influence an organization's security position will be essential both now and in the future.

Purpose of the Study

The purpose of this research is to analyze the relationship between organizational culture, management/supervisor participation, and their effects on an employee's security policy compliance intentions. Understanding the contribution made played various organizational elements in an information security management framework contributes to improving the framework's effectiveness. This study will contribute to the published body of literature by expanding our understanding of the most influential elements. Furthermore, a better understanding of the various organizational factors' contribution will consequently support improving information systems' security.

A significant body of published research has examined employee behaviors using cognitive-behavioral models such as the theory of planned behavior (Ajzen, 1985). This research has made an invaluable contribution towards understanding the human behavioral element of information security management systems. As the body of knowledge has been progressively expanded, additional factors that could potentially influence security behaviors have been identified. Links have been established between top management participation and information security culture (Kayworth & Whitten, 2010; Phillips, 2013; Singh et al., 2013; Whitman & Mattord, 2012). A smaller body of research examines the role of the manager/supervisor participation (Bernerth et al., 2016; Whitener et al., 1998; Yadav & Rangnekar, 2015), but the published literature does not explicitly explore the relationship between organizational culture, an employee's manager/supervisor, and an employee's security policy compliance intentions.

Research on the influential nature of the relationship between first-line supervisors and employee behaviors indicates causal links between supervisor attitudes and behaviors and employee attitudes and behaviors (Bonner et al., 2017; Jacobs et al., 2014). The studies that have examined this relationship are relatively small in number (Sguera et al., 2018), and they do not consider the role of the supervisor to employee relationship in an information security context. By examining the relationships between organizational culture, manager/supervisor participation, and employee policy compliance intentions in an information security setting, a positive contribution will be made towards closing an identified gap in the published literature. It may also make a positive contribution to information security practice.

Significance of the Study

Previous research examined employee cognitive beliefs (Bulgurcu et al., 2010; Sommestad et al., 2014; Tsohou et al., 2015), management participation and practices (Soomro et al., 2016), and organizational culture as it relates to information security (AlHogail & Mirza, 2014; Boss et al., 2009; Crossler et al., 2013; Tang et al., 2016). However, the potential connections between these respective elements have not been explicitly examined or tested. Research by Hu et al. (2012), and later by D'Arcy and Greene (2014) and Barton et al. (2016), began to examine the relationship between management participation, organizational culture, and employee cognitive beliefs. This earlier work did make an essential contribution by establishing a foundation for future research. There is a gap in the existing research regarding the role of organizational culture and manager/supervisor participation, and how these elements may influence employee security policy compliance intentions.

This study adds to the extant body of published literature by extending the theoretical model described by Hu et al. (2012) that examined the role of top management participation and organizational culture by examining the effect of management/supervisor participation and organizational culture on employee security policy compliance intentions. Previous research by Soomro et al. (2016) calls for a broader approach to management participation in information security and for this concept to be empirically tested. Research by Karlsson et al. (2015) on information security culture similarly suggested that further research is needed to expand the body of empirical data. Research conducted by Sguera et al. (2018) from the field of business ethics identified the limited but growing number of studies on the effects of the first-line supervisor's actions. While not directly related to business ethics, this study's results could indirectly improve understanding the relationships and the associated influences between employees and their supervisor.

Research Questions

Research Question 1: "Does perceived management/supervisor participation in information security positively influence employee security policy compliance intentions?"

Research Question 2: "Do organizational cultural values positively influence employee security policy intentions?"

Definition of Terms

Dutifulness. Dutifulness is an aspect of conscientiousness, and it correlates with rule compliance behaviors (Roberts & Jackson, 2017). It has been included to prevent a confounding effect on the model (Hu et al., 2012).

Individual Beliefs. Based on the theory of planned behavior (Ajzen, 1985), individual beliefs incorporate attitude, normative beliefs, and self-efficacy (controlling or influencing an outcome).

Management/supervisor Participation. Management/supervisor participation influences employee beliefs and attitudes, including normative and control beliefs (Hu et al., 2012). Management participation legitimizes a commitment to security initiatives; alternatively, an absence of management participation or priority may diminish employees' level of attention to information security (Albrechtsen, 2007).

Organizational Culture. Using the competing values framework developed by Quinn and Rohrbaugh (1983), organizational culture is defined by two specific elements: goal orientation and rule orientation (Hu et al., 2012). Goal orientation is based on rationality, accountability, performance indicators, and accomplishment. Rule orientation is based on a hierarchical structure that incorporates respect for authority, the rationality of processes, and the division of work (Van Muijen et al., 1999).

Policy Compliance Intentions. Policy compliance intentions indicate an individual's intention to carry out a particular behavior (Ajzen, 1991). According to Ajzen (1991), intentions are an "indication of how hard people are willing to try, or how much of an effort they are planning to exert, to perform the behavior" (p. 181). In this instance, the intention to comply with the organization's security policy.

Research Design

The research design for this study is a quantitative, single-stage, non-experimental, survey-based study. Seminal research on employee security compliance behaviors by Bulgurcu et al. (2010) utilized this approach, as did relevant subsequent studies by Hu et al. (2012) and D'Arcy and Greene (2014). Literature reviews by Lebek et al. (2014), Karlsson et al. (2015), and Sommestad et al. (2014) that examined various aspects of information security compliance behaviors show that quantitative research models are the predominant research method used for this type of research. The survey builds on previous research and utilizes the validated instrument developed by Hu et al. (2012) to collect specific organizational culture and top management participation data. A minor adjustment has been made regarding the definition of management; for this study, it is defined as an employee's immediate manager or supervisor instead of top management.

Quantitative research is aligned with a post-positivist approach where it is assumed that cause and effect relationships can be established (Creswell, 2014; Trochim, 2006). The realist/objectivist ontology associated with the post-positive approach infers a research approach that is detached, and where an emphasis is placed on measuring variables and testing hypothesis through the establishment of cause and effect relationships (Tuli, 2011). The use of a survey-based approach will enable data to be collected and analyzed to establish whether there is any causal relationship between manager/supervisor participation, organizational culture, and an individual's security policy compliance intentions.

Assumptions and Limitations

Assumptions

Consistent with a post-positivist approach, quantitative research assumes that cognitive behaviors can be both predicted and explained and that the probabilistic causes of behaviors can be successfully identified (Antwi & Kasim, 2015). For this study, it is assumed that a survey-based approach combined with the research model will enable probabilistic antecedents as they relate security policy compliance intentions in this context to be adequately measured and quantified.

Because this study is not using observed behaviors, it is assumed that each respondent to the questionnaire answered the questions honestly as they relate to the individual. Participants were advised the survey was being conducted on an anonymous basis, enabling individuals to answer questions on the understanding that a declared intent not to comply with their organization's security policy would remain confidential.

Limitations

This study utilized the same methodology as Hu et al. (2012) to measure the influence of organizational culture. However, as Hu et al. (2012) observed, organizational culture by its nature introduces a heightened degree of measurement complexity, and any measurement framework will, consequently, impose some limitations.

Regarding data collection, the study utilizes a survey instrument that requires individuals to self-report behavioral intentions; this, in turn, creates the risk of common method bias. The risk of common method bias needs to be controlled to ensure survey results are not adversely affected by issues such as social desirability, leniency bias, acquiescence, social desirability, or the tendency to behave in a socially expected manner (Podsakoff et al., 2003). Studies that rely on an individual stating a behavioral intention and do not subsequently validate the self-reported behavior through observation are inherently limited because actual behaviors are not recorded (Workman, 2008). No observed behaviors are captured or recorded as part of this study.

Organization of the Remainder of the Study

The purpose of this study was to examine the relationship between manager/supervisor participation, organizational culture, and an employee's information security policy compliance behavioral intentions. In this chapter, the background, purpose, significance, research questions, and limitations of the study have been discussed. Chapter 2 examines the published literature relevant to this study. Chapter 3 examines in greater detail the purpose of the study, the research questions and associated hypotheses, the research design, the data analysis, and the ethical considerations associated with the research. Chapter 4 discusses the results of the study, including the sample and the testing of the respective hypotheses, and Chapter 5 discusses the summary of the results, conclusions, limitations, the implications for theory and practice, and suggestions for the direction of future research.

CHAPTER 2. LITERATURE REVIEW

Modern organizations are more dependent than ever on information systems, and while such systems can be strategically beneficial, they can also be a potential and significant organizational risk (Lowry & Moody, 2015). Despite the extensive efforts to secure information using technical controls and countermeasures, the human element continues to be identified as the weakest link and the likely point of failure when considering the compromise of technical security measures (Gratian et al., 2018). Because of the significant and expanding interest in information security, there is a substantial body of extant literature that examines the human factor issue from different theoretical and practical perspectives.

A literature review's principal purpose is to examine past research, critically consider the results, and synthesize the findings and possible alternative views (Rowe, 2014). Reviewing previously published literature is a critical element of the research process. It provides a solid foundation for examining and developing ideas and theories, and it enables opportunities for further research ideas and directions to be identified (Bandara et al., 2015).

This literature review will begin by describing the methodology used to identify relevant published research and explain its theoretical orientation supported by relevant research. Following will be a review of the current literature, which will create a reference framework for synthesizing the findings and identified themes. The last section of the literature review will review and critique the reviewed research, identifying past research strengths, limitations, future opportunities, and their contribution to this study.

Methods of Searching

The expanding volume of the extant literature is an indicator of the importance of information security. While this accumulation of knowledge is a sign of the field's increasing maturity (Paré et al., 2015), the considerable volume of published research can present challenges. For example, a Google Scholar search using the search term "information security" returned approximately 3.6 million results. When considering this volume of information in the context of a literature review, the task is to achieve a saturation level that ensures the relevant body of research has been fully explored. In this context, a literature review achieves this objective when content searches cease to provide new, relevant citations or do not add to the theories, concepts, and research results already reviewed (vom Brocke et al., 2015).

The search methodologies described in previously published peer-reviewed literature reviews were utilized as an initial reference point to ensure the body of relevant research was fully explored. These literature reviews aided in developing search terms that would appropriately focus the search without excluding relevant material. Past literature reviews also provided insights into relevant research repositories, such as journals and databases, ensuring the literature review would be comprehensive.

The literature search was focused on identifying scholarly, peer-reviewed material. Published research papers, including past literature reviews, are the principal sources of material that support the review, and the volume of available research material is substantial. The Capella Library's database and journal search facilities were used extensively for the literature search. Online tools such as Google Scholar were also used in conjunction with general Google searches. However, the general searches were somewhat limited in providing useful references for rigorously researched and validated material.

Databases

The databases searched for relevant material were:

- ABI/Inform
- ProQuest Central
- EBSCOhost
- SAGE Journals
- Computers & Applied Sciences Complete
- ScienceDirect
- Business Source Complete

In addition to these databases, Google Scholar was also leveraged as an additional source for identifying relevant, peer-reviewed research papers. General searches were also conducted using the Google search engine. However, this search process was limited in its effectiveness when identifying peer-reviewed research; Google Scholar was a more effective tool for this purpose.

Journals

The Association of Information Systems publishes a guide to what is referred to as the *Senior Scholars' Basket of Journals* (Schryen, 2015; Silic & Back, 2014). This list of journals is compiled by senior scholars and is described by the Association for Information Systems (https://aisnet.org/page/SeniorScholarBasket) as the principal journals in information security.

The journal list was augmented by the addition of other journals identified as having material relevant to this study's interest areas.

The journals searched were:

- European Journal of Information Systems
- Information Systems Journal
- Information Systems Research
- Journal of the Association for Information Systems
- Journal of Information Technology
- Journal of Management Information Systems
- Journal of Strategic Information Systems
- MIS Quarterly
- Computers & Security
- Information Management & Computer Security
- Decision Support Systems
- Journal of Information Privacy and Security

Bibliographic Mining

Reference lists in reviewed research articles are a rich source of additional material that may not otherwise be identified in structured searches. These reference lists are a list of material leveraged in the extant research; they provide an insight into the paths pursued by researchers engaged in exploring related theories and concepts. The reference lists in the reviewed material were examined in detail. Research papers identified as relevant were the subject of a specific search and review activity. The definitive collection of material included these results where this material contributed to the overall literature review.

Search Terms

Search terms are the basis for ensuring that the discovery process is as comprehensive as possible. The methods and methodologies used to develop search terms in previous information security literature reviews were reviewed to inform the search process. This approach was adopted as it was an opportunity to learn from the strategies used by more experienced researchers to identify relevant databases and peer-reviewed material. In particular, several search terms were adopted from a literature review conducted by Karlsson et al. (2015) focused specifically on information security culture. Other search terms were added for completeness as the content of interest is broader than that explored by Karlsson et al. (2015).

The search terms and keywords used included “information security culture”, “information security climate”, “information security and organizational culture”, “information security and employee behavior”, “information security and policy compliance”, “information security culture and information security”, “information security and management participation”, and “information security and supervisor participation”.

Searches using variations of accepted spelling, for example, *organizations* and *organisations*, were conducted to ensure relevant material was not omitted based on the precise spelling of search terms. Advanced search functions within the respective databases and journals were used, as were Boolean operators (e.g., AND) to identify all relevant research material. Searches using Google Scholar and the Google search engine also included Boolean operators.

The search of Google Scholar and the Google search engine did not use wildcard operators due to the sheer volume of returned results.

The final stage of the search process was the use of forwards and backward searches. A backward search is conducted by screening the reference lists in the reviewed material (vom Brocke et al., 2015). A forward search is conducted by looking for subsequently published research that cites key articles (Schryen, 2015). The use of forwards and backward searches led to identifying additional studies of interest, further contributing to the review's completeness.

A good literature review must be comprehensive. It must identify all the relevant research associated with the concepts and theories of interest, and it must do this in a structured and rigorous way. In their seminal article concerning taking a structured approach to information systems literature reviews and identifying material, Webster and Watson (2002) propose the significant research contributions are likely to be found in the leading databases and journals. The early identification of the Senior Scholars Basket of Journals (Silic & Back, 2014) was advantageous when combined with in-depth searches of other relevant databases and journals. At the end of the search process, it was apparent the point of saturation described by vom Brocke et al. (2015) had been reached. Articles had ceased to offer up fresh, relevant publications and citations when compared to those already found. The reviewed material has substantially contributed to this study by creating a broad understanding of the extant research. However, it has also confirmed that the existent research gap identified as a part of this study is still present. The opportunity to make a positive contribution to the overall body of knowledge remains.

Theoretical Orientation for the Study

The use of theories in academic research serves several essential purposes. Theories provide a reference framework for the development of reasoned arguments that, in turn, support the justification of pursued research ideas (Stewart & Klein, 2016). Theories also guide the researcher through the stages of the research process, from the formative stages of an idea, through data collection and analysis, making sure ideas and approaches are structured (Iyamu, 2013). Well-developed theories make a valuable contribution to research efforts by providing an interpretive frame that enables knowledge to emerge from what might otherwise appear to be a disorganized collection of diverse results (Damschroder, 2019). Dankasa (2015) took this concept a step further by stating that any academic research being considered for publication should contain a theoretical element. Dankasa (2015) also noted that research underpinned by a sound theoretical foundation is more likely to be deemed to have made a positive contribution to the field of study. These observations suggest that research based on a sound theoretical footing will have a significantly greater likelihood of being structured, rigorous, and making a positive contribution to the relevant research field.

Information systems research has leveraged a broad range of social science theories to explore individual and organizational behaviors (Jones & Karsten, 2008). For example, general deterrence theory has been adopted from criminology and is widely used in information security studies (D'Arcy & Herath, 2011). The theory is based on the principle that the certainty, speed, and severity of sanctions will influence an individual's behavioral intentions (X. Chen et al., 2018). A literature review by Lebek et al. (2014) that examined theories used in information security behavioral research identified 54 different theories, some of which had been co-opted from the fields of sociology, criminology, and psychology.

With such a diverse range of theories used in this field, care had to be exercised when choosing the theoretical framework for this study. The purpose of the study is to understand an individual's behavioral intention in a specific context. Previously published studies that examined behavioral intentions in similar contexts provided a valid reference point and a better understanding of the various theoretical frameworks' mechanics and possible applicability. Other factors considered were the constructs within the respective theoretical models and how closely these constructs aligned to the environmental inputs of principle interest in this study. In his paper on theories used in information systems research, Iyamu (2013) noted that, in some instances, a single theory could not provide the necessary degree of coverage, which, through necessity, increases the use of complementary theories. This study examines several factors, including management participation and organizational culture, that are not directly accommodated by other behavioral theories. The need to accommodate these additional constructs makes Iyamu's point concerning complementary theories particularly relevant.

Considering all the individual factors, two individual and organizational behavioral theories are appropriate for this study: the theory of planned behavior (TPB) and the competing values framework (CVF). TPB was applicable because it accommodated the concepts of volitional control and expended effort and environmental factors such as the influence exerted through others' opinions and attitudes (Ajzen, 1985). In conjunction with the need to measure the effect of proximate individuals on behavioral intentions, there is also a need to capture the contributing effect of an organization's culture. The CVF provides an empirically tested means to achieve this outcome. The framework developed by Quinn and Rohrbaugh (1983) enables organizational effectiveness to be measured using a spatial model that considers influences such as how flexible (or inflexible) an organization is and whether it is more focused on goals or rules. Hu et al. (2012) utilized the CVF in their study on top management participation and security policy compliance, citing the framework's ability to capture an organization's cultural orientation and the need to integrate different theoretical frameworks. The following summarizes the published literature that examines the TPB and the CVT to identify these theories as appropriate for this study.

Theory of Planned Behavior (TPB)

Before TPB, the initial theory developed to describe volitional behavior was the theory of reasoned action (Fishbein & Ajzen, 1975). This theory posits that an individual's behavioral intentions are a product of their attitude towards a specific behavior and subjective norms, or their perception of attitudes towards people's behaviors they deem important (Fishbein & Ajzen, 1975). Responding to what he believed were shortcomings in the theory of reasoned action, Ajzen (1985) extended the theory by incorporating an individual's perceived level of control over a behavior into the model. Ajzen cited earlier work by Bandura (1977) on self-efficacy (the ability to overcome perceived obstacles through effort) and its ability to influence volitional behaviors. This extended model that incorporated the perceived behavioral control became the TPB.

The TPB posits that an individual's behavioral intentions are a product of an individual's attitude towards the behavior, subjective norms, and perceived behavioral control (Ajzen, 1991). According to Ajzen (1991), there is a direct correlation between an individual's perception of behavioral control, behavioral intention, and the ability to predict behavioral achievement. The theory's principle element is an individual's intention concerning a specific behavior as intentions capture the motivational factors, such as how much effort someone is willing to invest in performing the behavior (Ajzen, 1991). The TPB is an empirically tested theory, its ability to reliably explain behavioral intentions is considerable, despite the modest number of predictors (Sommestad & Hallberg, 2013). This reliability is one of the reasons why information security researchers have widely adopted it.

Bulgurcu et al. (2010) conducted seminal research into how employee beliefs affect security policy compliance intentions that utilized TPB. A theory-focused literature review by Lebek et al. (2014) found TPB to be one of the principal behavioral theories used in security awareness research. Iyamu (2013) observed that the use of complementary theories has also proved the applicability of TPB in this context. In a study exploring security policy compliance behaviors, Ifinedo (2012) utilized TPB in combination with protection motivation theory as they share a common element (self-efficacy). A longitudinal study by D'Arcy and Lowry (2019) examining cognitive-affective drivers of employee security compliance behaviors used both TPB and rational choice theory due to their consideration of a shared effect. The outcome was how an individual calculates cost-benefit. As this study utilizes two theories, successfully integrating TPB with an appropriate complementary theory will contribute to establishing a sound theoretical foundation.

Competing Values Framework (CVF)

Quinn and Rohrbaugh (1983) originally described CFV as a means of organizing the extant literature and as an empirically derived overarching framework to support efforts to assess organizational effectiveness. To develop the framework, Quinn and Rohrbaugh (1983) used a two-staged approach; an initial study comprised a small group of organizational theorists and researchers, followed by a second more extensive group of similar composition. Using a comparative method, Quinn and Rohrbaugh (1983) identified the central concepts of organizational effectiveness in the form of three dimensions: (a) organizational focus, (b) organizational structure, and (c) organizational means and ends. Organizational focus is related to whether an organization is predominately internally or externally focused (Quinn & Rohrbaugh, 1983). Internally focused relates to staff development; externally focused relates to its broader development (Quinn & Rohrbaugh, 1983). The organizational structure dimension emphasizes flexibility versus stability. The third dimension of means and ends considers whether an organization is more focused on processes, such as planning, or more focused on outcomes (Quinn & Rohrbaugh, 1983). Together, these value dimensions are representative of the valued characteristics of an organization (Hartnell et al., 2011).

The original framework developed by Quinn and Rohrbaugh (1983) has been progressively developed and refined. Van Muijen et al. (1999) simplified the spatial model by redrawing the dimensions axes; flexibility and control, and internal and external. Within the model, other orientations were added to illustrate the effect of the different axial positions. The quadrant between flexibility and external indicates a focus on innovation, whereas the quadrant between flexibility and internal indicates a focus on staff support (Van Muijen et al., 1999). This model also reflects whether an organization is goal-oriented, or focused on accomplishment, or rule-oriented, where the emphasis is on structure, hierarchy, and processes (Van Muijen et al., 1999). In their study that examined the effect of top management participation and organizational culture, Hu et al. (2012) utilized the CVF model developed by Van Muijen et al. (1999), focusing on the goal and rule orientation quadrants. A prior study by Chang and Lin (2007) that examined the effect of organizational culture and security management using CVF found that only goal and rule orientation significantly affect security outcomes. This earlier study informed the approach taken by Hu et al. (2012), and given the methodological alignment, the same approach is being adopted for this study.

Review of the Literature

The body of published literature that examines or considers organizational and security culture, security policy compliance and management participation is extensive. Numerous perspectives and positions are cited on what factors encourage or influence employee compliance behaviors. However, in some instances, the literature is inconsistent or differs regarding the principal factors that influence compliance intentions. Because information security draws on a diverse range of theories (Jones & Karsten, 2008), the logical structure for exploring the literature is by first examining the relevant seminal works. This foundation can then be built on by logically organizing the literature using the constructs of culture, compliance, and management participation used in this study's research model. Using this approach, understanding each area's similarities or departures will be easier to read and follow.

Foundation Research

Individual behaviors and the desire to understand the drivers of behavior have been the subject of a considerable research effort over many years. What factors influence the decision-making process and how these can be influenced have been studied and revisited to establish and refine theories and models that attempt to describe individual behaviors. In his seminal work, Simon (1955) described his behavioral model of rational choice. In this model, the concepts are introduced of individuals evaluating possible choices, calculating a return on effort, and determining the preferential order based on the perceived pay-off. The model of rational choice described by Simon (1955) forms part of the general deterrence theory, which according to Lebek et al. (2014), is one of the four most utilized theories in information security.

A different perspective on the model of rational choice was put forward by Tversky and Kahneman (1986). Tversky and Kahneman (1986) suggested the same question framed a different way should result in essentially the same choice being made from defined options, a characteristic referred to as invariance. According to Tversky and Kahneman (1986), invariance did not always hold, with choices influenced by individual norms, habits, and expectations. Ajzen and Fishbein (1973) also explored the concept that individual perceptions regarding people's behavior and attitudes that are important to the individual, referred to as subjective norms, would influence behavioral choices. The model proposed by Ajzen and Fishbein (1973) was subsequently refined by Ajzen (1985), and throughout several iterations, it became the theory of planned behavior. A later review of the theory by Ajzen (2011) noted the model's predictive power had been empirically proven over time and that it had become one of the most frequently cited models when examining social behaviors. The behavioral models developed by Simon (1955) and Ajzen (1985) have provided important insights into the decision-making processes. The role played by subjective norms, perceived return, and risk versus reward continue to be relevant. These concepts and theories have been adopted in a security context (Lebek et al., 2014) to understand policy compliance intentions better.

Another element of understanding user behavior is how individuals justify behaviors, such as policy noncompliance. The neutralization techniques first described by Sykes and Matza (1957) have found currency in the field of information security and compliance behaviors. Initially framed in the context of juvenile delinquency, Sykes and Matza (1957) described techniques such as denying responsibility and denying injury as a means for an individual to rationalize abhorrent behaviors. Information security studies that have focused on employee compliance behaviors have identified neutralization as an applicable model to explain the rationale used to describe some aspects of noncompliant behaviors (Barlow et al., 2013, 2018; Siponen & Vance, 2010).

Organizational culture and its role in influencing individual behaviors are also relevant to this study. Past studies have often assumed that an organization's culture is a direct reflection of its senior leadership, but empirical studies supporting this position are limited (O'Reilly et al., 2014). D'Arcy and Greene (2014) noted the assumption that organizational culture is top-down and homogeneous. Earlier work by Smircich (1983) stated that culture is not necessarily homogeneous and can be considered at a micro or macro level. Smircich (1983) also noted the literature refers to organizational culture as a singular entity, marginalizing the possibility of a multiplicity of sub-cultures or the existence of countercultures.

The seminal work by Bandura (1977) on self-efficacy and behavioral change noted the significance of behavioral modeling and that a significant proportion of behaviors are developed by modeling observed behaviors. The concept of behavioral modeling lends itself to a more localized setting. In a large, stratified organization where employees may be somewhat removed from the senior leadership, the idea of localized cultures and behaviors becomes a consideration.

Brown and Duguid (1991) noted in their research that people in organizations function as a community and that individuals can acquire the community's subject views. Brown and Duguid (1991) also noted that there is often a discrepancy between how work is described (the policy) and what happens in practice when considering policies. The difference between policy and practice also indicates the possible influence of localized cultures on work practices.

Early research on behavioral characteristics and aspects of organizational culture describes the spectrum of possibilities in examining outcomes in a specific context. The seminal works by Simon (1955), Ajzen (1985), Sykes and Matza (1957), and Bandura (1977), supported by later work by Smircich (1983) and Brown and Duguid (1991), remains relevant and has been adopted in later information security studies to support explaining aspects of user compliance behaviors. The body of knowledge related to information security has expanded considerably in the interceding period and needs to be further explored if this study is to make its contribution to the published body of knowledge.

Organizational and Information Security Culture

Organizational culture is often described as a system of shared values that enable individuals to understand what is important (shared norms); they also guide member attitudes and define accepted behaviors (Detert et al., 2000). Schein (2004) defined organizational culture as a pattern of basic assumptions learned by solving external adaptation and integration problems in his seminal work. The solutions to these problems worked sufficiently well to be taught to new group members as being the appropriate way to perceive, think, and feel concerning those problems (Schein, 2004). The concept of group-shared experiences and learning, and its connection to the need for stability and meaning, differentiates Schein's (2004) definition of culture from broader, more generic descriptions.

Smircich (1983) noted the possibility of macro and micro-level cultures and the possibility that cultures could compete to define specific situations within a group. D'Arcy and Greene (2014) also mentioned the possibility of multiple cultures, noting that culture could originate with groups (bottom-up) instead of merely cascading down from top management. A study by Goo et al. (2014) on organizational security climates noted much of the published literature assumed a homogeneous organizational culture and a failure to consider factors such as social groupings and group behaviors. Y. Chen et al. (2015), in their study of security programs and culture, also found that information security is a sub-culture influenced by the broader organizational culture. A study by Iivari and Huisman (2007) on organizational culture and systems development and deployment methodologies also stated that larger organizations do not have a singular, homogeneous culture but instead develop a multitude of sub-cultures.

The concept of micro or localized cultures can also be found in published research that considers group and team dynamics. In a longitudinal study of medical doctors that focused on how the team climate influenced technology use, Liang et al. (2010) noted that relational and positional proximity led to a shared understanding and similar behaviors among group members. Liang et al. (2010) also noted that individuals relied on their proximate social network for guidance on how to make sense of issues and to guide appropriate behavioral responses. The extensively cited work on social information processing by Salancik and Pfeffer (1978) supports this premise by stating the social environment provides a context for interpreting events and preferred attitudes and opinions within the group. Salancik and Pfeffer (1978) also state that individuals will adapt their attitudes, behaviors, and beliefs to their social context by focusing on specific information, increasing its relevance. Da Veiga and Eloff (2010) focused on developing a framework to assess security culture; they noted that culture operates at multiple levels, including group, individual, and organizational. Da Veiga and Eloff (2010) also noted that group dynamics could be influenced by management but with either positive or negative effects. Citing the seminal work by Hall (1959) on intercultural communication, in their case study of the security culture at a merged company, Dhillon et al. (2016) noted that interaction is pivotal in the development of culture. Dhillon et al. (2016) also noted the separation between top management and operational teams negatively affected the authority dynamic and caused issues with regards to task clarity. This perspective is supported by earlier work by Ruighaver et al. (2007). In their study that examined the dimensions of security culture using the cultural dimension model originally developed by Detert et al. (2000), Ruighaver et al. (2007) state that contextual factors have a substantial effect on influencing individual and group behaviors. The common theme across these respective studies is the role played by social factors, relationships, and how the proximate contextual setting influences perceptions regarding expected and acceptable attitudes, beliefs, and behaviors.

One of the effects of an organization's culture is shaping employee attitudes and perceptions at the local or macro level. In a study that examined issues associated with security awareness and organizational change, Lacey (2010) states organizational culture is a significant influence on individual perceptions. The degree of influence can be to the point where any differentiation between personally held views and organizational perspectives becomes increasingly difficult to distinguish. As Lacey (2010) describes it, "Organizational culture is an insidious, corrupting influence" (p. 6) that is difficult for individuals to resist. Da Veiga and Martins (2017) examined dominant information security cultures and subcultures and found that organizations have a dominant culture accompanied by subcultures. Da Veiga and Martins (2017) state the dominant culture is likely to be the broadly understood set of shared values; a subculture is likely to be formed in a smaller proximate group setting such as a department, peer group, or geographical area. Da Veiga and Martins (2017) share an example wherein a localized environment risk is perceived differently to head office, leading to employees circumventing or ignoring controls such as sharing passwords. Da Veiga and Martins (2017) note that there is limited research on why security subcultures diverge from the principal security culture and that future research could further investigate the presence of dominant information security cultures and subcultures. The link between organizational culture and information security behaviors was also explored by Connolly et al. (2017) in a study that examined the relationship between organizational culture and procedural security controls. Connolly et al. (2017) noted that while a link between organizational culture and behaviors is the accepted convention, their literature search only identified two conceptual studies that identified organizational culture as a strong predictor of security-related behaviors.

The examination of organizational culture has illustrated an inextricable link to organizational and individual behaviors and the consideration of what cultural factors positively or negatively contribute to security-related behaviors. In a study that examined the connection between organizational culture and security culture, Tang et al. (2016) noted there might be inconsistencies between the definition of an information security culture and its relationship to organizational culture. Tang et al. (2016) also noted that past studies identified security as principally being a management issue that required leadership. A study by Mubarak (2016) on security frameworks in healthcare organizations supports this need for leadership, stating that weak cultures lead to an absence of direction for employees concerning desired security outcomes. The need for clear leadership was also supported by Flores and Ekstedt (2016) in a study on information security and social engineering resistance factors. Flores and Ekstedt (2016) state that strong or transformational leadership is necessary if countermeasures, such as education and awareness, are to be effective. Barton et al. (2016) examined leadership from a different perspective, examining the effect of senior management commitment on information security. Barton et al. (2016) note that previous research illustrated that management commitment to security is critical because it increases employee participation; it was also noted that security management continues to be a primarily bottom-up driven approach.

The reference to bottom-up-driven security aligns with the cited research that identified disparate cultures. Specifically, with the observation from D'Arcy and Greene (2014), security culture was possibly organic and driven from the bottom-up. A study by Cox (2012) on why security policies may be ignored by users referred to an environment where employees respond only to the manager's demands, regardless of their alignment or adherence to security policies. Cox (2012) referred to this concept as "organizational narcissism" (p. 1851), linking it to the possible formation of attitudes that imply policies and rules are not consistently applied to individuals and groups. As a cultural consideration, the concept of an organization developing character traits usually affiliated with individuals, such as narcissism, is interesting and not widely considered in the published literature.

A reflection of an organization's culture is the policies created to establish a common understanding of the leadership's desired behavioral settings and outcomes. Thomson et al. (2006) state that cultural change can only occur by altering formative attitudes and that the management vehicle to achieve this by establishing a clear policy position. Furnell and Thomson (2009) examined employee security acceptance using three levels of corporate culture: artifacts or observed behaviors, espoused values that can be described in policies, and shared tacit assumptions. Schein (2009) described these levels as a hierarchy, with artifacts being the top layer, espoused values in the middle, and the deepest layer being shared tacit assumptions. Policies represent espoused values but are ultimately shared tacit assumptions that translate into practices accepted by management (Furnell & Thomson, 2009). If there is a misalignment, given the dynamics of localized culture identified in the published literature, the effectiveness of policies will likely be diminished. Van Niekerk and Von Solms (2010) recognized the need to maintain a balance in their paper that considered corporate culture and a conceptual model of information security culture. Van Niekerk and Von Solms (2010) noted that establishing a security subculture was an essential contributor to managing human security factors; they also identified a need to balance espoused values and tacit assumptions. Specifically, Van Niekerk and Von Solms (2010) stated that employee behaviors could not be reasonably predicted if there was an imbalance between management demands (being espoused values) and the effort or knowledge, willingness, or capacity of the employee (tacit assumptions).

While the literature indicates a misalignment or imbalance is undesirable, there are several reasons why this situation could conceivably arise. In their paper that investigated the role of trust and perceptual differences related to security behaviors, Kearney and Kruger (2016) noted that management often assumes that everyone has or shares a common view of security. Hedström et al. (2011) expressed a similar perspective, noting that security may not necessarily be consistent across groups, mainly where conflicts arise between desirable practices and professional beliefs, such as in the healthcare sector. A later study by Kolkowska et al. (2017) on value-based compliance appears to be consistent with the earlier research, noting that prioritizing rationalities was often left to individuals without any supporting guidance to assist the process.

Security policies can only be as effective if they can be practically implemented. In their study that examined data concerning security behaviors, Beautement et al. (2016) stated that security policies could be formulated without considering employees' capabilities regarding their capacity or willingness to comply. The misalignment may result in theoretically sound policies failing in practice, with management encouraging circumvention if they believe such policies impede productivity (Beautement et al., 2016). Aligned to the previously cited research, Beautement et al. (2016) also noted that organizational populations were not homogeneous. Consequently, policies may be interpreted differently, giving rise to behavioral inconsistencies (Beautement et al., 2016). Karlsson et al. (2017) also noted that as a means of providing direction, theoretically, sound security policies may prove impractical, and policy designers should be mindful of current work practices.

One way to overcome this is employee participation in policy development, as suggested by Alshare et al. (2018). In their study that examined security policy compliance in a higher education setting, Alshare et al. (2018) propose involving employees in the development process to reduce the likelihood of noncompliance due to an increased perception of fairness. Research by Niemimaa and Niemimaa (2017) into security policy implementation expressed a similar perspective regarding translating policies into practice. Niemimaa and Niemimaa (2017) identify the challenge of translating global policies into a local environment and the discrepancy that sometimes exists between the assumed simplicity of work practices and the actual complexities. To address this, Niemimaa and Niemimaa (2017) suggest policies should be negotiated instead of imposed and, by doing so, engaging the employees in the process. This approach begins to shift the perception of employees being a security liability to a potential asset that can positively contribute to improving the organization's security posture (Albrechtsen & Hovden, 2009; Posey et al., 2015).

Organizational culture and its logical extensions, and security culture and policies, play an essential role in setting the environmental context when considering employee security behaviors. The published literature shows that organizational culture is not homogeneous, nor does it necessarily flow in a single direction (top-down). Security policies, as an extension of organizational culture, also have environmental considerations. Like the assumptions made regarding the homogeneity of organizational culture, policies can assume a commonly shared viewpoint. Furthermore, the oversimplification of day-to-day work practices can make theoretically sound policies unworkable. The literature on organizational culture provides an important contextual setting. The logical extension is to explore the published literature for reasons why employees voluntarily or involuntarily fail to comply with established security policies. Seeking to understand the contributing factors associated with security policy compliance intentions is the focus of this study, and as such, an exploration of the relevant literature is necessary.

Information Security Policy Compliance

The body of published literature that examines information security policy compliance from several different perspectives is extensive, and it uses a variety of behavioral and theoretical models. The exploration of this literature will provide a contextual framework for this study and support an understanding of the opportunities still to be explored by future research efforts.

The principal question posed is why employees comply, or not, with organizational security policies and what factors influence their compliance decisions. The published literature shows that organizational culture plays a role in this process, but it is not the sole influencing factor. In a study that compared the security culture of employees familiar with security policies versus those that were not, Da Veiga (2016) noted various contributing factors that influence compliance intentions. Contributing factors included the perceived seriousness of security threats, perceptions regarding the organization's commitment to security, training, awareness, and management attitudes (Da Veiga, 2016). Da Veiga (2016) did find a positive correlation between awareness and improvements in security culture. In their study of security management factors, Singh et al. (2014) similarly identified a range of contributing factors, including top management support, security policies, training, awareness, and compliance monitoring. Research by Barlow et al. (2018) on anti-neutralization measures found that traditional security training and awareness programs are often ineffective because employees minimize the perceived adverse consequences, often citing a higher-order outcome. Barlow et al. (2018) also found the threat of sanctions had a limited effect on compliance intentions. Earlier research by Barlow et al. (2013) also considered the role played by neutralization techniques and found that rationalizing behaviors could lead non-malicious employees to violate information security policies, even overcoming the threat of formal sanctions. In their paper that proposed a theoretical model that examined the effects of neutralization, Siponen and Vance (2010) suggest its effects should be considered when developing security policies.

Another factor cited in the published research is the tension between the effort or cost to comply versus the perceived risk of noncompliance. In a study that used the theory of planned behavior and protection motivation theory to examine noncompliance, Karlsson et al. (2018) found conflicts between policy compliance requirements and perceived productivity resulted in noncompliance instances. Earlier research by Hwang et al. (2017) produced similar findings in cases where policy compliance was considered an impediment to productivity. Hwang et al. (2017) also found that, in such instances, employees were likely to follow the accepted norms of their peers, including the replication of noncompliant behaviors. Research by Sharma and Warkentin (2018) on the relationship between employment status and compliance also noted that the perceived cost of compliance was a significant influencing factor in compliance decisions. Somewhat offsetting this was the finding that organizational commitment positively influenced compliance intentions (Sharma & Warkentin, 2018). Recent research by Rajab and Eydgahi (2019) on the efficacy of behavioral models and security compliance found that perceived efficacy, perceived vulnerability, and response cost were the best indicators of compliance intentions among the sample group.

A variety of theories have been applied to the question of compliance. Beautement and Sasse (2009) used microeconomic utility theory to determine an individual’s compliance effort (budget) is finite. When the budget is nearing exhaustion, priority is given to tasks perceived to be more important (Beautement & Sasse,2009). Similarly, a qualitative study by Albrechtsen (2007) on security compliance found that perceptions regarding elevated compliance effort resulted in the focus being moved to what was believed to be more efficient and productive outcomes. Albrechtsen (2007) also found that employees would often fail to execute security-related tasks despite saying they were motivated. Besnard and Arief (2004) also found that employees would either ignore or circumvent security rules to maximize efficiency, often creating security risks by doing so. In a longitudinal study by Hedström et al. (2013) conducted in a hospital setting, compliance effort was also identified as a primary factor. Hedström et al. (2013) found that compliance decisions were essentially a means-end calculation and that decisions to share passwords were primarily based on practical outcomes. Hedström et al. (2013) also noted in their research the presence of rationality (neutralization) elements in explaining behaviors contrary to the security policy.

The perceived cost of compliance is mentioned in the theory of planned behavior described by Ajzen (1991). In the model, perceived cost is defined as perceived behavioral control, which relates to the perceived ease or difficulty associated with an action or task (Ajzen, 1991). Other factors in the model are subjective norms or the views of referent people or groups that are important to the individual, attitudes towards the behavior based on positive or negative beliefs, and perceived consequences associated with the behavior (Ajzen, 1991). In a subsequent study that considered the factors influencing technology use, Taylor and Todd (1995) decomposed the theory of planned behavior by expanding the respective elements to create a more granular model. The attitude element was extended to include perceived ease of use, perceived usefulness, compatibility, or the alignment with past experiences, current needs, and the individual’s values (Taylor & Todd, 1995). Subjective norms were decomposed into two specific elements; peer influence and supervisor’s influence (Taylor & Todd, 1995). Perceived behavioral control was decomposed into three additional components. Self-efficacy, described initially by Bandura (1977), is related to an individual’s perceptions of their ability (Taylor & Todd, 1995). The other two elements completing the set are resource conditions and technology conditions associated with the availability of resources such as time, money, and access to information that may facilitate or constrain technology use (Taylor & Todd, 1995). These seminal behavioral models and the respective elements, such as subjective norms, are relevant as they support a greater understanding of compliance-related behaviors’ influences.

A study by Boss et al. (2009) examined policy compliance and perceived mandatoriness. They found that policies developed by managers that had no line management responsibilities may be perceived as optional due to an absence of direct authority (Boss et al., 2009). In their study that examined security policy violation, Cheng et al. (2013) found that social pressures in the form of subjective norms exerted a significant influence over an individual’s intention to violate a security policy. Cheng et al. (2013) also noted that social bonds and pressures may act as a form of informal control and that neutralization diminished the effectiveness of formal sanctions. Using a mixed-methods approach, research by Ashenden (2018) on attitudes found that unless attitudes are reinforced continuously, they will become ineffective over time. The attitudes referred to by Ashenden (2018) are analogous to subjective norms. Cram et al. (2016) explore the concept of varying forms of control, including behavioral control implemented through management oversight and output control through monitoring an employee’s productivity. Cram et al. (2016) also describe the concept of clan control, or control exerted through social dynamics that consequently influence behaviors. The concept of clan control could be logically aligned with the subjective norm element in other behavioral models. Cram et al. (2016) do note that one of the issues of security control research is the perspective most often taken is that of the controller, and there is an absence of studies that consider controls designed to create a positive sentiment such as contentment or equality.

The concept of environmental conditions, such as organizational and social connections, influencing compliance behaviors is an important insight. The published literature also identifies other factors and behavioral models that provide alternative perspectives and explanations. Borena and Bélanger (2013) explore the relationship between religiosity and compliance, finding that it may positively influence compliance by indirectly inhibiting or suppressing undesirable compliance behaviors. In their study that examined core security behaviors, Chatterjee et al. (2015) noted the significant utility of the theory of planned behavior when examining security-related behaviors. Chatterjee et al. (2015) also describe a concept called opportunism, which assumes that individuals will act in their self-interest if given the opportunity. Self-interest is weighed against other factors such as ethical beliefs, subjective norms, and attitudes, but perceived gain played a substantial role in the decision process (Chatterjee et al., 2015). The concept of opportunism was also supported by Padayachee (2016), suggesting that controlling opportunities was perhaps a more effective control measure than attempting to influence an individual’s motives. In a survey of 124 business managers that combined protection motivation theory and the theory of planned behavior, Ifinedo (2012) found that self-efficacy, attitude, subjective norms, response efficacy, and perceived vulnerability contributed to compliance intentions. Ifinedo (2012) also found that their peers’ attitudes influenced behavioral intentions in conjunction with an individual's attitude. Utilizing social norms and norm activation theory, Yazdanmehr and Wang (2016) found that personal norms influence norm-based behaviors. Yazdanmehr and Wang (2016) also stated that over time social norms, such as those found in a group environment, would similarly influence behaviors once they are accepted and internalized by the individual, essentially converting them to personal norms. The concept of personal norms was also identified in research by Safa, Von Solms, and Furnell (2016) in their study on compliance models. Safa, Von Solms, and Furnell (2016) found that commitment and personal norms influence an individual's attitude; a close working relationship with supervisors and co-workers also reduced the likelihood of injurious behaviors. Earlier research by Warkentin et al. (2011) on the influence of informal (social) learning noted that external cues, such as verbal support from peers and managers, could influence perceptions of self-efficacy and compliance intentions.

While factors such as attitudes and subjective norms may influence compliance behaviors, there is also the role played by security policies and the possibility of sanctions in the event policies are circumvented or ignored. In a study that used deterrence theory as its theoretical foundation, D'Arcy et al. (2009) found that increased awareness of policies combined with compliance monitoring and the threat of sanctions influenced compliance intentions. D'Arcy et al. (2009) also found that the perceived severity of sanctions had a more significant effect on compliance intentions than the perceived certainty of sanctions being applied. A quantitative study by Liang et al. (2013) using industrial companies in China as a response pool produced a different outcome to D'Arcy et al. (2009). Liang et al. (2013) found that punishment expectancy significantly affected compliance intentions; reward expectancy was not a significant factor. In their paper that examines noncompliance through the lens of moral reasoning, Myyry et al. (2009) found preconventional reasoning, or self-interest, was a factor when considering sanctions. Myyry et al. (2009) also stated that individuals were more likely to comply with security policies if they believed a punishment would be applied as a result. As the published research indicates, the threat of sanctions implies an individual's assessment of the threat and the possible consequence. Security researchers have also adopted this model to explore other aspects of behavioral intentions.

Protection motivation theory was initially described by Rogers (1975). Rogers's (1975) theory is premised on invoking a fear response and a proportional protective response based on "the magnitude of noxiousness of a depicted event" (p. 93), the probability of an event occurring, and the perceived efficacy of an individual's protective response. This theory, and similar reactance-based behavioral models that consider the effect of threats and mitigating behaviors, have been adopted by security researchers to investigate behavioral dynamics in different contexts. In a study that examined dispositional and situational factors associated with noncompliance, Johnston et al. (2016) identified two personality traits, stability, and plasticity, that influence compliance intention. Johnston et al. (2016) describe stability and plasticity as "meta-traits" (p. 236), with the stability meta-trait contributing to risk aversion, and the plasticity meta-trait contributing to risk-taking when the possibility of a benefit by doing so is evident.

Research by Lowry et al. (2015) on reactance differed from other studies that found a positive correlation between compliance the effective threat of sanctions. Lowry et al. (2015) found a negative relationship between increasing the severity of sanctions and compliance, noting that a deterrence approach may, in effect, be counterproductive. This result differs from the often-cited earlier research by Herath and Rao (2009) that did find that perceptions regarding the threat and severity of sanctions were one of the factors that would influence compliance behaviors. In a study that proposed a reactance-based behavioral approach, Lowry and Moody (2015) utilized a different approach to applying sanctions. Rather than the threat of more traditional sanctions, Lowry and Moody (2015) suggest threats concerning the removal of personal freedoms as a means to provoke the desired protective emotional response. Conversely, Lowry and Moody (2015) also note that a security policy that is perceived as increasing personal freedoms is less likely to encounter resistance.

While a reactance-based model could be conceived as being a relatively blunt instrument to motivate desirable security behaviors, studies do support its effectiveness. Later research is refining possible models for its application. Researching user motivations, Menard et al. (2017) found that personalizing approaches to suit an individual’s intrinsic motivations, instead of a direct fear appeal, was more effective in encouraging positive engagement. The suggestion that personalization may enhance effectiveness was also supported in a study by Johnston et al. (2015) on improving the effectiveness of fear appeals. Johnston et al. (2015) state that a generic threat, such as the threat to information, may fail to achieve the necessary degree of personal relevance, negating its effectiveness. A further investigation of this approach by Warkentin, Johnston, Walden, et al. (2016) using medical imaging technology that maps neurological activity found that a fear appeal does provoke a threat assessment appraisal but not an actual fear response. Consequentially, Warkentin, Johnston, Walden, et al. (2016) suggest the focus on threats may be counterproductive and that an alternative approach is to make the response more appealing, encouraging the desired behavior.

Behavioral models such as the theory of planned behavior and deterrence theory have made an invaluable contribution towards understanding the factors that contribute to compliance behaviors and motivations. Building on these models is research that examines other behavioral factors related to the information security context. A study of 369 students by Gratian et al. (2018) examining human character traits found that characteristics such as financial risk-taking, rational decision-making, gender, and extroversion were unique predictors of security behaviors. In their earlier research, Hu et al. (2015) used a neurological activity mapping approach to examine the decision-making process, specifically focusing on self-control. Hu et al. (2015) found that study participants with lower levels of self-control had a reduced level of neural engagement in decision-making, leading to the suggestion that screening employees for self-control was not only practical but a positive contribution towards improved security. Research by Vance et al. (2013), based on accountability theory, found that accountability, defined as the pressure to justify actions to others, reduced policy noncompliance intentions. Measures described to achieve accountability included activity audits and ensuring the user's identifiability (Vance et al., 2013).

The published literature that examines information security policy compliance is extensive and identifies several factors that contribute to understanding an individual's compliance behaviors. Factors such as neutralization, perceived fairness of sanctions, loss of personal freedoms, cost-benefit assessments, and low-self-control (Wall et al., 2016) can all contribute depending on the contextual setting. A dominant element in many behavioral studies and the supporting theoretical frameworks is the focus on an individual's cognitive processes (Hu et al., 2012). The published literature shows that organizational culture is also a contributing factor; the supervisory contribution should also be considered if a complete picture is to be formed.

Management Participation

Previous studies have examined, and supported, the role of an organization's top management in fostering a positive information security environment (Barton et al., 2016; Knapp et al., 2006; Soomro et al., 2016). However, the published literature also notes that an organization's culture is not necessarily homogeneous and that culture, or the set of accepted behaviors, can be influenced by proximity (Liang et al., 2010). Cheng et al. (2013) state that while there is a substantial body of published literature that examines formal controls, governance at the informal level has received less attention. The exploration of the literature that explores this proximate supervisory relationship is of interest to this study.

Leader-member exchange theory focuses explicitly on the relationship between a leader and a subordinate or a follower (Day & Miscenko, 2016). In a healthcare sector study that utilized leader-member exchange theory, Wayne and Green (1993) found that employee behaviors were influenced by the relationship between the employee and the supervisor. An example cited by Wayne and Green (1993) is an employee supporting the supervisor with their specific responsibilities. In a literature review that examined compliance and conformity, Cialdini and Goldstein (2004) noted that individuals who align with the opinions, attitudes, and instructions of authority figures might realize benefits from doing so. Cialdini and Goldstein (2004) also noted that authority figures that are considerate of employee needs are likely to see higher behavioral compliance rates. The consideration of employee needs could conceivably manifest in abhorrent security behaviors. Beautement et al. (2016) noted that managers might support security measures being ignored or circumvented if productivity was negatively affected. The literature also established compliance costs as a factor in compliance decisions (Wall et al., 2016).

These observations indicate it is conceivable that a supervisor could encourage noncompliance based on expressed concerns for an individual’s workload. In their research on the effects of management transgressions and information security, Wall and Iyer (2012) note there is limited published research on the impact of negative management actions on security behaviors. Research by Skotnes (2015) on the effects of management commitment and systems security in the power generation sector explored top and middle management’s commitment to security awareness. Skotnes (2015) found that securing management commitment to security was difficult despite employees reporting the level of management commitment to security as being high. Skotnes (2015) noted that this discrepancy might result from complications associated with collecting data, specifically negative data, on an employee’s immediate supervisor. In their research on management’s tolerance of workarounds in information systems in a healthcare setting, Röder et al. (2014) found management will tolerate workarounds if they believe organizational policies and standards inhibit productivity. Röder et al. (2014) also found a willingness to tolerate workarounds if there is a view the workarounds are more suited to the immediate operational needs.

Managers and supervisors act as a referent group, affecting and shaping individual and group normative beliefs (Goo et al., 2014). In a security policy context, Stahl et al. (2012) state that policies are based on a power relationship dynamic that allows managers to define the scope of security. Stahl et al. (2012) also state that this dynamic implies management has an inalienable right to direct subordinates' behaviors. When examining organizational power relationships, Kolkowska and Dhillon (2013) found a contributing noncompliance factor was a failure to understand power relationships within the organization. Explicitly concerning management, Kolkowska and Dhillon (2013) found management's inability to utilize the power of meaning effectively or effectively communicate values contributed to noncompliance behaviors.

The importance of immediate management and supervisory relationships is also identified in research by Dang-Pham et al. (2017a) in their study that used social network analysis to examine security compliance. Dang-Pham et al. (2017a) noted the role of interpersonal influences and that such influences would play out at a local or microculture level. Dang-Pham et al. (2017a) also noted the effect of informal instructions that, again, would likely manifest at a local level; support and persuasion cues would serve to reinforce the local behavioral dynamic. The earlier seminal works by Bandura (1977) noted the role played by observed behaviors. Brown and Duguid (1991) observed that people in localized environments tend to acquire that group's viewpoints, supporting the importance of understanding these proximate relationships.

Research by Boh and Wong (2013) on perceived management effectiveness and knowledge sharing made several relevant observations regarding the role of proximate management relationships. Boh and Wong (2013) found that the action of co-workers shapes individual perceptions. Boh and Wong (2013) also stated that employees who believe their manager's actions were aligned to their expectations would engage in behavioral reciprocation, exhibiting behaviors and attitudes they believed were aligned with their supervisor's expectations. The concept of a reciprocal dynamic was also identified by Sguera et al. (2018) in their study on supervisory support for ethical or unethical behaviors. Sguera et al. (2018) found that supervisors could influence employee behaviors through perceived support for desirable behaviors, and because of this perceived increase in support, employees were more likely to reciprocate. A literature review by Thomson and van Niekerk (2012) that examined information security apathy suggested that in a prosocial environment where employees voluntarily protect information assets, management should be able to rely on employee cooperation to protect information assets in ambiguous scenarios. Thomson and van Niekerk (2012) state that a positive security culture will likely emerge if all employees exhibit prosocial behaviors. The need for all employees to exhibit this behavior is a significant dependency. The seminal work by Jensen and Meckling (1976), which is also referred to by Xue et al. (2011), notes that employees will often act as selfish agents, opportunistically engaging in behaviors that are contrary to the organization's interests.

Research by Walsh et al. (2010) on management and security culture notes that culture is a recursive environment continually evolving based on individual and group sub-cultures. In their research on information security influence. Dang-Pham et al. (2017b) made several relevant observations regarding the role of managers and supervisors. Dang-Pham et al. (2017b) noted power bases could influence the security setting, and perceptions of legitimacy are associated with hierarchical structures. Dang-Pham et al. (2017b) also stated that proximate interactions with supervisors and co-workers resulted in interpersonal influences.

The role of interpersonal influences and proximate relationships has been a recurring theme in the reviewed research. As agents of the organization, supervisors have the most immediate and frequent contact with employees (Chan et al., 2005). Their position places them in a unique position to influence attitudes and subjective norms, accommodating either positive or negative security behaviors through action or acceptance (Chan et al., 2005). The reviewed literature has also provided additional context with regards to organizational culture. The concept of a multiplicity of cultures within an organization shares a logical connection with the role of proximate relationships, which is relevant to this study.

Findings

The published literature that examines information security culture, policy compliance, and management participation has identified several central themes relevant to this study. Previous studies examining information security and culture have assumed that an organization's culture is monolithic and homogeneous, resulting in other environmental interrelationships being overlooked or obscured (Ramachandran et al., 2013). Earlier, seminal research by Smircich (1983) identified that culture could be a consequence of membership, and there is the possibility of multiple cultures, or even countercultures, within an organization. Several studies, including those by Goo et al. (2014), D'Arcy & Greene (2014), and Karlsson et al. (2017), support this premise. The possibility of multiple cultures creates an opportunity for disparate security cultures within a sufficiently large organization to emerge. It does not necessarily mean that a microculture would necessarily exhibit misaligned security behaviors, but it does present a variable that can be further explored.

The policy compliance literature identified several variables that were consistently referenced. These variables, such as self-efficacy, behavioral attitudes, and the effort or cost of compliance, were cited in studies that examined possible factors influencing security compliance decisions. These variables are associated with established behavioral theories, such as the theory of planned behavior, general deterrence theory, and protection motivation theory, that are frequently used in information security behavioral studies (Lebek et al., 2014). These variables' importance came into focus when considering the possible relationship between these variables and how the individual cognitive processes may be influenced by management and supervisor relationships. Individuals that base decisions on the cost of compliance, including considering risk versus reward elements, may factor in the possibility that noncompliant behaviors may be implicitly or explicitly sanctioned by supervisors (Röder et al., 2014). The literature also illustrated the connection between an individual's cognitive process, such as that described in the theory of planned behavior, and the influence of observed behaviors. The seminal work by Bandura (1977) drew attention to the importance of observed behaviors in the learning process with subsequent studies, including those by Cheng et al. (2013) and Guo et al. (2011), supporting this position.

Several papers focused on an alternative behavioral model. The effects of neutralization in the context of compliance provided an alternative perspective to view employee behaviors. Barlow et al. (2018) explained how neutralization techniques could justify noncompliant behaviors with claims to achieving a higher organizational objective. The research by Barlow et al. (2018) was supported by earlier work by Siponen and Vance (2010) and Barlow et al. (2013). Neutralization techniques are not the focus of this study. The chosen behavioral model is the theory of planned behavior, but its relevance in a security context has been demonstrated in the reviewed literature.

With the presence of multiple cultures and the individual cognitive influences established in the reviewed literature, the role of management participation and its possible connections to culture and policy compliance could be viewed through a different lens. Immediate managers and supervisors have the most proximate leadership relationship to employees (Chan et al., 2005). The reviewed research has shown that subjective norms and associated behaviors are influenced by authority figures and social interactions (Cialdini & Goldstein, 2004). The proximity of immediate management, their role as an authority figure, and their ability to directly influence and determine an acceptable work practice place them in a position of significant influence. The role of management in supporting workarounds has also been established (Röder et al., 2014), demonstrating the influential nature of the relationship between a supervisor and the employee.

When considered in its entirety, the reviewed literature paints a different contextual picture than the individual topic areas. In isolation, the published research on information security culture describes the various contributing factors. However, and understandably due to the research's focused nature, more explicit connections between culture, compliance, and management participation are not established. In a study that examined employee attitudes on compliance, Ashenden (2018) noted that conceptual studies based on behavioral models and theories often fail to account for the social context that influences behaviors and attitudes. A multithreaded picture has emerged that illustrates several possible connections where management participation elements could influence policy compliance and organizational culture by creating a different focal point. For example, the acceptance of workarounds leading to policy noncompliance outcomes, which are, in turn, the result of an impractical security policy being developed that is not reflective of the localized needs or environment.

The reviewed literature provides a valuable contextual setting for this study. Tang et al. (2016) noted in their research on organizational and security culture that a limited number of studies have examined the connection between organizational and security culture. In their study on cybersecurity culture, Gcaza et al. (2017) refer to cybersecurity culture as an "ill-defined domain" (p. 263), or one that lacks a single predominant theory that "defines the concepts, relationships, and procedures for the domain; and providing a means to validate problem solution or cases" (p. 263).

While not solving this particular problem, this study will extend the understanding of the possible connections between organizational culture and its relationship to policy compliance and management participation. The theory of planned behavior's appropriateness as a behavioral model for this study is supported by the literature (Chatterjee et al., 2015; Lebek et al., 2014). This study is not all-encompassing. For example, it does not explicitly consider all possible factors such as neutralization and its potential effects on compliance intentions. It will examine a larger picture that has not been extensively explored in the published literature.

Critique of Previous Research Methods

The reviewed literature has provided an opportunity to consider this quantitative study's respective aspects in greater depth. The literature has provided insights into the research methods employed, the sampling methodology and analytical approaches used, and the findings that have shaped the current security compliance perspectives.

It was observed that a significant proportion of the quantitative studies reviewed have what could be considered as limited sample sizes. While the required statistical power was achieved and validated in each study, the sample sizes, in some instances, were constrained or very close to the minimal size needed to reach statistical significance. There were some notable exceptions to this observation, such as the study by Menard et al. (2017) on user motivations and information security and O'Reilly et al. (2014) on the CEO's role concerning organizational culture. A contributing factor to the limited sample sizes may be linked to the survey distribution method. In some instances, surveys distributed by the researchers encountered poor response rates or incomplete responses, leading to responses being set aside. This study has addressed that problem by utilizing a professional survey entity to ensure an adequate number of completed responses. The issue is understandable, but it does affect the possible generalizability of the study results.

It was noted that several of the reviewed studies used highly regulated industries or individuals with domain knowledge as the sample group. Industries such as finance, healthcare, audit, and information technology security have either domain-relevant knowledge or are subject to a regulatory regime that incorporates information security requirements. Studies conducted using organizations and individuals that examine security policy compliance intentions could encounter results that may not necessarily represent the broader user population. Supporting this perspective, Cram et al. (2016) noted that much of the security-related research adopts the controller's view. In their often-cited study, Herath and Rao (2009) noted that some empirical studies that examine the effectiveness of information security practices used either technology professionals or top management as the principal participants. This view was supported by

Karlsson et al. (2016), noting that a significant proportion of security research is focused primarily on management issues. It does not suggest that such studies do not produce valuable results or insights. However, one needs to be mindful of this aspect if highly generalizable results are being sought.

Another observation was the assumption that an organization's culture was homogeneous and driven primarily by top management, overlooking the possible influences that microcultures could exert. It was noted by Da Veiga and Martins (2017) in their observation that there has been limited research conducted on the influence of information security subcultures. Karlsson et al. (2015) made a similar observation, noting no identified research examined the possible effects of different information security cultures. The potential influence of a diversity of cultures is the lack of attention paid to social factors and influences in the published research. Han et al. (2017) support this perspective by noting that while some studies have considered social factors, there is not enough to build a sound theoretical understanding. Ashenden (2018) made a similar observation that studies have failed to consider the social context element. The omission of the concept of multiple cultures and the associated social influences potentially overlooks important factors that influence security policy compliance behaviors.

A central element of this study is examining the effect of an organization's culture on security policy compliance. The reviewed research was mainly devoid of any analysis of the connection between organizational culture and information security culture or compliance. Da Veiga and Eloff (2010) noted the relationship between organizational culture and organizational behavior was poorly understood. Connolly et al. (2017) noted that when reviewing the published literature for their study into security and organizational culture, only two conceptual papers could be identified that identified organizational culture as a predictor of compliance behaviors. Tang et al. (2016) also noted that few studies examine organizational and information security culture. This study explicitly examines the relationship between an organization's culture and an individual's security policy compliance intentions, in doing so, hopefully making a positive contribution to broadening the understanding of this relationship.

A common theme or element of much of the published research focused on security policy compliance is behavioral models such as the theory of planned behavior, general deterrence theory, and protection motivation theory. A literature review by Lebek et al. (2014) identified no less than 54 different theories that had been used in compliance-related research. One of the considerations associated with such theories' exclusive use is that they primarily focus on the individual's cognitive processes, omitting other potential influences such as organizational culture and management participation. Dang-Pham et al. (2017b) identified this in their research, stating that much of the published research was almost entirely focused on individual cognitive processes. The extensive use of cognitive-behavioral theories in the published research supports this view. These behavioral models have been and continue to be invaluable in the field of security research, but an awareness of the potential limitations of these models must be maintained.

By examining the interrelationship between organizational culture, management participation, and employee compliance intentions, a contribution will be made towards closing some of the identified gaps in the published literature. The use of an established and empirically validated behavioral model is augmented by incorporating the influencing factors of organizational culture and management participation. This study's model will bring a different perspective by including what has been identified in the published literature as significant influences that have been largely omitted in previous studies and not integrated with how this study uses these constructs. By including these elements, the results of this study should provide a richer contextual picture, delivering results that will be broadly generalizable, and by doing so, contributing to the overall body of knowledge.

Summary

The reviewed literature has established several essential concepts that are directly relevant to this study. The assumption of a homogeneous organizational culture is inherently flawed. The presence of a multiplicity of cultures is a more likely outcome. There is also a lack of depth regarding understanding the relationship between organizational culture and security policy compliance outcomes. This study will make a positive contribution toward expanding the body of knowledge in this area.

Concerning the role of managers and supervisors, the literature identified several important areas of potential influence regarding security policy compliance. When considered in conjunction with normative influences and the importance of proximate relationships related to learned behaviors and attitudes, there is a genuine opportunity to learn more about how this relationship dynamic may influence an individual’s compliance intentions.

The use of an empirically validated behavioral model for this study has been broadly supported in the published literature. The theory of planned behavior is one of the most widely used behavioral theories in information security research (Lebek et al., 2014). Its predictive capacity has been empirically proved across multiple studies over a substantial period (Ajzen, 2011), making it suitable for this study.

The reviewed literature has provided a comprehensive foundation that supports this study’s premise, which is understanding the relationship between management participation, organizational culture, and individual cognitive processes. The reviewed literature has identified the constructs that form the research model are valid. The reviewed literature has also confirmed a gap in the body of knowledge that this study will positively contribute towards closing.

CHAPTER 3. METHODOLOGY

The intention and purpose of this research is to contribute to the existing body of knowledge, expanding its coverage, and adding to the overall understanding of the behavioral factors that influence information security compliance outcomes. The achievement of this objective and the avoidance of erroneous conclusions are dependent on the adoption and application of a suitably rigorous scientific approach. Ensuring the research approach is systematic and objective and that observations and results are replicable (Nardi, 2018) is critical to ensuring the value of any study's contribution. In this section, the research methodology, including the study's purpose, the research questions, and associated hypotheses, the design, and the research procedures, will be described in detail. Describing the study's methodology in detail will support its critical assessment and, in the process, ensure that any contribution is not diminished through error, omission, or oversight.

Purpose of the Study

The purpose of this study is to analyze the relationship between organizational culture, management/supervisor participation, and their effects on an employee's security policy compliance intentions. Studies on information security compliance behaviors often cite individuals as the weakest link in the information security structure (Flores & Ekstedt, 2016; Gratian et al., 2018; Johnston et al., 2016). In conjunction, attacks that explicitly target users and user behaviors such as ransomware have increased in frequency and sophistication (Ali, 2017). Previous studies have attempted to identify predictors of compliance and compliance behaviors (Karlsson et al., 2015; Sommestad et al., 2014; Soomro et al., 2016), but a definitive set of predictors has not been identified. Cram et al. (2019) have stated that while studies have identified numerous potential behavioral predictors, their relative importance is unknown. Cram et al. (2019) also note that policy noncompliance and deliberate policy violation should not necessarily be considered equal. While the focus is often placed on factors such as punishment and rewards that can be controlled by management, these may have lesser relative importance when predicting employee compliance behaviors (Cram et al., 2019).

Previous studies have established a connection between top management participation and information security culture (Kayworth & Whitten, 2010; Phillips, 2013; A. Singh et al., 2013; Whitman & Mattord, 2012). The available research that examines the role of the supervisor's participation is limited (Bernerth et al., 2016; Whitener et al., 1998; Yadav & Rangnekar, 2015). The published literature also does not explicitly explore the relationship between the organization's culture, an employee's supervisor, and how this relationship may influence an employee's security policy compliance intentions. Tang et al. (2016) note that despite the extent of the published research, the relationship between an organization's culture and information security outcomes remains unclear. When considering the relationship between first-line supervisors and employee behaviors, past studies indicate causal links between supervisor and employee attitudes and behaviors (Bonner et al., 2017; Jacobs et al., 2014). The studies that have examined this relationship are limited (Sguera et al., 2018), and they neglect the supervisor-employee relationship as it relates to security policy compliance behaviors.

The research problem this study explores is directly connected to the constructs of organizational culture, management participation, and compliance intentions. It will examine if a causal relationship between management/supervisor security policy compliance attitudes, organization culture, and an individual's security policy compliance intentions exists. The study setting is larger organizations with a stratified management structure. This setting has been chosen deliberately. It will create and test the hierarchical distance referred to by Hu et al. (2012) that may have contributed to the diminished influence of top management participation in their study on security policy compliance that this study extends.

Previous studies have identified gaps in the current understanding of influencing factors and their interrelationships (Connolly et al., 2017; Cram et al., 2017, 2019; Da Veiga & Eloff, 2010; Niemimaa & Niemimaa, 2017). The relationships between organization culture, management/supervisor participation, and employee policy compliance intentions will be better understood due to this study. Hopefully, improving the interpretation of these relationships will make a small but positive contribution towards addressing some of the gaps identified by more experienced researchers in the published literature.

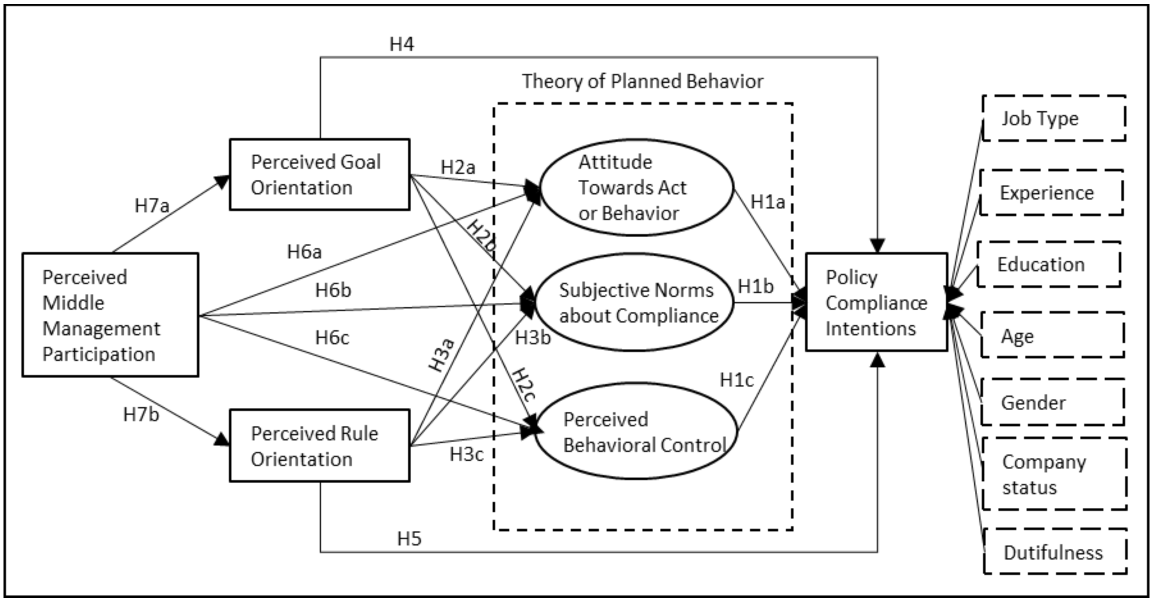
Research Questions and Hypotheses

This study focuses on understanding how organizational culture and the attitudes and beliefs of an employee's immediate manager towards information security may influence an employee's security policy compliance intentions. This focus is reflected in the two primary research questions for this study. The research questions are supported by seven hypotheses intended to test the presence and strength of the relationships between the elements of management participation, organizational culture, and an individual's policy compliance intentions.

Earlier research by Hu et al. (2012) explored the role of top management participation and organizational culture on compliance intentions. Hu et al. (2012) described how organizational culture and management participation elements could be integrated into a valid research model. Building on this earlier research by Hu et al. (2012), this study examines these elements through a fundamentally different lens by examining the relationship between an employee and a manager/supervisor and, consequentially, localized organizational cultures.

Figure 1

Research Model and Hypotheses


H4
Theory of Planned Behavior
Perceived Goal Orientation
H7a
H2a
Attitude Towards Act or Behavior
H1a
H2b
H6a
Perceived Middle Management Participation
H6b
Subjective Norms about Compliance
H1b
Policy Compliance Intentions
H6c
H3a
H3b
H2c
H1c
H7b
Perceived Rule Orientation
H3c
Perceived Behavioral Control
H5
Job Type
Experience
Education
Age
Gender
Company status
Dutifulness

Note. Adapted from "Managing compliance with information security policies: The critical role of top management and organizational culture" by Q. Hu, T. Dinev, P. Hart, and D. Cooke, 2012, *Journal of Decision Sciences, 43*(4), p. 631. Copyright 2012 by Journal of Decision Sciences. Adapted with permission.

The process of data collection and analysis is intended to support the exploration of the two research questions and the associated supporting hypotheses. The hypotheses have been logically grouped with their associated research question (Figure 1).

Research Question 1 and Supporting Hypotheses

RQ 1: "Does perceived management/supervisor participation in information security positively influence employee security policy compliance intentions?"

*H_0*6a: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to positive attitudes towards information security policy compliance behaviors.

*H_1*6a: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to positive attitudes towards information security policy compliance behaviors.

*H_0*6b: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to positive subjective norms towards information security policy compliance behaviors.

*H_1*6b: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to positive subjective norms towards information security policy compliance behaviors.

*H_0*6c: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to positive perceptions regarding behavioral control over compliance with information security policies.

*H_1*6c: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to positive perceptions regarding behavioral control over compliance with information security policies.

*H_0*7a: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to a stronger perceived goal-oriented organizational culture.

$H_1$7a: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to a stronger perceived goal-oriented organizational culture.

$H_0$7b: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to a stronger perceived rule-oriented organizational culture.

$H_1$7b: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to a stronger perceived rule-oriented organizational culture.

Research Question 2 and Supporting Hypotheses

RQ 2: “Do organizational cultural values positively influence employee security policy intentions?”

$H_0$1a: A positive attitude towards information security policy compliance will not lead to a stronger intent to comply with the organization’s security policies.

$H_1$1a: A positive attitude towards information security policy compliance will lead to a stronger intent to comply with the organization’s security policies.

$H_0$1b: A positive subjective norm about information security policy compliance will not lead to positive security policy compliance behavioral intentions.

$H_1$1b: A positive subjective norm about information security policy compliance will lead to positive security policy compliance behavioral intentions.

$H_0$1c: Increased positivity related to control over information security policy compliance will not lead to positive behavioral intentions regarding information security policy compliance behaviors.

$H_1$1c: Increased positivity related to control over information security policy compliance will lead to positive behavioral intentions regarding information security policy compliance behaviors.

$H_0$2a: Stronger perceived goal orientation as a cultural value does not lead to positive attitudes towards information security policy compliance.

$H_1$2a: Stronger perceived goal orientation as a cultural value leads to positive attitudes towards information security policy compliance.

$H_0$2b: Stronger perceived goal orientation as a cultural value does not lead to positive subjective norms regarding information security compliance behaviors.

$H_1$2b: Stronger perceived goal orientation as a cultural value leads to positive subjective norms regarding information security compliance behaviors.

$H_0$2c: Stronger perceived goal orientation as a cultural value does not lead to increased perceived behavioral control regarding security compliance behaviors.

$H_1$2c: Stronger perceived goal orientation as a cultural value does lead to increased perceived behavioral control regarding compliance behaviors.

$H_0$3a: Stronger perceived rule orientation as a cultural value does not lead to positive attitudes regarding information security compliance behaviors.

$H_1$3a: Stronger perceived rule orientation as a cultural value leads to positive attitudes regarding information security compliance behaviors.

$H_0$3b: Stronger perceived rule orientation as a cultural value does not lead to positive subjective norms regarding information security compliance behaviors.

$H_1$3b: Stronger perceived rule orientation as a cultural value leads to positive subjective norms regarding information security compliance behaviors.

$H_0$3c: Stronger perceived rule orientation as a cultural value does not lead to positive subjective norms regarding information security compliance behaviors.

$H_1$3c: Stronger perceived rule orientation as a cultural value leads to positive subjective norms regarding information security compliance behaviors.

$H_0$4: Stronger perceived goal orientation as an organizational cultural value does not lead to stronger information security policy compliance intentions.

$H_1$4: Stronger perceived goal orientation as an organizational cultural value leads to stronger information security policy compliance intentions.

$H_0$5: Stronger perceived rule orientation as an organizational cultural value does not lead to stronger information security policy compliance intentions.

$H_1$5: Stronger perceived rule orientation as an organizational cultural value leads to stronger information security policy compliance intentions.

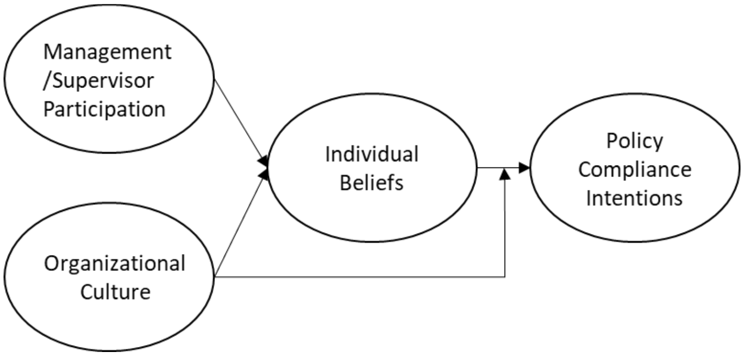
Research Design

This study utilizes a single-stage, non-experimental, survey-based research design that examines the relationships between organizational culture, management/supervisor participation, and an employee’s security policy compliance intentions. The theory of planned behavior is the central theoretical model used in the research design. Previous studies that examine information security in a behavioral context have used the theory of planned behavior (Lebek et al., 2014).

Augmenting the theory of planned behavior are the constructs of management participation, goal-oriented behavior, and rule-oriented behavior. Goal-oriented and rule-oriented behavioral elements are drawn from the competing values framework initially developed by Quinn and Rohrbaugh (1983). In a later research paper, the model developed by Quinn and Rohrbaugh (1983) was reinterpreted by Van Muijen et al. (1999). Hu et al. (2012) stated the Van Muijen et al. (1999) interpretation made the extraction and integration of the organizational culture constructs a more straightforward proposition to manage, given the need to integrate multiple theoretical frameworks.

Figure 2

Research Model Constructs


Management /Supervisor Participation
Organizational Culture
Individual Beliefs
Policy Compliance Intentions

Note. Adapted from "Managing compliance with information security policies: The critical role of top management and organizational culture" by Q. Hu, T. Dinev, P. Hart, and D. Cooke, 2012, Journal of Decision Sciences, 43(4), p. 622. Copyright 2012 by Journal of Decision Sciences. Adapted with permission.

Within the constructs shown in Figure 2, there is one dependent variable and six independent variables. The variables that support the construct model are listed in Table 1.

Table 1

Identification of Dependent and Independent Variables

Variables	Meaning	IV/DV
PMP	Perceived Management Participation	Independent
PGO	Perceived Goal Orientation	Independent
PRO	Perceived Rule Orientation	Independent
PBC	Perceived Behavioral Control	Independent
SN	Subjective Norms	Independent
ATT	Attitude Towards Behavior	Independent
INT	Behavioral Intention	Dependent

The variables of perceived behavioral control, subjective norms, and attitude towards behavior are the principal variables incorporated in the theory of planned behavior (Ajzen, 1991). Perceived goal orientation and perceived rule orientation are variables directly related to measuring organizational culture, as Van Muijen et al. (1999) described. Perceived management participation measures the employee’s perception of management/supervisor behaviors and actions in facilitating and supporting organizational outcomes related to information security policies and associated compliance behaviors (Hu et al., 2012; Liang et al., 2007).

The utilization of a survey-based instrument to collect the data has been widely used in information security behavioral studies (Warkentin et al., 2011). The utilization of a survey as the primary data collection method also has the advantage of reducing the amount of time needed to collect data while also expanding the pool of potential study participants (Ward et al., 2012). In his reflections on the theory of planned behavior and its contribution to social science research, Ajzen (2011) describes the importance of the role played by survey-based instruments in the theory's use over time. For these reasons, a survey-based approach using the variables and constructs described is the most appropriate approach to collect the data needed to support the study.

Target Population and Sample

These sections describe the population for this study and the sampling strategy utilized for selecting potential study participants. The target population's characteristics are defined, followed by the sampling strategy and elements, including the participation criteria. The last section will describe the power analysis calculation and the sample size needed for the study's findings to be statistically valid.

Population

According to the United States Census Bureau, the North American Industry Classification System is the standard used by federal agencies to classify businesses to support the collection and analysis of statistical data related to the U.S. economy (United States Census Bureau, 2017). The North American Industry Classification System Association figures published for November 2019 showed approximately 16,833 companies in the United States with over 1,000 employees (NAICS Association, 2020).

The principal population uses a computer in their day-to-day activities. They are not part of the organization's information management or technical support functions. To ensure that participant attitudes and behaviors would not be adversely influenced due to specific responsibilities associated with information technology positions, study participants could not have management or supervisory responsibilities. In their earlier study, Hu et al. (2012) noted the effect of top management participation was marginal. A possible reason cited for this outcome was the hierarchical distance between top management and employees (Hu et al., 2012); it was not explicitly tested. When considering other influencing factors such as the potential for a non-homogeneous culture and the observation by Hu et al. (2012) regarding hierarchical distance, it was a concept that could be further explored in this study’s context. For this reason, organizations with more than 1,000 employees were explicitly targeted. They are large enough to have a degree of hierarchical distance between top management and employees, increasing the emphasis on the manager/supervisor relationship.

Sample

The sample selection is an essential consideration as studying this smaller group supports learning more about the larger group from which the sample is drawn. This principle only holds if the sample is appropriately representative of the broader population (Vogt, 2007). Supporting the sample population selection is a set of selection criteria intended to ensure the sample is representative. The selection criteria, comprised of inclusion and exclusion boundary conditions, establish a baseline to support the sample selection process. The inclusion criteria for this study required potential participants to meet the following requirements:

- Participants must be based in the United States.
- Participants must be older than 18 years.
- Participants must be employed in a company with more than 1,000 employees.
- Participants must use a computer in their day-to-day work.
- Participants must have at least one level of management between the CEO and base employees.

- The participant’s organization must have a documented information security policy.
- The participant must be aware of and have knowledge of the organization’s information security policy.

Supporting the inclusion criteria is a set of exclusion criteria. The exclusion criteria are designed to ensure that participants that are not representative of the broader population are excluded from the study. The following are the exclusion criteria used to eliminate potential participants from the study:

- Participants working outside of the United States were excluded.
- Participants working in management or supervisory positions were excluded.
- Participants that work in the information technology or information security teams within the organization were excluded.
- Participants that did not have direct knowledge of the organization’s information security policy were excluded.
- Participants that did not use a computer in day-to-day work were excluded.
- Participants that were younger than 18 years were excluded.
- Participants whose organizations did not have a documented information security policy were excluded.
- Participants that did not work for a large organization and did not have at least one intermediate layer of management between themselves and the CEO were excluded.

The inclusion and exclusion criteria were designed to ensure the sample was representative of the broader employee population of interest. Using the inclusion and exclusion criteria as a sample frame, the professional survey company Qualtrics was engaged to recruit and screen study participants.

Supporting the sample frame, further organizational and demographic information was captured from participants to develop a deeper understanding of the sample’s other characteristics. Data was collected on the participant’s age, gender, the term of employment, level of education, industry sector, and whether the organization was publicly (listed on the stock exchange) or privately held. A probability sampling approach, random sampling, was used for this study as it supports the generalization of results back to the broader population (Trochim, 2006).

Power Analysis

Estimating the sample size for structural equation models is not a straightforward proposition, and in the past, various heuristic rules were applied when estimating sample sizes (Wolf et al., 2013). Heuristic rules, such as the sample size being at least ten times the maximum number of connections to a latent variable (Hair et al., 2017), have been widely used, but this can lead to inaccurately estimated sample sizes (Wolf et al., 2013). In a study that examined structural equation model sample sizes in information system studies, Westland (2010) noted a significant trend of selecting insufficient sample sizes for structural equation models. Specifically, a meta-analysis review of articles published in five prominent information systems journals found that 80% of the reviewed studies’ conclusions were based on insufficient sample sizes (Westland, 2010). While extremely useful, software packages such as G*Power are unsuitable for power analysis calculations for structural equation models due to their dependence on less complex analytic methods (Schoemann et al., 2017). Because of the difficulty of accurately calculating sample sizes using conventional tools such as G*Power, a different approach to calculating the required sample size was needed.

Muthén and Muthén (2002) examined sample sizes for structural models, proposing a Monte Carlo study to calculate the required sample size. The proposed use of Monte Carlo studies was based on its ability to accommodate various factors such as the model's dimensions, the number of variables, missing data, variable reliability, and the relationship between variables (Muthén & Muthén, 2002). Subsequent studies by Wolf et al. (2013) and Schoemann et al. (2017) also supported the proposition of using Monte Carlo studies for estimating sample sizes. The difficulty with using Monte Carlo studies is their complexity. Schoemann et al. (2017) noted this in their observation regarding the lack of the method's adoption, the limited number of available tools, and computational time burden.

Research by Kock and Hadaya (2018) examined sample size estimation in partial least squares modeling; it tested and validated an alternative approach to the use of Monte Carlo studies. The described approach uses two mathematical equations: the inverse square-root method and the gamma-exponential method (Kock & Hadaya, 2018). Testing these mathematical equations against three Monte Carlo experiments, Kock and Hadaya (2018) found they are sufficiently precise to avoid errors associated with sample size estimation as estimates will always be slightly above the actual minimum required. Faizan et al. (2018) supported the approach developed by Kock and Hadaya (2018) when assessing the use and application of partial least squares structural equation modeling in hospitality research. The detailed design of this validated approach for estimating sample sizes in structural equation models is why it is used to calculate the a priori sample size for this study.

The software used to estimate the sample size is the structural equation modeling analysis software WarpPLS 6.0. The inverse square-root and gamma-exponential equations produce different minimum sample sizes. The inverse square-root equation produced a minimum sample size of 279; the gamma-exponential equation produced a minimum sample size of 261. According to Kock and Hadaya (2018), the inverse square-root calculation provides greater certainty for an a priori sample size calculation because of its tendency to marginally overestimate the required minimum. For this reason, the minimum sample size for this study is 279 participants. The calculation is based on a confidence level of .95 and a significance level of .05. The minimum absolute significant path coefficient in the model is .197, a default path coefficient used in the software for a priori sample size estimates. Kock and Hadaya (2018) state this level is an acceptable estimate as it is effectively double the minimum acceptable effect size of .2. This minimum acceptable effect size is described in the seminal paper by Cohen (1992) on statistical power analysis and its relevance to behavioral sciences research.

Procedures

This section will describe the procedures used to support the conduct of the study. The methods used to select the participants will be examined first. It will be followed by the processes used to protect the participants' interests, followed by the procedures used to collect the survey data on which this study is based. The last element of this section will describe the methods used to analyze the collected data to test the related hypotheses.

Participant Selection

The participant selection commenced with defining essential information such as the minimum sample size, identifying the sample population, identifying the sample frame, and defining the participation criteria. The professional survey firm Qualtrics was engaged to support the study. Qualtrics provided assurances that willing participants who were representative of the target population could be readily identified due to their ability to reach significant numbers of potential candidates. The use of a professional organization such as Qualtrics also provided a high level of confidence that the screening and informed consent process would be rigorously applied.

The candidate sampling process was facilitated by Qualtrics using a random sampling methodology. Of the sampling methods, random sampling has the lowest probability of bias, and its results are more likely to be generalizable (Sekaran & Bougie, 2013). The study inclusion and exclusion criteria were given to Qualtrics, enabling them to assess the probability of delivering the required number of completed survey responses. On receipt of the requested number of completed responses and the inclusion and exclusion criteria, Qualtrics confirmed their screening and recruitment process would support the study.

The participants' recruitment was initiated by email, with Qualtrics sending an email to potential candidates with the approved explanatory information regarding the study and a link to the survey. Qualtrics hosted the survey. Before publication to candidate participants, Qualtrics allowed the researcher to test the survey's operation to ensure the informed consent and screening functions were working correctly. Once validated, Qualtrics distributed the invitational email to potential candidates from the target population. Once a candidate provided their informed consent and successfully passed through the screening questionnaire, they were directed to the survey.

Data Collection

The data collection process was directly facilitated by Qualtrics using their survey engine. The calculated minimum number of completed responses needed for this study was 279. To ensure there were no issues with achieving the required statistical power level, Qualtrics was engaged to collect a minimum of 400 completed responses. Leveraging their extensive pool of candidate participants, Qualtrics distributed invitational emails to candidate participants with the approved study information. Information provided to candidates included explaining the study's purpose and contact details if the candidate had questions. Once candidates had completed the informed consent and screening process, they became study participants. Participants were directed to the survey instrument, where they were asked to complete 23 questions using a 5-point Likert scale to record their responses.

Data Analysis

The survey responses were analyzed using the SmartPLS software package version 3.2.8 (Ringle et al., 2015). The software is specifically designed to support the analysis of structural models using partial least squares. The structural model is built within the software, with its graphical representation essentially identical to that in Figure 1. Recorded survey data is then attributed to each of the variables, completing the model.

When assessing the structural model, several key criteria must be examined. These criteria include the model's predictive ability (R^2) and the significance of the measured path coefficients (Hair et al., 2017). The model's predictive relevance or the model's ability to reconstruct observed values is also examined (Chin, 2010). Also used to assess the model's results are the recorded confidence intervals and the t-statistic values, which act as a significance indicator (Peng & Lai, 2012). As partial least squares is based on the use of a structural model and the relationships between variables, the size, and significance of the path coefficients and the coefficients of determination (R^2) are the primary evaluation criteria of interest (Hair et al., 2019). The enhanced reporting functions inherent to the software supported a detailed analysis of the data without using secondary analysis tools. The results ensured the relationship of the results to the hypotheses could be tested and validated, consequently supporting the central questions' investigation.

Instruments

This study used a single survey instrument to collect data on organizational culture, management participation, and the individual's perspectives on security policy compliance using the elements described in the theory of planned behavior. Developed by Hu et al. (2012), the instrument is a composite of instruments used in prior studies. The following sections provide a more detailed explanation of the instrument's foundations and the validation process.

Management and Organizational Culture Survey Instrument

The principal data collection instrument for this study is a survey instrument originally developed by Hu et al. (2012) for their research that examined top management participation and organizational culture in the context of information security policy compliance. Permission to use and republish the instrument for this study was obtained from a coauthor of the Hu et al. (2012) research paper. The instrument is a composite of survey questions used in previous studies that examined specific behavioral aspects of individual behaviors that were contextually relevant.

Survey questions focused on understanding behavioral intentions, attitudes towards behaviors, subjective norms, and perceived behavioral control were adapted from previously validated survey instruments developed by Taylor and Todd (1995) and Pavlou and Fygenson (2006). The research by Taylor and Todd (1995) examined two variants of the theory of planned behavior and the technology acceptance model to determine which was a better predictor of information technology usage. Pavlou and Fygenson (2006) conducted a longitudinal study into e-commerce using the theory of planned behavior as its theoretical basis to confirm the theory’s predictive power. Drawing on the validated instruments developed for these previous studies, Hu et al. (2012) adapted the relevant questions to capture information on attitudes, subjective norms, perceived behavioral controls, and behavioral intentions described by the theory of planned behavior.

To capture relevant information regarding organizational culture, Hu et al. (2012) adapted survey questions focused on goal and rule orientation from a previous study conducted by Van Muijen et al. (1999). The questionnaire developed by Van Muijen et al. (1999) was initially designed to study organizational culture. It was based on the competing values model developed by Quinn and Rohrbaugh (1983); it was subsequently validated by an international research group comprised of researchers from 12 different countries. The survey question that examines management participation’s role was adapted from a study by Liang et al. (2007). The study by Liang et al. (2007) investigated the assimilation of systems into organizations and the effect of management sponsorship assimilation activities.

The survey instrument developed by Hu et al. (2012) was appropriate for this study as it enabled information to be captured regarding an individual’s behavioral intentions, organizational culture, and management participation. The only modification needed to ensure the survey instrument was appropriately focused for this study was adjusting the management definition. The study by Hu et al. (2012) focused was on top management participation. In this study, the focus is on the influence of the employee’s immediate manager or supervisor. Altering the definition of management ensured the questions were interpreted with the appropriate context without changing the validated instrument’s integrity. The use of a single instrument was also advantageous as it aided in avoiding validity and reliability risks that might otherwise befall a researcher with a limited degree of experience in conducting quantitative studies.

Instrument Validity

The validity of the instrument was tested using a combination of content and construct validity. Content validity is the degree to which the survey questions will capture information that will enable the construct elements to be measured (Straub et al., 2004). As the measure is ordinarily based on judgment, it is typically assessed by relevant experts that are not part of the study, for example, a panel arrangement (Vogt, 2007). There are also quantitative measures that yield statistical information (correlations) that support the review process (Vogt, 2007).

In their study, Taylor and Todd (1995) used a panel to establish the relevance of questions against the study’s constructs. This process’s output was then pilot tested to validate further the instrument (Taylor & Todd, 1995). Pavlou and Fygenson (2006) used statistical indicators in their study to test whether an aggregate latent factor was highly correlated with the theory of planned behavior constructs. Their review indicated that the content for the perceived behavioral control construct was being captured as intended (Pavlou & Fygenson, 2006). The survey instrument developed by Van Muijen et al. (1999) as part of a study that examined organizational culture was somewhat unique. The study's primary purpose was to create an instrument that would accurately capture data on organizational culture. The study used a combination of an international panel of experts supported by statistical data to assess the developed instrument's validity (Van Muijen et al., 1999). The study by Liang et al. (2007) utilized a panel of experts to assess content validity, with adjustments made to measurement scales to reflect the study's Chinese cultural context. Hu et al. (2012) state that the question of content is principally addressed by using material drawn from previously validated instruments. Noting the measures undertaken to validate the content of the survey instruments from which Hu et al. (2012) adapted the survey questions, this appears to be a reasonable position.

Construct validity is a measure of how well the instrument measures the constructs of interest, and it is measured using a combination of convergent and discriminant validity (Vogt, 2007). Convergent validity is the extent to which multiple attempts to measure the same item are aligned, and discriminate validity is the extent to which measured items are unique (Bagozzi et al., 1991). Convergent validity is demonstrated when *t*-values of model loadings are statistically significant (Gefen & Straub, 2005). Hu et al. (2012) showed that all *t*-value loadings for each construct were significant at $p < .01$.

Discriminant validity is determined by the weakness of the correlation between constructs, except for the construct it is associated with (Gefen & Straub, 2005). Discriminant validity is tested using the average extracted variance (AVE) value by checking it is larger than the correlation value between constructs (Gefen & Straub, 2005). The approach to validating discriminant validity is to check the cross-loadings of indicators; the value of the outer values should be higher than any of the cross-loading values (Hair et al., 2017). For each indicator in the survey instrument, the outer value exceeded any of the cross-loading values (Hu et al., 2012), demonstrating the instrument has reasonable discriminant validity.

Instrument Reliability

The two principal reliability measures are Cronbach's alpha and composite reliability (Hair et al., 2017). Composite reliability is interpreted similarly to Cronbach's alpha, and according to Hair et al. (2017), it is a more reliable measure for partial least squares models. Cronbach's alpha assumes that all indicators have equal loadings whereas partial least squares order indicators based on reliability (Hair et al., 2017). A study by Peterson and Kim (2013) calls into question the supposed advantage of composite reliability over Cronbach's alpha; the paper does not dispute acceptable minimum reliability thresholds.

The lowest value of Cronbach's alpha recorded by Hu et al. (2012) was .675, and the lowest composite reliability value recorded was .862. Bagozzi and Yi (2012) state that while there is no universally accepted value for composite reliability, .70 or greater is a satisfactory value to ensure a reasonable level of reliability. Hair et al. (2017) state that composite reliability values of between .60 and .70 are acceptable. The Cronbach's alpha and composite reliability values indicate a reasonable level of reliability for the survey instrument.

Ethical Considerations

A critical element of a researcher's formative education is understanding the importance of ethics in research and the need to safeguard participants for current and future research projects. Capella University ensures that researchers learn the importance of ethical research while also implementing procedural measures to support researchers and protect study participants. Consequentially, researchers are introduced to the *Belmont Report* (National Commission, 1979). The *Belmont Report* summarizes the ethical guidelines and principles for research involving people as study participants and is an essential ethical guide for human-centric research.

The principles described in the *Belmont Report* are:

- The respect for persons and their right to make autonomous decisions, and the protection of those individuals who have a diminished degree of autonomy.
- Persons are treated ethically by respecting their decisions, protecting them from harm, and safeguarding their wellbeing.
- Justice, which requires equity in distribution and the fair treatment of persons.

A paper by Miracle (2016) on the application of these principles provided further guidance as to how they can be practically applied in a research setting. Ensuring people have the adequate and correct information, the appropriate use of informed consent, and the use of considered inclusion and exclusion criteria (Miracle, 2016) are all practical measures that can be applied that support the *Belmont Report's* ethical pillars. The measures described by Miracle (2016) were used to protect participants in this study.

Protection of Participants

The protection of participants is a critical consideration for this study. It also ensures that future research efforts are not compromised due to a negative participant experience. Participant protection in this study was essential as participants were asked to explicitly declare whether they may have had an intention to ignore or breach their organization's information security policy. Study participants were able to withdraw from the survey at any point in the process to ensure participation was entirely voluntary.

Qualtrics were asked to anonymize all survey responses, removing all information that could potentially lead to the participant's identification. Before the data was made available to the researcher, names, email addresses, logical (IP) address information, and any other personally identifiable information were removed. Per this study's submission to the University's Institutional Review Board, the recovered survey responses have been held in a secure format on removable media. Access to the raw survey data is controlled directly by the researcher. The only data stored on a network (Internet) connected device was survey responses that have been cleansed and coded to enable uploading to the SmartPLS analysis software used for this study.

Summary

This chapter explained the methodology used for this study. The purpose of the study was described, supported by the research questions and the associated hypotheses. The research design illustrated the relationships between the constructs and the target population's selection, and the sample frame was explored. A central element of the study is the survey instrument. The survey instrument's reliability and validity have been described, including the means used to assess the instrument's characteristics. As a final and essential element, two sections detailed the ethical considerations of this study and the measures to protect participants. This study's methodology and approach have been established; the next chapter will examine the study's results.

CHAPTER 4. RESULTS

The focus of this chapter is the review and analysis of the collected data. This chapter will describe the data sample, including the size and statistical power of the sample and information such as organizational and participant demographics to understand the sample coverage better. This chapter will also explore the survey instrument, including quality measures that support the instrument's ability to provide meaningful analytical results. This chapter's last element analyzes the data relating to the research questions and the associated hypotheses and summarizes the analysis results.

Background

This study explores how organizational culture and an employee's immediate manager's attitudes towards information security may influence an employee's security policy compliance intentions. This study's problem statement is reflected in the study's purpose; the purpose is reflected in the two primary research questions, which are, in turn, supported by seven hypotheses. The hypotheses are intended to test the presence and strength of the relationships between the elements of management participation, organizational culture, and an individual's policy compliance intentions.

The survey instrument was originally developed and validated by Hu et al. (2012). The survey instrument developed by Hu et al. (2012) comprises questions drawn from other independently validated survey instruments used in several previous studies. Hu et al. (2012) utilized accepted measures to validate the composite instrument independently, and this survey has been used unchanged in this study. The survey instrument used a 5-point Likert scale to collect data on the model's constructs. In conjunction with the model data, supporting demographic data were also collected, including a participant's age and gender, employment, and employer characteristics. The data has been anonymized to protect the survey participants. The data is also presented where the data sets cannot be correlated to build a profile of an individual.

Description of the Sample

The software package WarpPLS 6.0 was used to calculate the required sample size. The inverse square-root equation used by the software package aids in avoiding the sample sufficiency issue described by Westland (2010), where past studies have relied on insufficient sizes. Kock and Hadaya (2018) stated that using this equation to calculate the required sample size provides greater certainty due to its tendency to slightly overestimate the minimum necessary sample size. This study's minimum sample size to achieve a confidence level of .95 and a significance level of .05 was 279 completed responses.

The sample data is comprised of 420 completed survey responses, with all responses suitable for analysis. The survey data was collected by Qualtrics using the survey instrument provided by the researcher. A total of 400 completed responses was requested to ensure the data sample size exceeded the minimum of 279 completed responses needed to achieve the required statistical power. Qualtrics returned a higher number of completed responses than requested, and all have been included in the study's data set.

As part of the survey, a range of demographic data was collected from each survey participant. The demographic data served a dual purpose of ensuring participants aligned with the study's target demographic and provided further insights into the cross-section of market sectors and types of organizations where the participants are employed. Information regarding a participant's age, gender, job type, level of education, and work experience was collected. Data on the organization's size (number of employees), market sector, whether they have more than one location in the United States, and whether they are a public or private organization was also collected.

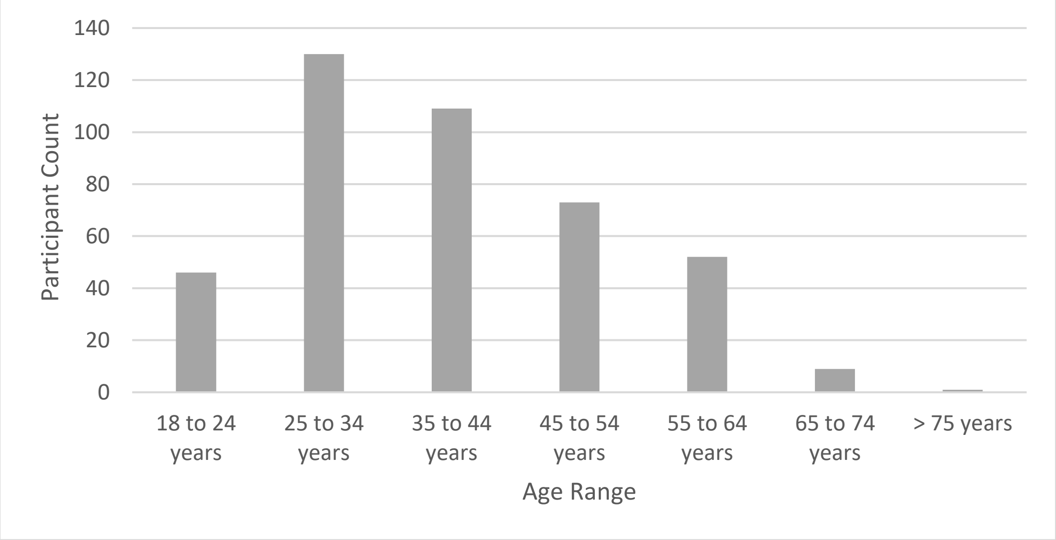
The demographic data, including the organizational demographic data, supports statistical testing to see whether any of these characteristics play a role in influencing an individual's behavioral intentions. Except for the industry sector information, each of these elements has been tested and analyzed to establish whether there is a statistically observable effect or play no role in influencing an individual's behavioral intentions.

Personal Demographic Characteristics

Information on several personal characteristics was collected as part of the survey once participants successfully passed through the initial screen questions. Unexpectedly, the gender of the survey participants was evenly split with exactly 210 male and 210 female participants. The participants' age was also captured, with several options given to provide greater granularity.

Figure 3

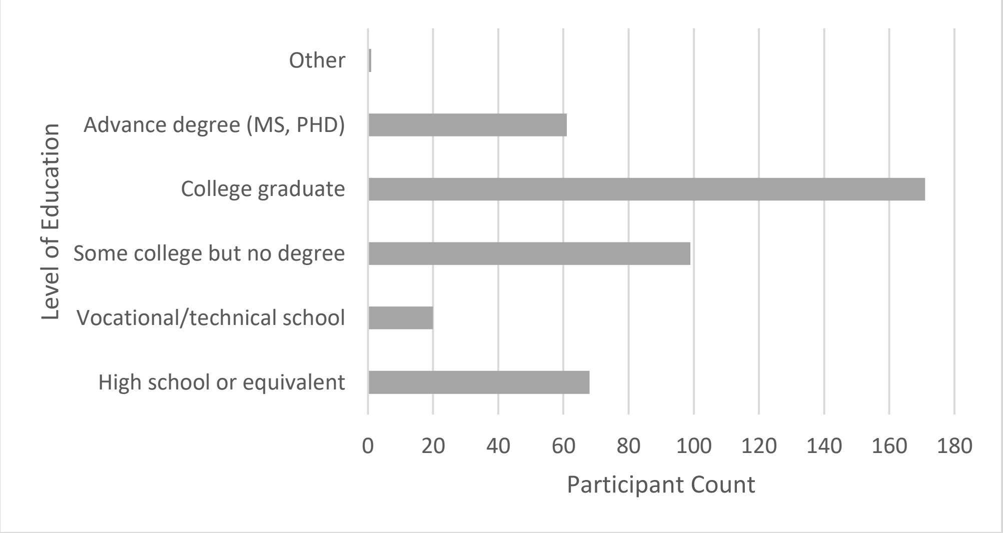
Age of Participants



The survey provided participants with seven different options to nominate their age bracket. The survey participants' distribution is mainly concentrated in the 25 to 44-year age bracket, with approximately 57% falling into this grouping.

Figure 4

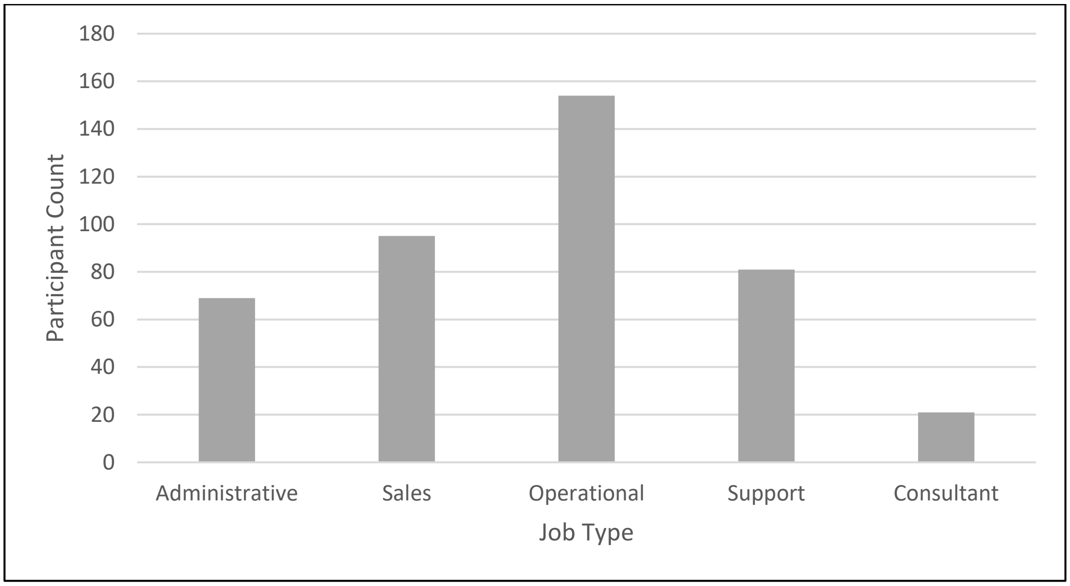
Level of Education of Participants



Survey participants were asked to nominate their completed level of education. The data shows most participants have completed some form of higher education, with approximately 55.2% of participants stating they have completed a college or an advanced degree. The next most significant group is those participants having completed some college but without awarding a degree. The smaller percentage of participants shown as having attended a vocational or technical school is interesting, given how many participants identified as being in operationally focused roles.

Figure 5

Job Type of Participants

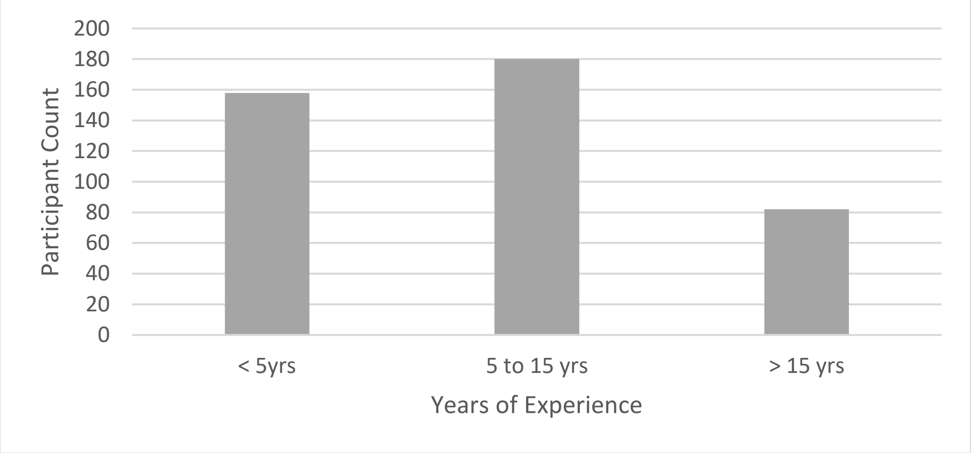


Participants were given five categories to nominate their job type. The category with the highest representation was the operational category, with 36.7% selecting this as their job type. This category could incorporate various positions within an organization, including back and front office positions and field-based roles. The significant number of participants nominating this category as being descriptive of their role may result from the category descriptor's inherent ambiguity.

The final individual characteristic captured as part of the demographic data collection was the length of experience in the participant's current role.

Figure 6

Participant Years of Experience



The most significant percentage of participants, 80.5%, fall within the category of fewer than five years and up to fifteen years of experience.

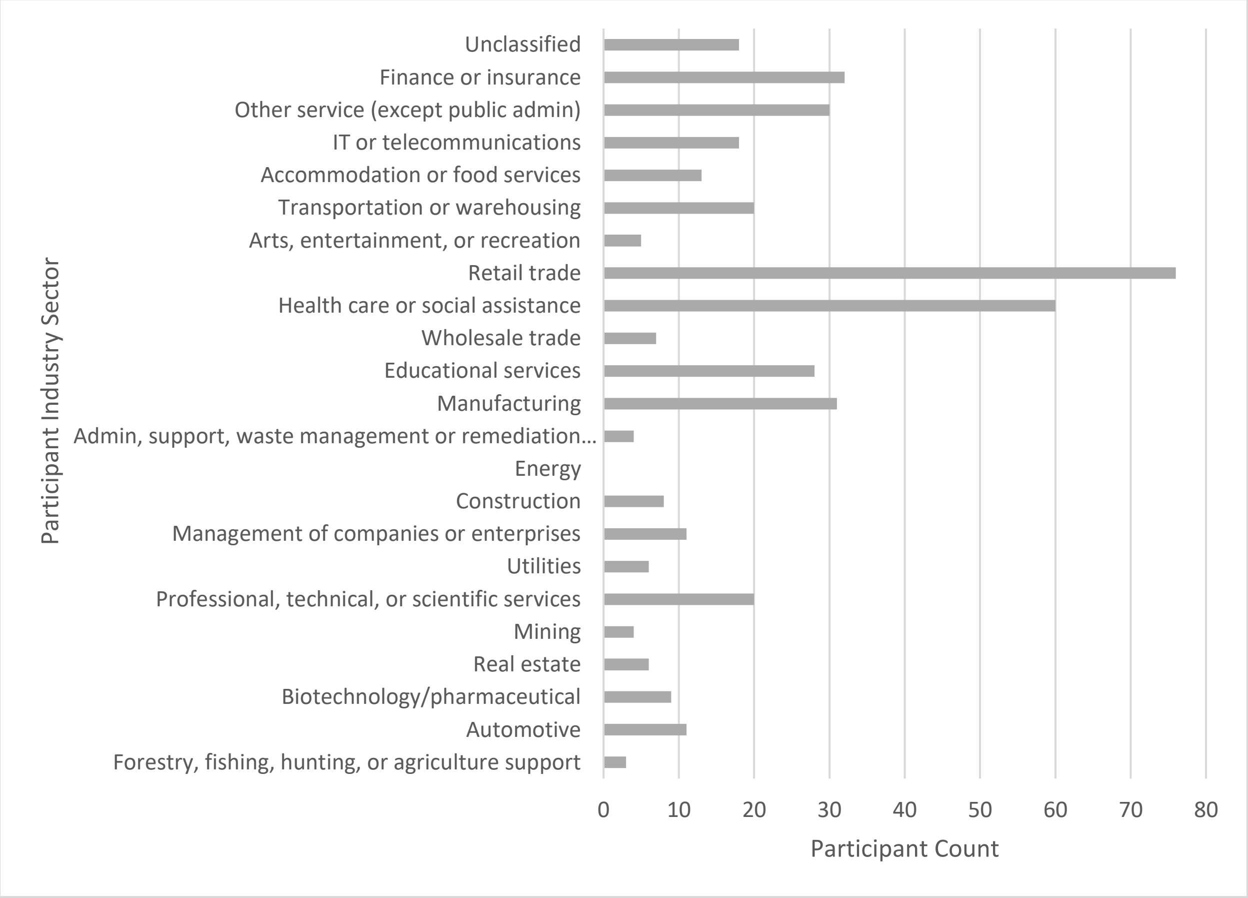
Organization Demographics

The survey asked participants several demographic questions regarding their employer. Information requested included the industry sector, how many locations the organization has, the number of employees, and whether it was a public (e.g., traded) organization or privately held. The data provide insights into the broader composition of the survey participants and identifies any sector concentrations; the question regarding the organization's industry sector used 23 distinct categories to capture the requested data.

Figure 7 illustrates the range of industry sectors captured in the survey data. The only listed industry sector that recorded no participants was the energy sector. Other industry sectors such as waste management and remediation, wholesale trade, forestry, real estate, biotechnology, and the arts had low numbers of participants. Specific industry sectors were not targeted as part of the sample criteria. While some industry sectors had lower participant rates, the diversity of industry sectors that did participate was an unexpected but positive outcome.

Figure 7

Participant Industry Sectors



Survey participants were asked to identify whether their organization has multiple locations or a single location. As seen in Table 2, a small number of survey participants were unable to answer this question.

Table 2

Number of Organization Locations

Company locations	Count
Only one location	39
More than one location	376
Do not know	5

Most participant organizations, approximately 89.5%, were identified as having more than one location in the United States. While this criterion was not specified as a survey screening criterion, having participants from many organizations with more than one location is positive. Considered in conjunction with the number of employees, it gives a sense of its size and scale.

The remaining organizational categories survey participants were asked to provide data for was the number of employees and whether the organization was a public or private entity. A demographic criterion specified as part of the data collection specification was those survey participants should come from organizations with more than 1,000 employees. It was a criterion because of a consideration mentioned by Hu et al. (2012) concerning the dimensions of an organization and the potential effect of hierarchical distance. As this study is focused on the effects of participation by the lower tiers of management, larger organizations create an opportunity to explore the issue of hierarchical distance in greater detail. The data captured regarding whether an organization is a public or private entity provides another context to test whether this influences an individual's behavioral intentions.

Of the 420 survey participants, 180 stated their organization has between 1,000 and 4,999 employees. The remaining 240 survey participants stated their organization has more than 5,000 employees. Securing survey participants from larger organizations was a positive outcome. Larger organizations logically create more significant opportunities for hierarchical distance, and a prerequisite for survey participants was that they had no staff management responsibilities. The survey participants also identified 162 of their organizations as private organizations, with the remaining 258 identified as publicly held.

The number of completed survey responses exceeded the minimum number required to achieve the desired statistical power level by a reasonable margin. The sample's demographic information for individual participants and their associated organizations provides important contextual information that illustrates the sample's randomness. The demographic data also enables attributes such as age, experience, job type, education, gender, and company status to be used as control variables. Using this information as a set of control variables will enable a better understanding of any latent factors that may or may not contribute to the analysis results.

Model Quality Indicators

When evaluating a model's measurement quality, there are several statistical tests established in the published literature. These tests provide a statistical basis to assess the model's internal consistency, discriminant validity, convergent validity, and predictive relevance.

Internal consistency is a check to ensure all items measure the same phenomenon (Petter et al., 2007). When evaluating internal consistency, Cronbach's alpha is one measure used to assess the consistency of summated rating scales (Vaske et al., 2017). The value of Cronbach's alpha should be equal to or greater than .708 and less than .95 as a value that exceeds .95 is an indication of indicator redundancy (Hair et al., 2019). While Cronbach's alpha is a well-established and accepted test, there are known limitations associated with its ability to validate internal consistency conclusively. The test assumes that all items are standardized or equally reliable (Cho & Kim, 2014). The test is also sensitive to the number of items, leading to errors in calculated reliability (McNeish, 2018).

Table 3

Quality Indicators

Latent construct	Item	Outer loading	AVE	Composite reliability	Cronbach’s alpha
ATT	ATT1	.899	.802	.924	.876
	ATT2	.910			
	ATT3	.877			
DUT	DUT1	.927	.830	.936	.898
	DUT5	.892			
	DUT7	.914			
INT	INT1	.881	.777	.913	.857
	INT2	.886			
	INT3	.879			
PBC	PBC1	.884	.795	.921	.871
	PBC2	.907			
	PBC3	.884			
PGO	PGO2	.905	.796	.887	.745
	PGO3	.880			
PMMP	PMMP1	.890	.810	.928	.883
	PMMP2	.910			
	PMMP3	.900			
PRO	PRO1	.705	.668	.857	.752
	PRO2	.874			
	PRO3	.862			
SN	SN1	.908	.802	.924	.877
	SN2	.899			
	SN3	.880			

Note. ATT = attitude towards behavior; DUT = dutifulness; INT = behavioral intention; PBC = perceived behavioral control; PGO = perceived goal orientation; PMMP = perceived middle management participation; PRO = perceived rule orientation; SN = subjective norm.

A complementary test referred to as composite reliability is recommended to address these potential issues (Hair et al., 2017). Composite reliability is calculated by taking the weights from partial least squares calculations and using them in conjunction with factor analysis loadings to calculate a more accurate reliability estimate (Aguirre-Urreta et al., 2013).

Composite reliability is interpreted similarly to Cronbach’s alpha, with the preferred minimum value being equal to or greater than .70 (Garson, 2016). As shown in Table 3, the values for both Cronbach’s alpha and composite reliability exceed the minimum threshold value of .70, indicating the model has good internal consistency.

Convergent validity assesses the extent to which an indicator positively correlates to other indicators in the same construct (Hair et al., 2017). Convergent validity is assessed by examining each indicator’s outer loadings’ values and the average variance extracted (AVE) for the construct (Hair et al., 2020). Measured values for indicator outer loadings should exceed .708, and the AVE value should be equal to or greater than .50 (Hair et al., 2017). The recorded values for the indicator outer loadings and AVE shown in Table 3 exceed the minimum thresholds, indicating the model has good convergent validity.

Discriminate validity measures a construct’s distinctiveness compared to the other constructs (Hair et al., 2017). Two measures established in the published literature to test for discriminate validity are indicator cross-loadings and the Fornell-Larcker criterion. An indicator’s cross-loading value should be greater than the comparative cross-loading of any other indicator (Garson, 2016). The results of the cross-loading analysis are shown in Table 4. The results show that each indicator’s cross-loading is greater than the comparable cross-loading from any other indicator, indicating good discriminate validity. The Fornell-Larker criterion is based on comparing each construct’s AVE’s square root, which should be greater than the correlation with any other construct (Garson, 2016). The Fornell-Larker criterion test results show each construct’s correlation is more significant than the highest correlation with any other construct, indicating good discriminant validity (Table 5).

Table 4

Indicator Cross Loadings

Item	ATT	DUT	INT	PBC	PGO	PMMP	PRO	SN
ATT1	**.899**	.670	.698	.646	.370	.544	.300	.710
ATT2	**.910**	.650	.680	.702	.378	.516	.344	.719
ATT3	**.877**	.676	.687	.667	.367	.486	.315	.740
DUT1	.681	**.927**	.776	.591	.356	.427	.377	.675
DUT5	.638	**.892**	.685	.578	.378	.421	.371	.610
DUT7	.709	**.914**	.792	.641	.390	.417	.385	.685
INT1	.655	.698	**.881**	0.711	.400	.485	.369	.697
INT2	.649	.676	**.886**	.643	.369	.460	.356	.636
INT3	.724	0.806	**.879**	.650	.370	.479	.391	.684
PBC1	.712	.629	.709	**.884**	.377	.521	355	.721
PBC2	.669	.591	.678	**.907**	.410	.523	.368	.691
PBC3	.623	.550	.638	**.884**	.413	.534	.338	.640
PGO2	.418	.412	.418	.421	**.908**	.395	.683	.409
PGO3	.318	.316	.347	.377	**.880**	.440	.638	.357
PMMP1	.499	.402	.486	.506	.378	**.890**	.425	.521
PMMP2	.517	.394	.453	.530	.414	**.910**	.438	.500
PMMP3	.537	.449	.514	.555	.463	**.900**	.446	.578
PRO1	.207	.215	.243	.214	.460	.341	**.705**	.253
PRO2	.362	.441	.426	.385	.642	.424	**.874**	.391
PRO3	.284	.323	.340	.348	.691	.420	**.862**	.316
SN1	.741	.661	.698	.705	.381	.512	.349	**.908**
SN2	.704	.634	.687	.685	.404	.532	.374	**.899**
SN3	.723	.646	.666	.672	.371	.550	.349	**.880**

Note. Indicator cross-loadings are in boldface. ATT = attitude towards behavior; DUT = dutifulness; INT = behavioral intention; PBC = perceived behavioral control; PGO = perceived goal orientation; PMMP = perceived middle management participation; PRO = perceived rule orientation; SN = subjective norm.

Table 5

Fornell-Larcker Criterion Analysis

Construct	ATT	DUT	INT	PBC	PGO	PMMP	PRO	SN
ATT	**.896**							
DUT	.743	**.911**						
INT	.769	.827	**.882**					
PBC	.750	.663	.758	**.892**				
PGO	.415	.411	.431	.448	**.892**			
PMMP	.576	.462	.539	.590	.466	**.900**		
PRO	.357	.414	.423	.397	.741	.485	**.818**	
SN	.807	.722	.764	.768	.430	.593	.399	**.896**

Note. Construct correlations are in boldface. ATT = attitude towards behavior; DUT = dutifulness; INT = behavioral intention; PBC = perceived behavioral control; PGO = perceived goal orientation; PMMP = perceived middle management participation; PRO = perceived rule orientation; SN = subjective norm.

The final quality test of the model is Stone-Geisser's Q^2 value. The Stone-Geisser test measures the model's predictive relevance or how well the model's observed values are reconstructed (Qazi et al., 2020). The evaluation criteria for the Stone-Geisser test are measured values for endogenous variables should be greater than zero (Kumar & Purani, 2018). Measured values greater than zero indicate the model has predictive relevance (Qazi et al., 2020). The results of the Stone-Geisser test are shown in Table 6. Measured results for each of the endogenous variables are greater than zero, indicating the model has good predictive relevance.

Table 6

Stone-Geisser Q^2 Test

Endogenous variables	Q^2 value
ATT	.285
INT	.594
PBC	.304
PGO	.172
PRO	.155
SN	.303

Note. ATT = attitude towards behavior; INT = behavioral intention; PBC = perceived behavioral control; PGO = perceived goal orientation; PRO = perceived rule orientation; SN = subjective norm.

The quality tests showed the model has good convergent and discriminant validity. The tests also showed the model has good internal consistency and predictive relevance. The model quality and validation test results indicate that any calculated results can be viewed and interpreted with a reasonable degree of confidence.

Hypothesis Testing

The analysis of the collected data uses partial least squares structural equation modeling. Developed initially by Wold (1974), the partial least squares algorithm has been broadly adopted by the social sciences for relationship modeling between variables because of its ability to support both explanatory and predictive modeling (Liengaard et al., 2020). Information systems research, including information security, is based on inquiry, identifying research problems and questions, and then developing models that enable further examination. Partial least squares path modeling is an effective approach for developing and operationalizing conceptual models, supporting its use in exploratory and confirmatory research (Benitez-Amado et al., 2017). The expanded use of partial least squares has been supported by an increase in the availability of specialist software tools (Wen-Lung et al., 2019) that support the analysis of conceptual models and the statistical tests needed to ensure results are reliable. Based on the published research, this study is consistent with the types of research identified as suitable for using partial least squares for analyzing the collected data.

The software tool used to conduct the partial least squares analysis was SmartPLS v.3.3.2 (Ringle et al., 2015). The research model illustrated in Figure 1 was built in the software, and the associated indicators were attached to the latent variables. The software indicates the model is ready for calculation when all latent variables have associated indicators, and all exogenous and endogenous variables are connected. Once the model has been successfully constructed, the next stage is to run the statistical tests designed to assess the model's quality and the collected data.

Structural Model Analysis

The structural model's path analysis using the SmartPLS software provides the data necessary to explore the research questions and the associated hypotheses. Several measurement parameters inform the interpretation of the output from SmartPLS and the evaluation of the results against the research questions and the related hypotheses. The value of R^2 is a measure of the endogenous variable's explanatory power (Hair et al., 2019). Values of R^2 fall between 0 and 1, with values closer to 1 indicating a higher level of explanatory power (Hair et al., 2019). The principle R^2 value of interest represents the model constructs' accumulated explanatory power for the dependent variable.

The R^2 value for the model was measured at .778 ($p \leq .001$), meaning the model explains 77.8% of the endogenous construct's variance (Figure 9). Values of R^2 above .75 are considered substantial (Hair et al., 2019), which is a positive indicator of the model's explanatory power. The detailed results of the path analysis are shown in Table 7. The table's hypotheses have been arranged to correspond to the order and structure of the research questions.

The *t*-statistic is a measure of statistical significance (Hair et al., 2017). Values of *t* that are greater than 1.96 are considered significant at a confidence level (*p*) of .05 (Garson, 2016). The *p*-value represents the likelihood that a null hypothesis will be incorrectly rejected (Field, 2013). The SmartPLS bootstrap process also produces confidence interval data. The confidence interval represents a range within which the actual population data will reside, assuming a certain level of confidence (Garson, 2016). For example, with a selected value of .05 (95%), confidence intervals will be displayed at 2.5% above (97.5%) and 2.5% below the nominated confidence level. For this study, the value used to calculate the confidence intervals is .05 (95%). A confidence interval of 95% is a typical value that provides good coverage of the population's parameters (Aguirre-Urreta & Rönkkö, 2018; Cousineau, 2017). When interpreting confidence interval data, the critical element for consideration is the presence of zero. For example, if the confidence interval values do not include (cross) zero, the coefficient is assumed to be statistically significant, and the hypothesis is accepted (Kock, 2016).

Path model coefficients (B) represent the hypothesized or inferred relationship between the respective constructs (Bagozzi & Yi, 2012). Values fall between -1 and 1. Unlike other measures, there is no threshold value as they are inferred statistics with values closer to 1 equating to a stronger positive relationship and -1 a negative relationship (Hair et al., 2017). The other threshold value hurdles for *p* and *t* must first be cleared for a path coefficient to be considered regarding a hypothesis.

Table 7

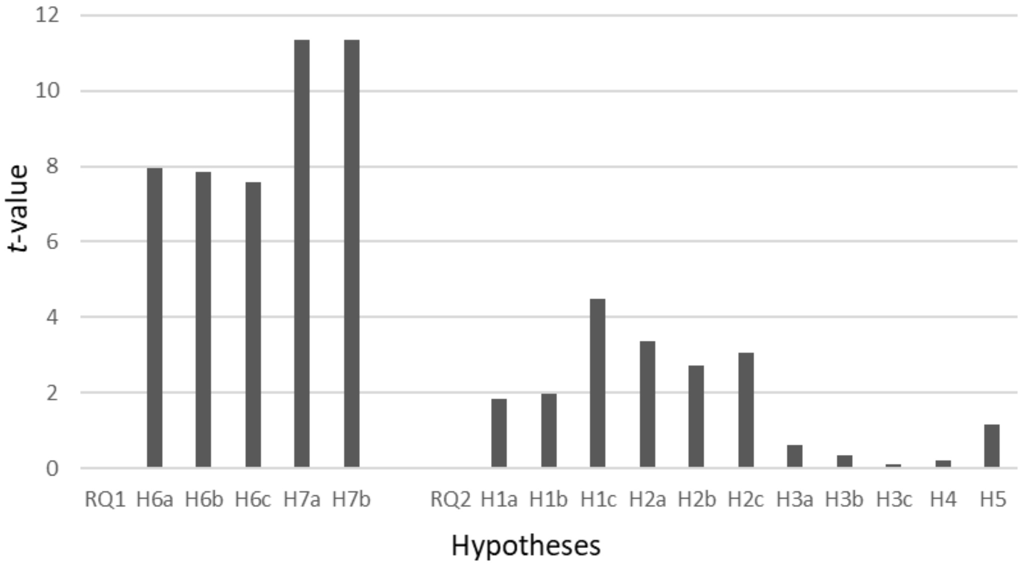
Path Model Analysis

Hypothesis		Path coefficient (B)	Confidence interval		*t*-statistic	*p*-value
			2.5%	97.5%		
RQ1						
H6a	PMMP -> ATT	.496	.369	.612	7.945	< .001
H6b	PMMP -> SN	.498	.368	.617	7.853	< .001
H6c	PMMP -> PBC	.488	.356	.606	7.579	< .001
H7a	PMMP -> PGO	.466	.380	.542	11.342	< .001
H7b	PMMP -> PRO	.485	.393	.562	11.343	< .001
RQ2						
H1a	ATT -> INT	.127	-.013	.260	1.835	.067
H1b	SN -> INT	.120	-.003	.234	1.969	.049
H1c	PBC -> INT	.247	.141	.355	4.493	< .001
H2a	PGO -> ATT	.216	.085	.337	3.357	< .001
H2b	PGO -> SN	.181	.049	.307	2.716	< .05
H2c	PGO -> PBC	.226	.083	.369	3.075	< .05
H3a	PRO -> ATT	-.043	-.185	.092	.617	.537
H3b	PRO -> SN	.024	-.117	.156	0.341	.733
H3c	PRO -> PBC	-.007	-.152	.135	.096	.924
H4	PGO -> INT	-.009	-.084	.079	.226	.821
H5	PRO -> INT	.045	-.033	.118	1.175	.240

Note. ATT = attitude towards behavior; DUT = dutifulness; INT = behavioral intention; PBC = perceived behavioral control; PGO = perceived goal orientation; PMMP = perceived middle management participation; PRO = perceived rule orientation; SN = subjective norm.

Figure 8

Hypotheses t-values



*H*₀1a: A positive attitude towards information security policy compliance will not lead to a stronger intent to comply with the organization's security policies.

*H*₁1a: A positive attitude towards information security policy compliance will lead to a stronger intent to comply with the organization's security policies.

For hypothesis *H*1a, *t* < 1.96, *p* > .05, and the confidence interval includes zero, all of which indicate the result is not significant. Therefore, the null hypothesis *H*₀1a is not rejected.

*H*₀1b: A positive subjective norm about information security policy compliance will not lead to positive security policy compliance behavioral intentions.

*H*₁1b: A positive subjective norm about information security policy compliance will lead to positive security policy compliance behavioral intentions.

For *H*1b, the *t*-statistic is marginally greater than 1.96 (*t* = 1.969) and *p* = .049, placing the result on acceptance threshold. However, the confidence interval includes zero (95% CI [-

.003, .234]), which indicates the result is not significant. Therefore, the null hypothesis $H_0$1b is not rejected.

$H_0$1c: Increased positivity related to control over information security policy compliance will not lead to positive behavioral intentions regarding information security policy compliance behaviors.

$H_1$1c: Increased positivity related to control over information security policy compliance will lead to positive behavioral intentions regarding information security policy compliance behaviors.

The *t*-statistic, *p*-value, and confidence intervals for *H*1c are significant. The path coefficient B of .247 indicates a positive relationship between perceived behavioral control and behavioral intentions. Therefore, the null hypothesis $H_0$1c is rejected.

$H_0$2a: Stronger perceived goal orientation as a cultural value does not lead to positive attitudes towards information security policy compliance.

$H_1$2a: Stronger perceived goal orientation as a cultural value leads to positive attitudes towards information security policy compliance.

The *t*-statistic, *p*-value, and confidence intervals for *H*2a are significant. The path coefficient B = .216 indicates a positive relationship between perceived goal orientation and positive attitudes towards compliance. Therefore, the null hypothesis $H_0$2a is rejected.

$H_0$2b: Stronger perceived goal orientation as a cultural value does not lead to positive subjective norms regarding information security compliance behaviors.

$H_1$2b: Stronger perceived goal orientation as a cultural value leads to positive subjective norms regarding information security compliance behaviors.

The *t*-statistic, *p*-value, and confidence intervals for *H*2b are significant. The path coefficient B = .181 indicates a positive relationship between perceived goal orientation and subjective norms. Therefore, the null hypothesis $H_0$2b is rejected.

$H_0$2c: Stronger perceived goal orientation as a cultural value does not lead to increased perceived behavioral control regarding security compliance behaviors.

$H_1$2c: Stronger perceived goal orientation as a cultural value does lead to increased perceived behavioral control regarding compliance behaviors.

The *t*-statistic, *p*-value, and confidence intervals for *H*2c are significant. The path coefficient B = .226 indicates a positive relationship between perceived goal orientation and perceived behavioral control. Therefore, the null hypothesis $H_0$2c is rejected.

$H_0$3a: Stronger perceived rule orientation as a cultural value does not lead to positive attitudes regarding information security compliance behaviors.

$H_1$3a: Stronger perceived rule orientation as a cultural value leads to positive attitudes regarding information security compliance behaviors.

For hypothesis H3a, $t < 1.96$ ($t = .617$), $p > .05$ ($p = .537$), and the confidence interval includes zero (CI [-.185, .092]), all of which indicate the result is not significant. Therefore, the null hypothesis $H_0$3a is not rejected.

$H_0$3b: Stronger perceived rule orientation as a cultural value does not lead to positive subjective norms regarding information security compliance behaviors.

$H_1$3b: Stronger perceived rule orientation as a cultural value leads to positive subjective norms regarding information security compliance behaviors.

For hypothesis H3b, the $t < 1.96$ ($t = .341$), $p > .05$ ($p = .733$), and the confidence interval includes zero (CI [-.117, .156]), all of which indicate the result is not significant. Therefore, the null hypothesis $H_0$3b is not rejected.

$H_0$3c: Stronger perceived rule orientation as a cultural value does not lead to positive subjective norms regarding information security compliance behaviors.

$H_1$3c: Stronger perceived rule orientation as a cultural value leads to positive subjective norms regarding information security compliance behaviors.

For hypothesis H3c, $t < 1.96$ ($t = .096$), $p > .05$ ($p = .924$), and the confidence interval includes zero (CI [-.152, .135]), all of which indicate the result is not significant. Therefore, the null hypothesis $H_0$3c is not rejected.

$H_0$4: Stronger perceived goal orientation as an organizational cultural value does not lead to stronger information security policy compliance intentions.

$H_1$4: Stronger perceived goal orientation as an organizational cultural value leads to stronger information security policy compliance intentions.

For hypothesis H4, $t < 1.96$ ($t = .226$), $p > .05$ ($p = .821$), and the confidence interval includes zero (CI [-.084, .079]), all of which indicate the result is not significant. Therefore, the null hypothesis $H_0$4 is not rejected.

$H_0$5: Stronger perceived rule orientation as an organizational cultural value does not lead to stronger information security policy compliance intentions.

$H_1$5: Stronger perceived rule orientation as an organizational cultural value leads to stronger information security policy compliance intentions.

For hypothesis $H5$, $t < 1.96$ ($t = 1.175$), $p > .05$ ($p = .240$), and the confidence interval includes zero (CI [-.033, .118]), all of which indicate the result is not significant. Therefore, the null hypothesis $H_0 5$ is not rejected.

$H_0 6$a: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to positive attitudes towards information security policy compliance behaviors.

$H_1 6$a: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to positive attitudes towards information security policy compliance behaviors.

The *t*-statistic, *p*-value, and confidence intervals for $H6$a are significant. The path coefficient B = .496 indicates a positive relationship between perceived middle management participation and the attitude towards policy compliance behaviors. Therefore, the null hypothesis $H_0 6$a is rejected.

$H_0 6$b: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to positive subjective norms towards information security policy compliance behaviors.

$H_1 6$b: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to positive subjective norms towards information security policy compliance behaviors.

The *t*-statistic, *p*-value, and confidence intervals for $H6$b are significant. The path coefficient B = .498 indicates a positive relationship between perceived middle management participation in information security initiatives and subjective norms. Therefore, the null hypothesis $H_0$6b is rejected.

$H_0$6c: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to positive perceptions regarding behavioral control over compliance with information security policies.

$H_1$6c: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to positive perceptions regarding behavioral control over compliance with information security policies.

The *t*-statistic, *p*-value, and confidence intervals for *H*6c are significant. The path coefficient B = .488 indicates a positive relationship between perceived middle management participation and perceived behavioral control. Therefore, the null hypothesis $H_0$6c is rejected.

$H_0$7a: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to a stronger perceived goal-oriented organizational culture.

$H_1$7a: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to a stronger perceived goal-oriented organizational culture.

The *t*-statistic, *p*-value, and confidence intervals for *H*7a are significant. The path coefficient B = .466 indicates a positive relationship between middle management participation in information security management and initiatives, leading to a stronger perceived goal-oriented organizational culture. Therefore, the null hypothesis $H_0$7a is rejected.

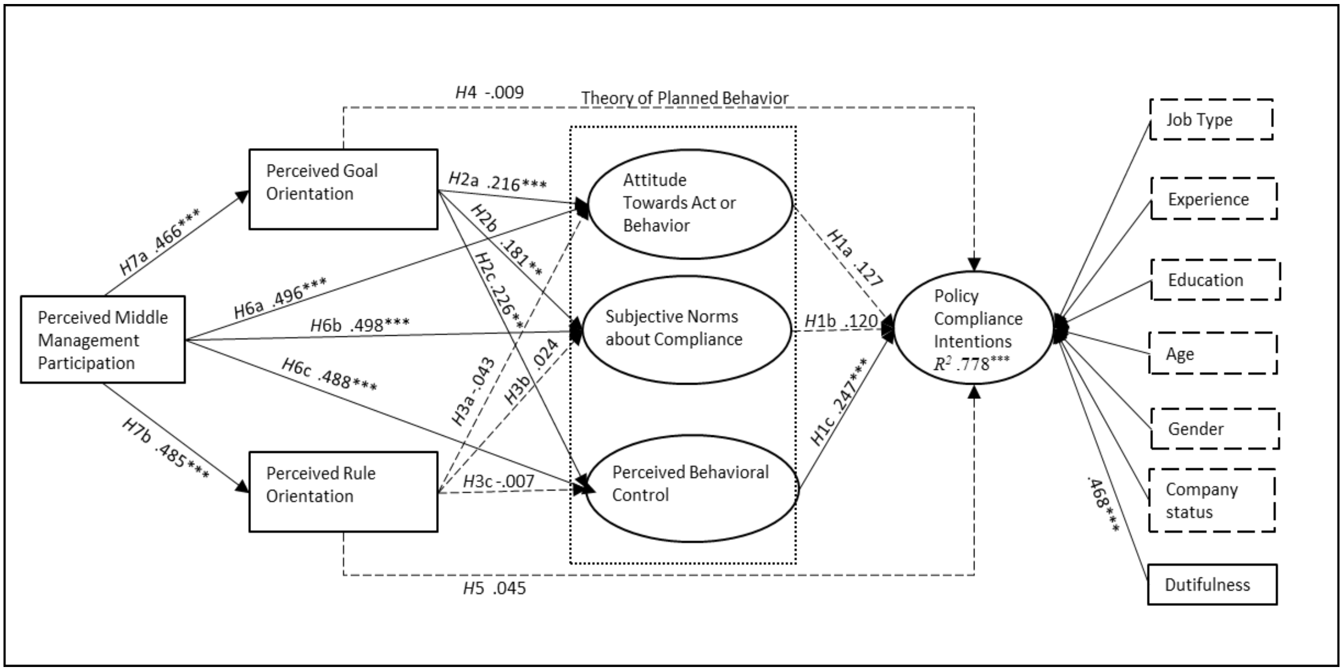
H$_0$7b: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives do not lead to a stronger perceived rule-oriented organizational culture.

H$_1$7b: Positive perceptions regarding middle management/supervisor participation in information security management and initiatives lead to a stronger perceived rule-oriented organizational culture.

The *t*-statistic, *p*-value, and confidence intervals for *H*7b are significant. The path coefficient B = .485 indicates a positive relationship between perceived middle management participation in information security management and initiatives and the development of a rule-oriented culture. Therefore, the null hypothesis *H*$_0$7b is rejected.

Figure 9

Hypotheses Path Coefficients


H4 -.009
Theory of Planned Behavior
Perceived Goal Orientation
H2a .216***
H2b .181**
H2c .226**
Attitude Towards Act or Behavior
H1a .127
H7a .466***
H6a .496***
H6b .498***
H6c .488***
Perceived Middle Management Participation
Subjective Norms about Compliance
H1b .120
Policy Compliance Intentions
R^2 .778***
H3a .043
H3b .024
H1c .247***
H7b .485***
Perceived Rule Orientation
H3c -.007
Perceived Behavioral Control
H5 .045
Job Type
Experience
Education
Age
Gender
Company status
Dutifulness
.468***

Note: Dotted lines represent nonsignificant relations; solid lines represent significant paths.
**p < .05. ***p < .001.

As part of the research model, several variables were added as controls. These control variables were considered to see if they played a role in influencing a participant's behavioral intentions (INT) towards complying with their organization's information security policy. Attributes including job type, age, gender, experience, education, and whether the company was publicly or privately held were all examined. The results of the analysis are shown in Table 8.

Table 8

Control Variables

Control variables	Path coefficient (B)	Confidence interval		*t*-statistic	*p*-value
		2.50%	97.50%		
Gender -> INT	-.028	-.073	.018	1.194	.233
Company status -> INT	-.001	-.046	.043	.064	.949
Experience -> INT	.014	-.036	.057	.582	.561
Age -> INT	-.016	-.073	.049	.496	.620
Job type -> INT	.053	-.059	.121	1.101	.271
Education -> INT	.008	-.031	.068	.304	.761

Note. INT = behavioral intention.

The results in Table 8 show that none of the control variables are statistically significant. The *t* and *p* values fall outside the accepted significance thresholds, and the B values for all variables are close to zero, indicating a very weak positive or negative relationship.

SmartPLS has the capability of reporting the model's total effects on endogenous variables. The report calculates all endogenous variables' total direct and indirect effects, and the results are shown in Table 9.

Table 9

Total Effect on Endogenous Variables

Constructs	Path coefficient (B)	Confidence interval		*t*-statistic	*p*-value
		2.5%	97.5%		
INT					
ATT -> INT	.127	-.010	.262	1.866	.062
SN -> INT	.120	-.004	.236	1.995	.046
PBC -> INT	.247	.135	.354	4.466	<.001
PGO -> INT	.095	.003	.197	1.918	.055
PRO -> INT	.040	-.058	.132	.847	.397
PMMP -> INT	.307	.227	.391	7.296	<.001
DUT -> INT	.468	.338	.599	6.975	<.001
ATT					
PGO -> ATT	.216	.085	.337	3.343	<.001
PRO -> ATT	-.043	-.179	.093	.625	.532
PMMP -> ATT	.576	.491	.651	14.562	<.001
SN					
PGO -> SN	.181	.048	.308	2.709	< .05
PMMP -> SN	.593	.510	.669	14.902	<.001
PRO -> SN	.024	-.118	.158	.347	.729
PBC					
PGO -> PBC	.226	.080	.370	3.090	< .05
PRO -> PBC	-.007	-.157	.139	.096	.923
PMMP -> PBC	.590	.507	.665	14.596	<.001
PGO					
PMMP -> PGO	.466	.380	.541	11.130	<.001
PMMP -> PRO	.485	.395	.563	11.400	<.001

Note. ATT = attitude towards behavior; DUT = dutifulness; INT = behavioral intention; PBC = perceived behavioral control; PGO = perceived goal orientation; PMMP = perceived middle management participation; PRO = perceived rule orientation; SN = subjective norm.

The total effects report does not alter the outcome of any of the tested hypotheses. It does calculate the value of two additional effects: the direct effect of dutifulness (DUT -> INT) and the indirect effect of perceived middle management participation on behavioral intentions (PMMP -> INT). The path coefficient value for perceived middle management participation effect on an individual's behavioral intention is statistically significant at *p* < .001. The path coefficient value of B = .307 indicates a reasonably strong positive correlation between perceived middle management participation and an individual's security policy compliance intentions. The other additional calculation is the effect of dutifulness on an individual's behavioral intentions. This path coefficient is also statistically significant at $p < .001$. The path coefficient value of B = .468 indicates a strong positive correlation between an individual's sense of duty, described in the survey instrument conscientiousness, and their behavioral intentions regarding security policy compliance.

Summary

This study explored the effects of perceived middle management participation and organizational culture on an individual's security policy compliance intentions. The research questions and associated hypotheses informed the development of the research model, designed to explore each construct's role on an individual's behavioral intentions. The survey instrument used for the study was originally developed and validated by Hu et al. (2012), with the only change made being the definition of management. A total of 420 responses were utilized for the statistical analysis. The software package SmartPLS was used to validate the model's quality and analyze the participant responses. The model's internal consistency, convergent and discriminate validity, and predictive relevance were validated within established thresholds.

An evaluation of the path model and the relationships between the dependent and independent variables showed that several hypotheses were supported, and several were not. The path modeling showed that perceived middle management participation positively affects an individual's attitudes towards compliance, perceived behavioral control, and subjective norms. The analysis also showed that perceived middle management participation positively affected the organizational culture elements of perceived goal orientation and perceived rule orientation. An individual's attitude towards compliance did not significantly affect their compliance intentions; subjective norms also did not affect compliance intentions. However, this assessment is based solely on the confidence intervals as, by any other measure, the null hypothesis would be rejected.

Table 10

Summary Data Analysis for All Hypotheses

Hypothesis		*t*-statistic	*p*-value	Supported?
RQ1				
H6a	PMMP -> ATT	7.945	< .001	Yes
H6b	PMMP -> SN	7.853	< .001	Yes
H6c	PMMP -> PBC	7.579	< .001	Yes
H7a	PMMP -> PGO	11.342	< .001	Yes
H7b	PMMP -> PRO	11.343	< .001	Yes
RQ2				
H1a	ATT -> INT	1.835	.067	No
H1b	SN -> INT	1.969	.049	No
H1c	PBC -> INT	4.493	< .001	Yes
H2a	PGO -> ATT	3.357	< .001	Yes
H2b	PGO -> SN	2.716	< .05	Yes
H2c	PGO -> PBC	3.075	< .05	Yes
H3a	PRO -> ATT	.617	.537	No
H3b	PRO -> SN	0.341	.733	No
H3c	PRO -> PBC	.096	.924	No
H4	PGO -> INT	.226	.821	No
H5	PRO -> INT	1.175	.240	No

Note. ATT = attitude towards behavior; DUT = dutifulness; INT = behavioral intention; PBC = perceived behavioral control; PGO = perceived goal orientation; PMMP = perceived middle management participation; PRO = perceived rule orientation; SN = subjective norm.

An individual's perceptions regarding their ability to influence or control behavior (perceived behavioral control) affect their behavioral intentions. Perceived goal orientation, which encompasses performance indicators, rationality, accomplishment, and reward (Van

Muijen et al., 1999), positively affects an individual's attitudes, perceived behavioral control, and subject norms. Perceived rule orientation, which is hierarchical and emphasizes respect for authority, the division of work, and procedural rationality (Van Muijen et al., 1999), did not affect an individual's compliance intentions.

This chapter explored the research model and hypotheses from a statistical analysis perspective. The next chapter will explore the results in greater detail, the conclusions that can be drawn from the results, what the results may mean from a practical perspective, and the possibilities for future research to expand on this study.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

The focus of Chapter 4 was the statistical analysis of the collected data. In Chapter 5, the results of the research are discussed and explored in greater detail. The first section of this chapter will summarize the results of the data analysis. The second section is a more in-depth exploration and a discussion of the results and what they mean. The third section explores the findings that can be drawn from the study's results. This section is followed by a description of the study's limitations, implications for practice, and further research recommendations. The chapter is closed with the study's conclusion.

Summary of the Results

Background

The information security threat and risk environment are rapidly evolving, with organizations becoming exposed to a greater risk of experiencing a cyber incident. Major incidents, such as the Equifax breach that exposed the details of approximately 148 million consumers (Zhang et al., 2018), have brought the issue into sharper focus for organizations and the public. The increasing risk of cyber incidents has seen the information security market expand considerably, with estimates of global investment equaling $93 billion in 2018 (Zhang et al., 2018) and forecasts exceeding $124 billion in 2019 (Aitken, 2018). While investments in technical countermeasures play a critical role, the individual user, or insider, is also an essential element in an organization's security management approach (Stewart & Jürjens, 2017).

Numerous research papers identify the security risks posed by internal users (Heartfield & Loukas, 2018) due to their access to information and their ability to influence security outcomes. To mitigate the risk posed by internal users, organizations have developed and implemented extensive security policy structures. Security policies have been cited as a critical element of an organization's information security management approach (Safa, Von Solms, & Furnell, 2016). These policy structures describe acceptable and unacceptable behaviors and the associated disciplinary consequences to positively influence user behaviors (Flowerday & Tuyikeze, 2016). However, it has been noted that in some instances, employees will ignore or deliberately attempt to circumvent security policies, despite their supposed importance and the potentially negative personal and organizational consequences (D'Arcy & Lowry, 2019).

A substantial body of published research is based on cognitive-behavioral models primarily focused on an individual's behavioral responses (Lebek et al., 2014). Top management's role and its influence on an organization's security culture is also well established in the published literature (Barton et al., 2016). The aspect that has been somewhat overlooked is how these elements interact. Numerous studies assume that an organization's culture is top-down and homogeneous (D'Arcy & Greene, 2014; Goo et al., 2014). The role of information security sub-cultures has been identified as needing further investigation (Da Veiga & Martins, 2017).

Similarly, the relationship between an employee and their immediate manager in a security context is also potentially influential if the possibility of micro or sub-cultures is considered (Barton et al., 2016). A limited number of studies consider the role of supervisory influences on employee ethical behaviors (Sguera et al., 2018). While studies examine individual behaviors, management/supervisory influences, and organizational culture, these elements' net effect in a combination is still to be fully explored.

Results

This study focused on answering two research questions:

1. "Does management/supervisor participation in information security positively influence employee security policy compliance intentions?"
2. "Do organizational cultural values positively influence employee security policy compliance intentions?"

Research Question 1 is supported by two hypotheses that examined perceptions regarding middle management's involvement in security management initiatives and middle management's contribution to the organization's security culture. The hypotheses were tested using partial least squares structural equation modeling. This method of analysis enables the significance and relative strength of relationships to be measured. The results show that management/supervisor participation does positively influence an individual's compliance intentions. The *t*-statistic values and associated path coefficients (B) for management participation were the most significant in the model, with all associated null hypotheses rejected. Perceived middle management participation positively affected an individual's attitude towards a behavior, the subjective norms, and perceived behavioral control. Perceived middle management participation also positively affected the cultural elements of the perceived rule and perceived goal orientation.

Research Question 2 examined the role of organizational values and their influence on employee compliance intentions. Organizational culture was examined through the lens of two elements of the competing values framework: perceived goal and perceived rule orientation. Perceived rule orientation is principally focused on formal authority. It is based on a hierarchical power structure that is top-down and based on respect for authority, the rationality of procedures, and the division of work (Van Muijen et al., 1999). Perceived goal orientation has the principal elements of rationality, accomplishment, performance indicators, accountability, and contingent reward (Van Muijen et al., 1999).

The study results show that organizational cultural values positively influence employee compliance intentions. However, the influence is limited to the perceived goal orientation element of the cultural values framework. Perceived rule orientation had no significant effect on an individual's behavioral intentions. The *t*-statistic and *p*-values for all perceived rule orientation hypotheses were not significant, and the associated path coefficients (B) were also close to zero, indicating a minimal effect. In contrast, perceived goal orientation positively affects an individual's attitude towards a behavior, subjective norms, and perceived behavioral control. Perceived goal orientation did not directly affect an individual's behavioral intentions; its influence is related to factors that influence predicted behaviors.

Discussion of the Results

Seven hypotheses supported the research questions focusing on the effect of management participation and organizational culture. The seven hypotheses were tested using a model initially developed by Hu et al. (2012), with the principle modification being the change to focus on an individual's immediate manager's role.

The first hypothesis examined the primary constructs that comprise the theory of planned behavior (Ajzen, 1985). The theory of planned behavior is well established in the published literature, with the model having been extensively tested in numerous studies (D'Arcy & Lowry, 2019). The hypotheses examined the relationship of an individual's attitude towards a behavior, the effect of subjective norms, and an individual's perceived behavioral control in the context of the intent to comply with their organization's information security policies. The results showed that an individual's attitude and the subjective norms did not significantly affect behavioral intentions; perceived behavioral control did have a positive effect. While this may appear to raise questions regarding the applicability of the theory of planned behavior's constructs, the results do not necessarily support this perspective. The *t*-statistic and *p*-values for both the attitude and subjective norms were very close to being statistically significant. In the case of subjective norms, only the confidence intervals resulted in the null hypothesis not being rejected.

The second hypothesis examined an element of the organizational culture measure, perceived goal orientation, on an individual's attitude, subjective norms, and perceived behavioral control. For all three constructs, perceived goal orientation had a statistically significant positive effect. According to the competing values framework developed by Van Muijen et al. (1999), the results indicate survey participants have a greater focus on their accountabilities, and organizational goals, regarding security policy compliance intentions.

The third hypothesis examined the effect of the other organizational culture element, perceived rule orientation, on an individual's attitudes, subjective norms, and perceived behavioral control. Perceived rule orientation did not have a statistically significant effect on any of the three constructs. All had *p*-values above .50, with the highest *t*-statistic being .617, well below the 1.96 needed to be considered significant. The results indicate a rule-driven, top-down approach is unlikely to influence survey participants' compliance intentions substantively.

The fourth hypothesis examined the direct effect of perceived goal orientation on an individual's behavioral intentions. The results show there is no substantive direct effect on an individual's behavioral intentions. This result was replicated for the fifth hypothesis, which examined the direct effect of perceived rule orientation on behavioral intentions. This result was also not statistically significant, indicating that a top-down authoritative approach did not resonate with the survey participants.

The sixth and seventh hypotheses focused on examining the effect of perceived middle management participation. The sixth hypothesis examined the effect of perceived middle management participation on attitudes towards a behavior, subjective norms, and perceived behavioral control. The seventh hypothesis examined the effect of perceived middle management participation on perceived goal and perceived rule orientation. These results were the most significant, showing a strong relationship between middle management participation and the other elements.

The relative strength of the effect of perceived middle management participation indicates it is a factor in influencing an employee’s compliance behaviors. This perspective is supported by the results of the total effect shown in Table 9. While the direct effect of perceived middle management participation on an individual’s behavioral intentions was not the subject of a specific hypothesis, the analysis results show the effect is substantial. In the context of the first research question regarding the role of management/supervisor participation on an individual’s security policy compliance intentions, the data in Table 9 shows a significant indirect effect (B = .307, *t* = 7.296, *p* < .001).

Another observation is the effect of dutifulness on an individual’s compliance intentions. Included in the original study by Hu et al. (2012) as a control variable, the results in Table 9 show dutifulness has a statistically significant effect (B = .468, *t* = 6.975, *p* < .001) on behavioral intentions. The survey instrument characterizes dutifulness as acting conscientiously. The survey questions inquired about the participant’s approach to the completion of tasks and their reliability. Analogous to perceived goal orientation characteristics, assumptions can be drawn regarding their perspectives regarding their responsibility and accountability. The results indicate that an individual’s perceptions of their conscientiousness in approaching tasks influences their security policy compliance intentions.

Conclusions Based on the Results

The initial conclusion that can be drawn is that middle management participation can significantly influence an individual’s security policy compliance intentions. Previous studies by Goo et al. (2014) and Dang-Pham et al. (2017a) identified the influential role of an individual’s immediate manager as a behavioral reference and the role of interpersonal relationships at a local level. An individual’s direct manager’s relative significance in information security initiatives indicates that such participation has a tangible effect. It does not necessarily mean that such intentions are misaligned or negative. It does suggest an immediate manager’s views and behaviors are influential in shaping an employee’s behavioral intentions regarding complying with the organization’s security policies.

A further inference that can be drawn from the results is related to the presence of organizational micro-cultures. Prior studies by Barton et al. (2016) and Beautement et al. (2016) discussed the assumed homogeneity of organizational cultures and the bottom-up instead of top-down development of information security cultures. An individual’s immediate manager’s influence aligns with the concept of localized security culture, particularly when considering the potential hierarchical distance to a large organization’s top management structure.

When considering the role of organizational culture, the relationship between perceived goal and perceived rule orientation provided further insights into additional factors that potentially motivate an individual’s behavioral intentions. Based on the premise of an external hierarchical power structure, perceived rule orientation had no observable effect. Perceived goal orientation, which is premised on individual accountabilities, did factor into an individual’s responses. Supporting this position is the significance of an individual’s sense of duty reflected in the results. The results indicate that an individual’s policy compliance intentions are influenced more by their understanding of the organization’s goals and conscientiousness instead of formalized procedures and rules. It does not mean security policies do not guide the individual. Their willingness to follow such policies has a more significant relationship to their perspectives and their alignment to its objectives. Previous studies by Connolly et al. (2017) and Menard et al. (2017) have identified the positive effect of appealing to an individual’s intrinsic motivations and how organizational solidarity creates greater awareness of organizational goals. Other studies, such as the study by Warkentin, Johnston, Walden, et al. (2016) that examined individual responses to fear appeals using functional magnetic resonance imaging, noted that such appeals are not universally effective. The absence of a personal connection results in diminished effectiveness.

The overall findings of the study were varied. There is strong support for the effect of perceived middle management participation on security policy compliance intentions. Organizational culture, specifically perceived goal orientation, positively affected the theory of planned behavior constructs of attitude, subjective norms, and perceived behavioral control. However, except for perceived behavioral control, this influence did not have a flow-through effect on an individual’s policy compliance intentions. Perceived rule orientation, or the presence of a larger hierarchical and authority-based structure, also had no effect. In conjunction with perceived behavioral control, an individual’s compliance intentions were directly influenced by dutifulness and indirectly influenced by perceived middle management participation. The results indicate an individual’s policy compliance intentions are primarily driven by their immediate manager’s influence, in combination with their perceptions of behavioral control or self-efficacy, and individual responsibility and accountability.

Limitations

By its nature, research is unavoidably subject to some limitations. This study was a quantitative study based on individuals’ survey responses regarding their attitudes and behavioral intentions. A limitation of the study is the absence of any confirmation regarding actual behaviors. Actual behaviors may differ from stated behavioral intentions. In a paper reflecting on the theory of planned behavior, Ajzen (2011) cited studies that showed intentions are not always reliable predictors of actual behaviors, even over short periods. The absence of an experimental or observational element is a limitation of this study.

Due to its inherent complexity, reliably measuring organizational culture remains a challenge. In an earlier study, Hu et al. (2012) cite the complexities of measuring organizational culture as any particular cultural measurement framework imposes its limitations. Chatman and O’Reilly (2016) note that there is still no unified approach to understanding organizational culture despite academics and practitioners’ level of interest. Alternative cultural measurement models may yield different results. While this is a limitation, it may also be an avenue for future research.

The study was conducted entirely within the United States. While this may serve as a reasonable indicator for western cultures, there is no guarantee that different cross-cultural influences from other national cultures would produce similar results. Karyda (2017) noted limited research on the effect of national cultures on information security culture and that more research is needed to understand how national cultures influence individual security behaviors. While limiting the study to organizations within the United States was a practical consideration, it limits the understanding of national cross-cultural influences' potential effect.

The final limitation of the study is the limited sample size. While the number of responses exceeded the minimum number required by a reasonable margin, it is still limited when considered against the potential population. Restricting the sample size was a question of time, practicality, and cost. Future studies with larger sample sizes may reveal different results and influences regarding factors that influence security policy compliance intentions.

Implications for Practice

This study has several implications regarding its applicability to practice. Information security culture and policy compliance continue to be areas of interest for public and private sector entities. Research outcomes that add to the overall body of knowledge regarding practical approaches to encouraging positive employee security behaviors have more considerable organizational benefits. Research outcomes also enable organizations to understand better how to approach information security with their employees to make it both personally and organizationally relevant.

The study identified the role played by an individual's immediate manager in shaping their attitudes and likely behaviors towards information security policy compliance. It was evident in the measured direct effects and the indirect effect on compliance intentions. Appropriately engaged and mobilized, this cohort could be a significant asset in an organization's efforts to engage its employees and, consequentially, improve their overall security posture. Prior research by Menard et al. (2017) based on fear appeals identified the importance of making compliance efforts relevant to the individual. The study results suggest an individual's immediate manager's inherent capacity to create this bridge, given the relationship's influential nature.

An individual's manager's influence is also related to improving the understanding of how micro-cultures develop and the effect micro-cultures could have on information security initiatives and management. D'Arcy and Greene (2014) noted that organizational culture is more organic and localized in its development than being strictly top-down. Da Veiga and Martins (2017) described the concept of a dominant organizational culture and the formation of subcultures comprised of values shared by a smaller group of employees. Yazdanmehr and Wang (2016) noted that social norms grounded in personal interactions could become personal norms. These personal norms shape individual behaviors as they guide an individual's behavioral responses. A group dynamic that views information security from a positive perspective is more likely to engender positive security behaviors. Again, the contribution of an individual's immediate management towards shaping a positive local security culture could be substantial.

Another area with practical implications is the additional factors that motivate individual compliance intentions. Menard et al. (2017) stated that a more effective approach to achieving compliance was to appeal to an individual's intrinsic motivations. In their recent study, Cram et al. (2019) found the elements with the most significant overall effect size on compliance behaviors were centered on an individual's values. The highest relevant factors in explaining an individual's intentions were their attitudes, personal beliefs, ethics, and normative beliefs; all centered around their values (Cram et al., 2019). This perspective is supported in the study results. Survey participants were more responsive to organizational culture aspects that focused on rationality, accomplishment, and personal accountability. These results were additionally supported by the data regarding the strength of the relationship between dutifulness and compliance intentions. The practical implications are related to how an organization approaches security policy compliance. The results suggest a security policy compliance approach based primarily on enforcement and sanctions may have diminished effectiveness. Menard et al. (2017) examined user motivations and the protection of information, identifying the potential benefits of an alternative approach to stringent compliance. Menard et al. (2017) found approaches that focus on an individual's competence, autonomy, and relatedness, led to an increased motivation to protect information. Developing a security policy approach focused on engagement, making the outcomes relevant to the individual, and linking it to organizational outcomes and personal accountabilities may be more effective. It does not suggest that other models in the published literature are not relevant. Research such as that by Sommestad et al. (2014) and Cram et al. (2019) has shown the understanding of compliance predictors is still developing.

As a final consideration, organizations need to take a flexible, multifaceted approach to security policy compliance efforts and adjust based on the observed results. Gcaza et al. (2017) refer to information security culture as an ill-defined domain utilizing theories from other fields.

There are no agreed criteria for what constitutes a cybersecurity culture. The published research continues to evolve, and at this juncture, there is no single approach or methodology that guarantees a positive outcome. Organizations need to consider strategies that fit their operating context and acknowledge that a combination of factors is necessary for a comprehensive security program.

Recommendations for Further Research

There are several opportunities for further research related to this study. The relationship between an organization's dominant culture, group sub-cultures, and the effect on information security compliance is yet to be fully explored. The element of developing attitudes and expectations towards corporate responsibility and information security is also an area of opportunity. Employee expectations regarding issues such as management transparency and social interactions, if and how these translate to subjective norms, and their effect on compliance would better explain the role of an organization's culture. It may be particularly relevant for the newer generation of employees, where expectations potentially differ from later generations (Cram et al., 2016).

Further research could adopt a longitudinal approach in conjunction with point-in-time studies such as this research. Further research could also consider examining the effect of interventions and practices. This study identified factors that potentially influence employee compliance intentions. There is no subsequent stage that formulates possible approaches or interventions and tests these against employee responses. Siponen and Baskerville (2018) identified a shortfall in the application of information systems research. Studies identify applicable theories and describe results; however, the next step of translation to practice is missing. It leaves practitioners in a position where they cannot ascertain whether research outcomes are in practice, improving current industry practices (Siponen & Baskerville, 2018).

This study was focused on the United States, and while this may represent Western cultural responses, it does not address the possible effect of cross-cultural influences. Some information security compliance studies have been conducted in Asian population centers, but there is a significant gap when considering the global population (Crossler et al., 2013). Further research could expand the scope of national cultures included in studies to ascertain whether different national cultural influences affect employee compliance.

This study's sample population comprised individuals with no management responsibilities and no relationship to their organization's information technology or security groups. Further research could alter the sample population to assess the relationship between middle management and top management and its influence on security compliance. Another aspect regarding a potential sample population is the attitudes of contract or 'gig' workers to information security. The rapid restructuring of the labor market and the expanding reliance on contract resources essentially make these works insiders with access to potentially sensitive information (Churchill et al., 2019; Sharma & Warkentin, 2018). Understanding how this cohort views information security, given the lack of any firm connection to a single organization, and the associated cultural influences, may further insights into their intrinsic motivations.

Conclusion

After more than three decades of information security research, understanding security policy compliance is still evolving. There is no consensus regarding the factors that drive information security policy compliance and the role played by organizational culture (Connolly et al., 2017; Cram et al., 2019; Sommestad et al., 2014). This study contributes to the body of knowledge regarding security policy compliance by examining the relationship between middle management participation, organizational culture, and security policy compliance intentions.

This study utilized a quantitative, non-experimental approach based on the theory of planned behavior and elements of the competing values framework that were most relevant to the area of inquiry. The survey instrument originally developed and validated by Hu et al. (2012) incorporated measures that enabled the relationship between middle management participation, organizational culture, and security policy compliance intentions to be examined. The study found a significant positive relationship between middle management participation and an individual’s security policy compliance intentions. Consistent with the theory of planned behavior constructs, perceived middle management participation directly affected an individual’s behavioral attitudes, subjective norms, and perceived behavioral control. Perceived middle management participation also had a significant and positive indirect effect on an individual’s compliance intentions.

The study also found the organizational culture elements of perceived goal and perceived rule orientation did not significantly affect an individual’s policy compliance intentions. Perceived goal orientation did have a positive indirect effect on an individual’s sense of perceived behavioral control described by the theory of planned behavior. Dutifulness also had a significant positive relationship with compliance intentions. The measurement of organizational culture is a complex undertaking (Chatman & O’Reilly, 2016), and the use of a different measurement framework may provide further clarity in a future study.

The study confirmed that middle management participation is positively correlated with an individual's security policy compliance intentions from a broader perspective. The study also identified that compliance intentions were influenced by personal accountability and conscientiousness related to an individual's inherent values. The absence of a significant relationship with the hierarchical authority aspect of organizational culture provides further context regarding an individual's intrinsic motivation regarding policy compliance.

The practical implications of the study's findings indicate that adopting a hierarchical, authoritative approach to security policy compliance based primarily on the application of sanctions will be less effective than one that engages the individual. Articulating an organizational value proposition, making it personally relevant, and connecting it to an individual's contribution to the overall outcome may have a higher likelihood of success for compliance initiatives.

Questions are arising from this study that would benefit from further research. While some studies have positively linked organizational culture to security outcomes, other studies, including this one, have identified the relationship between organizational culture and information security as being unclear. The contribution of middle management was significant, but further research is needed to validate this finding. Overall, further research is required to enhance the understanding of policy compliance predictors and understand how this knowledge can be practically applied to improve information security outcomes.

REFERENCES

Accenture. (2019). *The Cost of Cybercrime: The ninth annual cost of cybercrime study*. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Aggarwal, V. K., & Reddie, A. W. (2018). Comparative industrial policy and cybersecurity: the US case. *Journal of Cyber Policy*, *3*(3), 445–466. https://doi.org/10.1080/23738871.2018.1551910

Aguirre-Urreta, M. I., Marakas, G. M., & Ellis, M. E. (2013). Measurement of composite reliability in research using partial least squares: Some issues and an alternative approach. *SIGMIS Database*, *44*(4), 11–43. https://doi.org/10.1145/2544415.2544417

Aguirre-Urreta, M. I., & Rönkkö, M. (2018). Statistical inference with PLSc using bootstrap confidence intervals. *MIS Quarterly*, *42*(3), 1001–1020. https://doi.org/10.25300/MISQ/2018/13587

Aitken, R. (2018, August 19). Global information security spending to exceed $124B in 2019, privacy concerns driving demand. *Forbes*. https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/#680b1e767112

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11–39). Springer. https://doi.org/10.1007/978-3-642-69746-3

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Ajzen, I., & Fishbein, M. (1973). Attitudinal and normative variables as predictors of specific behavior. In *Journal of Personality and Social Psychology* (Vol. 27, Issue 1, pp. 41–57). https://doi.org/10.1037/h0034440

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers and Security*, *26*(4), 276–289. https://doi.org/10.1016/j.cose.2006.11.004

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers and Security*, *28*(6), 476–490. https://doi.org/10.1016/j.cose.2009.01.003

AlHogail, A., & Mirza, A. (2014, January 17-19). *Information security culture: A definition and a literature review* [Paper presentation]. 2014 World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, Tunisia. https://doi.org/10.1109/WCCAIS.2014.6916579

Ali, A. (2017). Ransomware: A research and a personal case study of delaing with this nasty malware. *Issues in Informing Science & Information Technology*, *14*, 87–99. https://doi.org/10.1080/13880290490480167

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information and Computer Security*, *26*(1), 91–108. http://dx.doi.org/10.1108/ICS-09-2016-0073

Antwi, S., & Kasim, H. (2015). Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European Journal of Business and Management*, *7*(7), 217–225. https://www.researchgate.net/publication/295087782_Qualitative_and_Quantitative_Research_Paradigms_in_Business_Research_A_Philosophical_Reflection

Ashenden, D. (2018). In their own words: Employee attitudes towards information security. *Information and Computer Security*, *26*(3), 327–337. http://dx.doi.org/10.1108/ICS-04-2018-0042

Bagozzi, R. P., & Yi, Y. (2012). Specification, evaluation, and interpretation of structural equation models. *Journal of the Academy of Marketing Science. 40*(1), 8–34. http://dx.doi.org/10.1007/s11747-011-0278-x

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly*, *36*(3), 421-458. https://doi.org/10.2307/2393203

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuyzen, J. (2015). Achieving rigor in literature reviews: Insights from qualitative data analysis and tool-support. *Communications of the Association for Information Systems*, *37*(8), 154–204. https://doi.org/10.17705/1CAIS.03708

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don’t make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39, Part B*, 145–159. http://dx.doi.org/10.1016/j.cose.2013.05.006

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don’t even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 689–715. http://dx.doi.org/10.17705/1jais.00506

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. https://doi.org/10.1016/j.cose.2016.02.007

Bass, B. M., & Avolio, B. J. (1993). Transformational leadership and organizational culture. *Public Administration Quarterly*, *17*(1), 112-121. http://www.jstor.org/stable/40862298

Beautement, A., Becker, I., Parkin, S., Krol, K., & Sasse, A. (2016, June 22-24). *Productive security: A scalable methodology for analysing employee security behaviours* [Paper presentation]. Twelfth Symposium on Usable Privacy and Security\, Denver, CO, United States. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement

Beautement, A., & Sasse, A. (2009). The economics of user effort in information security. *Computer Fraud & Security*, *10*, 8–12. https://doi.org/10.1016/S1361-3723(09)70127-7

Benitez-Amado, J., Henseler, J., & Castillo, A. (2017, July 26-20). *Development and update of guidelines to perform and report partial least squares path modeling in information systems research* [Paper presentation]. 21st Asia-Pacific Conference on Information Systems, Langkawi Island, Malaysia. https://ris.utwente.nl/ws/files/16785402/Development_and_Update_of_Guidelines_to_Perform_and_Report_Partia.pdf

Bernerth, J. B., Walker, H. J., & Harris, S. G. (2016). Rethinking the benefits and pitfalls of leader–member exchange: A reciprocity versus self-protection perspective. *Human Relations*, *69*(3), 661–684. https://doi.org/10.1177/0018726715594214

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, *23*(3), 253–264. https://doi.org/10.1016/j.cose.2003.09.002

Boh, W. F., & Wong, S. S. (2013). Organizational climate and perceived manager effectiveness: Influencing perceived usefulness of knowledge sharing mechanisms. *Journal of the Association for Information Systems*, *14*(3), 122–152. https://aisel.aisnet.org/jais/vol14/iss3/2/

Bonner, J. M., Greenbaum, R. L., & Quade, M. J. (2017). Employee unethical behavior to shame as an indicator of self-image threat and exemplification as a form of self-image protection: The exacerbating role of supervisor bottom-line mentality. *Journal of Applied Psychology*, *102*(8), 1203–1221. https://doi.org/10.1037/apl0000222

Borena, B., & Bélanger, F. (2013, August 15-17). *Religiosity and information security policy compliance* [Paper presentation]. Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, IL, United States. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.692.3681&rep=rep1&type=pdf

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

Brown, J. S., & Duguid, P. (1991). Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. *Organization Science*, *2*(1), 40–57. https://doi.org/10.1287/orsc.2.1.40

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-A7. https://doi.org/10.1093/bja/aeq366

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy & Security*, *1*(3), 18–41. https://doi.org/10.1080/15536548.2005.10855772

Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), 438–458. https://doi.org/10.1108/02635570710734316

Chatman, J. A., & O'Reilly, C. A. (2016). Paradigm lost: Reinvigorating the study of organizational culture. *Research in Organizational Behavior*, *36*, 199–224. https://doi.org/10.1016/j.riob.2016.11.004

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49–87. http://10.0.4.56/07421222.2014.1001257

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1049–1060. https://doi.org/10.1016/j.im.2018.05.011

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, *55*(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Chin, W. W. (2010). How to write up and report PLS analyses. In V. Esposito Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of partial least squares: Concepts, methods and applications* (pp. 655–690). Springer. https://doi.org/10.1007/978-3-540-32827-8_29

Cho, E., & Kim, S. (2014). Cronbach's coefficient alpha. *Organizational Research Methods*, *18*(2), 207–230. https://doi.org/10.1177/1094428114555994

Churchill, B., Ravn, S., & Craig, L. (2019). Gendered and generational inequalities in the gig economy era. *Journal of Sociology*, *55*(4), 627–636. https://doi.org/10.1177/1440783319893754

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, *55*, 591–621. https://doi.org/10.1146/annurev.psych.55.090902.142015

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour. *Information and Computer Security*, *25*(2), 118–136. http://dx.doi.org/10.1108/ICS-03-2017-0013

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

Cousineau, D. (2017). Varieties of confidence intervals. *Advances in Cognitive Psychology*, *13*(2), 140–155. http://dx.doi.org/10.5709/acp-0214-z

Cram, W. A., Brohman, K., & Gallupe, R. B. (2016). Information systems control: A review and framework for emerging information systems processes. *Journal of the Association for Information Systems*, *17*(4), 216–266. https://doi.org/10.17705/1jais.00427

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605–641.http://dx.doi.org/10.1057/s41303-017-0059-9

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed method approaches* (4th ed.). Sage.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

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. http://search.proquest.com.library.capella.edu/docview/1634006771?accountid=27965

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

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

D’Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*, 43–69. https://doi.org/10.1111/isj.12173

D’Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56*(7), 1-14.https://doi.org/10.1016/j.im.2019.02.006

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information and Computer Security*, *24*(2), 139–151. http://dx.doi.org/10.1108/ICS-12-2015-0048

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

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72–94. https://doi.org/10.1016/j.cose.2017.05.002

Damschroder, L. J. (2019). Clarity out of chaos: Use of theory in implementation research. *Psychiatry Research*, *283*, 1-6. https://doi.org/10.1016/j.psychres.2019.06.036

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017a). Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers & Security*, *68*, 1–15. https://doi.org/10.1016/j.cose.2017.03.010

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017b). Investigation into the formation of information security influence: Network analysis of an emerging organisation. *Computers & Security*, *70*, 111–123. https://doi.org/10.1016/j.cose.2017.05.010

Dankasa, J. (2015). Developing a theory in academic rsearch: A review of experts' advice. *Journal of Information Science Theory and Practice*, *3*(3), 64–74. http://dx.doi.org/10.1633/JISTaP.2015.3.3.4

Day, D. V, & Miscenko, D. (2016). Leader-member exchange (LMX): Construct evolution, contributions, and future prospects for advancing leadership theory. In *The Oxford handbook of leader-member exchange.* (pp. 9–28). Oxford University Press.

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A framework improvement for linking culture and in initiatives organization. *Academy of Management Review*, *25*(4), 850–863. https://doi.org/10.5465/AMR.2000.3707740

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, *56*, 63–69. https://doi.org/10.1016/j.cose.2015.10.001

Ezingeard, J.-N., & Bowen-Schrire, M. (2007). Triggers of change in information security management practices. *Journal of General Management*, *32*(4), 53–72. https://doi.org/10.1177/030630700703200404

Faizan, A., Rasoolimanesh, M. S., Sarstedt, M., Ringle, C. M., & Ryu, K. (2018). An assessment of the use of partial least squares structural equation modeling (PLS-SEM) in hospitality research. *International Journal of Contemporary Hospitality Management*, *30*(1), 514–538. https://doi.org/10.1108/IJCHM-10-2016-0568

Field, A. P. (2013). *Discovering statistics using IBM SPSS statistics (and sex, drugs and rock'n'roll)* (4th ed.). Sage. https://doi.org/10.5860/CHOICE.50-2114

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Addison-Wesley. http://people.umass.edu/aizen/f&a1975.html

Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Flowerday, S. V, & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183. https://doi.org/10.1016/j.cose.2016.06.002

Furnell, S., & Thomson, K.-L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, *2009*(2), 5–10. https://doi-org.library.capella.edu/10.1016/S1361-3723(09)70019-3

Garson, E. D. (2016). *Partial least squares: Regression and structural equation models.* Statistical Associates Publishers. https://www.smartpls.com/resources/ebook_on_pls-sem.pdf

Gcaza, N., von Solms, R., Grobler, M. M., & Vuuren, J. J. van. (2017). A general morphological analysis: delineating a cyber-security culture. *Information and Computer Security*, *25*(3), 259–278. http://dx.doi.org.library.capella.edu/10.1108/ICS-12-2015-0046

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*(5), 91–109. https://doi.org/10.17705/1CAIS.01605

Goo, J., Yim, M., & Kim, D. J. (2014). A Path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication*, *57*(4), 286–308. https://doi.org/10.1109/TPC.2014.2374011

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

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. http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=67194187&site=ehost-live&scope=site

Hair, J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research*, *109*, 101–110. https://doi-org.library.capella.edu/10.1016/j.jbusres.2019.11.069

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage Publications.

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*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hall, E. T. (1959). *The silent language*. Doubleday & Company. https://monoskop.org/images/5/57/Hall_Edward_T_The_Silent_Language.pdf

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. https://doi.org/10.1016/j.cose.2016.12.016

Hartnell, C. A., Ou, A. Y., & Kinicki, A. (2011). Organizational culture and organizational effectiveness: A meta-analytic investigation of the competing values framework's theoretical suppositions. *Journal of Applied Psychology*, *96*(4), 677–694. https://doi.org/10.1037/a0021987

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*, *76*, 101–127. https://doi.org/10.1016/j.cose.2018.02.020

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, *21*(4), 266–287. http://dx.doi.org/10.1108/IMCS-08-2012-0043

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems*, *20*(4), 373–384. https://doi.org/10.1016/j.jsis.2011.06.001

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

Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security*, *21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, *31*(4), 6–48. https://doi.org/10.1080/07421222.2014.1001255

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2–18. http://dx.doi.org/10.1108/OIR-11-2015-0358

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

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Iivari, J., & Huisman, M. (2007). The relationship between organizational culture and the deployment of systems development methodologies. *MIS Quarterly*, *31*(1), 35–58. https://doi.org/10.2307/25148780

Iyamu, T. (2013). Underpinning theories: Order-of-use in information systems research. *Journal of Systems and Information Technology*, *15*(3), 224–238. http://dx.doi.org.library.capella.edu/10.1108/JSIT-11-2012-0064

Jacobs, G., Belschak, F. D., & Den Hartog, D. N. (2014). (Un)ethical behavior and performance appraisal: The role of affect, support, and organizational justice. *Journal of Business Ethics*, *121*(1), 63–76. http://dx.doi.org/10.1007/s10551-013-1687-1

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

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.http://dx.doi.org/10.1057/ejis.2015.15

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-A7. https://doi.org/10.25300/MISQ/2015/39.1.06

Jones, M. R., & Karsten, H. (2008). Giddens’s structuration theory and information systems research. *MIS Quarterly*, *32*(1), 127–157.https://doi.org/10.2307/25148831

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture - state-of-the-art review between 2000 and 2013. *Information and Computer Security*, *23*(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, *67*, 267–279. https://doi.org/10.1016/j.cose.2016.12.012

Karlsson, F., Kolkowska, E., & Prenkert, F. (2016). Inter-organisational information security: A systematic literature review. *Information and Computer Security*, *24*(5), 418–451. http://dx.doi.org/10.1108/ICS-11-2016-091

Karlsson, M., Denk, T., & Joachim, Å. (2018). Perceptions of organizational culture and value conflicts in information security management. *Information and Computer Security*, *26*(2), 213–229. http://dx.doi.org/10.1108/ICS-08-2017-0058

Karyda, M. (2017). Fostering information security culture in organizations: A research agenda. *Proceedings of the Mediterranean Conference on Information Systems*, *28,* 1–11. https://aisel.aisnet.org/mcis2017/28

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *Mis Quarterly Executive*, *9*(3), 163–175. https://ssrn.com/abstract=2058035

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, *61*, 46–58. https://doi.org/10.1016/j.cose.2016.05.006

Knapp, K. J., Marshall, T. E., Rainer Jr., R. K., & Morrow, D. W. (2006). The top information security issues facing organizations: What can government do to help? *Information Systems Security*, *15*(4), 51–58. https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95124.6

Kock, N. (2016). Hypothesis testing with confidence intervals and P values in PLS-SEM. *International Journal of E-Collaboration*, *12*(3), 1–6. https://doi.org/10.4018/IJeC.2016070101

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

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, *33*, 3–11. https://doi.org/10.1016/j.cose.2012.07.001

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. *The Journal of Strategic Information Systems*, *26*(1), 39–57. https://doi.org/10.1016/j.jsis.2016.08.005

Kumar, D. S., & Purani, K. (2018). Model specification issues in PLS-SEM. *Journal of Hospitality and Tourism Technology*, *9*(3), 338–353. http://dx.doi.org/10.1108/JHTT-09-2017-0105

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4–13. http://dx.doi.org/10.1108/09685221011035223

Larson, S. (2017, March 20). *The hacks that left us exposed in 2017*. CNN. http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2013, January 7-10). *Employees’ information security awareness and behavior: A literature review* [Paper presentation]. 46th Hawaii International Conference on System Sciences, Maui, HI, United States. https://doi.org/10.1109/HICSS.2013.192

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, *31*(1), 59–87. https://dl.acm.org/doi/10.5555/2017327.2017332

Liang, H., Xue, Y., Ke, W., & Wei, K. K. (2010). Understanding the influence of team climate on IT use. *Journal of the Association for Information Systems*, *11*(8), 414–432. https://doi.org/10.17705/1jais.00235

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring employees’ IT compliance: Carrot or stick? *Information Systems Research*, *24*(2), 279–294. http://10.0.5.7/isre.1120.0427

Liengaard, B. D., Sharma, P. N., Hult, G. T. M., Jensen, M. B., Sarstedt, M., Hair, J. F., & Ringle, C. M. (2020). Prediction: Coveted, yet forsaken? Introducing a cross-validated predictive ability test in partial least squares path modeling. *Decision Sciences*, 1–31. https://doi.org/10.1111/deci.12445

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433–463. https://doi.org/10.1111/isj.12043

Lowry, P. B., Posey, C., Bennett, R. (Becky) J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193–273. https://doi.org/10.1111/isj.12063

Mbowe, J. E., Zlotnikova, I., Msanjila, S. S., & Oreku, G. S. (2014). A conceptual framework for threat assessment based on organization's information security policy. *Journal of Information Security*, *5*(4), 166–177. https://doi.org/10.4236/jis.2014.54016

McNeish, D. (2018). Thanks coefficient alpha, we'll take it from here. *Psychological Methods*, *23*(3), 412–433. https://doi.org/10.1037/met0000144

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Miracle, V. A. (2016). The Belmont Report the triple crown of research ethics. *Dimensions of Critical Care Nursing*, *35*(4), 223–228. https://doi.org/10.1097/DCC.0000000000000186

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. *Journal of Information, Communication & Ethics in Society*, *14*(3), 254–271. http://dx.doi.org/10.1108/JICES-06-2015-0018

Muthén, L. K., & Muthén, B. O. (2002). How to use a monte carlo study to decide on sample size and determine power. *Structural Equation Modeling: A Multidisciplinary Journal*, *9*(4), 599–620. https://doi.org/10.1207/S15328007SEM0904_8

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*, 126–139. https://doi.org/10.1057/ejis.2009.10

North American Industry Classification System. (2020). *Counts by company size*. https://www.naics.com/business-lists/counts-by-company-size/

Nardi, P. M. (2018). *Doing survey research: A guide to quantitative methods* (4th ed.). Routledge. https://doi.org/10.4324/9781315172231

National Commission for the Protection of Human Subjects of Biomedial and Behavioral Research. (1979). *The Belmont Report*. https://doi.org/10.1002/9780471462422.eoct093

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information and Management*, *52*, 123–134. https://doi.org/10.1016/j.im.2014.10.009

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1–20. http://dx.doi.org/10.1057/s41303-016-0025-y

O'Reilly, C. A., III., Caldwell, D. F., Chatman, J. A., & Doerr, B. (2014). The promise and problems of organizational culture: CEO personality, culture, and firm performance. *Group & Organization Management*, *39*(6), 595–625. https://doi.org/10.1177/1059601114550713

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems*, *92*, 47–56. https://doi.org/10.1016/j.dss.2016.09.012

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, *52*(2), 183–199. https://doi.org/https://doi.org/10.1016/j.im.2014.08.008

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, *30*(1), 115–143. https://doi.org/10.2307/25148720

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

Peterson, R. A., & Kim, Y. (2013). On the relationship between coefficient alpha and composite reliability. *Journal of Applied Psychology*, *98*(1), 194–198. https://doi.org/10.1037/a0030767

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *31*(4), 623–656. https://misq.org/catalog/product/view/id/146

Phillips, B. (2013). Information technology management practice: Impacts upon effectiveness. *Journal of Organizational and End User Computing*, *25*(4), 50–74. https://doi.org/10.4018/joeuc.2013100103

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100 million dollar data breach. *Journal of Information Technology Teaching Cases*, *8*(1), 9–23. https://doi.org/10.1057/s41266-017-0028-0

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 1–61. https://doi.org/10.1080/07421222.2015.1138374

Qazi, A., Qazi, J., Naseer, K., Zeeshan, M., Hardaker, G., Maitama, J. Z., & Haruna, K. (2020). Analyzing situational awareness through public opinion to predict adoption of social distancing amid pandemic COVID-19. *Journal of Medical Virology*, *92*(7), 849–855. https://doi.org/10.1002/jmv.25840

Quinn, R. E., & Rohrbaugh, J. (1983). A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis. *Management Science*, *29*(3), 363–377. http://search.proquest.com.library.capella.edu/docview/205852012?accountid=27965

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211–223. https://doi.org/10.1016/j.cose.2018.09.016

Ramachandran, S., Rao, C., Goles, T., & Dhillon, G. (2013). Variations in information security cultures across professions: A qualitative study. *Communications of the Association for Information Systems*, *33*, 163–204. https://doi.org/10.17705/1CAIS.03311

Ringle, C. M., Wende, S., & Becker, J.M. (2015). *SmartPLS 3*. SmartPLS GmbH. http://www.smartpls.com

Roberts, B. W., & Jackson, J. J. (2017). Conscientiousness. In T. A. Widiger (Ed.), *The Oxford handbook of the five factor model* (1st ed.). Oxford University Press.

Röder, N., Wiesche, M., Schermann, M., & Krcmar, H. (2014, August 7-9). *Why managers tolerate workarounds – The role of information systems* [Paper presentation]. Twentieth Americas Conference on Information Systems, Savannah, GA, United States. https://www.researchgate.net/profile/Manuel_Wiesche/publication/271204813_Why_Managers_Tolerate_Workarounds--The_Role_of_Information_Systems/links/54f46b0a0cf299c8d9e7536b.pdf

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rowe, F. (2014). What literature review is not: Diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241–255. http://dx.doi.org/10.1057/ejis.2014.7

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers and Security*, *26*(1), 56–62. https://doi.org/10.1016/j.cose.2006.10.008

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, *40*(247–257). https://doi.org/10.1016/j.jisa.2017.11.001

Safa, N. S., von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), 15–18. https://doi.org/10.1016/S1361-3723(16)30017-3

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Salancik, G. R., & Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. *Administrative Science Quarterly*, *23*(2), 224–253. https://doi.org/10.2307/2392563

Schein, E. H. (2004). *Organizational culture and leadership* (3rd ed.). Jossey-Bass.

Schein, E. H. (2009). *The corporate culture survival guide* (2nd ed.). Jossey-Bass.

Schoemann, A. M., Boulton, A. J., & Short, S. D. (2017). Determining power and sample size for simple and complex mediation models. *Social Psychological and Personality Science*, *8*(4), 379–386. https://doi.org/10.1177/1948550617715068

Schryen, G. (2015). Writing qualitative IS literature reviews - guidelines for synthesis, interpretation, and guidance of research. *Communications of the Association for Information Systems*, *37*(12), 286–325. http://aisel.aisnet.org/cais/vol37/iss1/12

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach* (6th ed.). John Wiley & Sons.

Sguera, F., Bagozzi, R. P., Huy, Q. N., Boss, R. W., & Boss, D. S. (2018). The more you care, the worthier I feel, the better I behave: How and when supervisor support influences (un)ethical employee behavior. *Journal of Business Ethics*, *153*(3), 615–628. http://dx.doi.org/10.1007/s10551-016-3339-8

Sharma, S., & Warkentin, M. (2018). Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security*. https://doi.org/10.1016/j.cose.2018.09.005

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, *22*(3), 279–308. https://doi.org/10.1108/IMCS-05-2013-0041

Simon, H. A. (1955). A behavioral model of rational choice. *Quarterly Journal of Economics*, *69*(1), 99–118. https://doi.org/10.2307/1884852

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, *27*(5), 644–667. https://doi.org/10.1108/JEIM-07-2013-0052

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225–239. https://doi.org/10.1007/s40171-013-0047-4

Siponen, M., & Baskerville, R. (2018). Intervention effect rates as a path to research relevance: Information systems security example. *Journal of the Association for Information Systems*, *19*(4), 247–265. http://dx.doi.org/10.17705/1jais.00491

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-A12. https://misq.org/catalog/product/view/id/1391

Skotnes, R. Ø. (2015). Management commitment and awareness creation – ICT safety and security in electric power supply network companies. *Information and Computer Security*, *23*(3), 302–316. http://dx.doi.org/10.1108/ICS-02-2014-0017

Smircich, L. (1983). Concepts of culture and organizational analysis. *Administrative Science Quarterly*, *28*(3), 339–358. https://doi.org/10.2307/2392246

Sommestad, T., & Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. In L. J. Janczewski, H. B. Wolfe, & S. Shenoi (Eds.), *IFIP International Information Security Conference* (pp. 257–271). Springer. https://doi.org/10.1007/978-3-642-39218-4_20

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

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal*, *22*(1), 77–94. https://doi.org/10.1111/j.1365-2575.2011.00378.x

Stewart, D., & Klein, S. (2016). The use of theory in research. *International Journal of Clinical Pharmacy*, *38*(3), 615–619. https://doi.org/10.1007/s11096-015-0216-y

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security*, *25*(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(24), 380–427. https://doi.org/10.17705/1CAIS.01324

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469. https://doi.org/10.2307/249551

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670. https://doi.org/10.2307/2089195

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management*, *17*(2), 179–186. http://dx.doi.org/10.1007/s10799-015-0252-2

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, *6*(2), 144–176. https://doi.org/10.1287/isre.6.2.144

Thomson, K.-L., & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, *20*(1), 39–46. http://dx.doi.org/10.1108/09685221211219191

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11. https://doi.org/10.1016/S1361-3723(06)70430-4

Trochim, W. M. K. (2006). *Research Methods Knowledge Base*. http://www.socialresearchmethods.net/kb/index.php

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128–141. https://doi.org/10.1016/j.cose.2015.04.006

Tuli, F. (2011). The basis of distinction between qualitative and quantitative research in social science: Reflection on ontological, epistemological and methodological perspectives. *Ethiopian Journal of Education and Sciences*, *6*(1), 97–108. http://www.ajol.info/index.php/ejesc/article/view/65384/53078

Turel, O. (2016). Untangling the complex role of guilt in rational decisions to discontinue the use of a hedonic information system. *European Journal of Information Systems*, *25*(5), 432–447. http://dx.doi.org/10.1057/s41303-016-0002-5

Tversky, A., & Kahneman, D. (1986). Rational choice and the framing of decisions. *Journal of Business*, *59*(4), S251–S278. http://links.jstor.org/sici?sici=0021-9398%28198610%2959%3A4%3CS251%3ARCATFO%3E2.0.CO%3B2-C

United Nations Conference on Trade and Development. (2017). *Information Economy Report 2017: Digitalization, Trade and Development*. https://unctad.org/en/PublicationsLibrary/ier2017_en.pdf

United States Census Bureau. (2017). *North American Industry Classification System*. https://www.census.gov/eos/www/naics/2017NAICS/2017_NAICS_Manual.pdf

Van Muijen, J. J., Koopman, P., De Witte, K., De Cock, G., Susanj, Z., Lemoine, C., Bourantas, D., Papalexandris, N., Branyicski, I., Spaltro, E., Jesuino, J., Neves, J. G. D., Pitariu, H., Konrad, E., Peiro, J., Gonzalez-Roma, V., & Turnipseed, D. (1999). Organizational culture: The focus questionnaire. *European Journal of Work and Organizational Psychology*, *8*(4), 551–568. https://doi.org/10.1080/135943299398168

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. In *Computers & Security* (Vol. 29, Issue 4, pp. 476–486). https://doi.org/10.1016/j.cose.2009.10.005

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263–290. https://doi.org/10.2753/MIS0742-1222290410

Vaske, J. J., Beaman, J., & Sponarski, C. C. (2017). Rethinking internal consistency in Cronbach's alpha. *Leisure Sciences*, *39*(2), 163–173. https://doi.org/10.1080/01490400.2015.1127189

Vogt, P. W. (2007). *Quantitative research methods for professionals*. Pearson Education.

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Communications of the Association for Information Systems*, *37*, 205–224. https://doi.org/10.17705/1CAIS.03709

Wall, J. D., & Iyer, L. (2012, August 9-12). *The dark side of leadership in information systems security: A model of the effect of manager transgressions on employee security behaviors* [Paper presentation]. 18th Americas Conference on Information Systems, Seattle, WA, United States. http://www.scopus.com/inward/record.url?eid=2-s2.0-84877912733&partnerID=40&md5=1bce2fda125f8ed58662d6255ef255e4

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems*, *17*(1), 39–76. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2611567

Walsh, I., Kefi, H., & Baskerville, R. (2010). Managing culture creep: Toward a strategic model of user IT culture. *The Journal of Strategic Information Systems*, *19*(4), 257–280. https://doi.org/10.1016/j.jsis.2010.09.002

Ward, P., Clark, T., Zabriskie, R., & Morris, T. (2012). Paper/pencil versus online data collection: An exploratory study. *Journal of Leisure Research*, *44*(4), 507–530. https://doi.org/10.1080/00222216.2014.11950314

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267–284. http://dx.doi.org/10.1057/ejis.2010.72

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 194–215. https://doi.org/10.17705/1jais.00424

Wayne, S. J., & Green, S. A. (1993). The effects of leader-member exchange on employee citizenship and impression management behavior. *Human Relations*, *46*(12), 1431. https://doi.org/10.1177%2F001872679304601204

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), 11. http://cci.drexel.edu/faculty/sgasson/Readings/Webster&Watson%5B2002%5D-WritingALiteratureReview.pdf

Wen-Lung, S., Marko, S., & F., H. J. (2019). Internet research using partial least squares structural equation modeling (PLS-SEM). *Internet Research*, *29*(3), 398–406. https://doi.org/10.1108/IntR-10-2018-0447

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

Whitener, E. M., Brodt, S. E., Korsgaard, M. A., & Werner, J. M. (1998). Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior. *Academy of Management Review*, *23*(3), 513–530. https://doi.org/10.5465/AMR.1998.926624

Whitman, M. E., & Mattord, H. J. (2012). Information security governance for the non-security business executive. *Journal of Executive Education*, *11*(1), 97–111. http://digitalcommons.kennesaw.edu/jee/vol11/iss1/6

Wold, H. (1974). Causal flows with latent variables: Partings of the ways in the light of NIPALS modelling. *European Economic Review*, *5*(1), 67–86. https://doi.org/10.1016/0014-2921(74)90008-7

Wolf, E. J., Harrington, K. M., Clark, S. L., & Miller, M. W. (2013). Sample size requirements for structural equation models: An evaluation of power, bias, and solution propriety. *Educational and Psychological Measurement*, *73*(6), 913–934. https://doi.org/10.1177/0013164413495237

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. https://doi.org/10.1002/asi.20779

Wu, W.-Y., Ke, C.-C., & Nguyen, P.-T. (2018). Online shoping behavior in electronic commerce: An integrative model from utilitarian and hedonic perspectives. *International Journal of Entrepreneurship*, *22*(3), 1–16. https://search.proquest.com/openview/beb2c696e4bde15f5c9e75e6c0fe98ec/1?pq-origsite=gscholar&cbl=29727

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, *22*(2), 400–414. https://doi.org/10.1287/isre.1090.0266

Yadav, M., & Rangnekar, S. (2015). Supervisory support and organizational citizenship behavior. *Evidence - Based HRM*, *3*(3), 258–278. https://doi.org/ 10.1108/EBHRM-04-2014-0014

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36–46. http://dx.doi.org/10.1016/j.dss.2016.09.009

Zhang, H., Chari, K., & Agrawal, M. (2018). Decision support for the optimal allocation of security controls. *Decision Support Systems*, *115*, 92–104. https://doi.org/10.1016/j.dss.2018.10.001

APPENDIX A. SURVEY INSTRUMENT

Note: References to senior managers in questions 1-3 means your immediate manager or supervisor.

Please indicate the extent to which you agree with the following statements: 1-Strongly Disagree, 3-Neutral, 5-Strongly Agree

1. (PMP1) Senior managers of our company have articulated a clear vision about information security.
2. (PMP2) Senior managers of our company have formulated a clear strategy for achieving a high degree of information security.
3. (PMP3) Senior managers of our company have established clear goals and objectives for achieving a high degree of information security.
4. (ATT1) I believe that it is beneficial for an organization to establish clear information security policies, practices, and technologies.
5. (ATT2) I believe that it is useful to for an organization to enforce its information security policies, practices, and technologies.
6. (ATT3) I believe that it is a good idea for an organization to establish clear information security policies, practices, and technologies.
7. (SN1) People who are influential to me would think that I should follow the policies and procedures and use the security technologies.
8. (SN2) People who are important to me would think that I should follow the policies and procedures and use the security technologies.
9. (SN3) People whom I respect would think that I should follow the policies and procedures and use the security technologies.
10. (PBC1) I am able to follow the policies and procedures and use the security technologies.
11. (PBC2) I have the resources and knowledge to follow the policies and procedures and use the security technologies.
12. (PBC3) I have adequate training and skills to follow the policies and procedures and use the security technologies.
13. (INT1) I intend to follow the information security policies and practices at work.
14. (INT2) I intend to use the information security technologies at work.
15. (INT3) I intend to use common sense on good information security practices at work.
16. (DUT1) I try to perform all the tasks assigned to me conscientiously.
17. (DUT5) When I make a commitment, I can always be counted on to follow through.
18. (DUT7) I try to do jobs carefully, so they won’t have to be done again.

Please answer the questions based on your observation of the whole company: How often .... 1- Never, 3 – Often, 5 – Always

19. (PRO1) Are instructions written down?
20. (PRO2) Are jobs performed according to defined procedures?
21. (PRO3) Do the management follow the rules themselves?
22. (PGO2) Do management specify the targets to be attained?
23. (PGO3) Is it clear how performance will be evaluated?

Note. Adapted from "Managing compliance with information security policies: The critical role of top management and organizational culture" by Q. Hu, T. Dinev, P. Hart, and D. Cooke, 2012, Journal of Decision Sciences, 43(4), p. 657. Copyright 2012 by Journal of Decision Sciences. Adapted with permission.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346 USA