HODGES, DARIN Ph.D. The Mediating Effect of Intrinsic Motivation on Perceived Work Uncertainty for Individual Information Security Policy Compliance. (2022)
Directed by Dr. Kane Smith. 229 pp.

This dissertation is centered on investigating how employees' intrinsic motivation mediates the relationship between perceived work uncertainty and individual information security policy compliance. As stay-at-home orders, and unemployment increased, surveys indicated that 49% of traditional office employees experienced remote working for the first time. Work systems rapidly shifted to a reliance on home WIFI networks, personal computers, and personal anti-virus software. This move created vulnerabilities to information security policies and procedures where almost 20% of work from home employees were given no tips to improve information security at home (Security 2020). Unemployment increased, and remaining employees had to adapt to changing work tasks, reduced or lacking resources, and minimal technical or managerial support to navigate job uncertainty while maintaining overall information security. With organizational threats to information security increasing, it is becoming clear that little attention has been given to how individuals become intrinsically motivated when the design of work itself becomes uncertain. Taking into account the changing work and job environment and the uncertainty which this environment facilitates, we have identified a research gap in which the need for individuals to rely on their skills and abilities to interpret work needs during uncertain times, and the overall intrinsically driven work motivation required to comply with organizational ISP's during times of perceived work uncertainty, has not been investigated.

Using a theoretical basis of Work Design theory (Wall et al., 2002) and Self-determination theory of work motivation (Gange and Deci, 2005), we performed a cross-sectional survey of 269 participants at the onset and height of the global pandemic. One of the

primary implications of this study and our results is the indirect mediation by intrinsic motivation of the relationship between perceived work uncertainty and intentions to comply with information security policies. Another vital aspect of our study's findings is the view that information security policies (ISP) themselves can become the source of uncertainty in compliance decisions. Most all ISPs are developed to bring clarity to employees on how to address security threats while making compliance decisions. Where ISPs have been investigated about the demands (and impositions) they place on work goal attainment (or inhibiting work requirements), we have found that ISPs may not be able to provide answers to all security threats encountered. Overall, our results should invigorate the debate about which strategies increase intrinsic motivation and what methods should be deployed to maximize positive reactions during uncertainty concerning information security compliance behaviors. This study has provided evidence that organizations should design work practices, especially ISPs, that allow employees latitude to make ISP compliance decisions when ISPs are unclear or uncertain and where managers similarly cannot provide correct courses of remedy or action.

THE MEDIATING EFFECT OF INTRINSIC MOTIVATION ON PERCEIVED WORK UNCERTAINTY FOR INDIVIDUAL INFORMATION SECURITY POLICY COMPLIANCE

By

Darin Hodges

A Dissertation

Submitted to

the Faculty of The Graduate School at

The University of North Carolina at Greensboro

in Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

Greensboro

2022

Approved by

Committee Chair

DEDICATION

This dissertation is dedicated to my wife, Heidi, and my two children, Addin and Yates, who make my life complete. What started as a ‘go back to school and finish a degree’ conversation ended with a doctorate nine years later. I could not have accomplished this without your unwavering support and sacrifice. The many days I spent away from home (and my family obligations) have culminated in a degree I never thought possible. I am genuinely thankful for you and love you all.

APPROVAL PAGE

This dissertation written by Darin Hodges has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair

Dr. Kane Smith

Committee Members

Dr. Gurpreet Dhillon

Dr. Indika Dissanayake

Dr. Franck Loic Soh Noume

November 5, 2021

Date of Acceptance by Committee

November 19, 2021

Date of Final Oral Examination

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I: INTRODUCTION

1.1 Problem Statement

This dissertation investigates how employees' intrinsic motivation mediates the relationship between perceived work uncertainty and individual information security policy compliance. It is essential to pursue this line of inquiry during the present times when we are engulfed in a pandemic. In the US, for instance, 20.6 million jobs were rapidly lost since mid-March 2020, resulting in a 14.7% unemployment rate unequaled since the depression era of the 1930s (Soucheray 2020) and rising higher in the first three months of the pandemic than during two years of the Great Recession of 2008/09 (Kochhar 2020). Job losses have affected all strata of society. Women and men (14.3% and 11.9%, respectively), minority and majority worker populations (16.3% and 10.8%, respectively), all education levels (High School grad and lower/some college averaging 12.1% and college-educated or better averaging 7.2%) and ages have experienced unemployment rates higher than that of the Great Recession even with the option of teleworking is a unique factor in employment during the pandemic (Kochhar 2020).

As stay-at-home orders and unemployment increased, surveys indicated that 49% of traditional office employees experienced remote working for the first time. Work systems rapidly shifted to a reliance on home WIFI networks, personal computers (56%), and personal anti-virus software, which created vulnerabilities to information security policies and procedures where almost 20% of work from home employees was given no information security tips (Security 2020). As unemployment increased, remaining employees had to adapt to changing work tasks, reduced or lacking resources, and minimal technical or managerial support to navigate job uncertainty while maintaining overall information data and system security. This article argues that during these periods of extreme and rapid work uncertainty, information security policy

compliance can only be achieved through intrinsic motivation, security education, and employee training. We conduct our argument by first reviewing the informing literature, establishing our theoretical foundation, and presenting findings from the empirical study.

1.2 Significance

Work has changed for many in the last two years. During this time, organizations have developed novel work methods and policies which grant individuals new freedoms to accomplish organizational goals. While change has always been a mainstay for the business enterprise, rarely have times existed where uncertainty exists within the individual on achieving work tasks and organizational goals. Through a literature review and empirical findings, Grant and Parker (2009) stipulated that organizations must manage two contexts to attain organizational goals effectively. First, organizations must address and facilitate the interdependence between work roles and social systems of interdependent behavior (Scott and Davis 2015; Thompson 1967), and secondly, organizations must mitigate the uncertainty and unpredictability of inputs, processes, or outputs of the work system (Wall et al. 2002; Wright and Cordery 1999). Work design theory has long held an understanding that when predictability in accomplishing work tasks or requirements is low individual job control should increase. This has been shown to increase decision-making authority over task implementation (Wall et al. 2002). Increasing job control has also increased intrinsic motivation and satisfaction during more significant uncertainty, allowing individuals to exhibit problem-solving responsibilities and showcase skills and abilities in performing work Fields(Wright and Cordery 1999). When individuals self-reported work uncertainty, proactive behaviors have been observed to make adjustments to job tasks (known in work design as ‘job crafting’), allowing individuals the autonomy to meet work performance goals (Clegg and Spencer 2007; Wrzesniewski and Dutton 2001). Self-

determination theory (SDT) argues that autonomous work motivation can lead to better worker performance through methods of intrinsic satisfaction (Gagné and Deci 2005). For ISP compliance, little attention has been paid to how individuals utilize their problem-solving skills and abilities to comply with security policies during work and policy uncertainty.

Extrinsic and intrinsic motivations are two primary factors on which investigators have centered previous research to study why (or why not) individuals choose to comply with information security policy (D'Arcy et al. 2009; Dhillon et al. 2019; Herath and Rao 2009a; Son 2011a; Yazdanmehr et al. 2020). Generally, extrinsic motivators include positive persuaders (rewards and bonuses) and adverse sanctions (employee termination or sanction), but these types of motivation have shown limited positive information security outcomes (D'Arcy et al. 2014; Herath and Rao 2009a). However, recent evidence suggests internal motivators may play a more significant role in individual choices surrounding information security policy choices and positive outcomes (Dhillon et al. 2019; Yazdanmehr et al. 2020). Intrinsic motivators are such things as self-efficacy (Chan et al. 2005) and security values alignment with the organization (Son 2011b). Deci and Ryan (1980)linked intrinsic motivation to self-regulation given any individual perception to engage in activities by choice (autonomy), with competence to deter undesired consequences, or an ability to connect with others to accomplish a task (relatedness) when designing Self-Determination theory (SDT). A recently performed meta-analysis of ISP literature by Cram et al. (2019)indicated antecedents that predicted ISP compliance had been predominately rooted in criminology theories such as deterrence theory (DT), protection motivation theory (PMT), and rational choice theory (RCT). These investigations utilize and borrow intrinsic motivators as the *antecedents* to ISP compliance. Research considering intrinsic motivators and ISP compliance have attempted to determine which motivators are essential

predictors for individuals to choose compliance with ISPs over non-compliance (Cram et al. 2019). However, Dhillon et al. (2019) investigated antecedents that trigger individuals to rely on these internal mechanisms and then how they mediate the relationships between antecedents and ISP compliance performance.

Some investigations have attempted to pivot from criminological theory to explain ISP compliance by looking at the issue through the Jobs Demands-Resources (JDR) model (Pham et al. 2016) or other work-stress-related topics (D'Arcy et al. 2014). Work-stress models, such as the JDR, propose a lack of resources or high job demands influence overall employee commitment and performance due to burnout and general work engagement (Crawford et al. 2010; Demerouti et al. 2001). Such investigation tends to focus on overall access to resources and how demands of work policies can overwhelm individuals to achieve tasks. This type of investigation assumes work tasks and daily work functions are (1) stable and (2) the resources offered (either written or provided from management) accurately stipulates how employees handle work situations. That approach fails to address when uncertainty created in changing work and task atmospheres makes work policies and resources insufficient to accomplish performance goals, such as complying with information security policies. With organizational threats to information security increasing, little attention has been given to how individuals become intrinsically motivated when the design of work itself becomes uncertain. Taking into account the changing work and job environment and the uncertainty which this facilitates, the need for individuals to rely on their skills and abilities to interpret work needs, and the overall intrinsically driven work motivation required to comply with organizational ISPs, this dissertation seeks to fill this research gap.

With our overview and significance of the research problem identified, this study seeks to answer the following research questions:

1. How do perceived effectiveness, perceived self-efficacy, perceived value congruence, and perceived ownership enhance intrinsic work motivation?
2. How does perceived work uncertainty (through the lens of resources, task, and input/output ambiguity) enhance intrinsic work motivation?
3. What is the mediating effect of individual intrinsic work motivation on the relationship between perceived work uncertainty and information security policy compliance and SETA?
4. What is the mediating effect between intrinsically motivated individuals of organizational security education, training, and awareness (SETA) on information security policy compliance?

This study will incorporate a conceptual research framework that combines elements of intrinsic motivation Self-Determination theory and Work Design theory to address these questions. By understanding these concepts, this investigation will enhance the understanding of employees' work motivations when work uncertainty exists and improve the knowledge of how individual behavior can be positively enhanced through bottom-up job crafting processes during turbulent work environments. From a practical standpoint, this research will give organizations and managers essential insights into how they can motivate employees to make positive ISP compliance decisions when resources and tasks become uncertain.

1.3 Structure of the Thesis

This dissertation is composed of six chapters. Following the introduction, which presents the argument and significance of this study, chapter two will review the literature for employee

ISP compliance. This review will be facilitated through the lens of Self-determination and work motivation theory and elements of Work Design theory. It will present identified antecedents affecting individual employee intrinsic motivation and ISP compliance intentions. Additionally, the research hypotheses will be proposed. In the third chapter, we will define the research methodology utilized to operationalize the research framework, including data collection and analysis in the third chapter. The fourth chapter will provide the results of the analysis/study. The fifth chapter will discuss the results from the previous chapter. The final chapter will draw conclusions based on the findings and discuss the study's overall practical and theoretical implications and the limitations of this investigation and future research this study provides.

CHAPTER II: LITERATURE REVIEW

2.1 Introduction

Information security policies are not always followed. It is reasonable to assume that just because an information security policy has been initiated, or codified within an organization, does not guarantee individuals will act responsibly with information security needs (Bulgurcu et al. 2010). This chapter will review recent and relevant literature surrounding individual behavior of information security policy compliance. This review will explore motivations for ISP compliance, which have generally been identified as intrinsic and extrinsic to the individual. While extrinsic motivations have been extensively investigated utilizing social control-criminal deterrence criminological theories (Menard et al. 2017), recent discoveries have yielded indications of external sanctions and/or rewards becoming less important as a motivator of ISP compliance intentions (Yazdanmehr et al. 2020). Intrinsic motivators have been identified to predict more variance than extrinsic motivators on ISP intention behaviors (Menard et al. 2018).

This chapter will also review the literature of work uncertainty through the lens of Work Design theory. Organizational change research has identified how uncertainty is crated through the breakup of existing social structures and rational choice frameworks leading to new-decision making processes (Ciborra 1996). Furthermore, disrupted workflows and high complexity within the work environment have created tension between organizational rules and individual behavior (Njenga and Brown 2012; Raza et al. 2019). However, work design theory allows for uncertainty to empower positive individual behavior if the workplace is aligned to allow for such mechanisms. During organizational stress and work uncertainty, the work environment and worker roles can be designed to enable individual empowerment and motivation to create

positive outcomes. Next, we will explore the foundational definitions which drive our theoretical and research model.

2.2 Foundational Definitions

This section will establish the foundational definitions of the primary concepts within our research framework and theoretical model. Foundational definitions provide the basis for recognizing and understating the conceptual and theoretical concepts of our ISP compliance intention model.

2.2.1 Work Uncertainty

Uncertainty has been used and defined in different ways; however, as Argote (1982) noted, incomplete information remains a common thread which "makes it difficult to predict the future states of many factors associated with an organization's environment or tasks (p.420)." Work uncertainty is related to job characteristics and contextual aspects of work predicated by contextual generalizations under which job task uncertainty occurs. Work uncertainty emerges when individuals have difficulty determining or anticipating the nature of work demands or the number of exceptional events outside standard work conditions (Griffin et al. 2007). Work uncertainty is generally associated with factors that inhibit or enhance the completion of work tasks and have been investigated primarily through the reliability of technological work needs and the overall complexity of operational aspects, which are sources of uncertainty (Leach et al. 2013).

Uncertainty is a concept that has been investigated across many different disciplines, including organizational theory (Burns & Stalker, 1961; Lawrence & Lorsch, 1967), human factors (Clegg et al. 1989), supply chain, and production total quality management (Douglas and Judge, 2001; Sitkin et al. 1994), decision making (Atuahene-Gima & Li, 2004; Hult et al. 2010),

human resource management (Datta et al. 2005; Wright and Snell, 1998), and occupational health and safety (Grote, 2007; Jackson, 1989). The literature defines uncertainty sources as either internal or external to the individual (Avgoustaki 2016). Internal uncertainty is rooted within organizations and is experienced when individuals encounter non-routine tasks with little information, such as rapid schedule changes. Additionally, the complexity and variability of the job can lead to uncertainty of accomplishing the task. External uncertainty is brought on by environments associated with rivals in industry and markets.

Wall et al. (2002)) noted that during times of high uncertainty, individuals are asked to take more responsibility for work tasks, increase problem-solving, and become more reactive to rapidly changing work conditions. Overall, the larger information system security literature has generally studied uncertainty from environmental and organizational contexts, which seek to place individuals in stressful organizational environments and attempt to gauge reactions to security policy and procedures due to uncertainty in job-related aspects (Li and Siponen 2011). However, while this approach has garnered considerable knowledge concerning those specific contexts, little attention has been applied to the work context, in which aspects directly related to the task become unpredictable or uncertain (Leach et al. 2013).

Organizations and scholars have exerted substantial efforts to determine how work design can facilitate organizationally oriented outcomes (Knight and Parker 2019) during uncertain working conditions. Griffin et al. (2007) concluded that within "uncertain and interdependent organizational contexts," it has been difficult for researchers to determine which individual activities contribute to effective employee performance. Work design has been shown to have both positive and negative effects. Work design theories have revealed attempts to create empowerment strategies (within the work context) that can compensate for uncertain conditions

where individuals leverage resources or applied knowledge leading to better performance and outcomes (Bruns and Stalker 1961; Knight and Parker 2019; Leach et al. 2013; Wall et al. 2002). Inside workplace settings, individual behaviors surrounding information security conduct have been studied through the lens of security training and education, IS misuse, and security policy compliance.

2.2.2 Intrinsic Motivation

Intrinsic motivation involves individual self-regulation as a motivation to act and encompasses almost all motivation which cannot be linked to external factors or outcomes (Broedling 1977). Intrinsically motivated individuals have been found to engage in tasks for the pleasure and fulfillment the task provides (Vallerand 1997), where no reinforcement for the performance of the task is needed due to the task becoming the reward (Deci and Ryan 2010). Self-motivated individuals have been found to engage in autonomous tasks whereby a feeling of competence to complete the task and connect with others who have the same interests (Deci and Ryan 1980; Vallerand 1997). Intrinsic motivation research within the IS discipline has focused on various feelings surrounding individual levels of competence to perform a task (Herath and Rao 2009a). Intrinsic motivation differs from extrinsic motivators. Extrinsic motivators deal more with structural influences put into place by organizations concerning security-related compliance issues such as sanctions against individuals, pay rewards, job promotions, and the like (Menard et al. 2017). Intrinsic motivation is closely associated with individual empowerment when coupled with tasks completed by individuals whereby performing the task may be rewarded and/or sanctioned enough with external reinforcement of task accomplishment becoming unnecessary (Deci and Ryan 1980).

2.2.3 Information System Security

Information system security (IS Security) encompasses activities that control threats to data and information while ensuring the same's availability, integrity, and confidentiality. Securing information systems and their components can range from technical/physical management and control (such as password managers) and network management techniques on one side to policies and access limitations on the other. IS security measures are implemented to control and manage threats posed to data and information inside and outside the organization. IS security can take many forms but can have mainly been identified and researched in three main categories of technical, formal, and informal controls (Dhillon 2007). Generally, all three types (or levels) of IS security must be coordinated to work in conjunction to maintain security. Dhillon (2007)argues that any incongruence between the three identified categories in practice and implementation can result in IS security failure. Formal controls, controls that have executive oversight and are codified, must be accepted and adopted by individuals to work Field (Bulgurcu et al. 2010; Dhillon 2007) effectively. Additionally, good organizational communication and access to resources can influence individual participation and adoption.

Technical categories of IS security include any component managed and deposited within the overall computer information system apparatus. For example, limits on password character utilization and length, biometric access controls, and digital signatures fall into the technical control category. Information system security encompasses dangers to hardware, software, information, and/or data that jeopardize organizational data security and corporate risk limits. These dangers have been identified as modifications, disclosure, destruction, interception, interruption, or fabrication of network communications or records (Dhillon 2007). Organizations can spend considerable resources developing technical controls to safeguard employees, and

organizational interests, which 'force' stakeholders to comply with IS security objectives (Dhillon et al. 2019).

Without a technical control implementation in place, formal and informal controls cannot be implemented for IS security. In addition, communication about policies and practices from organizational stakeholders, employees, and managers is needed to make sure technical controls are not breached.

2.2.4 Information Security Policy

Information system security policies are codified documents that implement formal organization controls on individual/employee information security behavior (Höne and Eloff 2002). The information security policy primarily establishes the organizational strategy of securely protecting information and provides details on the appropriate use of organizational technology resources (D'Arcy et al. 2009). As a strategic document, the information security policy declares management's desires and commitment to achieving organizational goals and missions related to information security. As with most rules and/or policies, it is an attempt to give guidance that mitigates risk to organizational objectives while guiding protection of information and knowledge-based resources, usage of information technology hardware and infrastructure, and task management practices to protect and secure organizational information (Kwok and Longley 1999). Examples of information system policy include information security-related issues such as password development guidelines and password sharing, authorized access to computers and network resources, storage, and backup requirements, and encryption methods (Dhillon 2007; Herath and Rao 2009a).

Not all information security policies are alike in composition, strategy, or security goals. However, Kwok and Longley (1999)summarized what most information security policies should

encompass. Generally, a security policy should include: (1) the defemination of information security for the organization, (2) the intentions of organizational management to support policy goals and information security in general, (3) compliance requirements and explanations of policies and principles, and (4) individual and organizational responsibilities of what to do in the event of a security incident. Diver (2007) added to these guidelines with the inclusion of sanctions and violations in the event of a breach, definition of technical terms in the document for more straightforward interpretation, and policy revision history and responsibility for policy revision and review.

2.2.5 Information Security Policy Compliance

COVID-19 has introduced increasing uncertainty to work environments where managers and network administrators no longer have direct control of workspaces designed to facilitate social aspects of work and complete tasks in a 'constructed' environment. New technologies are being introduced (and created) for individuals that attempt to allow working environments access to organizational data and information technology systems while also maintaining security protocols. The United States Cybersecurity and Infrastructure Security Agency has issued alerts about "advanced persistent threats" posed by cybercriminals' exploitation of the global pandemic's ongoing uncertainty through phishing attacks and exploitation of teleworking infrastructure (CISA 2020). Gartner, Inc. recently identified several focus areas IS security teams should concentrate on due to "most of the security and risk team now operating in completely different environments and mindsets" which cannot monitor employees (that have more distractions than usual) and may not be as vigilant about IS security (where cybercriminals will attempt to exploit the underlying chaos of the pandemic) (Panetta 2020).

Information Security Policy (ISPs) have recently needed to adapt to these changing work structures and designs to align with the new working environments of stay and work from home orders. Generally speaking, individuals are apprehensive when dealing with security risk decisions during uncertain times and outcomes (West 2008). Organizations have undergone substantial changes concerning working conditions and overall policy structures surrounding COVID-19 and the worldwide pandemic. Even during normal working conditions, employees have been regarded as the least reliable piece of the information system security apparatus (Dhillon et al. 2019; Guo et al. 2011). During this period, employees have been removed from regular work routines and the 'closed' IS system security system apparatus that contains secure networks within organizational offices. ISPs must now be examined under rapidly changing and uncertain environments to maintain information security. Furthermore, ISPs may no longer provide employees with needed support or resources to accomplish work from home tasks concerning data transfers and secure networks. maintained and integrated to remote and uncertain environments is becoming increasingly important. New strategies are needed to determine how employees deal with a changed work and social system and uncertainty in daily routines surrounding work, family, and social settings and how ISPs are affected by uncertainty within the workplace during this time. Additionally, identifying how individuals are motivated outside the workplace and adhere to ISP requirements during uncertain life events concerning job-based resources, managerial input, and work task changes and issues become increasingly

2.3 Key Constructs

The relevant literature search appears in Appendix 1. The key concepts used in this research are summarized below.

2.3.1 Motivating Individuals for ISP Compliance

This section will discuss the key concepts used in this research and develop the hypotheses tested as part of our research framework.

2.3.1.1 Perceived Work Uncertainty and Security Policy Compliance.

Information system policies are considered by many to be a legal formulation of what organizations expect from employees surrounding issues of technology use, information processing, and information sharing. Organizations and employers develop information security policies with the expectation that subordinates and employees will engage in activities concerning information transfer and access that comply with the stated policies and organizational goals. During times of work uncertainty, when the ISP can be less clear about security practices, the ISP itself does not address or detail individual needs surrounding information access and transfer, or managerial guidance surrounding policy attributes is lacking, employees are expected to draw on their agency and intrinsic motivations to determine the best course of action between compliance parameters and work progress. Griffin et al. (2007) proposed that work context was better defined within an organizational social system that, when facing uncertainty (which existed within the work role), individuals exhibited behaviors associated with proficiency, adaptability, and proactivity by acclimating to the new environment. Worker psychological empowerment is closely associated with individual intrinsic motivation toward positive ISP compliance behaviors (Dhillon et al. 2019). While empowerment has been promoted as a foundation to enhance individual work performance, it has been shown to be reliant on the extent of uncertainty within the operational environment which allows the individual to rely on their skills and abilities (Wall et al. 2002). The correlation between intrinsic empowerment and uncertainty is recognized in work design literature (Cordery et al. 2010; Wall

et al. 2002) Njenga and Brown (2012)suggested employees improvised through rational and adaptive ways to secure information in volatile and uncertain organizational environments concerning information system security.

2.3.1.2 Intrinsic Motivation and Security Policy Compliance.

Information system literature has been attentive to intrinsic rationales of motivation concerning information security (Yazdanmehr et al. 2020). This attention has focused on perceived feelings of self-efficacy or feelings of competence (Dhillon et al. 2019; Herath and Rao 2009b; Vance et al. 2012), perceived effectiveness of security-related engagements (Boss et al. 2015; Dhillon et al. 2019; Herath and Rao 2009a), goal and value alignment (Li et al. 2014; Son 2011a), and perceived ownership of information assets without accountability (Anderson and Agarwal 2010; Lee and Chen 2011).

Son (2011a) incorporated intrinsic and extrinsic motivators to understand why employees choose to follow or not follow information security policies within their organization. As a result, explaining ISP compliance behaviors was better illuminated with intrinsic motivators. Menard et al. (2017) compared intrinsic motivations with from Deci and Ryan (1980) self-determination theory with more extrinsic factors from Protection Motivation Theory (PMT). When security messages were constructed to appeal to individual intrinsic motivations and provide more choice for computer users to engage with information security problems, observers reported better ISP compliance behavior (Menard et al. 2017). These results differ from fear-based motivations which is part of the criminological theory associated with PMT,

Chan et al. (2005) argued that individual perceptions concerning the overall security climate and individual beliefs that they could identify and mitigate security threats were beneficial to positive ISP compliant behaviors. Generally, security breaches are caused mainly

by individual employees' unwillingness to comply with ISP's set forth by the organization, especially concerning the opening and forwarding of malicious email attachments (Chan et al. 2005) or general file-sharing habits (Nguyen and Kim 2017). Cuganesan et al. (2018)identified that informal workplace norms such as managerial support and overall organizational security compliance influenced ISP behavioral compliance self-efficacy beliefs. Senior management support was recognized to influence how employees think about information security both directly and indirectly (Cuganesan et al. 2018).

Perceived effectiveness has been identified as an antecedent to ISP compliance in individuals. Even though organizations that are heavily dependent on data collection and storage for operations tend to implement vast arrays of technology tools to provide data security, tracking end-users security behaviors is not entirely possible with such capabilities (Herath and Rao 2009a). Herath and Rao (2009a)argued technological (hardware) implementation is not sufficient to secure information finding end-users intrinsic motivation (including perceived effectiveness in the implementation of technological and policy tools) was more applicable to positive compliance behaviors. Perceived effectiveness has also been identified as an antecedent for employees' intentions to routinely act in accordance with ISP's when referring to the scope of the policy. Park and Yim (2012) argued that more comprehensive information security policies influenced one's perceived effectiveness of the policy and compliance with the behavior. Still, the scope of the policy itself did not affect persistent policy compliance intentions. This indicated that words matter to individuals when dealing with whether to comply with IS policies showcasing how one perceives the policy to implement security procedures is more important than the policy itself (Park and Yim 2012).

As organizations establish security policies surrounding network and information resources, value alignment concerning organizational and individual security priorities plays a significant role in compliance behaviors (Gangire et al. 2019; Herath and Rao 2009b; Qu et al. 2019). Trustworthy and accurate leadership of the organization, regardless of value alignment, has encouraged unconditional positive behavioral performance; however, positive outcomes are limited when coupled with leadership seeking power and control (Qu et al. 2019). These findings indicate power structures that inhibit intrinsic motivation and elevate extrinsic reward or sanction are counter to positive ISP behavior. Li et al. (2014)identified intrinsic values of organizational justice and personal ethical objections toward network and information infrastructure abuse leading to positive compliance behavior. Findings indicated that as organizational justice and personal ethics come closer in congruence, self-regulation (an intrinsic motivation antecedent) influences ISP compliance behavior directly and indirectly (Li et al. 2014).

2.3.1.3 Security, Education, Training, and Awareness and Security Policy Compliance.

Misuse of organizational information systems resources is a threat to organizations and accounts for many of the security violations organizations encounter (D'Arcy et al. 2009). However, security education, training, and awareness (SETA) programs to teach individual employees organizational information security policies and identify and deal with security threats have created work environments that empower ISP compliance behavior (Dhillon et al. 2019; Kim et al. 2019). Modern organizations are dependent on those who have access to organizational information and information-based systems to secure said systems and data. Burns et al. (2018) argue SETA programs motivate proactive and omissive behaviors concerning ISP behavior due to expected outcomes. Organizations can develop behavioral expectations, specific

outcomes associated with protecting organizational data, and an attitude that the induvial can make a difference when engaging in information protection for the firm when given appropriate SETA access (Burns et al. 2015).

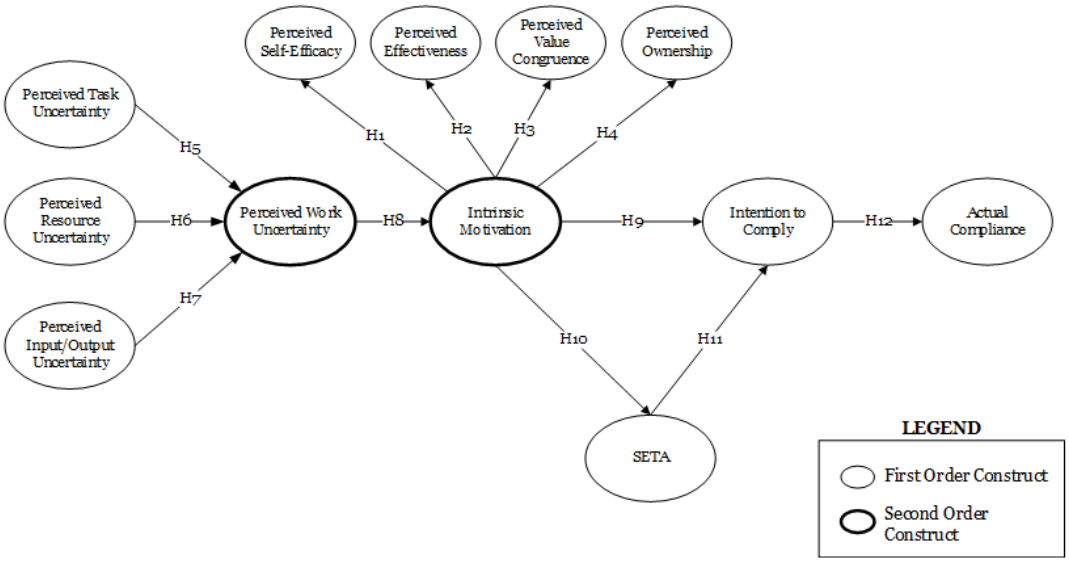
2.3.2 Perceived Work Uncertainty and Intrinsic Motivation

Within work design literature, uncertainty has long been investigated concerning how employees execute tasks through a general lack of information (Lawrence and Lorsch 1969) and the resources needed to perform such tasks (Cherns 1976). Job crafting is one such premise that allows the organization to take a bottom-up, employee-driven approach to make job adjustments when work uncertainty is high (Grant and Parker 2009). In addition, work design theory has empirically found that autonomy in the job should sometimes mimic the level of uncertainty encountered, allowing for increased intrinsic and work motivation to accomplish work tasks (Cordery et al. 2010; Knight and Parker 2019). However, increased control during low uncertainty does not yield better worker performance (Knight and Parker 2019; Wright and Cordery 1999).

Increases in work uncertainty have been linked with proactive perceptions by employees to engage in the work environment showing initiative to foresee and create changes in accomplishing work (Grant and Parker 2009). Creating new work processes is inherently central to intrinsic motivation to carry out tasks. When the environment shifts rapidly, work characteristics have shown autonomy in work groups to enhance work motivation, quicker response times to shifting environments, and learning about new work requirements as core mechanisms to increased performance (Knight and Parker 2019). These findings closely align with SDT and work motivation as integral to increased work performance and are closely associated with intrinsic motivations (Gagné and Deci 2005).

2.4 Conceptual Model and Research Framework

Figure 1: Conceptual Model and Research Framework



2.5 The Role of Intrinsic Motivation

Opposite from which organizational security policies and procedures are implemented and how individuals are disciplined for non-compliance external to employees, intrinsic motivation is associated with what desires and preferences individuals utilize to motivate themselves for ISP compliance. As a result, intrinsic motivations are becoming more important within the ISP compliance literature (Dhillon et al. 2019; Yazdanmehr et al. 2020). Intrinsic motivation is self-regulatory and allows individuals to determine whether or not to participate in ISP compliance decisions without external reinforcement.

Self-determination theory (Deci and Ryan 1980; 2010) describes self-motivation through autonomy, competence, and relatedness that individuals feel by performing tasks themselves. On the other hand, intrinsic motivation is closely associated with individual empowerment allowing persons to complete tasks simply for "the pleasure and satisfaction derived from participation

(Vallerand et al. 1992, p. 279)". Recent findings had investigated both internal and external motivations for ISP compliance issues and found that external motivations associated with ISP compliance become less meaningful when internal motivations are also included (Yazdanmehr et al. 2020), that intrinsic motivators explain more variance on intention to comply with ISP (Menard et al. 2017), and act as stronger predictors toward ISP compliance (Son 2011a).

Perceived self-efficacy is an intrinsic belief that an individual can perform tasks due to ones' ability or competence and is tied to social cognitive theory (Bandura 1986). For ISP compliance, individuals who feel they have the necessary skills or knowledge to carry out security policy could become empowered to perform functions that may (or may not) be explicitly stated. Previous investigations in information systems literature found perceived self-efficacy influenced or mediated individual information security policy performance (Abraham and Chengalur-Smith 2019; Chan et al. 2005; Dhillon et al. 2019; Rhee et al. 2009). Dhillon et al. (2019)noted the importance self-determination plays in employee's choices which can create higher levels of empowerment toward ISP compliance decisions, while Chan et al. (2005)found that attaining additional knowledge of information security issues through training or other means has a positive impact on an employee's ISP compliance behavior. Therefore, we hypothesize:

H1*: An individual's perceived self-efficacy to correctly identify information security breaches and policy failures increases individual intrinsic motivation.*

Perceived or psychological ownership is an individuals' psychological state for connections toward objects and concepts, including ownership of corporate data, computer devices, and data transmissions (Anderson and Agarwal 2010). Closely associated with self-efficacy and self-identity, investigations have indicated that individuals who experience a sense

of ownership can exhibit behaviors motivated toward higher levels of ethics and/or responsibility on security-related outcomes (Lee and Chen 2011). For example, Menard et al. (2018) showed that individuals who perceived ownership of organizational information sensed the data were more susceptible to threats, generally more severe, and were more likely to follow recommended responses to security threats. For this reason, if an employee develops higher levels of perceived ownership over organizational data, we may conclude that:

H2: *An individual's perceived sense of personal ownership over organizational data and technological resources increases individual intrinsic motivation.*

Intrinsic motivation allows individuals to exhibit behavior whereby actions associated with individual preference and aspiration outweigh external rewards and sanctions. Employees can investigate differences between employer values and their own through experiential contact and belief domains (Tyler and Blader 2005) concerning ISP compliance decisions. Perceived value congruence is identified as the alignment of values between employer and employee. Son (2011a)found intrinsic motivators such as perceived value congruence to be stronger predictors of ISP compliance for employees over extrinsic motivators. We would then expect those perceptions of employees that the value set between themselves and the organization would lead to higher levels of intrinsic motivation of ISP compliance decisions by employees. Therefore:

H3: *An individual's perceived value congruence with the organization increases individual intrinsic motivation.*

Employees' perceptions of information security countermeasures can influence employee motivation to comply with a given policy. As employees react to security threats, measures that seem overly disruptive to work flows (i.e.: long or complicated password requirements) or are perceived to be ineffective due to non-compliance (such as password sharing) can influence

compliance decisions. Employee perceptions of the effectiveness of their actions have shown to be partly responsible for positive ISP compliance decisions and create favorable impacts and benefits for the organization (Herath and Rao 2009a). We would then hypothesize that:

H4: *An individual's perceived ability to effectively control ISP-related breaches and failures increases individual intrinsic motivation.*

2.6 The Role of Work Uncertainty

Employees' fundamental assumptions about the system they work in are called into question as operations become disrupted during a crisis, and basic norms about work and organizational activities become challenged (Carmeli and Schaubroeck 2008). Uncertainty increases during these periods as managers and employees lack needed information from superiors (generally due to the inability to provide answers). Additionally, resources to determine acceptable outcomes for any given decision and variability in everyday work tasks can limit employees' ability to counteract work disruptions.

During organizational and environmental change, failures of existing structures and rational choice frameworks can create uncertainties requiring employees to develop new decision-making arrangements, leading to new decision processes (Ciborra 1996). A changing structural work environment can lead to tasks surrounding information security policy and management becoming unpredictable, resources scarce, and employees' knowledge and feedback from managers regarding work policies insufficient or inconsistent. Work design theory investigations have advocated for increasing job control by employees due to higher levels of organizational or environmental uncertainty where work demands generally do not match job descriptions, policies, or procedures specifying how employees should carry out work tasks (Leach et al. 2013; Parker et al. 2001; Wall et al. 2002).

The literature generally defines uncertainty as to the inability to determine an outcome of a choice surrounding work activities (Milliken 1987). *However, perceived work uncertainty* related to work design (and re-design) differs from job uncertainty, where the primary concern for individual workers is composed of "job characteristics and the broader work context" (Leach et al. 2013, p. 86) and not job security or role ambiguity. Leach et al. (2013) also suggested and verified work uncertainty to be separate from process clarity concerning how individuals accomplish tasks and job control whereby employees experience higher task management responsibilities.

Organizational change research has identified instances where the breakup of existing work structures, work resources, and rational choice framework create uncertainty leading to increased ISP tension from disrupted workflows and information scarcity (Ciborra 1996; Njenga and Brown 2012). Work design literature identified uncertainty as a core contingency where reliability and complexity of work needs affect work outcomes (Leach et al. 2013), such as job performance per policies and procedures to perform work. Parker et al. (2001) noted work designs are in many cases not aligned with circumstances facing employees. Leach et al. (2013) defined *perceived resource uncertainty* (in the work design context) as the lack of reliable and available information to execute work tasks effectively in any given job design as a contributing measure of overall work uncertainty. Given this definition, studies have shown that resource uncertainty creates stress leading to less work engagement (Hornung et al. 2010), decreased mental health, impaired work function, and hampered goal attainments (Schneider et al. 2017). Bulgurcu et al. (2010b) noted the importance of ISP quality characteristics (ISP clarity, completeness, and consistency of the ISP resource) on individual intentions to comply. For ISP-related resources, when employees perceive work tasks have no straightforward, reliable

resource for reference--or policies and procedures are not delineated--the ability to carry out work functions surrounding security-related issues and procedures will be limited. Therefore, we hypothesize:

H5: *A perceived lack of access to resources concerning Information Security Policies is positively related to perceived ISP work uncertainty*

Task uncertainty stems from employees' perceptions that work roles may be overly complex, dynamic, and non-routine (Ben-Ner et al. 2012; Ujma and Ingram 2019). Employees understandably encounter variability and unexpected issues when performing work tasks (Leach et al. 2013), especially during times of crisis or organizational change. When workers have set work descriptions or policies that formalize expectations of task accomplishment, anticipating how work gets completed within uncertain environments may become difficult (Griffin et al. 2007; Leach et al. 2013). Our second hypothesis reflects the perceptions that tasks surrounding ISP are variable and dynamic, leading to difficulty in accomplishing the job at hand:

H6: *An individual's perceived uncertainty surrounding the completion of daily work tasks related to ISPs is positively related to perceived work uncertainty variability*

Employees serve as both givers and receivers of information. Individuals who provide information concerning policies, procedures, work requirements, or other work-related materials can affect employee performance (Leach et al. 2013). As employees seek materials and information to carry out specified work roles, the supply of materials or information may become limited or unreliable (Cherns 1976). When employees become uncertain about specific policies to execute work tasks and seek help from managers to alleviate conflicts to provide guidance. Therefore, we hypothesize:

H7*: Perceived uncertainty concerning managerial knowledge/input regarding ISPs is positively associated with perceived work uncertainty.*

2.7 Perceived Work Uncertainty and Intrinsic Motivation

Under work design strategies, empowerment of individuals during a time of more significant uncertainty is more effective than job simplification, allowing individuals to rely on intrinsic skills to determine the best courses of action (Clegg 1984; Leach et al. 2013; Perrow 1967). The breakup of existing 'mechanistic' work structures and rational choices can create periods of work uncertainty where employees have been found to develop their decision-making arrangements and processes (Ciborra 1996). Organizational theory suggests more flexibility and decentralized decision-making under unpredictable or uncertain environments (Bruns and Stalker 1961) and is associated with more 'organic' work structures (Wall et al. 2002). For example, Njenga and Brown (2012)found that employees improvised information security activities to compensate for the loss of rational choices during uncertain periods. Employees have also sought to alleviate ISP tensions from disrupted work flows in reactions to digital transformations through 'non-malicious' internal motivations (Raza et al. 2019). We would therefore determine that as uncertainty increases, individuals will rely on intrinsic motivators to alleviate ISP work-related stresses and hypothesize:

H8: *Perceived work uncertainty will positively increase intrinsic motivations to engage in ISP compliance behaviors*

Additionally, self-determination theory suggests individuals will self-motivate during uncertain times due to more autonomy, competence, and relatedness needs to prevent undesired consequences and the lack of reinforcing procedures to externally motivate when performing tasks (Deci and Ryan 1980). During times of uncertainty, such as the COVID-19 pandemic,

employees have been faced with new work structures, work environments, and overall uncertainty about work procedures concerning ISP, including work from home arrangements, home Wi-Fi security needs, or practical use of personal computing devices to use, store, or analyze secure data. Given prior research that as uncertainty increases, employees will (and should) seek to self-determine courses of action concerning ISPs, then we believe:

H9: *Intrinsic Motivation mediates the relationship between work uncertainty and individual intentions to comply with information security policies (ISPs)*.

Empowered working conditions have underpinned organizational theory advocating for increasing job control and decision-making authority, leading to improved job performance (Wall et al. 2002). Work structures allowing for access where individuals can seek knowledge or academic opportunism has contributed to intrinsic motivation increases of perceived competence in task performance (Spreitzer et al. 1997; Thomas and Velthouse 1990). Security education, training, and awareness (SETA) programs generally provide information and knowledge to individuals concerning the IS security environment while offering guides for employees to equate their understanding of information security policy and procedures (Bandura 1986; D'Arcy et al. 2009). Recently, antecedents to intrinsic motivators, such as SETA, increased intentions to comply with ISPs (Dhillon et al. 2019). However, during times of uncertainty and stress, employees rely on intrinsic motivations to self-determine courses of action concerning ISPs. Intrinsic motivators (such as perceived psychological ownership) have shown positive impacts on the effectiveness of successful SETA completion (Yoo et al. 2018). As uncertainty on work processes increases and employees become tasked with determining the best course of action concerning information security requirements and needs, employees will be intrinsically motivated to seek out knowledge concerning the security environment. We propose:

H10: *Intrinsic Motivation mediates the relationship between work uncertainty and organizational SETA programs.*

2.8 The Mediating Role of SETA

SETA programs can take many forms and provide individual users with information necessary to understand different security environments while providing the skills necessary to implement security procedures (D'Arcy et al. 2009). SETA program awareness relies on the employee's perceptions about the organization's rules, policies, and procedures of information security governance (Kim et al. 2019). Work design theory indicates that individual empowerment and intrinsic work motivations should be allowed to increase during uncertainty (Leach et al. 2013). Hui and Lee (2000), for example, identified intrinsic motivators as tools to help individuals process the structural and/or environmental situation surrounding specific courses of action while denoting "the relationship between a person and his/her job (p.216)." SETA is a structural empowerment external to individual motivation where education concerning security policies and procedures is learned. Still, the extent of the threat of sanction and reprisals when policies are not followed is also discussed (Dhillon et al. 2019). During times of uncertainty, employees rely on intrinsic motivations to administer compliance decisions through the structural or environmental situation process. When accessing self- and response-efficacy concerning ISP compliance decisions and determining external security threats, individuals will access if the necessary skills have been acquired to respond to any security-related event (Herath and Rao 2009ab). Given any lapses in personal knowledge or skills needed to comply with ISP requirements, we propose that employees will seek out structural knowledge bases, such as the organizational SETA programs, as intrinsic motivation to attempt to comply

with ISP's increases during times of uncertainty. Such engagements with the SETA program will mediate between IM and intentions to comply with the ISP. Thus:

H11: *SETA will mediate the relationship between intrinsic motivation and intention to comply with ISPs.*

2.9 Intentions to Comply with ISP's and Actual ISP Compliance

Behavioral intention is connected to an induvial intention to carry out a specified behavior, including compliance with an information security policy. Therefore, in conjunction with Limayem et al. (2007)and Siponen et al. (2010)calls to include the actual behavior compliance within IS research so that IS research may not reach the wrong conclusion, we hypothesize:

H12: *Individuals who intend to comply with ISPs during uncertain work conditions will comply with ISPs.*

2.10 Conclusion

This concludes our discussion of the literature, research framework, and hypothesis development. We will continue next with a discussion of the methodological approach taken to test the above hypotheses in Chapter 3.

CHAPTER III: RESEARCH METHODOLOGY

3.1 Introduction

In the previous chapter, we presented the literature on uncertainty and intrinsic motivation related to security policy compliance. This chapter explains how the various constructs relate to reaching others and how we conducted the research. A methodology provides a roadmap to present our analysis and our findings in any research. Our proposed research framework scientific presents an investigative report of the quantified relationships between our theorized constructs. In other words, our research examines the cause and effect of the various relationships. Therefore, the objective of this chapter is to present a research methodology that was used to conduct the research.

3.2 Quantitative Research Design

Research can take many forms while being rooted in different approaches to address varying investigative inquiries. Phenomena of research interests can be approached through qualitative, qualitative, or combining the two approaches to reach conclusions or test hypotheses. Different paradigms influence how each approach is investigated and how theories are developed. Quantitative approaches are contained within the positivist paradigm, where theory testing manifests from formal propositions. These variables can be quantified, leading to hypotheses tests and inferences made about the phenomena of interest about a specific population (Orlikowski and Baroudi, 1991). Under the positivist approach, investigators believe in objective reality fixed from measurable observation allowing for theory testing. Positivist research adheres to the principle that the researcher is removed from the phenomena and only acts as an independent observer to collect data for analysis. Data collection is developed through an empirical setting allowing for the investigation of theory through hypothesis development.

This chapter will lay out the methodology incorporated into our research. We will begin with the research population of interest and our sample collection method, followed by our construct measurement techniques. We will then follow our data collection procedures and finish with our data analysis.

3.2.1 Research Population and Sample

Our study focuses on how intrinsic motivation mediates the relationship between work uncertainty involving organizational uncertainty and/or crisis times and information security policy compliance. The unit of analysis for this study is the individual worker, as all workers are responsible for ISP compliance issues. The target population is any full-time employee operating in all functional areas of an organization and at all job and skill levels. Zikmund (2000)identified the convince sampling method to sample populations of interest, which is our choice technique. Therefore, we will sample individuals who work full time in the United States during organizational change and stress/crisis identified as the COVID-19 pandemic. The rationale for selecting this sample is rooted in the crisis that many organizations find themselves in when ISPs are not uniquely suited to large, and rapid shifts in workforce settings. This period, therefore, provides the individual worker with little information and precedent to define ISP policy concerning transfers of information form work-from-home offices and contact with sensitive information within and outside organizational intra- and extranet settings. Because individuals have systemically moved to WFH settings and traditional means of sampling, the individual has progressed to online methods, and we utilized Amazon Mechanical Turk to sample our target population. This sampling method provides a unique setting from which the intersecting of intrinsic motivations and perceived work uncertainty can be sampled and tested—the underlying issue of this study.

Structural equation modeling has been performed well with sample sizes between 100 and 400 participants (F. Hair Jr et al. 2014). However, sample sizes larger than 400 have yielded non-significant improvement in statistical analysis using SEM methods (F. Hair Jr et al. 2014). Other considerations, such as the number of constructs within the model, the number of derived items for measurement, and the extent by which missing or imputed data are used, can influence the sample size needed. Other researchers have indicated sample sizes of around 300 participants can adequately derive SEM modeling needs. Comrey and Lee (1992) and Comrey and Lee (1992) indicate a general rule of 300 as a satisfactory sample size. Given this analysis, we will adopt a sample of at least 300 participants as sufficient to conduct statical analysis and hypothesis testing.

3.2.2 Measurement of Constructs

A common source for measurement error is that of common method variance. Common method variance references the illegitimate covariance shared between variables of interest due to the common method to data collection (Malhotra et al. 2006) and is typically found in cross-sectional studies. For survey studies where individuals are asked to respond to items in a single survey or questionnaire simultaneously, common method variance in the data is generally present (Lindell and Whitney 2001). Podsakoff et al. (2003)indicated common method variance could impact relationships between independent and dependent variables and suggested two techniques to control this influence: Procedural remedies within the survey and a statistical control to provide mathematical limits on item outcomes. Procedural strategies can be implemented within the survey instrument to limit common method variance between predictor and outcome variables. One such strategy is to source dependent and independent item responses from different sources (Podsakoff et al. 2003). For purposes of this dissertation, independent

items such as intrinsic motivation, perceived work uncertainty, security education, and training, and the independent variable for information security policy compliance would need to be obtained from different individuals for this mitigation technique to work. However, due to the need to examine relationships between identified variables for each individual, this technique cannot be applied and/or utilized.

A second procedural method suggested by Podsakoff et al. (2003)included a temporal separation of the independent and dependent variables through a longitudinal study. Longitudinal studies are different from cross-sectional studies because they involve measurements over a selected period instead of a measurement at a single point in time. For purposes of this study, longitudinal measurement is not possible due to a lack of resources and time, and a cross-sectional approach is applied.

Podsakoff et al. (2003)provided a third procedural method to combat common method variance if the cross-sectional approach is taken that of respondent anonymity. This approach suggests that the respondent's identity be kept confidential, allowing for the honest answering of questions for independent and dependent variables without risk of respondents succumbing to social pressures based on their response or some judgment to a response from the investigator. For this study, we adopted this technique and communicated to all respondents the lack of data collection on identity, or IP addresses, for which any response can be traced.

Podsakoff et al. (2003) suggested a final procedural method to combat CMV is segregating item questions about each construct and not keeping them clustered together. We utilized and adopted this technique in this study. The identified counterbalancing technique reduces an item-context-mood state that can be developed by the respondent (Podsakoff et al.

2003). In addition, items were coded with unique identifiers to help the researcher identify the parent group of each item question for data analysis purposes.

Statistical methods to test for and reduce CMV have been widely utilized. Statistical construct validity and reliability tests are examples of determining if CMV exists. Construct validity is performed to determine how the researcher accurately measured what was intended. Because psychological constructs are not observable, challenges exist to measure them convincingly and validly (Smith 2005). Straub (1989) identified three types of instrument validation: content validity, construct validity, and reliability. Hair (2009)suggests two primary validity tests for construct validity and overall model fit. Content validity stipulates that the researcher draws item questions from a representative pool to disallow bias within the results and is sometimes difficult to create (Smith 2005). Cronbach (1971) suggests evaluating questions by experts in the field until a consensus is reached on the content of the questions for each construct or item. For this research, content validity was not tested as all item measurements had previously been vetted and established as quality items to measure the desired constructs.

Construct validity seeks to determine if the items chosen to develop the construct accurately performed that service while also determining if the theories generated before data collection are accurately reflected in the statistical analysis (Hair 2009). As stated previously, because of the inability for many constructs to be physically observable due to psychological constraints (such as emotion), the operationalization of the constructs must be translated into a set of items intended to measure theoretical accuracy truthfully. Our study develops measurements based on well-tested theories and past empirical analysis. As Smith (2005) stipulates in the five-step model for construct validation, construct validity is an ongoing and cyclical process whereby previously validated items are consistently scrutinized and base

theories revised over time. This study continues with that tradition of assessing the chosen items for measurement and an analysis of the results of statistical analysis for construct validity will be presented later.

Reliability analysis deals with an "internal consistency of a measurement instrument," with the common usage of Cronbach's alpha for the coefficient of internal consistency as a computation "for each of the construct components (factors) determined from the factor analysis, using the same data (Lewis et al. 2005, p. 393)". Therefore, when items are used repeatedly to test constructs with data from different respondents, reliability tests should generate consistent results between those individuals. Cronbach's alpha (α) averages split-half correlations to determine this value whereby $\alpha > 0.70$ are considered to be highly reliable (Hair 2009). Therefore, we only utilized previous items with high reliability when developing our constructs.

We will now discuss the definitions utilized within the research framework. All measurements utilized for our study were developed and validated previously in various behavioral and empirical research.

3.2.2.1 Intended and Actual Information Security Policy Compliance.

Information security policy compliance can be attributed to the degree to which employees intend to (or actually follow through with) comply with the organizational information security policy as stipulated. While compliance can be a range of behaviors prescribed by the policy, no one behavior, by the individual employee, supersedes another. Additionally, when employees recognize and constructively protect organizational information security behavior mechanisms, they aggregate into mitigating security threats or breaches. For this study, intentions to comply with information security policies were borrowed from Bulgurcu et al. (2010). They included three questions with responses ranging from (1) strongly disagree to

(5) strongly agree on a Likert-type scale. However, the internal consistency was reported at acceptable levels of $\alpha = 0.75$.

Actual behavior differs from intentions, whereas actual compliance is more closely related to moral reasoning and accounts for factors that influence a hypothetical position on compliance (Siponen et al. 2006). However, much the same with intentions, actual behaviors (when strung together) can help mitigate security threats or breaches. Three items were used from Siponen et al. (2006)to measure actual information security policy compliance. For example, respondents were asked how much they agree or disagree with statements such as "I complied with information security policies," "I recommend other comply with information security policies," and "I assisted others in complying with information security policies." The same Likert-type scale was used as the intention to comply with respondents asked to (1) strongly disagree to (5) strongly agree.

3.2.2.2 Intrinsic Motivation.

Intrinsic motivation involves behaviors that cannot be clearly linked to some external outcome and exist from an individual's desire to regulate oneself and not be regulated by others (Deci and Ryan 1980). Additionally, Deci and Ryan (1980)indicated intrinsic motivation endures between a person and a task which suggests that performing a task can be reward enough for the individual to be fulfilled in, or satisfied with, a particular behavior. IS researchers have incorporated intrinsic motivations, including perceived self-efficacy (Chan et al. 2005; Dhillon et al. 2019; Herath and Rao 2009a; Workman et al. 2008), perceived ownership (Anderson and Agarwal 2010; Van Dyne and Pierce 2004), feeling about organizational and individual value alignment (Son 2011a) and perceived effectiveness of the policy when behavior is activated (Herath and Rao 2009a).

3.2.2.3 Perceived Effectiveness.

Perceived effectiveness addresses employee beliefs surrounding information security policy activities or behaviors that, if adopted and activated, would be beneficial to the organization (Herath and Rao 2009b). For our investigation, we accept this view as the intrinsic incentive that individual employees will partake in positive behaviors to secure information for the organization when that contribution is beneficial to the workplace environment or overall organizational stability. Herath and Rao (2009b)detailed that perceived effectiveness as a measure of intrinsic motivation could help determine individual actions to comply with information security policies. Therefore, we adopted the measure utilized by Herath and Rao (2009b)containing three items such as "Employees can make a difference when it comes to helping secure the organization's information systems and data," "There is not much that any one individual can do to help secure the organization's information systems," and "If I follow the organization information security policies, I can make a difference in helping to secure my organization's information systems," and which demonstrated high reliability of $\alpha = 0.79$.

3.2.2.4 Perceived Self-Efficacy.

The theory of self-efficacy maintains low self-efficacy will lead to behaviors meant to avoid specific tasks and vice versa. Perceived self-efficacy references when an individual believes they have the capability to perform a particular task (Bandura 1986). Self-efficacy is pervasive in information security research finding individual efficacy influencing behavior in a decision to engage (or not engage) in security policy tasks, continue information security-related technology use, and increase knowledge about security-related issues (Chan et al. 2005; Dhillon et al. 2019; Rhee et al. 2009; Workman et al. 2008). the theory of self-efficacy maintains low self-efficacy will lead to behaviors meant to avoid specific tasks and vice versa. Items for this

measure were borrowed from Herath and Rao (2009b), which showed high-reliability rates. These items' reliability was reported to be at acceptable levels above $\alpha = 0.70$.

3.2.2.5 Perceived Ownership.

Perceived ownership emanates from protection motivation theory and directs individual behavior based on the level of ownership one may perceive on the resource that needs protection, such as the information security policy (Anderson and Agarwal 2010). A component of intrinsic motivation, connected with the efficacy one has toward some entity, perceived ownerships can facilitate activities that a person can find as affirmative and appropriate for a particular behavior (Anderson and Agarwal 2010), such as information security policy compliance. Therefore, we adapted item measures from Anderson and Agarwal (2010), which demonstrated high-reliability measures and internal consistency greater than $\alpha = 0.70$

3.2.2.6 Perceived Value Congruence.

Son (2011a)identified perceived value congruence as the alignment between organizations' security values and polices and that of the individuals' values and beliefs toward information security. When the value systems between an individual and organization are similar and follow similar standards of information security protection, long-term behaviors toward securing information will be attained, and employees will be intrinsically motivated to perform security tasks for the organization (Son 2011a). However, the reverse was also found to be true. When the value systems about information security were not aligned, the individual could threaten the organizational information security apparatus (Son 2011a). Therefore, employees who have perceived value congruences are believed to have positive information security behaviors. Items for this measure were adopted from Son (2011a), which reported an acceptable level of reliability ($\alpha = 0.89$).

3.2.2.7 Security Education, Training, and Awareness (SETA).

Security education, training, and awareness are defined as the beliefs an employee may have about the information security policy of the organization, and the continuing accumulation of knowledge about information security problems and issues, underlying consequences for the organization and individual for non-compliance, and appropriate means to take proactive action to prevent security breaches (D'Arcy et al. 2009; Dhillon et al. 2019). Dhillon et al. (2019)found SETA positively empowered and motivated employees (both directly and indirectly) in information security behaviors. Five items for this measure were borrowed from D'Arcy et al. (2009). They comprised questions including an individual's ability to deal with security-related issues, if they felt the organization provided them with the proper education on consequences of non-compliant information security-related issues, and if they felt trained adequately to identify information security threats. In addition, D'Arcy et al. (2009)reported a reliability level of α = 0.88 which is an adequate level.

3.2.2.8 Perceived Resource Uncertainty.

Resource uncertainty is defined as having an adequate organizational apparatus or appropriate information available to the employee to undertake work tasks effectively (Leach et al. 2013). Within work design literature, access to resources has been found to support individual self-efficacy when adequate resources were in place to afford task discretion allowing for reduced work stress and increased employee well-being (Schneider et al. 2017; Xu and Payne 2020). Conversely, when resources are limited or lacking, especially during organizational change or stress, employees may fear the decision environment, which leads to negative outcomes for the organizational apparatus (Jordan et al. 2020) and thus increases task ambiguity and decreases job-self-efficacy (Xu and Payne 2020). Examples of such mechanisms are

information security-related tasks. Resource uncertainty items were borrowed from Leach et al. (2013)and included three measures and an acceptable internal consistency reported at $\alpha = 0.76$.

3.2.2.9 Perceived Task Uncertainty.

Perceived task uncertainty is defined as the variability that tasks may have when executed, unexpected problems associated with task accomplishment, or a general complexity involved with carrying out a work requirement (Leach et al. 2013). When information security policies do not effectively define what is expected from an employee to sufficiently perform one's job (or provide measures to attain work goals), employees will be left to determine proper paths to alleviate the uncertainty created from the lack of IS policy clarity. Studies have shown task uncertainty to reduce work performance initially when coupled with enhanced education and autonomy to allow for employee discretion; positive relationships emerged to increase overall performance when task uncertainty was present (Cordery et al. 2010). Additionally, task uncertainty can affect organizational commitment (Ujma and Ingram 2019) and affect individual decision-making that employees can control (Ben-Ner et al. 2012). Three task uncertainty measures were borrowed from Leach et al. (2013) with a reported Cronbach's alpha of $\alpha = 0.79$.

3.2.2.10 Perceived Input/Output Uncertainty.

Employees or individuals can provide information or other job-related materials and influence the work-related demands of individual employees--such as managers (Leach et al. 2013). Input/output uncertainty concerns the reciprocal relationship between a manager and/or employee who depends on providing information and clarifying job-related responsivities (Leach et al. 2013), such as interpretation of information security policy. Input/output uncertainty-related items were borrowed from Leach et al. (2013) and had an acceptable internal reliability level of $\alpha = 0.87$.

All items for the survey instrument utilized a seven-point Likert scale ranging from (1) Strongly Agree to (7) Strongly Disagree. Table 1 summarizes the items utilized in the dissertation.

3.3 Instrument Pre-Testing

This study aims to determine the extent to which intrinsic motivation mediates the relationship between perceived work uncertainty and information security policy compliance. While we borrowed measurement items from existing and established research, modifications were made to items to reflect the thrust of this dissertation better.

While we borrowed measurement items from existing and established research, modifications were made to items to reflect the thrust of this dissertation better. While no modification was performed from a data collection perspective, any changes in wording and coding can negatively affect the overall reliability and internal validity of identified constructs. Therefore, initial pre-tests were performed to determine that the original construct maintained statistical adherence to original reliability calculations.

Part of this review process involved utilizing experts in the corresponding fields to determine that changes were consistent with the original intent of the items of interest before initialization and pre-testing. The questionnaire was submitted to non-study participants to address language, clarity, and reliability issues before final survey adoption. Some slight modifications were adopted based on feedback received, and final adoption occurred.

3.4 Data Collection Procedures

This dissertation (and overall study) focused on a single point in time for data collection, which is defined as a cross-sectional study. The questionnaire was distributed electronically (online), where individuals were given instructions on how to complete the self-administered

Table 1: Measurement Items and Sources

Variable	Item	Source
RU1	The Information Security Policy at your organization sufficiently lays out the rules to perform work functions.	Desmond Leach et al. (2013)
RU2	The Information Security Policy at your organization is consistent in terms of the rules and procedures.	Desmond Leach et al. (2013)
RU3	The Information Security Policy at your organization provides sufficient information to perform work functions.	Desmond Leach et al. (2013)
TU1	My work tasks vary on a day-to-day basis with little or no warning concerning transfer of secure data.	Desmond Leach et al. (2013)
TU2	I come across unexpected problems in my work surrounding information security related issues.	Desmond Leach et al. (2013)
TU3	The order in which I do tasks change with little or no warning concerning transfers of secured data	Desmond Leach et al. (2013)
IOU1	I can rely on managers to provide information concerning Information Security rules and procedures	Desmond Leach et al. (2013)
IOU2	I can rely on managers to provide precise answers pertaining to Information Security Policy rules and procedures	Desmond Leach et al. (2013)
IOU3	Information Security Policy requirements are consistent for internal users of systems	Desmond Leach et al. (2013)
PE1	Employees can make a difference when it comes to helping secure the organization's information systems and data.	Herath and Rao (2009b)
PE2	There is not much that any one individual can do to help secure the organization's information systems.	Herath and Rao (2009b)
PE3	If I follow the organization information security policies, I can make a difference in helping to secure my organization's information systems.	Herath and Rao (2009b)
PSE1	I am able to identify a breach in information security even if there is no one to help me.	Chan et. al (2005)
PSE2	I am able to identify a breach in information security, even if I do not have a copy of written procedures and rules to refer to.	Chan et. al (2005)
PSE3	I am able to identify a breach in information security even if I have not seen a similar situation occurring before.	Chan et. al (2005)
PSE4	I am aware of what to do in the event of an information security breach even though I have not been instructed	Chan et. al (2005)

PSE5	I am aware of what to do in the event of a information security breach, even if I do not have a copy of written procedures and rules to refer to.	Chan et. al (2005)
PVC1	I find that my values and the values where I work are very similar.	Son (2011)
PVC2	What my company stands for is important to me.	Son (2011)
PVC3	I agree with the values that define the goals of my company.	Son (2011)
PVC4	I am seldom asked at work to do anything that goes against my personal moral values.	Son (2011)
PO1	The Internet is my network and my data	Anderson and Agarwal (2010); Dyne and Pierce (2004)
PO2	I feel a high degree of personal ownership for my organization's information and communication technologies.	Anderson and Agarwal (2010); Dyne and Pierce (2004)
PO3	I sense that the organization's information and communication technologies are mine	Anderson and Agarwal (2010); Dyne and Pierce (2004)
PO4	This is my company and my data.	Anderson and Agarwal (2010); Dyne and Pierce (2004)
PO5	I feel a high degree of personal ownership for organizational data	Anderson and Agarwal (2010); Dyne and Pierce (2004)
PO6	I sense that organizational information belongs to me.	Anderson and Agarwal (2010); Dyne and Pierce (2004)
SETA1	My organization provides training to help employees improve their awareness of computer and information security issues.	D'Arcy (2009)
SETA2	My organization provides employees with education on computer software copyright laws.	D'Arcy (2009)
SETA3	In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	D'Arcy (2009)
SETA4	My organization educated employees on their computer security responsibilities.	D'Arcy (2009)
I1	I intend to protect information and technology resources according to the requirements of the Information Security Policy of my organization in the future, especially during times of organizational change and uncertainty.	Bulgurcu et al. 2010/ Dhillon et al. 2019

I2	I intend to carry out my responsibilities prescribed in the Information Security Policy of my organization when I use information and technology in the future, especially during times of organizational change and uncertainty.	Bulgurcu et al. 2010/ Dhillon et al. 2019
I3	I intend to comply with the requirements of the Information Security Policy of my organization in the future especially during times of organizational change and uncertainty.	Bulgurcu et al. 2010/ Dhillon et al. 2020
AC1	During times of organizational change and uncertainty I complied with information security policies	Siponen et al. (2014)
AC2	During times of organizational change and uncertainty I recommended others comply with information security policies	Siponen et al. (2014)
AC3	During times of organizational change and uncertainty I assisted others in complying with information security policies	Siponen et al. (2014)

Note. RU=Resource Uncertainty; TU=Task Uncertainty; IOU=Input/output Uncertainty; PE=Perceived Effectiveness; PSE=Perceived Self-Efficacy; PVC=Perceived Value Congruence; PO=Perceived Ownership; SETA=Security Education, Training, and Awareness; I=Intention to Comply; AC=Actual Compliance

survey. Data collection from self-administered surveys and questionnaires can deliver low-cost access to many respondents in a short time period (Zikmund 2000) while also providing high levels of confidentiality and anonymity to the respondent (Davis 2005). Self-administered surveys are not intended to be the only method of data collection; however, for this investigation, with considerations given to the number of respondents needed and time allotted, this data collection system was selected.

Participants for the survey were invited from Amazon Mechanical Turk (MTurk), which required participants to have full-time employment (a minimum of 35 hours worked per week), be employed in their current job for six months, and reside in the United States. Data collection occurred during extraordinary organizational change where most workers moved from an in-

person place of business settings to non-traditional work-from-home settings. Therefore, data collection from this respondent body was deemed optimal given the lack of traditional data collection pools or clusters. In addition, MTurk's advantages include low cost and high utility for data collection and recruitment, making it a well-liked and common data collection marketplace for the social sciences (Huff and Tingley 2015).

MTurk workers provide investigators with diverse and sufficient groups of participants. Some researchers have noted that MTurk workers tend to be younger, more educated, and more liberal than the population (Paolacci and Chandler 2014). Others have noted a tendency for Mturk workers to be mostly from urban work areas while lacking underrepresented populations within the United States (Huff and Tingley 2015). Given the capability to underrepresent certain demographic groups within the US, MTurk respondents have been typically found to be more diverse demographically than typical internet sampling for social surveys and substantially more diverse than that of a college sample setting (Buhrmester et al. 2016).

Before procuring respondents to any survey, a requesting person (or entity) must set up an MTurk account and describe the performed study. Additionally, the requestion must set limitations for worker qualifications and determine a compensation rate for each response. The description for this study simply stated: “Survey about Information Security Policy Compliance surrounding work stress and uncertainty.” Information provided to workers includes the duration of the survey (25 minutes) and compensation rate ($2.00 per completed and approved response), which did not include associated MTurk administration fees. This level of compensation was slightly above average for the estimated time for completion. An additional $0.10 allows MTurk requesters to only allow workers with a ‘master’ designation to participate in the survey. Amazon has selected Masters for demonstrating high performance and approval rates to

requesters and maintaining this performance for long periods providing a higher quality participant for the requester. Therefore, this study required such a designation.

MTurk respondents who wished to participate in this study were provided a URL link to the survey administered in Qualtrics. In addition, upon the completion of the survey, participants were provided with a unique passcode, which was entered on the MTurk website to be compensated.

As with any university or academic study, the researcher requested approval from the University of North Carolina at Greensboro's Institutional Review Board (IRB). The study did not proceed until approval and consent were obtained. At the outset of the survey administration, any participant was required to agree to the approved informed consent document before access would be granted to the survey instrument. The consent document stipulated to each respondent of the risk-free nature of the study that the researcher had no method to determine a respondent's identity, and those respondents would remain anonymous to the researcher. Additionally, respondents were notified that all data collected would be summarized, analyzed as a group, and kept in a secure and encrypted method only accessible to the principal investigator and supervisor. Contact information of the principal investigator and supervisor was also provided.

Overall, 365 responses were collected from Amazon MTurk workers, and 269 responses were kept and utilized for analysis with a response utilization rate of 73.9%. Responses were discarded for various reasons, including duplicating worker responses, incomplete survey responses, or overall lack of effort.

3.5 Data Analysis Procedures

This study utilized structural equation modeling (SEM) to analyze the research model and corresponding constructs. SEM allows researchers to differentiate and observe both factor and path models simultaneously, giving researchers insight into the research model's structural and measurement features (Gefen et al. 2000). Additionally, Gefen et al. (2000)indicated theory testing utilizing confirmatory factor analysis (CFA) and SEM is a widely applied tool in IS research. Therefore, when exploring research frameworks with multiple dependent and independent variables, which can be differentiated and identified, SEM is an appropriate mechanism that can be used for analysis and measurement (Hair et al. 2010).

The grounds for utilizing SEM modeling for behavioral research are plentiful. One such reason for SEM methodological use is when constructs become established in the literature and proven reliable, providing a good tool for theory confirmation. Another reason for this methodology applies when research includes multiple path relationships where constructs act as independent and dependent constructs, providing the researcher with reliable and accurate results. Our research mimics this reasoning structure, and therefore SEM selection is appropriate (Hair et al. 2010). SmartPLS v3.0 (Ringle et al. 2015b) was utilized to determine the significance and strength of hypothesized relationships and evaluate our SEM model. SmartPLS is a statical software package utilizing partial least squares SEM (PLS-SEM) analysis.

In contrast to covariance-based SEM analysis, which requires normally distributed data, PLS-SEM analysis is agnostic to data normality research objectives (confirmatory or exploratory) and seeks to explain relationships between exogenous and endogenous constructs (Hair et al. 2017). In addition, PLS-SEM-based analysis seeks to maximize the overall explained variance within the data set and structural model and is less vulnerable to data size (Hair et al.

2017). It is for these reasons PLS-SEM-based analysis was chosen for this study. Accordingly, and in the recommendations of (Hair et al. 2010), a six-stage SEM decision process is utilized. The first three stages of the process are covered previously in this dissertation involving the definition of individual constructs, development of the overall measurement model, and study design. The remaining stages will be discussed in the next section(s) and formulate how the measurement model will be validated and assessed, specify the structural model, and finally assess structural model validity.

3.5.1 Measurement Model Validity

The fourth stage in the decision-making process involves the process of measurement model validity and assessment. Measurement model validity within SEM utilizes two separate but unique tests to determine if the relationships between measurement items and latent variables are supported. The first test is termed the test for construct validity, and the second is for goodness-of-fit for the measurement model (Hair et al. 2010).

Construct validity seeks to determine whether items used for measurement accurately reflect the latent theoretical constructs using confirmatory factor analysis (CFA) (Hair et al. 2010). CFA can be utilized to test relationships between observed (measurement items) and unobserved or theoretical constructs using convergent and divergent validities. Convergent validities determine if measurement items share a high proportion of explained variance for the latent construct. Output for convergent validities comprises factor loadings and/or average extracted variance (AVE). AVE is the average of all variance removed by the measurement items of a latent construct. These standardized models provide estimated correlations between items and latent variables (the relationship's relative strength) and can be statistically verified for significance. For example, AVE loadings higher than 0.50 indicated the construct explains more

variance than what remains as an error (Hair et al. 2010). Hair et al. (2010)and Kline (2015)indicated acceptable item factor loadings onto theoretical constructs are typically higher than 0.70, but loadings as low as 0.50 could also be deemed adequate.

Discriminant validity determines uniqueness among constructs in a research model. This validity operation is important to ensure no two constructs are attempting to measure the same phenomena within the model. Tests for discriminant validity can follow a test developed by Fornell and Larcker (1981), which compares AVE with all correlations associated with the latent construct. The square root of AVE should not exceed the value of correlation coefficients (Fornell and Larcker 1981). Hair et al. (2010)describe discriminant validity as the variance unique to a construct and not greater than between construct variance. Additional construct validity assessments are Cronbach's alpha (individual item reliability) and composite reliabilities with 0.70 to determine acceptable limits for theoretical insight (Hair et al. 2010).

The second unique test for measurement model validity is the test for goodness-of-fit. Goodness-of-fit tests provide an average fit for a model and can be tested in multiple ways. Generally, goodness-of-fit tests compare the theoretical approach of the researcher and what data is collected by comparing the measurement of similarities between observed indicator items and estimates of those items' covariances matrices. Goodness-of-fit measures generally fall into three categories: Absolute measures: incremental measures, and parsimony fit measures (Hair et al. 2010).

The most straightforward measure to provide a goodness-of-fit test is the absolute fit indices, which assess how the data fit the developed theory. While helpful, these indices are sensitive to sample sizes. The model chi-square (X^2) is the most basic fit statistic but is sensitive to sample size and can indicate a poor overall model fit when larger sample sizes are present.

Chi-square statistics search for differences between the proposed model and the collected data with lower values preferable and a statistical significance test greater than 0.05 ($p > .05$) (Hair et al. 2010; Kline 2015). The Root Mean Square Error of Approximation (RMSEA) takes sample size into account when adjusting for the noncentral chi-square distribution. Values greater than .10 are considered a poor fit, with values between .05 and .08 a generally good fit of the data (Browne and Cudeck 1993).

Incremental measures for model fit include the comparative fit index (CFI) and the Tucker Lewis index (TLI). Incremental fit indices compare alternate baseline models (null model) to the estimated model to look for differences (Hair et al. 2010). CFI and TLI are sample size agnostic and range in value between 0.00 and 1.00 with values greater than roughly .95, indicating an excellent model fit (Hair et al. 2010).

Additional goodness-of-fit models include the root mean square residual (SRMR), which assesses differences in sample covariance matrices, and the covariance model that the researcher proposed. SRMR values less than .08 indicate a reasonably good fit with overall test ranges between 0.0 and 1.0 (Hair et al. 2010; Kline 2015).

3.5.2 Structural Model Validity

Structural model validity tests the structural relationships between constructs. These relationships are indicated within the proposed research framework. For our proposed framework and model, we developed hypotheses H_1 to H_{12} and represented in Table 2. We follow recommendations as set forth by Hair et al. (2010), who accentuated two tests concerning model fit and that of a theoretical expectation between the structural relationship of the proposed framework. Structural model validity is similar to measurement model validity and utilizes Chi-square and RMSEA examinations. In addition, factor loading estimates will be utilized to test

structural relationships to determine if a modification to the structural model is warranted. If no change is necessary after all measurement validations are complete, the expectation exists that provided loadings would be similar to CFA model loadings and construct reliability (Hair et al. 2010).

Individual structural path estimates should also be tested to assess structural model validity. General tests to determine consistency with expected directions of relationships and statistical significance include t-tests, standardized path coefficients, and variance explained (R^2) (Hair et al. 2010; Kline 2015).

3.6 Conclusion

We now conclude our discussion of the methodology utilized in this dissertation. We now move to Chapter 4, where we will provide the results of our description of the data collected, statistical methods deployed testing of the research model, and analysis of the results.

Table 2: Hypothesis Table and Latent Variable Relationships

Hypothesis	Direct/Indirect Relationship
H1: An individual's perceived sense to identify information security breaches and policy failures increases individual intrinsic motivation.	PSE->IM
H2: An individual's perceived sense of personal ownership over organizational data and technological resources increases individual intrinsic motivation.	PO->IM
H3: An individual's perceived value congruence with the organization increases individual intrinsic motivation.	PVC->IM
H4: An individual's perceived ability to effectively control ISP related breaches and failures increases individual intrinsic motivation.	PE->IM
H5: A perceived lack of access to resources concerning Information Security Policies is positively related to perceived ISP work uncertainty	PRU->PWC
H6: An individual's perceived uncertainty surrounding completion of daily work tasks related to ISP's is positively related to perceived work uncertainty variability	PTU->PWC
H7: Perceived uncertainty concerning managerial knowledge/input regarding ISP's is positively associated with perceived work uncertainty.	PIOU->PWC
H8: Perceived work uncertainty will positively increase intrinsic motivations to engage in ISP compliance behaviors	PWC->IM
H9: Intrinsic Motivation mediates the relationship between work uncertainty and individual intentions to comply with information security policies (ISP's).	PWU-> IM-> INT
H10: Intrinsic Motivation mediates the relationship between work uncertainty and organizational SETA programs.	PWU-> IM->SETA
H11: SETA will mediate the relationship between intrinsic motivation and intention to comply with ISPs.	IM-> SETA->INT
H12: Individuals who intended to comply with ISPs during uncertain work conditions will actually comply with ISPs.	IM->ACT

CHAPTER IV: ANALYSIS RESULTS

4.1 Introduction

This chapter will describe the data collected for analysis and which statistical methods were deployed to test the research model and the analysis results. For this research, and as indicated in earlier chapters, we utilized the variance-based approach of statistical analysis of partial least squares (PLS) structural equitation modeling (SEM). Generally, two approaches exist when testing SEM-based research: (1) Testing for the measurement model, which examines relationships between measured items and the latent variables they depict, and (2) testing and evaluation of the structural equation model, which analyzes both direct and indirect relationships between the latent variables.

Hair et al. (2010) suggest using PLS-SEM when research goals are centered on identifying key constructs, while theory testing is in the early stages of development or complex structural modeling. Differing from earlier statistical methods associated with the analysis of variance approaches (ANOVA) or multiple regression when measurements relationships are limited to singular analysis at any given time, SEM allows for more complex relationship analysis systemically and comprehensively using variance-based estimation (F. Hair Jr et al. 2014). SEM provides researchers the capability to observe both the measurement model (or factors) and the structural model (or paths) in a coordinated and simultaneous fashion (Gefen et al. 2000). PLS-SEM analysis forms a composite model and maximizes explained variance in the data, whereas covariance-based SEM fits the data with common factors to generate relationships (Henseler et al. 2016). Additionally, PLS path modeling allows researchers to assess multidimensional (or hierarchical) latent construct models and their relationships (Wetzels et al. 2009). SmartPLS 3.0 was used to analyze and generate results for this study.

This chapter will proceed as follows. First, we will begin with a description and review of hierarchical latent variable modeling and a description of the data, including how we addressed common method bias during data collection and the participant's demographic data. We will then describe specific types of SmartPLS models, emphasizing multidimensional models utilized in this study. Finally, we will present the measurement and structural modeling results and differences in demographic groups concerning uncertainty and ISP compliance.

4.2 Hierarchical Latent Variable PLS-SEM Modeling

Hierarchical latent variables models utilize higher order or multidimensional constructs on higher levels of abstraction (Becker et al. 2012). Hierarchical construct models are based on many theoretical and empirical justifications, with many arguing they allow for more parsimonious theories and less complex modeling (Becker et al. 2012; Edwards 2001; Law et al. 1998; Wetzels et al. 2009). Theoretical constructs are not necessarily deemed multidimensional or unidimensional, allowing for a particular construct to be operationalized at any level of abstraction needed or theorized by the researcher (Law et al. 1998). Generally, hierarchical construct models are limited to second-order levels but can expand to higher levels of abstraction and are also characterized by the formative or reflective nature of the construct relationship (Becker et al. 2012; Edwards 2001; Wetzels et al. 2009). Ringle et al. (2012)and Jarvis et al. (2003)have classified four different types of multidimensional construct models based on the type of relationships between (1) first-order constructs and their measurement items, and (2) the second-order constructs and the first-order construct relationship. We will describe each in the following sections.

4.2.1 Type I: Reflective-Reflective Models

The first multidimensional latent construct model, reflective-reflective type I modeling, consists of lower- or first-order constructs reflectively measured by lower-order construct measurement items (Becker et al. 2012). This model has been referred to as a 'hierarchical common factor model,' indicating the conceptualization of higher-order constructs representing many particular factors of some common factor (Becker et al. 2012; Lohmöller 2013). This approach is appropriate to ascertain common factors of related and distinct reflective constructs when lower-order latent measures are correlated (Becker et al. 2012). However, it should be noted that some have argued this type of model is meaningless and misleading (Lee and Cadogan 2013). Others have viewed this modeling approach as defensible due to the multiple underlying factors which can be found in the natural world and are distinct phenomena (Becker et al. 2012).

4.1.2 Type II: Reflective-Formative Model

In this model configuration, lower-order latent variables are measured reflectively, and higher-order constructs are measured formatively by the lower-order latent constructs. However, the latent variables themselves are not caused by common elements but consist of generalized concepts that mediate endogenous variables within the SEM (Chin 1998). Hierarchical constructs of this type can be used to find the measurement errors of regular occurring formative construct indicators (Becker et al. 2012). When utilizing this type of model, operationalization occurs by items onto reflective constructs specifically for the ability to gain insight into measurement errors (Edwards 2001; Lee and Cadogan 2013).

4.1.3 Type III: Formative-Reflective Model

This model is utilized when lower-order constructs are measured with specific formative items part of a common concept in the higher-order latent variable (Becker et al. 2012).

Unfortunately, this model has not been widely utilized in academic practice. However, performance measurements that combine various characteristics and have good representation in the literature in the use of formative constructs have been one such application of this type of model (Jarvis et al. 2003; Petter et al. 2007). Objectives include the representation of several factors that seem to measure similar construct but utilize different techniques while helping to yield more robust analysis when measurement may be weak (such as single item measurement) (Becker et al. 2012).

4.1.4 Type IV: Formative-Formative Model

When seeking to measure a more abstract general concept, this model is utilized where both higher- and lower-order constructs are measured formatively. This type of model is rarely utilized but can estimate both constructs and indicators simultaneously, which leads to better interpretation of results (Becker et al. 2012; Ringle et al. 2012). Much like formative-reflective model usage, this model is generally utilized when seeking casual investigations of performance-related or relevant managerial insight into organizational activities (Becker et al. 2012; Jarvis et al. 2003; Petter et al. 2007). This model can split complex formative constructs into many lower constructs for analysis (Becker et al. 2012).

All four models can be found within empirical research applications, with reflective-formative, formative-formative, and reflective-reflective being most predominant even though only reflective-reflective has the clearest guidelines on usage and reflective-formative specification guidelines only recently becoming more clear (Sarstedt et al. 2019).

4.2 Higher-order Construct Identification Approaches

To utilize PLS-SEM, investigators must compute values for each latent variable in the structural model. However, when developing hierarchical constructs, higher-order constructs are

not directly measured and therefore have no value estimated, which is used for path modeling. Three general approaches have been proposed in the literature to estimate the higher-order construct scores and overcome this issue: (1) the repeated indicator approach (Lohmöller 2013), (2) the two-stage approach (Ringle et al. 2012), and (3) the hybrid approach (Wilson 2010).

Repeated measurement approaches use indicators associated with lower-order constructs are also allocated to the higher-order construct as its measurement instrument (Lohmöller 2013). For example, suppose more than one lower-order construct is used to measure the higher-order latent variable. All measurement items used in each lower-order construct are used to measure the higher-order component. When using manifest variables in this fashion, first-order (or lower-order) variables are stipulated as primary (or outer, measurement model) loadings, and higher-order (or second-order) variables then specify the inner (or structural) model (Wetzels et al. 2009). Construct scores are needed to determine PLS-SEM path analysis. This approach provides values for the lower-order construct, which are then used as manifest variables for the higher-order construct scores (Wetzels et al. 2009). Specification of higher-order values and constructs do not follow the same methods as lower-order constructs and must be calculated by hand to determine appropriate reliability and validity of component scores (Sarstedt et al. 2019). Specification of higher-order constructs is dependent on which modeling method was operationalized and theorized when conducting the study. Sarstedt et al. (2019)have described the methods to calculate specification measures for each model and approach for proper PLS-SEM deployment. This approach can estimate all constructs simultaneously, which is an advantage in PLS-SEM data analysis (Becker et al. 2012).

In some instances, when antecedent constructs are used in a path model developed in the repeated indicator approach, determined path coefficients may be non-significant to the second-

order construct. Becker et al. (2012)proposed the two-stage approach as an alternative to the repeated indicator approach in which lower-order construct scores are calculated as a new data point (first stage) that is then used as a single standardized measurement for both higher- and lower-order variables (second stage). However, the specification of higher-order constructs must again be manually calculated as determined by model choice and theoretical development (Sarstedt et al. 2019).

The hybrid approach was developed by Wilson (2010)and is similar to the repeated indicator approach. However, measurement items are only used once in this approach to mitigate artificially correlated residuals (Becker et al. 2012). In addition, the hybrid approach only uses half of each lower-order constructs measurement item to estimate latent variable scores. The other half estimates higher-order scores to sidestep correlation issues when using all measurement items in the model twice (Wilson 2010).

The reflective-reflective model (Type I) with repeated indicators approach was utilized to operationalize the research framework for this research. Results of this analysis for both measurement and structural models will be discussed in subsequent sections.

4.3 PLS Measurement Models

PLS-SEM data analysis is divided into two separate parts. The first assesses the measurement model (outer model), while the second analyses the structural path (or SEM inner portion) of the model (F. Hair Jr et al. 2014). Investigators must first determine if measurement items are reflective or formative (Diamantopoulos et al. 2008). Generally, three indicators are present in a measurement model: (1) effect indicators (covariates), (2) casual indicators, and (3) composite indicators (Hair et al. 2012). Methods to determine individual indicators and construct reliabilities will depend on the measurement perspective.

Unlike formative measures, reflective measures utilize analysis consisting of composite measures of consistency reliability (CR), convergent (average variance extracted, AVE) and discriminate validities (Heterotrait-Monotrait, HTMT), and Cronbach's alpha which are commonly applied by the analysis of the individual indicator or as a group of indicators for a latent variable (Diamantopoulos et al. 2008). Decisions for measurement models are generally theoretically based (Jarvis et al. 2003). Effect indicators are associated with reflective measurement models and are dependent on common associations among indicators for the latent variable (Hair et al. 2017). These are chosen due to the consideration of indicators demonstrating the variable of interest (Bollen 1984). Causal indicators, associated with formative modeling, have conceptual unity and should correspond to a latent variable's definition or how it comes into being (as opposed to how it affects an entity) (Bollen 2011). Composite indicators are weighted elements and differ from causal indicators through error (or disturbance) terms which can have implications for model validity evaluation (Bollen 2011).

Inner, or structural, model assessment in PLS-SEM focuses on variance-based, non-parametric evaluation (Hair et al. 2012). This assessment defines the amount of explained variance of endogenous constructs within the model and provides a value called the coefficient of determination (R^2) (Hair et al. 2012). Unlike covariance-based modeling, PLS-SEM has limited inner models' model goodness-of-fit indices (GoF). This is because GoF values rely on outer model commonalities in reflective models and R^2 values that are more precisely dependent on theoretical context (Hair et al. 2012). Therefore, inner model quality should also be assessed using path coefficients and report t-value statistics and corresponding p-values (Hair et al. 2012).

Hierarchical Component Modeling (HCM) assessment involves second, third, or higher layer structures, allowing for analysis based on higher levels of abstraction instead of specific

individual relationships (Becker et al. 2012). This type of modeling is an advanced feature of PLS-SEM-based analysis and provides more parsimonious path models, generalized relationships, and strongly reflective attributes of constructs (Becker et al. 2012; Hair et al. 2017). Higher-order and lower-order constructs in reflective-reflective and formative-reflective hierarchical models can be analyzed as abstract entities with lower and higher levels of abstraction of related constructs (Hair et al. 2017). SmartPLS has been a useful tool for modeling HCMs using methods such as bootstrapping. Bootstrapping is a nonparametric test for statistical significance using subsamples randomly picked from the original set of observations. We will discuss bootstrapping in the context of this study in a future section.

4.4 Responses and Participant Psychometric Data

Data was gathered from a self-administered survey on Amazon MTurk as previously discussed for response generalization and response bias to the greater US population. A total of 365 responses were gathered through Qualtrics and a self-administered survey instrument for full-time employees in the United States. After evaluating the data for survey completion, time taken to complete the survey, or erroneous responses, 269 responses were accepted for evaluation. Barclay et al. (1995)indicated the minimum sample size for SmartPLS analysis is the greater of ten times the number of indicators for a construct with the largest item number, or ten times the largest number of independent variables that affect the dependent variables. The 269 responses fulfill this requirement and are deemed adequate for analysis using SmartPLS techniques.

The study was administered in an as wide-ranging and inclusive way as possible. Table 3 illustrates the demographic breakdown of respondents for this research.

4.5 The Outer (Measurement) Model

Measurement models in SmartPLS estimate relationships between the measurement items gathered from responses and the underlying latent variable the item represents (Henseler et al. 2016). To determine if a measurement model accurately depicts the latent construct, the researcher must first determine if the indicators are causal (formative) or exert an effect reflective) on the variable of interest. This is an important consideration as the determination of cause or effect on the underlying construct will put in place the methods for evaluating the model. For this research, the items form a reflective (effect) relationship with the underlying latent construct and will be evaluated for composite item measures of internal consistency, consistent reliability (CR), convergent (average variance extracted, AVE), and discriminate validities (Heterotrait-Monotrait, HTMT), and Cronbach's alpha.

With the use of HCM, measure models must take on a multi-step process that first addresses lower-order constructs and their corresponding measurement items followed by a measurement model evaluation of second or higher-order constructs and their corresponding latent variables of interest (Sarstedt et al. 2019).

Table 3: Demographic Information

Demographics	Frequency (n=269)	Percentage
Gender		
Male	164	61.0
Female	104	38.7
Other	1	0.4
Age		
18-25	10	3.7
25-35	108	40.1
35-45	88	32.7
45-55	40	14.9
55-65	19	7.1
over 65	4	1.5
Education		
High School	57	21.2
Associates Degree	46	17.1
Undergrad Degree	125	46.5
Grad Degree	38	14.1
Other	3	1.1
Job Tenure		
0-5	103	38.3
5-10	98	36.4
10-15	34	12.6
15-20	18	6.7
Over 20	16	5.9

Demographics	Frequency (n=269)	Percentage
Work Status		
Employed	243	90.3
Self-Employed/Contractor	21	7.8
Unemployed	4	1.5
Missing	1	0.4
Work Role		
Senior Manager	16	5.9
Middle Manager	96	35.7
Individual Contributor	155	57.6
Missing	2	0.7
Department		
Finance/Administration	43	16.0
Legal	7	2.6
Marketing/Sales	50	18.6
Operations	14	5.2
Human Resources	9	3.3
IT	65	24.2
Supply Chain	29	10.8
Other	50	18.6
Missing	2	0.7
Work Environment		
At Site/Essential Employee	64	23.8
Virtual	174	64.7
Hybrid	25	9.3
Missing	6	2.2

4.5.1 First-Order Measurement Assessment

The initial assessment focuses on the factor loading of measurement items to their respective first-order construct, as shown in Table 4. Hair et al. (2012)specifies loadings of at least .50 or higher and be statically significant; however (Sarstedt et al. 2019) indicate loading of .6or higher to be sufficient to indicate factor reliability. Generally, loadings in this range will indicate 50% of the variance of the factors and thus will be reliable measures. All measures in our study met the .7 cutoff sans for two indicator variables, PQ1 (.613) and AC3 (.641), which continued to meet factor loading requirements. Each factor was assessed within the model, and it was determined that PO1 should be removed from the set of indicators while AC3 would remain. Factor analysis indicated all indicator variables adequately represented the underlying first-order construct concluding the first assessment step.

The second method for assessing measurement model quality is for internal consistent reliability, including composite reliability (CR) scores and measures for Cronbach's alpha on identified latent constructs in the first-order model. Hair et al. (2017)indicate high values of CR are deemed more reliable and should exceed 0.70 for confirmatory research, while values between .60 and .70 are acceptable for exploratory research. Values lower than 0.60 indicate low reliability. Values between .70 and .90 are considered good measures in confirmatory analysis, with values exceeding .95 possibly being redundant constructs and causing high correlations between error terms (Hair et al. 2017). Cronbach's alpha is an additional test of internal consistent reliability with similar cut-offs and specifications a CR measures. Cronbach's alpha assumes indicators are all similar in their reliability, unlike composite reliability, for which Hair et al. (2017)addresses as being less suitable for PLS-SEM applications. Still, we utilize both measures to determine measurement model specifications. As Table 4 shows, all first-order

Table 4: Measurement Model Quality Criteria

Construct	Item	Mean	Variance	Loading	α/CR
Task Uncertainty	TU1	3.41	1.83	.902	.84/.80
	TU2	3.30	1.71	.810	
	TU3	3.25	1.73	.879	
Resource Uncertainty	RU1	2.43	1.12	.915	.88/.93
	RU2	2.24	1.12	.892	
	RU3	2.32	1.15	.892	
I/O Uncertainty	IOU1	2.51	1.28	.889	.87/.92
	IOU2	2.67	1.38	.907	
	IOU3	2.39	1.15	.867	
Perceived Self-Efficacy	PSE1	2.94	1.41	.863	.92/.94
	PSE2	2.92	1.38	.854	
	PSE3	3.04	1.42	.871	
	PSE4	2.69	1.37	.872	
	PSE5	2.74	1.43	.894	
Perceived Effectiveness	PE1	2.16	1.14	.887	.81/.89
	PE2	2.63	1.62	.761	
	PE3	2.21	1.22	.891	
Perceived Value Congruence	PVC1	2.57	1.23	.892	.88/.92
	PVC2	2.54	1.34	.863	
	PVC3	2.5	1.27	.903	
	PVC4	2.16	1.31	.757	
Perceived Ownership	PO1	3.39	1.63	.613[1]	.94/.95
	PO2	3.50	1.73	.889	
	PO3	3.71	1.69	.942	
	PO4	3.71	1.79	.924	
	PO5	3.70	1.81	.939	
	PO6	3.96	1.79	.934	
Security, Education, Training & Awareness (SETA)	SETA1	2.77	1.66	.908	.90/.93
	SETA2	3.40	1.93	.797	
	SETA3	2.77	1.68	.866	
	SETA4	2.53	1.48	.912	
Intention to Comply	I1	1.75	0.85	.925	.91/.94
	12	1.80	0.96	.914	
	I3	1.71	0.79	.922	
Actual Compliance	AC1	1.80	0.90	.880	.70/.80
	AC2	2.32	1.43	.736	
	AC3	2.78	1.52	.641**	

[1]Item Checked for Removal at <.70

Note. α=Cronbach's Alpha; CR=Composite Reliability

constructs indicate acceptable levels for internal consistent reliability with both CR's and Cronbach's alpha for all items above measurement parameters. Cronbach's alpha measures between 0.70 and .94 while CR's fall between 0.80 and 0.94.

The next step in the measurement model assessment addresses the convergent and divergent validities of the measurement models. Convergent validities are examined through the average variance extracted (AVE) and should exceed values of 0.50 (Fornell and Larcker 1981). Hair et al. (2012) stipulate AVE's higher than 0.50 have an acceptable level of convergent validity, designating that when this threshold is met and exceeded, more than half of an indicator's variance has been explained; thus, providing more explanation than what is left in the model. AVE results of this study meet all applicable requirements.

Discriminant validity is needed to assess the correlation between constructs and determine that latent variables do not share more variance with other latent variables than with their indicators (Fornell and Larcker 1981). Assessment for this measurement involves the Fornell-Larcker criterion, which stipulates that the AVE of a latent construct should exceed that of the highest squared correlation of another construct and/or that all indicators loadings should exceed all its cross-loadings (Hair et al. 2012). This measurement method has been criticized due to it becoming an unreliable measure when loadings for specified constructs are within a close approximation (Sarstedt et al. 2019). Table 5 provides measures for AVE for each construct, the squared AVE, and associated correlations. The squared AVE is reported on the diagonal of the correlation matrix. All squared AVEs are larger than corresponding off-diagonal correlations, thus supporting discriminate validity utilizing this assessment method.

Table 5: Convergent and Discriminant Validities

		AVE	1	2	3	4	5	6	7	8	9	10
1	ACT	0.575	**0.759**									
2	INT	0.847	0.673	**0.92**								
3	IOU	0.789	0.461	0.519	**0.888**							
4	PE	0.72	0.563	0.602	0.452	**0.848**						
5	PO	0.777	0.253	0.13	0.302	0.226	**0.881**					
6	PSE	0.759	0.351	0.376	0.410	0.502	0.308	**0.871**				
7	PVC	0.732	0.480	0.504	0.581	0.476	0.468	0.335	**0.856**			
8	RU	0.81	0.513	0.622	0.796	0.500	0.296	0.453	0.568	**0.900**		
9	SETA	0.760	0.452	0.372	0.558	0.407	0.368	0.449	0.385	0.623	**0.872**	
10	TU	0.747	-0.141	-0.246	-0.195	-0.266	0.132	-0.031	-0.183	-0.238	-0.043	**0.864**

An alternate method for assessing discriminate validity is the correlations' Heterotrait-Montrait (HTMT) ratio. This method of discriminant validity testing has been shown to have higher sensitivity and specificity assessments than that of Fornell-Larcker (Henseler et al. 2016) and provide higher quality assessments for PLS-SEM applications. This is due to concerns surrounding Fornell-Larcker discriminant validity measures regarding PLS-SEM or other variance-based SEM analyses (Yusoff et al. 2020). Discriminant validity is a particularly important measure as biased estimates for this test can invalidate hypothesized results (Henseler et al. 2016). Values above 0.90 indicate discriminant validity problems (Henseler et al. 2016). All HTMT ratio values fall at or below 0.90, indicating discriminant validity of the constructs. Heterotrait-Monnotrait values for latent variables can be seen in Table 6.

Table 6: Heterotrait-Monotrait (HTMT) Ratio

		1	2	3	4	5	6	7	8	9
1	ACT	-								
2	INT	0.698								
3	IOU	0.549	0.577							
4	PE	0.630	0.677	0.508						
5	PO	0.386	0.137	0.330	0.234					
6	PSE	0.438	0.394	0.445	0.558	0.321				
7	PVC	0.568	0.562	0.661	0.539	0.511	0.362			
8	RU	0.583	0.694	0.090	0.564	0.317	0.487	0.647		
9	SETA	0.597	0.389	0.622	0.441	0.405	0.489	0.431	0.682	
10	TU	0.256	0.271	0.214	0.340	0.154	0.097	0.206	0.268	0.108

All first-order constructs fall within acceptable parameters concerning internal consistency, including construct reliability and validity and convergent and divergent validities. We will now validate second-order constructs depicted by relationships between higher and lower-order latent variables.

4.5.2 Second-Order Measurement Assessment

Sarstedt et al. (2019)indicate that higher-order constructs are held to the same internal consistency, reliability, and validity criteria as lower-order constructs. As our approach is the repeated indicator approach, three aspects of construct validation must be recognized (Chin 2010; Sarstedt et al. 2019): (1) second-order constructs are not to be evaluated using the repeated measures from the lower-order construct, (2) discriminant validity assessment requires

special investigation, and (3) lower-order components are not evaluated a being part of the structural model.

First, lower-order construct indicators do not define the higher-order construct but are only used to identify the higher latent variable (Sarstedt et al. 2019). Second, the measurement of the second-order construct is defined between the higher-order to lower-order component or latent relationship. Third, reflective-reflective models, where the direction of relationships moves from higher-to lower-order constructs, indicate loadings between constructs and are assessed between higher and lower-order components the same as lower-order factor identification and internal consistency (Sarstedt et al. 2019).

Second, except for their higher-order construct, discriminate validity for all lower-order constructs must be maintained for each other and all other constructs identified in the measurement model (Sarstedt et al. 2019). Higher-order constructs must maintain discriminant validity with all other latent variables in the model, and assessment of discriminate validity measures are operationalized by looking at lower-order latent variables and not the repeated measures (Sarstedt et al. 2019).

Finally, as lower-order constructs are not considered part of the structural model path, only higher-order constructs need to be assessed as part of the structural model (Sarstedt et al. 2019). Analysis of the structural model should also be checked through structural robustness tests.

For higher-order consistency, reliability, and validity checks, manual calculations are needed to assess measurement model accuracy for the second-order construct. Our research model manually calculated AVE, CR, and Cronbach's alpha calculations as set forth by Sarstedt et al. (2019). All other parameters for HCM modeling were consistent with the prescribed

evaluation techniques listed above. Specification and test results for second-order constructs are reported in Table 7.

Sarstedt et al. (2019)also recommend validation for higher-order formative constructs such as Perceived Work Uncertainty. Tests for this higher-order formative construct include VIF statistics and weight analysis for each lower-order construct in the reflective-formative

Table 7: Hierarchical Model Assessment

Hierarchical Model Assessment Second-Order Model[a]		
	Perceived Work Uncertainty	**Intrinsic Motivation**
CR	.823	.862
AVE	.579	.538
Cronbach **α**	.677	.793
Task Uncertainty	0.403 (.22, .56)***	
Resource Uncertainty	0.938 (.92, .97)***	
Input/Output Uncertainty	0.925 (.90, .95)***	
Perceived Self-Efficacy		0.747 (.66, .81)***
Perceived Effectiveness		0.685 (.61, .75)***
Perceived Value Congruence		0.769 (.70, .83)***
Perceived Ownership		0.731 (.66, .80)***

[a]Manual calculation as set forth by Sarstedt et al. (2020) for 2nd order construct specification

Note. Values in () indicate biased corrected CI's at 95% percentile confidence

***= p < .001

relationship. These measures are reported in Table 8. Given that VIF collinearity statistics are below conservative estimates of 3.0 and all weights for each LOC on the HOC are significant, the higher-order construct is verified and used in the structural path.

Table 8: Formative Hierarchical Model Assessment

Formative Hierarchical Model Assessment Perceived Work Uncertainty		
	Collinearity Statistics (VIF)	**Weight**
Task Uncertainty	1.063	0.146***
Resource Uncertainty	2.759	0.517***
Input/Output Uncertainty	2.701	0.517***

*** $p < .001$

Given all the above information, the lower-order model is specified, and the measurement model shows no issues. Therefore, structural model analysis can proceed.

4.6 The Structural (Inner) Model

Structural model assessment can follow many paths. For this study, we will investigate collinearity measures of the inner model to confirm all structural model components do not exhibit multicollinearity issues. Then, we will follow with structural model path—assessments, including a report on hypothesis significance and support. Finally, data analysis of the structural model will continue with reports of R^2, f^2, and Q^2 quality and finish with global fit measures for PLS as suggested by Wetzels et al. (2009).

Multi-collinearity can be a problem for SmartPLS statistical assessment. This occurs when constructs are inter-correlated causing higher standard errors and reliability issues in which statistical significance cannot be ascertained or determined.

To assess the structural model using SmartPLS, Hair et al. (2017)suggest a bootstrapping method with a minimum of 5000 resamples to estimate path coefficients and overall path significance (Ringle et al. 2012). Therefore, investigation of the Variance Inflation Factor (VIF) is warranted for all inner-model predictors. Values of VIF below 5.0, with a conservative estimation of values no greater than 3.0, are considered suitable and that no collinearity exists

within the predictor constructs. You can see the VIF values for the structural model in Table 9. This model shows no multicollinearity issues as values of all VIF statistics are well below the conservative value of 3.0.

When assessing the research model, the structural path, and path coefficient significance using SmartPLS, it is recommended to bootstrap the model with the minimum number of resamples suggested by Hair et al. (2017)to be 5000 with the number of cases equal to the original number of observations in the investigation. Once completed, path assessment can be made by analyzing the critical t-values for a two-tailed test. The results of the analysis can be seen in Figure 2. Additionally, Tables 10 and 11 address hypothesis significance, including reporting confidence intervals, t-statistics, and corresponding p-values for direct and indirect (mediating) paths. While all paths were significant at the $p<.05$ level, only the direct path between SETA and Intention to Comply with ISP fell above a p-value of .001.

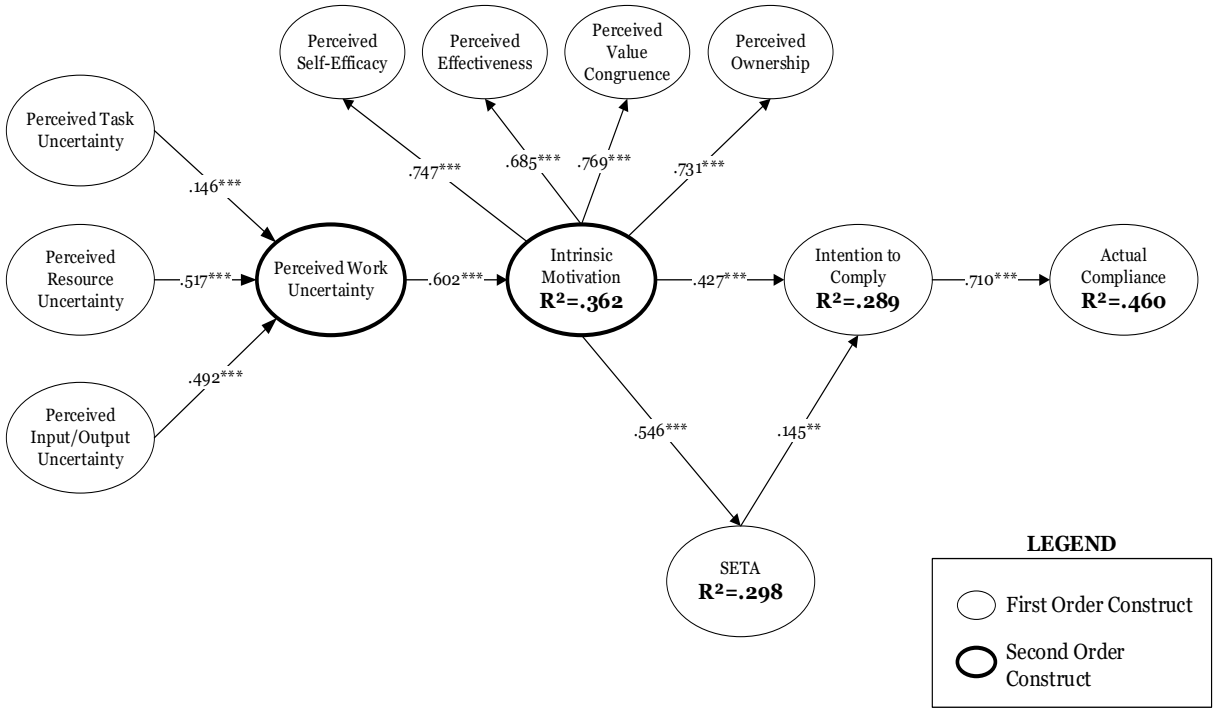
Based on these results, this model explains 28.9% of the variation in employees' intention to comply with ISP and 46.0% of employees' actual compliance with ISPs.

Table 9: VIF Statistics for the Structural Model

Variance Inflation Factor (VIF) for the Structural Model

Construct	ACT	INT	IM	IOU	PWU	PE	PO	PSE	PVC	RU	SETA	TU	AGE	GEN
ACT														
INT	1.019													
IM		1.434				1.000	1.000	1.000	1.000		1.000			
IOU														
PWU			1.000	1.000						1.000		1.000		
PE														
PO														
PSE														
PVC														
RU														
SETA		1.435												
TU														
age	1.027	1.016												
gen	1.014	1.016												

Figure 2: Research Model with Results



Note. *** p < .001; ** p < .01; R^2=explained variance.

4.6.1 Direct Path Data Analysis

Perceived Self-Efficacy (β= .747, t= 19.936, p<.001), Perceived Effectiveness (β= .685, t= 18.129, p<.001), Perceived Value Congruence (β= .769, t= 24.561, p<.001), and Perceived Ownership (β= .732, t= 17.725, p<.001) all significantly loaded onto the multidimensional construct Intrinsic Motivation which shows an employee's work motivation towards self-regulated decisions concerning information security policies. This supports hypotheses H1, H2, H3, and H4. Hypothesis 4, 5, and 6 predicted that Perceived Work Uncertainty surrounding ISPs would affect Perceived Task Uncertainty, Perceived Resource Uncertainty, and Perceived Input/Output Uncertainty concerning information security policies. All three hypotheses were supported with Perceived Resource Uncertainty (β= .517, t= 34.010, p<.001)

Table 10: Direct Hypothesis Results

Direct Hypothesis Testing						Confidence Intervals		
Hypothesis	**Direct Relationship**	**Point Estimate (β)**	***SE***	**T-stat**	**p-value**	**Lower**	**Upper**	**Supported**
H1*: An individual's perceived sense to identify information security breaches and policy failures increases individual intrinsic motivation.*	PSE->IM	0.747	0.037	19.936	<0.001	0.666	0.812	**YES**
H2: *An individual's perceived sense of personal ownership over organizational data and technological resources increases individual intrinsic motivation.*	PO->IM	0.732	0.041	17.725	<0.001	0.641	0.801	**YES**
H3: *An individual's perceived value congruence with the organization increases individual intrinsic motivation.*	PVC->IM	0.769	0.031	24.561	<0.001	0.701	0.824	**YES**
H4: *An individual's perceived ability to effectively control ISP related breaches and failures increases individual intrinsic motivation.*	PE->IM	0.685	0.038	18.129	<0.001	0.608	0.753	**YES**
H5: *A perceived lack of access to resources concerning Information Security Policies is positively related to perceived ISP work uncertainty*	PRU->PWC	0.517	0.015	34.010	<0.001	0.488	0.547	**YES**
H6: *An individual's perceived uncertainty surrounding completion of daily work tasks related to ISP's is positively related to perceived work uncertainty variability*	PTU->PWC	0.146	0.041	3.550	<0.001	0.054	0.217	**YES**
H7*: Perceived uncertainty concerning managerial knowledge/input regarding ISP's is positively associated with perceived work uncertainty.*	PIOU->PWC	0.492	0.016	31.154	<0.001	0.461	523.000	**YES**
H8: *Perceived work uncertainty will positively increase intrinsic motivations to engage in ISP compliance behaviors*	PWC->IM	0.602	0.051	11.856	<0.001	0.494	0.695	**YES**
H12: *Individuals who intended to comply with ISPs during uncertain work conditions will actually comply with ISPs.*	IM->ACT	0.674	0.028	23.854	<0.001	0.622	0.734	**YES**

Table 11: Indirect Hypothesis Results

Indirect Hypothesis Testing						Confidence Intervals		
Hypothesis	**Indirect Relationship**	**Point Estimate (β)**	***SE***	**T-stat**	**p-value**	**Lower**	**Upper**	**Supported**
H9: Intrinsic Motivation mediates the relationship between work uncertainty and individual intentions to comply with information security policies (ISP's).	PWU-> IM-> INT	0.259	0.049	5.239	<.001	0.168	0.371	**YES**
H10: Intrinsic Motivation mediates the relationship between work uncertainty and organizational SETA programs.	PWU-> IM-> SETA	0.332	0.050	6.699	<0.001	0.234	0.429	**YES**
H11: SETA will mediate the relationship between intrinsic motivation and intention to comply with ISPs.	IM-> SETA-> INT	0.079	0.037	2.149	<0.05	0.011	0.158	**YES**

and Perceived Input/Output Uncertainty (β= .492, t= 31.154, p<.001) having moderate, significant effects toward employees having adequate information to perform work functions. Perceived Task Uncertainty had a weak but still significant effect on Perceived Work uncertainty (β= .146, t= 3.550, p<.001). The multidimensional construct of Perceived Work Uncertainty significantly impacted Intrinsic Motivation (β= .602, t= 11.856, p<.001) supporting H8.

Overall, the research model explained 36.2% of Intrinsic Motivation variance. It was predicted that individuals who intended to comply with ISPs would comply with ISPs during uncertain work conditions (H12) concerning information security policies. This hypothesis was supported (β= .674, t= 23.854, p<.001).

4.6.2 Indirect Path Data Analysis

Hypothesis 9, 10, and 11 all proposed mediating, indirect relationships. Hypothesis 9 proposed that Intrinsic Motivation mediated the relationship between Perceived Work Uncertainty and Intentions to Comply with ISPs. The indirect effect ($\beta_{PWC->IM->INT)}$ was .259 and was statistically significant (t=5.239, p<.001), and the hypothesis was supported with a bootstrapped analysis showing a 95% bias-corrected confidence interval excluded zero ([.168, .371]). Hypothesis 10 proposed that Intrinsic Motivation mediated the relationship between Perceived Work Uncertainty and employees' desire to seek training and education to comply with ISPs. The indirect effect ($\beta_{PWC->IM->SETA)}$ was .332 and was statistically significant (t=6.699, p<.001), and the hypothesis was supported with a bootstrapped analysis showing a 95% bias-corrected confidence interval excluded zero ([.234, .429]). Hypothesis 11 proposed that SETA programs mediated the relationship between Intrinsic Motivation and employees' Intention to Comply with ISPs. The indirect effect ($\beta_{IM->SETA->INT)}$ was .079 and was statistically significant

(t=2.149, p<.05), and the hypothesis was supported with a bootstrapped analysis showing a 95% bias-corrected confidence interval excluded zero ([.011, .158]).

4.7 Quality Measure Reporting

A measurement of the influence, or the explanatory power, which explains how each exogenous construct's variance is a result of an endogenous construct is the R^2 value. It relies on the number of predictors in the model. While the interpretation of values concerning R^2 can be subjective and vary in context and meaning from study to study, targets of research models in SEM should exhibit high values (Hair et al. 2011). In some disciplines, values of .75 could be the benchmark for high quality and explanation (some call this substantial). However, lower values can also show the quality results of the investigation (Hair et al. 2011). Values of 0.50 or 0.25 for endogenous constructs in a structural model can be labeled moderate to weak (Hair et al. 2011). For this study, a multidimensional second-order exogenous (Perceived Work Uncertainty) construct predicts a second multidimensional endogenous construct (Intrinsic Motivation) and three unidimensional constructs of SETA, Intention to Comply, and Actual Compliance. For this model, R^2=.362 (36.2%), which is a moderate explanation of variation explanation for Intrinsic Motivation. R^2 values for SETA (.298, 29.8%) and Intention to Comply with ISP (.289, 28.9%) have weak explanations from the exogenous construct. Actual Compliance has a moderate R^2 value of 0.460 (46%).

Levels of f^2 and Q^2 are effect sizes that can also show quality within a research model. For example, Cohen (1998) indicated that f2 values of 0.02, 0.15, and 0.35 indicate effect sizes from small to large within an exogenous construct. This value helps differentiate statistical significance from meaningful effects. These values can be seen in Table 12.

Table 12: Quality Measures for Latent Variable Paths

	Q^2	Values of f^2				
		ACT	**IM**	**INT**	**PWU**	**SETA**
ACT	0.216					
IM	0.14			0.185		0.424
INT	0.237	0.836				
PWU	0.494		0.568			
SETA	0.223			0.017		

Note. f2 or Q2 >.02=weak effect; f2 or Q2 >.15=moderate effect; f2 or Q2 >.35=strong effect.

F. Hair Jr et al. (2014)indicated that any value of Q2 over zero (0) should indicate a good predictive fit. Table 12 shows values of f^2 and Q^2 for our research model. For values of f^2, Intention to Comply has a strong effect on Actual Intention to Comply (.836), Intrinsic Motivation has a weak effect on Intention to Comply (.185) and a strong effect on SETA (.424), and Perceived Work Uncertainty has a strong effect on Intrinsic Motivation (.568). SETA has little effect on Intention to Comply (0.17) during times of uncertainty.

For values of Q^2, the predictive relevance for Perceived Work Uncertainty (.494), SETA (.223), Intention to Comply (.237), and Actual Compliance (.216) and Intrinsic Motivation (0.14) all have values above '0' for predictive relevance. The values obtained in this analysis indicate the constructs are important for the research framework being investigated.

For overall model fit, Ringle et al. (2015a), p. 70) suggests an evaluation of proposed Goodness-of-Fit (GoF), which is calculated by obtaining "the geometric mean (square root of the product of two indicators) between the median R2 (goodness-of-fit of the structural model) and the mean weighted of the AVE (goodness-of-fit for the measuring model)" as developed by (Tenenhaus et al. 2005).

Table 13: Goodness-of-Fit Measures

Construct	GoF Measures	
	AVE	**Avg R^2**
ACT	0.575	0.460
INT	0.847	0.289
IOU	0.789	
PE	0.720	
PO	0.777	
PSE	0.759	
PVC	0.732	
RU	0.810	
SETA	0.760	0.298
TU	0.747	
IM	n/a	0.362
TOTAL	7.516	1.409
AVERAGE	0.752	0.352
GoF = $\sqrt{(AVE*R^2)} = \sqrt{(0.752*0.352)}$ **= 0.514**		

Note. GoF=Goodness of Fit

A value greater than 0.36 is considered acceptable for social and behavioral sciences (Wetzels et al. 2009). Our calculation for GoF is .615 and is deemed a good fit of the data to the research model under this measurement. The GoF calculation can be found in Table 13. Additional goodness of fit models includes SRMR values and d_ULS. However, Hair et al. (2017) have indicated that researchers should approach these measures with caution as the values

generated are not widely known or understood when utilizing SmartPLS, especially for multidimensional constructs. When testing only reflectively measured or common factor, constructs researchers can mimic covariance-based SEM (CB-SEM) models with consistent modeling in SmartPLS (SmartPLSc) and determine model fit thorough comparison modeling approaches (Dijkstra and Henseler 2015; Lohmöller 2013). As this research contains mixed reflective, formative, and multidimensional modeling and constructs, model fit statistics are unreliable, and interpretation is not warranted.

4.8 Demographic Reporting for Employee Perceived Uncertainty and ISP Compliance

Employee ISP compliance is measured by the multidimensional construct of perceived work uncertainty. Table14 and Table15 break down mean scores for each demographic property obtained during this investigation for each lower-order construct. Research has warned not to determine if PLS path modeling was influenced by population heterogeneity, leading to biased results and inaccurate interpretations and results (Sarstedt et al. 2009). Therefore, multi-group analysis was performed to determine if any moderating effect occurred between different demographic groups within the original data sample and to check for any needed control group analysis within the inner model. As PLS-MGA allows for multigroup analysis and Hair et al. (2011) have indicated unobserved heterogeneity should be considered when conducting SEM investigations, differences between groups were analyzed for both the outer and inner models. In addition, Henseler et al. (2009)developed the bootstrapped-based PLS-MGA to compare estimates of a single group to all other bootstrapped parameter estimates in the opposing group, thus yielding an interpretable result for both measurement and structural models.

Considerations for sample size requirements were identified. As some groups for each demographic variable of interest have small samples, we found group analysis would be better if

Table 14: Perceived Work Uncertainty Demographic Data

Demographics	Task Uncertainty	Resource Uncertainty	Input/Output Uncertainty	Average Overall Uncertainty
	Mean Score (*SE*)			
Gender				
Male	3.43 (1.5)	2.31(1.04)	2.47 (1.09)	2.74 (0.90)
Female	3.14 (1.51)	2.35 (.99)	2.62 (1.19)	2.70 (0.98)
Age				
18-25	3.60 (1.72)	2.97 (1.33)	2.87 (1.48)	3.14 (1.08)
25-35	3.46 (1.52)	2.28 (0.89)	2.43 (1.05)	2.72 (0.83)
35-45	3.09 (1.42)	2.32 (1.12)	2.52 (1.12)	2.64 (0.99)
45-55	3.27 (1.55)	2.28 (.96)	2.52 (1.20)	2.69 (0.97)
55-65	3.47 (1.65)	2.37 (1.11)	2.96 (1.33)	2.94 (1.00)
over 65	4.17 (1.14)	2.67 (.9)	2.33 (.67)	3.06 (0.86)
Education				
High School	3.45 (1.55)	2.52 (1.22)	2.65 (1.21)	2.87 (1.06)
Associates Degree	2.88 (1.34)	2.12(0.84)	2.43 (1.12)	2.42 (0.82)
Undergrad Degree	3.34 (1.5)	2.35 (1.00)	2.52 (1.13)	2.74 (0.92)
Grad Degree	3.70 (1.56)	2.29 (0.90)	2.52 (1.06)	2.84 (0.79)
Other	2.33 (1.20)	1.83 (1.00)	1.78 (.69)	1.93 (0.97)
Job Tenure				
0-5	3.39 (1.45)	2.47 (1.01)	2.68 (1.16)	2.84 (0.93)
5-10	3.287 (1.6)	2.32 (1.04)	2.45 (1.08)	2.68 (0.93)
10-15	3.15 (1.53)	2.03 (0.94)	2.43 (1.30)	2.54 (1.03)
15-20	3.28 (1.18)	2.17 (0.73)	2.31 (0.81)	2.59 (0.60)
Over 20	3.69 (1.59)	2.33 (1.26)	2.42 (1.13)	2.81 (1.00)
Work Status				
Employed	3.44 (1.84)	2.21 (0.97)	2.56 (1.33)	2.66 (0.91)
Self-Employed/Contractor	3.51 (1.59)	2.42 (1.17)	2.61 (1.25)	3.21 (0.84
Unemployed	3.17 (1.40)	2.29 (.92)	2.46 (1.03)	3.64 (1.30)
Work Role				
Senior Manager	3.01 (1.48)	2.29 (1.13)	2.45 (1.12)	2.74 (1.17)
Middle Manager	4.33 (1.54)	1.86 (0.47)	2.19 (1.10)	2.85 (0.98)
Individual Contributor	3.27 (1.49)	2.27 (1.02)	2.31 (0.99)	2.64 (0.87)
Department				
Finance/Administration	3.01 (1.48)	2.29 (1.13)	2.45 (1.12)	2.58 (0.96)
Legal	4.33 (1.54)	1.86 (0.47)	2.19 (1.10)	2.79 (0.80)
Marketing/Sales	3.27 (1.49)	2.27 (1.02)	2.31 (0.99)	2.62 (0.94)
Operations	3.17 (1.55)	2.19 (0.94)	2.43 (1.05)	2.60 (1.01)
Human Resources	4.15 (1.78)	3.11 (0.99)	3.59 (1.56)	3.62 (0.48)
IT	3.43 (1.55)	2.18 (0.92)	2.35 (1.01)	2.65 (0.83)
Supply Chain	3.41 (1.52)	2.61 (1.22)	2.86 (1.34)	2.96 (1.09)
Other	3.17 (1.38)	2.42 (0.93)	2.67 (1.11)	2.75 (0.91)
Work Environment				
At Site/Essential Employee	3.43 (1.37)	2.54 (1.03)	2.83 (1.14)	2.93 (0.93)
Virtual	3.31 (1.55)	2.26 (1.00)	2.45 (1.13)	2.67 (0.91)
Hybrid	3.09 (1.40)	2.24 (0.97)	2.24 (0.99)	2.52 (0.96)

Table 15: ISP Intentions and Actual Demographic Report (Mean Score)

Demographics	Intention			Actual			Overall	
	Protection Intention	Responsibility Intention	Compliance Intention	Actual Compliance	Recommended Compliance	Actual Assistance	Overall Intention	Overall Actual Compliance
Gender								
Male	1.81	1.85	1.73	1.88	2.37	2.80	1.80	2.35
Female	1.66	1.71	1.67	1.66	2.24	2.74	1.68	2.21
Other	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00
Age								
18-25	2.40	3.20	2.30	2.50	2.60	2.20	2.63	2.43
25-35	1.77	1.83	1.69	1.80	2.24	2.85	1.77	2.30
35-45	1.69	1.68	1.70	1.78	2.31	2.64	1.69	2.24
45-55	1.80	1.70	1.73	1.68	2.43	3.03	1.74	2.38
55-65	1.58	1.63	1.53	1.79	2.58	2.84	1.58	2.40
over 65	1.50	1.50	1.50	1.50	1.75	2.50	1.50	1.92
Education								
High School	1.93	1.98	1.79	1.89	2.35	2.98	1.90	2.41
Associates Degree	1.59	1.52	1.63	1.63	2.39	3.02	1.58	2.35
Undergrad Degree	1.81	1.83	1.76	1.84	2.29	2.67	1.80	2.27
Grad Degree	1.58	1.74	1.58	1.74	2.34	2.55	1.63	2.21
Other	1.00	1.67	1.00	1.33	1.67	2.33	1.22	1.78
Job Tenure								
0-5	1.84	1.88	1.78	1.84	2.35	2.85	1.83	2.35
5-10	1.76	1.81	1.69	1.80	2.46	2.82	1.75	2.36
10-15	1.68	1.65	1.56	1.79	2.06	2.68	1.63	2.18
15-20	1.50	1.44	1.61	1.61	2.44	2.78	1.52	2.28
Over 20	1.63	1.88	1.81	1.69	1.69	2.25	1.77	1.88
Work Status								
Employed	1.73	1.77	1.70	1.78	2.26	2.74	1.73	2.26
Self-Employed/Contractor	1.86	1.81	1.71	1.71	3.00	3.10	1.79	2.60
Unemployed	2.50	2.50	2.25	2.25	2.25	3.25	2.42	2.58
Work Role								
Senior Manager	1.81	1.75	1.81	2.13	2.25	2.81	1.79	2.40
Middle Manager	1.77	1.91	1.83	1.92	2.06	2.47	1.84	2.15
Individual Contributor	1.74	1.74	1.63	1.70	2.47	2.95	1.70	2.37
Department								
Finance/Administration	1.72	1.79	1.65	1.70	2.58	3.02	1.72	2.43
Legal	1.57	1.43	1.29	1.29	1.71	2.00	1.43	1.67
Marketing/Sales	1.76	1.88	1.72	1.92	2.26	2.50	1.79	2.23
Operations	1.43	1.36	1.36	1.50	2.29	2.86	1.38	2.21
Human Resources	2.56	2.44	2.33	2.22	1.78	3.11	2.44	2.37
IT	1.74	1.77	1.80	1.82	2.20	2.68	1.77	2.23
Supply Chain	1.79	1.83	1.79	2.00	2.38	3.07	1.80	2.48
Other	1.72	1.74	1.66	1.70	2.44	2.82	1.71	2.32
Work Environment								
At Site/Essential Employee	1.88	1.94	1.89	1.92	2.22	2.86	1.90	2.33
Virtual	1.70	1.75	1.65	1.75	2.29	2.68	1.70	2.24
Hybrid	1.64	1.56	1.64	1.72	2.52	3.08	1.61	2.44

we combined groups into meaningful sets. This approach allowed for an increased sample size for statistical analysis while still generating interesting results. This method is useful for group identification of unobserved population heterogeneity**.** We held to the standard 5000 bootstrap criteria for group analysis. Results of the analysis indicated some group differences due to population heterogeneity existed for both the outer measurement model and the inner structural model. The following sections will report on this data analysis.

4.8.1 Outer (Measurement) Model Group Differences

4.8.1.1 Females vs. Males.

Group analysis results indicated significant differences in PLS path loadings between Females (0.234, p<.001) and Males (0.083), non-significant). In addition, females were found to significantly have more perceived uncertainty about how they carried out daily work tasks concerning organizational information security policies ($\beta_{(Fem-Male)} = 0.157$, $p = 0.039$). Females were also found to exhibit more perceived ownership directed toward organizational information and communication technologies, data, and IT networks. Both females (0.806, p<.001) and males (0.678, p<.001) significantly felt a sense of ownership towards organizational IT assets; however females exhibited a somewhat significantly higher level of ownership to these assets than males ($\beta_{(Fem-Male)} = 0.119$, $p < .10$) at the p<.10 level. You can examine the measurement model path loading in Table 16 for males and females.

Differences existed between gender groups concerning individual measurement instrument factors. Female and males differed in responses to AC1, “During times of organizational change and uncertainty, I complied with information security policies.” Females were significantly more likely actually to comply with organizational ISPs during times of

Table 16: PLS-MGA Gender Path Differences

Significant Reflective Lower-Order Group Differences (Path)

PLS-MGA Group		Path Difference/ Construct	Outer Loading (p-value) (Group A)	Outer Loading (p-value) (Group B)	CI (Group A)	CI (Group B)	Path Difference (A-B)	bootstrapped T-value		p-value (A-B)
Group A	Group B							Group A	Group B	
Female	Male	PTU->PWU	0.234 (<.001)	0.083 (n.s.[1])	0.115, 0.324	-0.007, 0.178	0.157	4.534	1.553	0.039**
Female	Male	PO->IM	0.806 (<.001)	0.678 <.001)	0.715, 0.816	0.506, 0.788	0.119	22.590	9.673	0.093*

[1]n.s.= not significant

Significance level *p<.10; ** p<0.05.

Table 17: PLS-MGA Significant Lower Order Gender Group Differences (Item)

PLS-MGA Group		Measurement Item	Path Difference/ Construct	Outer Loading (p-value) (Group A)	Outer Loading (p-value) (Group B)	CI (Group A)	CI (Group B)	Outer Loading Difference (A-B)	bootstrapped T-value		p-value (A-B)
Group A	Group B								Group A	Group B	
Female	Male	AC1	Actual Compliance	0.940***	0.859***	0.880,.0996	0.802,0.895	0.088	29.242	36.125	0.027**

Significance level *p<.10; ** p<0.05; *** p<.001.

Organizational change. Table 17 provides the results concerning individual item loading for gender group differences.

4.8.1.2 Work Role Demographics.

One other demographic group was identified contributing to significant group differences for path coefficient in the outer measurement model. Work roles between managers (senior or middle) and employees self-identified as individual contributors to the organization were significantly different for the relationship of Perceived Value Congruence and Intrinsic Motivation. Managers (0.870, $p < .001$) were significantly more likely than that of individual contributors (0.684, $p < .001$) to have stronger similarities in values between themselves and the organization ($\beta_{(MGR-IC)} = 0.182$, $p = .001$) even though both groups contributed significantly to the construct.

In addition to path differences in the measurement model for work role demographic groups, differences existed in responses to individual items. While each item contributed significantly to each construct concerning work role, differences existed between groups. Mangers (I1: 0.873, $p<0.001$; I2: 0.883, $p<.001$) were less likely than individual contributors (I1: .970, $p<.001$; I2: 0.944; $p<.001$) to have compliance intention surrounding Item I1 and I2. Item I1 asks for a response to: "I intend to protect information and technology resources according to the requirements of the Information Security Policy of my organization in the future, especially during times of organizational change and uncertainty." Managers were somewhat less likely than Individual Contributors to have ISP compliance intentions during uncertain times (I1: $\beta_{(MGR-IC)} = -.095$, $p = .001$), although both groups indicated they both have strong intention compliance preferences. The same is true for item I2, which asks: "I intend to carry out my responsibilities prescribed in the Information Security Policy of my organization when I use

information and technology in the future, especially during times of organizational change and uncertainty." Managers were somewhat less likely than Individual Contributors to carry out ISP compliance responsibilities during uncertain times (I1: $\beta_{(MGR-IC)}$ = -.0.060, p = .044). However, both groups indicated they have strong intention compliance preferences for this item. A significant difference also existed for item AC3 ($\beta_{(MGR-IC)}$ = 0.237, p = .040), which loads onto the Actual Compliance construct asking: "During times of organizational change and uncertainty, I assisted others in complying with information security policies." Mangers (0.775, p<.001) were significantly more likely than individual contributors (0.532, p<.001) to assist others in complying with organizational ISPs in uncertain environments. Table 18 provides the details for the work role demographics, item and path differences within the measurement model.

4.8.1.3 Other Demographic Findings.

We discovered significant differences between demographic groups and individual items concerning factor loading in the measurement model. These items can be found in Table 19. Except for one item, SETA1, between the demographic groups of those with at least an undergraduate degree and those without, differences between the groups identified to have significant differences between them and a particular item all loaded significantly on the items of interest, just at varying degrees. For SETA1, which asks for a response to the statement: "My organization provides training to help employees improve their awareness of computer and information security issues", those without a college education (0.07, n.s.) did not feel as if adequate training concerning ISPs were offered organizationally compared to those with more education (0.19, p<.001) with a loading difference of -.064 and p-value of 0.004. Significant

Table 18: PLS-MGA Lower Order Work Role Group Differences (Item and Path)

PLS-MGA Group		Measurement Item	Path Difference/ Construct	Outer Loading (p-value) (Group A)	Outer Loading (p-value) (Group B)	CI (Group A)	CI (Group B)	Outer Loading Diff (A-B)	bootstrapped T-value		p-value (A-B)
Group A	**Group B**								**Group A**	**Group B**	
Manager	Individual Contributor	I1	Intention to Comply	0.873***	0.970***	0.777, 0.937	0.953, 0.982	-0.095	22.224	134.330	0.001**
Manager	Individual Contributor	I2	Intention to Comply	0.883***	0.944***	0.822, 0.926	0.909, 0.976	-0.06	33.988	53.610	0.044**
Manager	Individual Contributor	AC3	Actual Compliance	0.775***	0.532***	0.632, 0.867	0.308, 0.719	0.237	13.005	5.126	0.040**

PLS-MGA Group		Measurement Item	Path Difference/ Construct	Outer Loading (p-value) (Group A)	Outer Loading (p-value) (Group B)	CI (Group A)	CI (Group B)	Outer Loading Diff (A-B)	bootstrapped T-value		p-value (A-B)
Group A	**Group B**								**Group A**	**Group B**	
Manager	Individual Contributor	PVC->IM	-	0.870***	0.684***	0.508, 0.785	0.810, 0.905	0.182	37.221	10.170	0.001**

Note. Significance level *** p<0.001; ** p<0.05; *p<0.10

Table 19: Significant Reflective Lower-Order Group Differences (Item)

PLS-MGA Group		Measure-ment Item	Path Difference/ Construct	Outer Loading (p-value) (Group A)	Outer Loading (p-value) (Group B)	CI (Group A)	CI (Group B)	Outer Loading Diff (A-B)	bootstrapped T-value		p-value (A-B)
Group A	**Group B**								**Group A**	**Group B**	
College	No College	I1	Intention to Comply	0.90***	0.97***	0.83, 0.94	0.94, 0.98	-0.07	31.79	97.50	0.006**
College	No College	SETA1	SETA	0.19***	0.07	0.82, 0.91	.91, .96	-0.06	42.47	75.52	0.004**
Tenure <5Years	Tenure >5 Years	PO2	Perceived Ownership	0.84***	0.92***	0.76, 0.90	0.89, 0.95	-0.09	28.77	140.08	0.012**
Tenure <5Years	Tenure >5 Years	PO5	Perceived Ownership	0.92***	.96***	0.89, 0.96	0.95, 0.97	-0.04	20.85	65.51	0.025**
Age >35	Age <35	I1	Intention to Comply	0.97***	0.89***	0.92, 0.98	0.94, 0.98	0.08	79.43	28.96	0.006**
Age >35	Age <35	I2	Intention to Comply	0.96***	0.89***	0.93, 0.98	0.83, 0.93	0.07	78.97	40.34	0.005**
Age >35	Age <35	IOU1	Input/Output Uncertainty	0.94***	0.83***	0.92, 0.96	0.69, 0.91	0.11	82.29	14.96	0.006**
Age >35	Age <35	PO5	Perceived Ownership	0.97***	0.93***	0.95, 0.98	0.90, 0.95	0.04	150.60	63.08	0.015**
Age >35	Age <35	RU1	Resource Uncertainty	0.95***	0.85***	0.91, 0.97	0.65, 0.93	0.13	70.38	12.62	0.038**
Age >35	Age <35	RU3	Resource Uncertainty	0.92***	0.86***	0.89, 0.95	0.77, 0.91	0.07	64.39	24.72	0.042**
Work at Site/Hybrid	Work Virtual	PE2	Perceived Efficacy	0.89***	0.68***	0.78, 0.93	0.51, 0.80	0.21	22.70	9.83	0.010**
Work at Site/Hybrid	Work Virtual	PE3	Perceived Efficacy	0.93***	0.87***	0.88, 0.95	0.82, 0.90	0.06	53.02	45.28	0.015**

Note. Significance level *** p<0.001; ** p<0.05; *p<0.10.

differences were also discovered between education groups for item I1. Those respondents who reported having at least an undergraduate degree differed in response to a question concerning intentions to comply with ISPs. Those with a college education (.898, <.001) were significantly less likely than those without a college education (0.969, <.001) to hold intentions to comply with ISPs during times of organizational uncertainty (College-No College: -0.068, p =.006) for measured by item I1.

Age differences for those older and younger than thirty-five (35) were identified as having differences on six different items. While both groups contributed to the respective construct of interest, those above the age of thirty-five (35) were found to have stronger preferences toward intentions to comply for items I1 (35_{Over}-35_{Under}: 0.077, p =.006), I2 (35_{Over}-35_{Under}: 0.067, p =.005), IOU1 (35_{Over}-35_{Under}: 0.11, p =.006), PO5 (35_{Over}-35_{Under}: 0.036, p =.015), RU1 (35_{Over}-35_{Under}: 0.126, p =.038), and RU3 (35_{Over}-35_{Under}: 0.068, p =.042).

Those who worked virtually seemed to perceive that the efficacy of their ISP-related actions toward organizational data security was significantly less than those who worked on-site or in a hybrid fashion. Virtual employees seemed more pessimistic than their counterparts about helping the organization secure its information systems, or if employees could make a difference in their attempts to secure organizational systems (PE2: $W_{(onsite)} - W_{(virtual)}$ 0.210, p =.010; PE3: $W_{(onsite)} - W_{(virtual)}$ 0.060, p =.015).

Finally, those who had been at the organization for greater than five years seemed to have significantly stronger ownership perceptions in response to PO2 and PO5. Response question PO2 asks: “I feel a high degree of personal ownership for my organization's information and communication technologies,” with those who have longer tenure feeling higher degrees of personal ownership of organizational technologies than those tenured less than five years

(Tenure $_{(<5)}$ – Tenure $_{(>5)}$ -.086, p =.012). For response PO5 which inquiries about personal ownership of organizational data, again, those with longer tenure feel a stronger sense of ownership (Tenure $_{(<5)}$ – Tenure $_{(>5)}$ -.041, p =.025)

4.8.2 Inner (Structural) Model Group Differences

After reviewing the outer measurement model and identifying path differences for first-order constructs, tests were performed to determine if any control variables would be needed to moderate heterogenetic population differences in the inner structural model for either Intention to Comply or Actual Compliance. Becker et al. (2012)suggested controls should be placed on any endogenous dependent variable of interest when using SmartPLS. Upon this analysis, no identified demographic group contributed significantly to the endogenous dependent variables of interest.

As with the measurement model, checks for heterogeneity should also be performed for inner structural path measurements (Hair et al. 2011). For individual path analysis on the inner structural model, two interesting findings were identified for specific paths between constructs and can be viewed in Table 20.

For the path Perceived Work Uncertainty and Intrinsic Motivation, significant differences ($\beta_{(MGR-IC)}$ = 0.256, p = .005) existed between mangers (0.766, p<.001) and individual contributors (0.510, p<.001). Managers were significantly more likely to have increasing Intrinsic Motivation initiations over individual contributors and therefore rely more on their skills and abilities to solve ISP issues or failures during times of organizational uncertainty. For the path from Intention

Table 20: Significant Reflective Lower-Order Group Differences (Item)

PLS-MGA Group		Measurement Item	Path Difference/ Construct	Outer Loading (p-value) (Group A)	Outer Loading (p-value) (Group B)	CI (Group A)	CI (Group B)	Outer Loading Diff (A-B)	bootstrapped T-value		p-value (A-B)
Group A	**Group B**								**Group A**	**Group B**	
Manager	Individual Contributor	I1	Intention to Comply	0.87***	0.97***	0.78, 0.94	0.95, 0.98	-0.095	22.220	134.30	0.001**
Manager	Individual Contributor	I2	Intention to Comply	0.88***	0.94***	0.82, 0.93	0.91, 0.98	-0.06	33.980	53.61	0.044**
Female	Male	AC1	Actual Compliance	0.94***	0.86***	0.88, .996	0.80, 0.90	0.088	29.240	36.12	0.027**
Manager	Individual Contributor	AC3	Actual Compliance	0.78***	0.53***	0.63, 0.87	0.31, 0.72	0.24	13.01	5.13	0.040**

Note. Significance level *** p<0.001; ** p<0.05; *p<0.10.

to Comply to Actual Compliance with ISPs, it was found that those who responded and who work virtually (0.735, $p<.001$) as opposed to those who work on-site or in a hybrid fashion (0.575, $p<.001$) were significantly more likely to engage in ISP compliance when they intended to do so ($\beta_{(WO\text{-}SH\ -\ WV)} = -0.160$, $p = .043$). Even though both groups significantly contributed to these inner path coefficients, virtual workers seemed more likely to follow through with compliance decisions when uncertainty existed than those who worked on-site.

This concludes Chapter 4 and our analysis of the data. Next, we will discuss these data and findings in Chapter 5 concerning our research questions and conclude with Chapter 6, introducing our theoretical and practical contributions and the study limitations.

CHAPTER V: DISCUSSION

5.1 Introduction

This chapter aims to synthesize the results from the previous chapter and discuss discoveries uncovered by the research and their overall findings. We will also discuss how this research contributes to the IS security theoretical knowledge base and if our investigation can confirm previous research for which this study is based.

The next section will discuss our results concerning the research questions considered at the beginning of this dissertation. This discussion will be followed by examining the overall results concerning previous research paths and implications of new research findings during this examination. Finally, we will also discuss where this investigation excelled and where it has shortcomings.

5.2 Discussion of the Research Questions

In information security policy compliance investigations, intrinsically motivated individuals are granted the ability to work within appropriate guidelines to secure information and data without external regulation (Pham et al. 2017). Social control and criminal deterrence approach compliance issues extrinsically through the initiation of fear mechanisms (such as sanctions or dismissal) and/or rewards (promotions or awards) (Menard et al. 2017). Previous research has investigated extrinsic factors extensively, finding that fear-based sanctions, awards (or rewards), and even social influences can help us understand individual compliance decisions (Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009a; Straub 1989). These investigations focus on what (or which) external regulations would deter individuals from compiling with organizational security policies. This external factor approach makes motivation a choice not to engage in an activity instead of a choice *to* engage in more proactive security-

based activities. While extrinsic rewards have been studied extensively, intrinsic rewards have also been identified as important avenues of investigation (Herath and Rao 2009a; Son 2011a; Yazdanmehr et al. 2020).

Intrinsic motivation is closely associated with individual empowerment, whereby tasks completed by individuals are sufficient activities in and of themselves and guided by personal self-sanctions, norms, and values (Guo and Yuan 2012; Li et al. 2014; Yazdanmehr et al. 2020). While investigations have responded to calls promoting further investigation into intrinsically motivating factors of ISP compliance (Herath and Rao 2009a; Son 2011b), most have focused on intrinsic motivation as the antecedent that triggers a self-determined course of action. Dhillon et al. (2019)noted the lack of investigations that look for external factors which can trigger intrinsic motivations. That study found structural factors such as SETA, access to information, and decision-making participation enhanced psychological empowerment (or intrinsic motivations) to engage in positive ISP compliance activities. This investigation answered the call made by Thomas and Velthouse (1990), which implemented an intrinsic motivation model utilizing psychological empowerment as the motivational factor reflecting task attributes such as competence, meaning, impact, and choice, allowing employees to feel positive toward accomplishing organizational tasks associated with self-value congruence and efficacy. However, the identified structural empowerments antecedents were unidimensional and relegated antecedents of psychological employment as individual contributors to intrinsic motivations.

Self-determination theory has long argued empowerment structures give individuals the space to execute tasks as they see fit in any given circumstance (Deci and Ryan 1980; Shalley and Oldham 1985; Thomas and Velthouse 1990; Yazdanmehr et al. 2020). Deci and Ryan (1980) developed self-determination theory as a foundation that rests on individual autonomy to engage

in activities that interest them, competence to effectively interact with situational environments to prevent outcomes that may be undesirable, and motivation to fulfill social controls which give a person relatable experience with others in similar situations.

Researchers have focused on individual intrinsic motivators such as perceived effectiveness, self-efficacy, ownership, and value congruence as important intrinsic motivators which can influence behavior concerning individual ISP compliance decisions (Anderson and Agarwal 2010; Herath and Rao 2009b; Rhee et al. 2009; Son 2011a; Workman et al. 2008). However, each construct has been identified as intrinsic motivation itself and not a dimension of intrinsic motivation for which many single dimensions may exist. For example, Dhillon et al. (2019)have been one of a few that asserted individuals become intrinsically motivated when task cognitions associated with competence, meaning, impact, and choice are encountered on a multidimensional level. This previous investigation was predicated on the idea that work structures were in place to increase individual empowerment and found supporting evidence to conclude that intrinsic motivators were likely to mediate between individual, unidimensional extrinsic motivators and ISP compliance outcomes. However, these empowerment structures were designed to enhance psychological empowerment motivators. Work design literature supports this finding that during times of instability in the work contest, employees are happier when they can draw on their skills and abilities to carry out tasks rather than have them dictated by policies that may not match the situation they find themselves facing (Cordery et al. 2010; Knight and Parker 2019).

Previous theoretical insights and research have found empowerment structures influence individual performance but have only focused on structural empowerment antecedents to trigger intrinsic motivations (Dhillon et al. 2019) or have identified how individuals self-regulate when

autonomy, relatedness, and competence trigger moral commitments to security compliance with regards to specific situations (Chen et al. 2012; D'Arcy et al. 2009; Li et al. 2014; Siponen and Vance 2010). We responded to this gap in the IS literature to investigate what may influence intrinsic motivations when structural empowerment motivators may not exist (or maybe lacking altogether) by investigating dimensions of intrinsic motivation when structural uncertainty surrounding ISP compliance behavior is the unexpected norm.

Our argument, presented in the first chapters, is predicated on extrinsic factors motivating individual intrinsic initiatives when faced with uncertain work situations. Work design theory allows for such uncertain extrinsic factors in which individuals can be proficient, adaptable, and proactive when facing new work environments (Griffin et al. 2007). In this situation, structural empowerment is woven into the work task itself and not predicated on any singular attribute associated with the task that workers are asked to perform. During times of high work uncertainty for which there is no structure for the employee to rely, individuals are asked to trust their skills and abilities to make decisions surrounding adherence to organizational policies (Cordery et al. 2010; Wall et al. 2002). This is a direct example of individual empowerment. Njenga and Brown (2012)correlated intrinsic empowerment with uncertainty and suggested that employees secured information in rational and adaptive methods when organizational environments became volatile. This, however, did not address our central theme of when the structural empowerment arrangements themselves are no longer relevant or become uncertain in how one carries out compliance behaviors.

Intrinsic motivation as a mediator has been supported for outcomes concerning individual performance in previous studies (Dhillon et al. 2019; Maynard et al. 2012; Spreitzer et al. 1997). Work design theories have indicated that in situations with increasing work uncertainty,

employees seek more job control leading to increases in intrinsic satisfaction (Parker et al. 2001). These studies have been reinforced by significant results showing that employees can self-regulate an appropriate response to job situations during times of increasing uncertainty and have more autonomy and job crafting capability (Leach et al. 2013). Gagné and Deci (2005)conceptualized self-determination theory as a theory of work motivation where individuals maintain their intrinsic motivation by feeling that they are competent to carry out a task while having the autonomy to self-select a course of action. Furthermore, SDT conceptualized the need for relatedness in which satisfaction becomes internalized and associated with aligned values and regulatory processes put in place by the organization (Gagné and Deci 2005). Therefore, this study sought out relationships between increasingly uncertain and multidimensional work environments and dimensions of intrinsic motivations in information security policy compliance. These previous arguments led us to investigate the mediating role of intrinsic motivation between the multidimensional elements of perceived work uncertainty and intended and actual ISP compliance behavior.

To summarize, our above review showcased what motivated this study and led to our research questions: How does the multidimensional construct of perceived work uncertainty, including resource, task, and input/output uncertainty augment intrinsic motivations concerning ISP compliance? Do first-order dimensions impact multidimensional intrinsic motivations and its mediating role of ISP intended and actual compliance behavior? Does SETA mediate relationships between intrinsically motivated individuals who seek out these programs to craft responses to ISP requirements during times of perceived work uncertainty? We discuss the findings of this study and the implications surrounding these findings in the following sections.

5.2.1 Research Question 1

This study argues that intrinsic motivation is a multidimensional construct composed of many different single dimensions. We investigated perceived effectiveness, perceived self-efficacy, perceived value congruence, and perceived ownership. Intrinsic motivation has been identified as a complex multidimensional construct by multiple academic endeavors (Deci and Ryan 2000; Gottschalg and Zollo 2007; Ke et al. 2012).

The findings of this study are unambiguous in that all hypotheses associated with first-order dimensions of perceived self-efficacy, effectiveness, value congruence, and ownership are positively related and significant with intrinsic motivation related to ISP compliance. This is in line with hypotheses 1, 2, 3, and 4. This is not surprising as these same independent dimensions of intrinsic motivation have been studied previously and independently influence ISP compliance behaviors (Anderson and Agarwal 2010; Chan et al. 2005; Herath and Rao 2009b; Son 2011b; Workman et al. 2008).

Spreitzer et al. (1997)concluded psychological empowerment to be a second-order construct. Studied as associated with activities of work, Dhillon et al. (2019)concluded these work behaviors to be that of psychological empowerment activities and "intrinsic motivation factors" of ISP compliance in line with Thomas and Velthouse (1990). They defined intrinsic motivation as "positively value experiences that the individual derives directly from the task" (p. 668). This evaluation of the second-order inclusion of intrinsic motivation supports our research goal and supports overall study objectives.

5.2.2 Research Question 2

We argued in this study that employees would be affected by intrinsic motivations when surrounded by uncertain work conditions or practices. To be more specific, we investigated how

the multidimensional aspect of intrinsic motivation (formed from perceived self-efficacy, effectiveness, ownership, and value congruence) influenced behaviors of ISP compliance. Gagné and Deci (2005)and Parker et al. (2001)stipulated that intrinsic satisfaction leads to a relatedness between organizational work regulations, autonomy to select appropriate actions, and self-identified competence to craft a response. SDT would argue this increases intrinsic work motivation, while work design theory argues intrinsic satisfaction increases during uncertain work situations through more job control, including job crafting (Leach et al. 2013).

Leach et al. (2013)developed the multidimensional construct of work uncertainty formed from three different measures of resource uncertainty, task uncertainty, and input/output uncertainty for manufacturing and non-manufacturing work settings. Our findings generally support these developed measures of work uncertainty in the context of information security policy compliance. We found significant positive support for Hypotheses 5, 6, and 7, which shows perceived resource, task, and input/output uncertainty concerning information security policies are related to perceived work uncertainty as a multidimensional construct. While support from resource uncertainty and input/output uncertainty was fairly robust, support from perceived task uncertainty was relatively weak.

These results indicate that managers who are not familiar with information security policies and cannot provide precise guidance in uncertain IS security situations significantly contributes to overall perceived work uncertainty surrounding IS security. Employees found that if managers cannot be relied upon to provide information about the ISP. As with the previous studies, we found that input/output uncertainty is somewhat correlated with resource uncertainty (Leach et al. 2013). Managers who can supply information as a service to the worker to accomplish work functions can be viewed as a resource to attain work goals. Employees can be

viewed as both givers and receivers of work policies' information. This is consistent with knowledge-sharing literature where managers can reduce ambiguity during unexpected events (Juneau Jr 2013; Oldham and Fried 2016; Sterna and Wolfe 2019).

The results also indicate that the information security policy contributes to perceived work uncertainty if viewed as an uncertain resource. We witnessed significant effects that employees who feel a degree of resource uncertainty surrounding information security policies will also have increased feelings of general job uncertainty when attempting to carry out work functions. These feelings do not need to be a lack of guidance in the information system policy as a whole, but as a lack of a resource to help determine what course of action to embark on given an uncertain situation surrounding information security. This is consistent with Bulgurcu et al. (2010), which found the quality of an ISP as a resource that was clear, complete, and consistently allowing for better overall compliance decisions. When these components are not utilized, the resources can lead to less goal attainment and work engagement (Hornung et al. 2010; Schneider et al. 2017). When developing the measures for perceived work uncertainty, Leach et al. (2013)noted the relationship between clarity and resource uncertainty and the availability of information to carry out work tasks. Results for resource and input/output-related uncertainty are supported in the extant literature. Still, due to the lack of investigation of the clarity of the ISP as a resource to engage in IS security compliance behaviors, there is limited IS security literature from which to compare these results.

Task uncertainty was also significantly supported in our analysis. However, the strength of its relevance to provide insight into perceived work uncertainty was comparatively weak. Larsen (2003)defined task uncertainty as the difference between the information required to perform a task and information possessed by an organization that allows that task to be

completed. Considering the entire respondent population, employees were neutral about task uncertainty surrounding ISP-related tasks changing unexpectedly, varying daily, or with little warning. This suggests most workers find ISPs to be generally stable, but when unexpected tasks occur concerning ISPs, at least some uncertainty to carry out work goals is generated. Furthermore, when checking for heterogeneity in population responses, gender significantly affected this construct, with females being the only contributor to task uncertainty significance. We found that females were more likely to encounter unexpended work tasks surrounding ISPs than males. Additionally, males did not significantly contribute to the work uncertainty construct. While finding that task uncertainty can provide insight into overall work uncertainty, these results are not generalizable to the population of interest. Many studies in the information systems literature have dealt with task uncertainty to implement decision support systems and how it affects end-user computing. (Blili et al. 1998; Harris and Weistroffer 2009). Other findings support task uncertainty associated with a lack of resources to perform work processes (Rocha 2011). As with the other uncertainty constructs, we cannot find reciprocal investigations where uncertain tasks were investigated concerning IS security issues.

For our second-order analysis, we found strong support and significant evidence that generalized perceived work uncertainty influences feelings of overall intrinsic motivations for employees concerning ISP compliance issues. This finding supports hypothesis H8. As work design theory indicates, during times of uncertainty, employees tend to develop their own work-decision making arrangements on how best to carry out work goals when rational choice is depleted due to an uncertain environment (Clegg 1984; Perrow 1967; Wall et al. 2002). Self-determination as a theory of work motivation is centered on autonomous motivation as a means to have effective employee performance and well-being (Gagné and Deci 2005). Our findings

support these theories and are consistent with previous research in IS security literature where Njenga and Brown (2012)identified employees who improvised ISP compliance activities during uncertain periods.

Additionally, Raza et al. (2019)found internal motivations alleviated ISP tension that disrupted work flows. Our findings show that when an ISP is uncertain about its rules and procedures and managers do not have adequate answers to ISP-related questions, and employees will activate intrinsic work motivations to overcome their feelings of work uncertainty to overcome any disruption associated with work ambiguity. These motivations will be related to how effective and capable they perceive themselves to be when addressing inadequate policy issues, how aligned they perceive their values to be with the organization, and if they feel as if any danger to organizational data and networks concerning security threats is viewed as a personal threat.

All hypothesized relationships between perceived work uncertainty and its measurement elements were supported. However, task uncertainty exhibited heterogeneity issues surrounding gender by only identifying females as contributors to perceived task uncertainty concerning ISPs. Perceived resource uncertainty and perceived input/output uncertainty was also significant contributor to perceived work uncertainty as lower-order dimensions as predicted by (Leach et al. 2013). Additionally, Perceived Work Uncertainty significantly increased individual intrinsic work motivations to continue with work tasks. Although not identical, this is in line with previous investigations pointing to uncertainty as a means to increase intrinsically motivated behavior (Gagné and Deci 2005; Wall et al. 2002).

5.2.3 Research Question 3

A primary objective of this research was to establish the mediating effect of intrinsic work motivation on the relationship between perceived work uncertainty and information security policy compliance behavior and SETA. This study proves that intrinsic motivation mediates the relationship between work uncertainty when considering IS policies and ISP compliance intentions. This research also found significant evidence for the mediating effect intrinsic motivation plays when employees uncertain about information system policies seek out additional support in the form of organizational SETA programs. This confirms hypotheses H9 and H10 and suggests that when ISPs become uncertain about work issues concerning security threats, employees will develop intrinsic work motivations to comply with IS policies while attempting to continue with work goals. Additionally, when faced with uncertain IS policies, this suggests organizations should have options surrounding education and training (SETA) programs where employees can locate additional resources to complete work goals and reduce ISP uncertainty.

Intrinsic motivations have been studied through IS policy compliance literature (Dhillon et al. 2019; Herath and Rao 2009b; Li et al. 2010; Son 2011b), but only recently has intrinsic motivation been investigated as a mediating factor to ISP compliance behaviors (Dhillon et al. 2019) and our findings support that intrinsic motivators can play an important role in mediating individual compliance decisions. It has been noted that drivers of intrinsic motivations concerning ISP behavior should be investigated further (Dhillon et al. 2021; Karjalainen et al. 2019).

To our knowledge, this is the first time that research has shown that intrinsic motivation has a mediating effect on individuals seeking out organizational SETA programs. While SETA

has been utilized as an antecedent to psychological empowerment (Dhillon et al. 2019), this construct is primarily utilized as an antecedent to security related outcomes for either compliance or non-compliance behaviors (Barlow et al. 2018; D'Arcy et al. 2009; Hu et al. 2021). Intrinsic motivation played a strong role in the seeking out of organizational SETA programs and is in line with Herath and Rao (2009b)who found, when faced with security threats, individuals self-assess their response capability and determine if they have the necessary skills to respond to a security threat. SETA programs can directly influence ISP compliance behaviors, but our analysis suggest once SETA program in place, it is beneficial to understand how employees may seek out or utilize such programs when faced with, in our analysis, uncertainty about the ISP as a resource.

An ad hoc analysis was performed to determine if intrinsic motivation played a full or partial mediating role between general work uncertainty and both intentions to comply with ISPs or SETA. This study found that intrinsic motivation only partially mediated the relationships between both intentions to comply with ISPs and with SETA.

5.2.4 Research Question 4

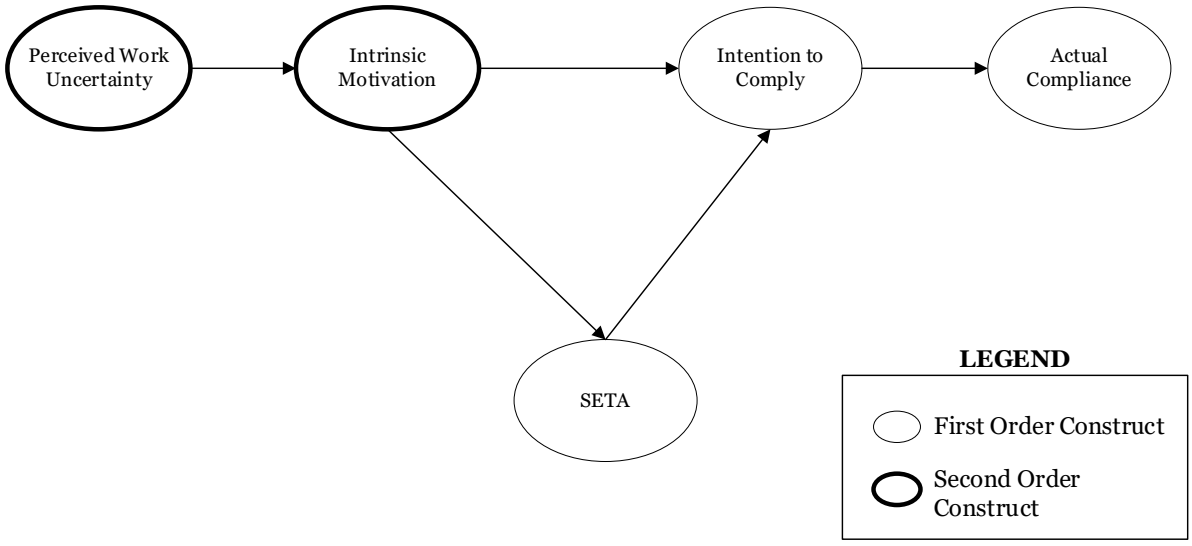
Our final research question explored the mediating role that SETA plays between general intrinsic motivation and intentions to comply with ISPs. This study provides evidence that SETA has a weak role in mediating the relationship between these two constructs and supports hypotheses H10 and H11. The predictive quality of the results showed that SETA was a good fit to determine if workers who sought out SETA programs would generally comply with ISPs. However, SETA has little effect on individual ISP compliance decisions as a mediator. Our study showed that SETA could play a mediating role between intrinsic motivation and intentions to

comply with ISPs. Post hoc analysis indicated a partially mediated relationship between intrinsic motivation and intention to comply with ISPs.

5.3 Summary

This study sought to identify elements of intrinsic motivation - perceived self-efficacy, perceived effectiveness, perceived ownership, and perceived value congruence – and develop a second-order generalized component to give explanations based on theory about antecedents of employees' intentions to comply with information security policies. Additionally, we hypothesized that work design elements associated with job crafting and job control, including perceived resource, task, and input/output uncertainty, would develop a second-order variable that would indirectly encourage employees to comply with ISPs through intrinsic motivation. The theoretical model in this study was supported in its entirety. Based on 269 respondents who had knowledge of organizational ISP rules and procedures, all of the hypotheses were supported. Figure 3 provides a visual representation of the ISP compliance model resulting from this study.

Figure 3: Resulting ISP Compliance Model



One of the primary implications from this study and our results is the indirect mediation of the relationship between perceived work uncertainty and intentions to comply with information security policies. External and internal motivations for individual compliance with information security polices are important to develop a clear understanding of employees' thoughts and behaviors. It should be noted that, for our study, a focus on employees' perceptions of uncertain IS policies when attempting to complete work goals or requirements would be insufficient to provide a complete picture of individual employee ISP compliance behavior.

The second-order, multidimensional construct of intrinsic motivation, developed with four single dimensions of perceived self-efficacy, effectiveness, ownership, and value congruence, indicated that intentions to comply with ISPs when the policy itself is deemed unsatisfactory, contradictory, or unreliable to accomplish specific work requirements is an important consideration. Employees are influenced during those times when ISPs may be unclear about how to carry out a work requirement as to how effective their response may be or the confidence of the skill set, and they have to make informed decisions about ISP compliance. Additionally, if they sense that making compliance decisions are personal to themselves or those security threats would harm them in a personal way, they are more inclined to make positive ISP behavior decisions. One other element of intrinsic motivation we found was that individuals would respond positively to ISP threats if they considered the organizations and their own ethical values to be similar. All this is to say that individual perceptions about intrinsic motivations and how they are perceived through the identified unidimensional constructs, which formed our intrinsic motivation multidimensional construct, are vital to IS security-related compliance behaviors. This is further evidence that intrinsic motivators influence ISP compliance intentions

and behaviors and backs previous IS literature in this area (Anderson and Agarwal 2010; Bulgurcu et al. 2010; Dhillon et al. 2019; Herath and Rao 2009b; Son 2011a).

Another important aspect of our study and findings is the view that the ISP can become the source of uncertainty in compliance decisions. Most all ISPs are developed to bring clarity to employees on how to address security threats while making compliance decisions. However, where ISPs have been investigated about the demands and impositions they place on work goal attainment or inhibiting work requirements, we have noted that the ISP may not be able to provide answers to all threats encountered. Nor might it be comprehensive enough to guide employees through periods of work uncertainty including mangers.

Overall, our results should invigorate the debate about which strategies increase intrinsic motivation and what strategies should be deployed to maximize positive reactions during times of uncertainty concerning IS compliance behaviors. This study has provided evidence that organizations should design work practices that allow employees latitude to make ISP compliance decisions when ISPs are unclear or uncertain. Managers also cannot provide correct courses of remedy or action during these periods. We have also demonstrated that when employees face such uncertainty, they become intrinsically motivated to seek out organizational SETA programs, which will provide skills necessary to increase intrinsic motivators and thus positive ISP compliance behaviors. Previous studies have shown employees desire to be incorporated into decision-making where they can provide their insight about risk assessment, overall ISP design, and ISP implementation (Dhillon 2004; Dhillon et al. 2019). When faced with uncertainty surrounding the ISP and work requirements, it allows individuals to feel more informed about organizational IPS goals and values, which further exploits individual intrinsic motivators. Work design theory has shown that during periods of high uncertainty, workers want

to rely on their own skillset and abilities, and our research bears this out in relation to ISP compliance issues.

To our knowledge, no previous information security study has tested the effects of ISP-related work uncertainty and IS security outcomes. Needless to say, to our knowledge, no previous study has tested how that uncertainty triggers intrinsic motivations to comply with ISPs as an individual sees fit and in close resemblance with organizational ISP goals. Only a few ISP-related investigations have tested the mediating effects of intrinsic motivators selecting instead to focus on direct effects between work environments or job demands concerning ISPs, among others (Cram et al. 2019; Dhillon et al. 2021). SETA has been shown to have direct effects on ISP compliance behaviors (D'Arcy et al. 2009) and as an antecedent to psychological empowerment structures (Dhillon et al. 2019), but we also show it can serve as a mediator between intrinsic motivations and intentions to comply with ISPs by giving employees an outlet to gain skills and abilities if they feel their current capabilities are insufficient or need improvement.

CHAPTER VI: CONCLUSION

6.1 Introduction

We have examined the relationships between perceived work uncertainty, intrinsic motivations, SETA, and intentions to comply with IS security policies in this thesis. We encapsulated two theories to gain our theoretical insight. The focus of our research questions and which drove our inquiry was: How does intrinsic motivation mediate relationships between perceived work uncertainty, with respect to ambiguous IS policies, and intentions to comply with IS policy requirements. We investigated all relevant literature, which helped us identify and answer the research questions, and presented our hypotheses and conceptual model in Chapter 2. Chapter 3 revealed our quantitative research methods and quantitative research approach. Our conceptual model was put to the test in Chapter 4, and the results of our analysis were presented. A discussion of the results is followed in Chapter 5. This chapter will discuss the theoretical and practical inferences from this investigation along with what possibilities this research allows in future investigations.

6.2 Theoretical and Practical Contributions

It goes without saying that the purpose of academic research is to contribute to the academic body of knowledge. We will present our theoretical and practical contributions to IS security, work design, and general information system literate in the coming sections.

6.2.1 Theoretical Contributions

Given our investigation of the literature, we believe this is the first investigation looking at information security policy as an unreliable resource and how employees seek relief from that uncertainty when attempting to comply with IS policies. In order to engage in this study, we extended the use of self-determination theory by Gagné and Deci (2005)and their

conceptualization of intrinsic work motivation. While we are not the first in the information security field to investigate intrinsic work motivation as a mediator to information security tasks (Dhillon et al. 2019), however, this course of investigation is rare in the context of ISP research. We distinguish ourselves from previous studies that have utilized self-determined work motivation (Boss et al. 2009; Bulgurcu et al. 2010; D'Arcy et al. 2009; Dhillon et al. 2019; Son 2011b; Straub 1989) by (1) investigating multidimensional intrinsic work motivation as a mediator of IS policy compliance intentions and developed by one-dimensional intrinsic elements, and (2) how perceived work uncertainty created by imprecise ISPs motivate IS policy compliance intentions. This study seeks to assess how individuals are motivated through perceived ownership, self-efficacy, effectiveness, and value congruence when faced with uncertainty related to work uncertainty elements. Within this frame, we used variables identified from work design theory utilized to identify multidimensional work uncertainty issues, and associated with job control and job crafting, to predict intrinsic motivation. Decoupling direct relationships between uncertainty issues, we used these variables to predict employee intrinsic work motivations, how those motivations pushed employees to seek additional training and education, and ultimately comply with ISPs. Therefore, the results of this study show how the identification of perceived work uncertainty in the ISP itself can help to explain and improve IS security-related behaviors via increased intrinsic work motivation.

A second contribution is the extension of ISP compliance intentions to a new domain, specifically that of work uncertainty and work design, and validated measures of multidimensional work uncertainty as antecedents of intrinsic motivation on ISP compliance intentions. Measures of work uncertainty were developed with the intention they could be utilized to examine uncertainty in many work settings. To our knowledge, this is the first study to

test these measures on specific work tasks in information systems literature. The results validate past work design concepts which draw conclusions that increased job control and job crafting can enhance intrinsic satisfaction (and this intrinsic motivation) when carrying out specific tasks through a bottom-up approach rather than a top-down approach (Clegg and Spencer 2007; Grant and Parker 2009), especially during times of work uncertainty (Leach et al. 2013). This research validates previous findings from different research settings and allows further generalization of contextual work uncertainty insights.

Third, this study makes contributions to the intrinsic motivation literature by investigating drivers of intrinsic motivation, in this case, increased reliance on individual skills and abilities during times of work uncertainty. This study provides deliberations on how intrinsic motivation is driven with respect to IS security compliance which has received little attention in the ISP literature and answers the call from Dhillon et al. (2019) that antecedents of intrinsic motivations be identified for ISP compliance behaviors.

Fourth, this study investigated the mediating role of SETA between intrinsic motivation and intentions to comply with ISPs. The mediating effect identified in this study enhances what is currently known about SETA programs within the ISP literature. Many previous studies have identified SETA as an antecedent of ISP compliance and psychological empowerment (D'Arcy et al. 2009; Dhillon et al. 2019). We found that employees who are uncertain about are security policies become intrinsically motivated and will seek additional development of skills and abilities through SETA programs if they are available. This expands current research on SETA-driven investigations by explicitly examining the mediating effect SETA has on compliance intentions and providing evidence of why employees will seek out such programs.

6.2.2 Practical Contributions

This research primarily focused on relationships between the multidimensional construct of intrinsic motivation, measured through four unidimensional elements, perceived work uncertainty in the ISP, and intentions to comply with the ISP. Employee behavior with respect to ISPs and how they make decisions based on ambiguous information within the work context to complete work goals and requirements is critical to overall IS security. Understanding employee compliance behaviors and what motivates them to act in specific ways is an important consideration for organizations (Bulgurcu et al. 2010; Donalds and Barclay 2021; Herath and Rao 2009a; Li et al. 2021). We paid particular attention to drivers of intrinsic motivation, which show an ability to be stronger predictors of employee behavior than that of extrinsic motivators (Menard et al. 2018; Son 2011a).

This investigation sought to investigate antecedents of intrinsic motivation which can allow organizations to manage employees who may face situations where the ISP becomes ambiguous or uncertain, and how that uncertainty can encourage employees to rely on their own skills and abilities to determine a correct course of action with respect to ISP compliance. This study offers elements of work design strategies that can be deployed to increase compliance intentions and behaviors. In general, ISPs are designed to be rigorous, inflexible guidelines for which employees are expected to adhere and support organizational data security. However, malicious threat actors are constantly and consistently attempting to determine new and novel approaches to engage employees to gain access to organizational data and networks. Unfortunately, even the best ISPs cannot account for all situations employees may face allowing for some measure of uncertainty in the ISP to disrupt work requirements. This research indicates policies should be designed, in accordance with work design techniques, to allow employees to

become intrinsically motivated to determine a course of action beneficial to the organization. As employees are faced with work situations for which the ISP did not foresee, it is useful to consider the methods for which ISPs can be modified to incorporate skills and abilities so that they are positively able to secure the necessary information or networks of the organization during these times of work uncertainty.

This study provides a pathway for organizations to increase employee intrinsic work motivations. While organizations should make every effort to develop a comprehensive ISP policy, they should also understand the limitations of any written policy. ISPs should be written to allow for, and encourage, active employee participation in the development of ISP, specifically during times of uncertainty. ISP can be designed to outline guidelines for employees to engage in ISP compliance of their own volition and intrinsic satisfaction.

6.3 Limitations

We have several limitations in this study. First, this study is cross-sectional and only looks at specific periods of time when considering ISP compliance behaviors. Cross-sectional research does not give causal directions and does not allow for conclusions of causality—something that experimentation or longitudinal studies can ascertain. Another limitation of this study is the method of data collection. Self-reported surveys allow the possibility that participants were not truthful due to the compliance (or rule) oriented intentions. Additionally, Herath and Rao (2009a)reference a halo effect from which survey participants can be influenced by the environment in which they find themselves. Future investigations should consider obtaining actual workplace data or observations to correct this limitation, as well as the use of case studies to gain further insight into this phenomenon.

This study was also limited in the participant selection method. As we noted in previous chapters, MTurk gives a good representation of demographics for participant selection. However, it has limitations through the investigator's ability to validate the target population was actually utilized or attained. For instance, we wanted only working adults in the United States to respond to the survey request. While every effort to check responses to identify targeted populations, there remains the possibility that respondents were not fully employed or residents of the US. The participant pool was also nonrandomized and limited to only those who hold Amazon MTurk respondent accounts-a, a generally homogenous population. Therefore, generalization to the entire work population is limited. Future studies in this topic area should attempt to adhere to a randomized selection of employees across cultures, organizations, and/or countries.

A final limitation is that of common method variance (CMV), for which we controlled but remains a possibility due to the self-reporting nature of our data collection process. Fortunately, discriminate validity was attained and thus abates CMV issues.

6.4 Future Research Directions

This study can be extended to identify further periods of work uncertainty surrounding ISP compliance behaviors. First, while all hypothesized relationships surrounding work uncertainty were found to be significant, the unidimensional construct of task uncertainty was weak and provided little insight into the overall multidimensional work uncertainty construct. Although the measures of work uncertainty were developed with both manufacturing and non-manufacturing work environments in mind, issues of work uncertainty for ISP compliance behavior may be more process-oriented than task-driven. Future research should attempt to identify if differences in such measures would be useful for further investigation. Additionally, although divergent and convergent validities were within acceptable norms, it is suggested future

research focus on areas where policy may be uncertain to determine if managers a viewed as a recourse to relieve uncertainty much the same as the policy itself.

Another future research direction is to further developed and find antecedents of intrinsic motivation concerning ISP compliance decisions. As our main intent of this study focused on perceived work uncertainty emanating from the ISP policy, the effects of other factors of intrinsic motivation should be identified and which was beyond the scope of this study. Additionally, researchers should attempt to classify additional factors for all main constructs identified in this study to help understand ISP compliance decisions and uncertainty.

This study also was broad in its description of ISP-related compliance and uncertainty issues. Future research should attempt to identify more specific facets of the uncertainty of ISS policies and determine more meaningful results for IS-specific tasks, which were beyond the scope of this research.

REFERENCES

Abraham, S., and Chengalur-Smith, I. (2019). "Evaluating the Effectiveness of Learner Controlled Information Security Training," *Computers & Security*, 87), p.101586.

Anderson, C. L., and Agarwal, R. (2010). "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS quarterly*), pp.613-643.

Argote, L. (1982). "Input Uncertainty and Organizational Coordination in Hospital Emergency Units," *Administrative science quarterly*), pp.420-434.

Avgoustaki, A. (2016). "Work Uncertainty and Extensive Work Effort: The Mediating Role of Human Resource Practices," *ILR Review*, 69(3), pp.656-682.

Bandura, A. (1986). "Social Foundations of Thought and Action," *Englewood Cliffs, NJ*, 1986).

Barclay, D., Higgins, C., and Thompson, R. (1995). *The Partial Least Squares (Pls) Approach to Casual Modeling: Personal Computer Adoption Ans Use as an Illustration*.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. (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), p.3.

Becker, J.-M., Klein, K., and Wetzels, M. (2012). "Hierarchical Latent Variable Models in Pls-Sem: Guidelines for Using Reflective-Formative Type Models," *Long range planning*, 45(5-6), pp.359-394.

Ben-Ner, A., Kong, F., and Lluis, S. (2012). "Uncertainty, Task Environment, and Organization Design: An Empirical Investigation," *Journal of Economic Behavior & Organization*, 82(1), pp.281-313.

Blili, S., Raymond, L., and Rivard, S. (1998). "Impact of Task Uncertainty, End-User Involvement, and Competence on the Success of End-User Computing," *Information & Management*, 33(3), pp.137-153.

Bollen, K. A. (1984). "Multiple Indicators: Internal Consistency or No Necessary Relationship?," *Quality and Quantity*, 18(4), pp.377-385.

Bollen, K. A. (2011). "Evaluating Effect, Composite, and Causal Indicators in Structural Equation Models," *MIS Quarterly*, 35(2), pp.359-372.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS quarterly*, 39(4), pp.837-864.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and 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), pp.151-164.

Broedling, L. A. (1977). "The Uses of the Intrinsic-Extrinsic Distinction in Explaining Motivation and Organizational Behavior," *Academy of Management Review*, 2(2), pp.267-276.

Browne, M. W., and Cudeck, R. (1993). "Alternative Ways of Assessing Model Fit in Bollen Ka & Long Js (Eds.), Testing Structural Equation Models (Pp. 136–162)." Newbury Park, CA: Sage.[Google Scholar].

Bruns, T., and Stalker, G. (1961). "The Management of Innovation," *Tavistock, London*), pp.120-122.

Buhrmester, M., Kwang, T., and Gosling, S. D. (2016). "Amazon's Mechanical Turk: A New Source of Inexpensive, yet High-Quality Data?,").

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly*, 34(3), pp.523-548.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010b). "Quality and Fairness of an Information Security Policy as Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation,").

Burns, A., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. (2015). "Assessing the Role of Security Education, Training, and Awareness on Insiders' Security-Related

Behavior: An Expectancy Theory Approach," *2015 48th Hawaii International Conference on System Sciences*: IEEE, pp. 3930-3940.

Burns, A., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. (2018). "Intentions to Comply Versus Intentions to Protect: A Vie Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational Seta Efforts," *Decision Sciences*, 49(6), pp.1187-1228.

Carmeli, A., and Schaubroeck, J. (2008). "Organisational Crisis-Preparedness: The Importance of Learning from Failures," *Long range planning*, 41(2), pp.177-196.

Chan, M., Woon, I., and Kankanhalli, A. (2005). "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of information privacy and security*, 1(3), pp.18-41.

Chen, Y., Ramamurthy, K., and Wen, K.-W. (2012). "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems*, 29(3), pp.157-188.

Cherns, A. (1976). "The Principles of Sociotechnical Design," *Human relations*, 29(8), pp.783-792.

Chin, W. W. (1998). "Commentary: Issues and Opinion on Structural Equation Modeling." JSTOR.

Chin, W. W. (2010). "Bootstrap Cross-Validation Indices for Pls Path Model Assessment," in *Handbook of Partial Least Squares*. Springer, pp. 83-97.

Ciborra, C. U. (1996). "The Platform Organization: Recombining Strategies, Structures, and Surprises," *Organization science*, 7(2), pp.103-118.

CISA. (2020). "Covid-19 Exploited by Malicious Cyber Actors." Retrieved June 16, 2020, 2020, from https://www.us-cert.gov/ncas/alerts/aa20-099a

Clegg, C., and Spencer, C. (2007). "A Circular and Dynamic Model of the Process of Job Design," *Journal of Occupational and Organizational Psychology*, 80(2), pp.321-339.

Clegg, C. W. (1984). "The Derivation of Job Designs," *Journal of Organizational Behavior*, 5(2), pp.131-146.

Cohen, J. (1998). "Statistical Power Analysis for the Behavioural Sciences, Xxi," *Hillsdale, NJ: L Erlbaum Associates*).

Cordery, J. L., Morrison, D., Wright, B. M., and Wall, T. D. (2010). "The Impact of Autonomy and Task Uncertainty on Team Performance: A Longitudinal Field Study," *Journal of organizational behavior*, 31(2-3), pp.240-258.

Cram, W. A., D'Arcy, J., and 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).

Crawford, E. R., LePine, J. A., and Rich, B. L. (2010). "Linking Job Demands and Resources to Employee Engagement and Burnout: A Theoretical Extension and Meta-Analytic Test," *Journal of applied psychology*, 95(5), p.834.

Cronbach, L. J. (1971). "Test Validation," *Educational measurement*).

Cuganesan, S., Steele, C., and Hart, A. (2018). "How Senior Management and Workplace Norms Influence Information Security Attitudes and Self-Efficacy," *Behaviour & Information Technology*, 37(1), pp.50-65.

D'Arcy, J., Herath, T., and Shoss, M. K. (2014). "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective: Jmis Jmis," *Journal of Management Information Systems*, 31(2), p.285.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, 20(1), pp.79-98.

Davis, D. (2005). *Business Research for Decision Making*. Thomson/Brooks/Cole.

Deci, E. L., and Ryan, R. M. (1980). "Self-Determination Theory-the Iteration of Psychophysiology and Motivation," *Psychophysiology*: SOC PSYCHOPHYSIOL RES 1010 VERMONT AVE NW SUITE 1100, WASHINGTON, DC 20005, pp. 321-321.

Deci, E. L., and Ryan, R. M. (2000). "The" What" and" Why" of Goal Pursuits: Human Needs and the Self-Determination of Behavior," *Psychological inquiry*, 11(4), pp.227-268.

Deci, E. L., and Ryan, R. M. (2010). "Intrinsic Motivation," *The corsini encyclopedia of psychology*), pp.1-2.

Demerouti, E., Bakker, A. B., Nachreiner, F., and Schaufeli, W. B. (2001). "The Job Demands-Resources Model of Burnout," *Journal of Applied psychology*, 86(3), p.499.

Dhillon, G. (2004). "Realizing Benefits of an Information Security Program," *Business Process Management Journal*, 10(3), pp.260-261.

Dhillon, G. (2007). *Principles of Information Systems Security: Texts and Cases*. John Wiley & Sons Incorporated.

Dhillon, G., Abdul Talib, Y., and Picoto, W. N. (2019). "The Mediating Role of Psychological Empowerment in Information Security Compliance Intention," *Journal of the Association for Information Systems*, 19(4), pp.247-265.

Dhillon, G., Smith, K., and Dissanayaka, I. (2021). "Information Systems Security Research Agenda: Exploring the Gap between Research and Practice," *The Journal of Strategic Information Systems*, 30(4), p.101693.

Diamantopoulos, A., Riefler, P., and Roth, K. P. (2008). "Advancing Formative Measurement Models," *Journal of business research*, 61(12), pp.1203-1218.

Dijkstra, T. K., and Henseler, J. (2015). "Consistent and Asymptotically Normal Pls Estimators for Linear Structural Equations," *Computational statistics & data analysis*, 81), pp.10-23.

Diver, S. (2007). "Information Security Policy-a Development Guide for Large and Small Companies," *Sans Institute*), pp.1-37.

Donalds, C., and Barclay, C. (2021). "Beyond Technical Measures: A Value-Focused Thinking Appraisal of Strategic Drivers in Improving Information Security Policy Compliance," *European Journal of Information Systems*), pp.1-16.

Edwards, J. R. (2001). "Multidimensional Constructs in Organizational Behavior Research: An Integrative Analytical Framework," *Organizational research methods*, 4(2), pp.144-192.

F. Hair Jr, J., Sarstedt, M., Hopkins, L., and G. Kuppelwieser, V. (2014). "Partial Least Squares Structural Equation Modeling (Pls-Sem) an Emerging Tool in Business Research," *European Business Review*, 26(2), pp.106-121.

Fornell, C., and Larcker, D. F. (1981). "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics." Sage Publications Sage CA: Los Angeles, CA.

Gagné, M., and Deci, E. L. (2005). "Self-Determination Theory and Work Motivation," *Journal of Organizational behavior*, 26(4), pp.331-362.

Gangire, Y., Da Veiga, A., and Herselman, M. (2019). "A Conceptual Model of Information Security Compliant Behaviour Based on the Self-Determination Theory," *2019 Conference on Information Communications Technology and Society (ICTAS)*: IEEE, pp. 1-6.

Gefen, D., Straub, D., and Boudreau, M.-C. (2000). "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the association for information systems*, 4(1), p.7.

Gottschalg, O., and Zollo, M. (2007). "Interest Alignment and Competitive Advantage," *Academy of management review*, 32(2), pp.418-437.

Grant, A. M., and Parker, S. K. (2009). "7 Redesigning Work Design Theories: The Rise of Relational and Proactive Perspectives," *Academy of Management annals*, 3(1), pp.317-375.

Griffin, M. A., Neal, A., and Parker, S. K. (2007). "A New Model of Work Role Performance: Positive Behavior in Uncertain and Interdependent Contexts," *Academy of management journal*, 50(2), pp.327-347.

Guo, K. H., and Yuan, Y. (2012). "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model," *Information & Management*, 49(6), p.320.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. (2011). "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of management information systems*, 28(2), pp.203-236.

Hair, J., Hollingsworth, C. L., Randolph, A. B., and Chong, A. Y. L. (2017). "An Updated and Expanded Assessment of Pls-Sem in Information Systems Research," *Industrial Management & Data Systems*, 117(3), pp.442-458.

Hair, J. F. (2009). "Multivariate Data Analysis,").

Hair, J. F., Anderson, R. E., Babin, B. J., and Black, W. C. (2010). "Multivariate Data Analysis: A Global Perspective (Vol. 7)." Upper Saddle River, NJ: Pearson.

Hair, J. F., Ringle, C. M., and Sarstedt, M. (2011). "Pls-Sem: Indeed a Silver Bullet," *Journal of Marketing theory and Practice*, 19(2), pp.139-152.

Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A. (2012). "An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research," *Journal of the academy of marketing science*, 40(3), pp.414-433.

Harris, M. A., and Weistroffer, H. R. (2009). "A New Look at the Relationship between User Involvement in Systems Development and System Success," *Communications of the Association for Information Systems*, 24(1), p.42.

Henseler, J., Hubona, G., and Ray, P. A. (2016). "Using Pls Path Modeling in New Technology Research: Updated Guidelines," *Industrial management & data systems*).

Henseler, J., Ringle, C. M., and Sinkovics, R. R. (2009). "The Use of Partial Least Squares Path Modeling in International Marketing," in *New Challenges to International Marketing*. Emerald Group Publishing Limited.

Herath, T., and Rao, H. R. (2009a). "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems*, 47(2), pp.154-165.

Herath, T., and Rao, H. R. (2009b). "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems*, 18(2), pp.106-125.

Höne, K., and Eloff, J. (2002). "What Makes an Effective Information Security Policy?," *Network security*, 2002(6), pp.14-16.

Hornung, S., Rousseau, D. M., Glaser, J., Angerer, P., and Weigl, M. (2010). "Beyond Top-Down and Bottom-up Work Redesign: Customizing Job Content through Idiosyncratic Deals," *Journal of Organizational Behavior*, 31(2-3), pp.187-215.

Hu, S., Hsu, C., and Zhou, Z. (2021). "The Impact of Seta Event Attributes on Employees' Security-Related Intentions: An Event System Theory Perspective," *Computers & Security*, 109), p.102404.

Huff, C., and Tingley, D. (2015). "'"Who Are These People?" Evaluating the Demographic Characteristics and Political Preferences of Mturk Survey Respondents," *Research & Politics*, 2(3), p.2053168015604648.

Hui, C., and Lee, C. (2000). "Moderating Effects of Organization-Based Self-Esteem on Organizational Uncertainty: Employee Response Relationships," *Journal of Management*, 26(2), pp.215-232.

Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. (2003). "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journal of consumer research*, 30(2), pp.199-218.

Juneau Jr, H. L. (2013). *Knowledge Sharing and Mobilization Barriers within a Matrix Organization*. Northcentral University.

Karjalainen, M., Sarker, S., and Siponen, M. (2019). "Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective," *Information Systems Research*, 30(2), pp.687-704.

Ke, W., Tan, C.-H., Sia, C.-L., and Wei, K.-K. (2012). "Inducing Intrinsic Motivation to Explore the Enterprise System: The Supremacy of Organizational Levers," *Journal of Management Information Systems*, 29(3), pp.257-290.

Kim, H. L., Choi, H. S., and Han, J. (2019). "Leader Power and Employees' Information Security Policy Compliance," *Security Journal*, 32(4), pp.391-409.

Kline, R. B. (2015). *Principles and Practice of Structural Equation Modeling*. Guilford publications.

Knight, C., and Parker, S. K. (2019). "How Work Redesign Interventions Affect Performance: An Evidence-Based Model from a Systematic Review," *Human Relations*), p.0018726719865604.

Kochhar, R. (2020). "Unemployment Rose Higher in Three Months of Covid-19 Than It Did in Two Years of the Great Recession." Retrieved June 17, 2020, 2020, from https://www.pewresearch.org/fact-tank/2020/06/11/unemployment-rose-higher-in-three-months-of-covid-19-than-it-did-in-two-years-of-the-great-recession/

Kwok, L.-f., and Longley, D. (1999). "Information Security Management and Modelling," *Information Management & Computer Security*, 7(1), pp.30-39.

Larsen, K. R. (2003). "A Taxonomy of Antecedents of Information Systems Success: Variable Analysis Studies," *Journal of Management Information Systems*, 20(2), pp.169-246.

Law, K. S., Wong, C.-S., and Mobley, W. M. (1998). "Toward a Taxonomy of Multidimensional Constructs," *Academy of management review*, 23(4), pp.741-755.

Lawrence, P. R., and Lorsch, J. W. (1969). "Organization and Environment. Homewood, Illinois: Richard D. Irwin," *Inc. LawrenceOrganization and Environment1969*).

Leach, D., Hagger-Johnson, G., Doerner, N., Wall, T., Turner, N., Dawson, J., and Grote, G. (2013). "Developing a Measure of Work Uncertainty," *Journal of occupational and organizational psychology*, 86(1), pp.85-99.

Lee, N., and Cadogan, J. W. (2013). "Problems with Formative and Higher-Order Reflective Variables," *Journal of Business Research*, 66(2), pp.242-247.

Lee, Y., and Chen, A. N. (2011). "Usability Design and Psychological Ownership of a Virtual World," *Journal of Management Information Systems*, 28(3), pp.269-308.

Lewis, B. R., Templeton, G. F., and Byrd, T. A. (2005). "A Methodology for Construct Development in Mis Research," *European Journal of Information Systems*, 14(4), pp.388-400.

Li, H., Luo, X. R., and Chen, Y. (2021). "Understanding Information Security Policy Violation from a Situational Action Perspective," *Journal of the Association for Information Systems*, 22(3), p.5.

Li, H., Sarathy, R., and Zhang, J. (2010). "Understanding Compliance with Internet Use Policy: An Integrative Model Based on Command-and-Control and Self-Regulatory Approaches."

Li, H., Sarathy, R., Zhang, J., and Luo, X. (2014). "Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance," *Information Systems Journal*, 24(6), pp.479-502.

Li, Y., and Siponen, M. T. (2011). "A Call for Research on Home Users' Information Security Behaviour."

Limayem, M., Hirt, S. G., and Cheung, C. M. (2007). "How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance," *MIS quarterly*), pp.705-737.

Lindell, M. K., and Whitney, D. J. (2001). "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of applied psychology*, 86(1), p.114.

Lohmöller, J.-B. (2013). *Latent Variable Path Modeling with Partial Least Squares*. Springer Science & Business Media.

Malhotra, N. K., Kim, S. S., and Patil, A. (2006). "Common Method Variance in Is Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management science*, 52(12), pp.1865-1883.

Maynard, M. T., Gilson, L. L., and Mathieu, J. E. (2012). "Empowerment—Fad or Fab? A Multilevel Review of the Past Two Decades of Research," *Journal of management*, 38(4), pp.1231-1281.

Menard, P., Bott, G. J., and Crossler, R. E. (2017). "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," *Journal of Management Information Systems*, 34(4), pp.1203-1230.

Menard, P., Warkentin, M., and Lowry, P. B. (2018). "The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination," *Computers & Security*, 75), pp.147-166.

Milliken, F. J. (1987). "Three Types of Perceived Uncertainty About the Environment: State, Effect, and Response Uncertainty," *Academy of Management review*, 12(1), pp.133-143.

Nguyen, Q. N., and Kim, D. J. (2017). "Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives," *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Njenga, K., and Brown, I. (2012). "Conceptualising Improvisation in Information Systems Security," *European journal of information systems*, 21(6), pp.592-607.

Oldham, G. R., and Fried, Y. (2016). "Job Design Research and Theory: Past, Present and Future," *Organizational Behavior and Human Decision Processes*, 136), pp.20-35.

Panetta, K. (2020). "7 Security Areas to Focus on During Covid-19." Retrieved June 14, 2020, 2020, from https://www.gartner.com/smarterwithgartner/7-security-areas-to-focus-on-during-covid-19/

Paolacci, G., and Chandler, J. (2014). "Inside the Turk: Understanding Mechanical Turk as a Participant Pool," *Current directions in psychological science*, 23(3), pp.184-188.

Park, C.-j., and Yim, M.-S. (2012). "An Understanding of Impact of Security Countermeasures on Persistent Policy Compliance," *Journal of Digital Convergence*, 10(4), pp.23-35.

Parker, S. K., Wall, T. D., and Cordery, J. L. (2001). "Future Work Design Research and Practice: Towards an Elaborated Model of Work Design," *Journal of occupational and organizational psychology*, 74(4), pp.413-440.

Perrow, C. (1967). "A Framework for the Comparative Analysis of Organizations," *American sociological review*), pp.194-208.

Petter, S., Straub, D., and Rai, A. (2007). "Specifying Formative Constructs in Information Systems Research," *MIS quarterly*), pp.623-656.

Pham, H.-C., El-Den, J., and Richardson, J. (2016). "Stress-Based Security Compliance Model–an Exploratory Study," *Information & Computer Security*).

Pham, H. C., Pham, D. D., Brennan, L., and Richardson, J. (2017). "Information Security and People: A Conundrum for Compliance," *Australasian Journal of Information Systems*, 21).

Podsakoff, P., MacKenzie, S., Lee, J., and Podsakoff, N. (2003). "Common Method Biases in Behavioral Research: A Critical Common Method Biases in Behavioral Research: A Critical," *Journal of Applied Psychology*, 88(5), pp.879-903.

Qu, Y. E., Dasborough, M. T., Zhou, M., and Todorova, G. (2019). "Should Authentic Leaders Value Power? A Study of Leaders' Values and Perceived Value Congruence," *Journal of Business Ethics*, 156(4), pp.1027-1044.

Raza, H., Baptista, J., and Constantinides, P. (2019). "Conceptualizing the Role of Is Security Compliance in Projects of Digital Transformation: Tensions and Shifts between Prevention and Response Modes,").

Rhee, H.-S., Kim, C., and Ryu, Y. U. (2009). "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Computers & security*, 28(8), pp.816-826.

Ringle, C., Da Silva, D., and Bido, D. (2015a). "Structural Equation Modeling with the Smartpls," *Bido, D., da Silva, D., & Ringle, C.(2014). Structural Equation Modeling with the Smartpls. Brazilian Journal Of Marketing*, 13(2).

Ringle, C. M., Sarstedt, M., and Straub, D. W. (2012). "Editor's Comments: A Critical Look at the Use of Pls-Sem in" Mis Quarterly"," *MIS quarterly*), pp.iii-xiv.

Ringle, C. M., Wende, S., and Becker, J.-M. (2015b). "Smartpls 3. Smartpls Gmbh, Boenningstedt," *Journal of Service Science and Management*, 10(3).

Rocha, J. (2011). "A Study on Uncertain Dynamic Disaster Management Tasks, Knowledge Sharing, and Task Performance." Florida International University.

Sarstedt, M., Hair Jr, J. F., Cheah, J.-H., Becker, J.-M., and Ringle, C. M. (2019). "How to Specify, Estimate, and Validate Higher-Order Constructs in Pls-Sem," *Australasian Marketing Journal (AMJ)*, 27(3), pp.197-211.

Sarstedt, M., Schwaiger, M., and Ringle, C. M. (2009). "Do We Fully Understand the Critical Success Factors of Customer Satisfaction with Industrial Goods?-Extending Festge and Schwaiger's Model to Account for Unobserved Heterogeneity," *Journal of business market management*, 3(3), pp.185-206.

Schneider, A., Hornung, S., Weigl, M., Glaser, J., and Angerer, P. (2017). "Does It Matter in the Long Run? Longitudinal Effects and Interactions in the Differentiated Job Demands–Resources Model," *European Journal of Work and Organizational Psychology*, 26(5), pp.741-754.

Scott, W. R., and Davis, G. F. (2015). *Organizations and Organizing: Rational, Natural and Open Systems Perspectives*. Routledge.

Security. (2020). "Increasing Cybersecurity Gaps and Vulnerabilities Due to Remote Work During Covid-19." Retrieved June 17, 2020, 2020, from https://www.securitymagazine.com/articles/92571-increasing-cybersecurity-gaps-and-vulnerabilities-due-to-remote-work-during-covid-19

Shalley, C. E., and Oldham, G. R. (1985). "Effect of Goal Difficulty and Expected Evaluation on Intrinsic Motivation: A Laboratory Study," *Academy of Management Journal*, 28(3), pp.628-640.

Siponen, M., Baskerville, R., and Heikka, J. (2006). "A Design Theory for Secure Information Systems Design Methods1," *Journal of the Association for Information Systems*, 7(11), pp.725-770.

Siponen, M., Pahnila, S., and Mahmood, M. A. (2010). "Compliance with Information Security Policies: An Empirical Investigation," *Computer*, 43(2), pp.64-71.

Siponen, M., and Vance, A. (2010). "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly*), pp.487-502.

Smith, G. T. (2005). "On Construct Validity: Issues of Method and Measurement," *Psychological assessment*, 17(4), p.396.

Son, J.-Y. (2011a). "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow Is Security Policies," *Information & Management*, 48(7), p.296.

Son, J.-Y. (2011b). "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow Is Security Policies," *Information & Management*, 48(7), pp.296-302.

Soucheray, S. (2020). "Us Job Losses Due to Covid-19 Highest since Great Depression." Retrieved June 17, 2020, 2020, from https://www.cidrap.umn.edu/news-perspective/2020/05/us-job-losses-due-covid-19-highest-great-depression

Spreitzer, G. M., Kizilos, M. A., and Nason, S. W. (1997). "A Dimensional Analysis of the Relationship between Psychological Empowerment and Effectiveness Satisfaction, and Strain," *Journal of management*, 23(5), pp.679-704.

Sterna, S. J. D., and Wolfe, J. (2019). "Cyber Liability: Managing Evolving Exposures," *Journal of Accountancy*, 227(1), pp.14-15.

Straub, D. W. (1989). "Validating Instruments in Mis Research," *MIS quarterly*), pp.147-169.

Tenenhaus, M., Vinzi, V. E., Chatelin, Y.-M., and Lauro, C. (2005). "Pls Path Modeling," *Computational statistics & data analysis*, 48(1), pp.159-205.

Thomas, K. W., and Velthouse, B. A. (1990). "Cognitive Elements of Empowerment: An "Interpretive" Model of Intrinsic Task Motivation," *Academy of management review*, 15(4), pp.666-681.

Thompson, J. (1967). "Organizations in Action, 1967," *SHAFRITZ, Jay M.; OTT, J. Steven. Classics of Organization Theory*, 4).

Tyler, T. R., and Blader, S. L. (2005). "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings," *Academy of Management Journal*, 48(6), pp.1143-1158.

Ujma, M., and Ingram, T. (2019). "Perception of Ability-Motivation-Opportunity Oriented Hrm Practices and Organizational Commitment: The Role of Task Uncertainty," *Journal of Entrepreneurship, Management and Innovation*, 15(4), pp.139-162.

Vallerand, R. J. (1997). "Toward a Hierarchical Model of Intrinsic and Extrinsic Motivation," in *Advances in Experimental Social Psychology*. Elsevier, pp. 271-360.

Vallerand, R. J., Pelletier, L. G., Blais, M. R., Briere, N. M., Senecal, C., and Vallieres, E. F. (1992). "The Academic Motivation Scale: A Measure of Intrinsic, Extrinsic, and Amotivation in Education," *Educational and psychological measurement*, 52(4), pp.1003-1017.

Van Dyne, L., and Pierce, J. L. (2004). "Psychological Ownership and Feelings of Possession: Three Field Studies Predicting Employee Attitudes and Organizational Citizenship Behavior," *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, 25(4), pp.439-459.

Vance, A., Siponen, M., and Pahnila, S. (2012). "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, 49(3-4), pp.190-198.

Wall, T. D., Cordery, J. L., and Clegg, C. W. (2002). "Empowerment, Performance, and Operational Uncertainty: A Theoretical Integration," *Applied Psychology*, 51(1), pp.146-169.

West, R. (2008). "The Psychology of Security," *Communications of the ACM*, 51(4), pp.34-40.

Wetzels, M., Odekerken-Schröder, G., and Van Oppen, C. (2009). "Using Pls Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration," *MIS quarterly*), pp.177-195.

Wilson, B. (2010). "Using Pls to Investigate Interaction Effects between Higher Order Branding Constructs," in *Handbook of Partial Least Squares*. Springer, pp. 621-652.

Workman, M., Bommer, W. H., and Straub, D. (2008). "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in human behavior*, 24(6), pp.2799-2816.

Wright, B. M., and Cordery, J. L. (1999). "Production Uncertainty as a Contextual Moderator of Employee Reactions to Job Design," *Journal of Applied Psychology*, 84(3), p.456.

Wrzesniewski, A., and Dutton, J. E. (2001). "Crafting a Job: Revisioning Employees as Active Crafters of Their Work," *Academy of management review*, 26(2), pp.179-201.

Xu, X., and Payne, S. C. (2020). "When Do Job Resources Buffer the Effect of Job Demands?," *International Journal of Stress Management*, 27(3), p.226.

Yazdanmehr, A., Wang, J., and Yang, Z. (2020). "Peers Matter: The Moderating Role of Social Influence on Information Security Policy Compliance," *Information Systems Journal*).

Yoo, C. W., Sanders, G. L., and Cerveny, R. P. (2018). "Exploring the Influence of Flow and Psychological Ownership on Security Education, Training and Awareness Effectiveness and Security Compliance," *Decision Support Systems*, 108), pp.107-118.

Yusoff, A. S. M., Peng, F. S., Abd Razak, F. Z., and Mustafa, W. A. (2020). "Discriminant Validity Assessment of Religious Teacher Acceptance: The Use of Htmt Criterion," *Journal of Physics: Conference Series*: IOP Publishing, p. 042045.

Zikmund, W. (2000). "Business Research Methods, Dryden." Harcourt) Fort Worth, Orlando.

APPENDIX A: BIOGRAPHICAL LISTING OF RELEVANT LITERATURE

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Perceived Work Uncertainty						
Developing a measure of work uncertainty	Journal of Occupational and Organizational Psychology	Leach et al. (2013)	Quantitative	Resource Uncertainty; Task Uncertainty; Input/Output Uncertainty	-	Work Uncertainty
A New Model of Work Role Performance: Positive Behavior in Uncertain and Interdependent Contexts	Academy of Management Journal	Griffin et al. (2007)	Quantitative	Role Clarity; Openness to Change; Role Breadth Self-Efficacy; Team Support; Organization Commitment	-	Subdimensions of Work Role Performance: (Individual task proficiency, adaptivity, and proactivity; Team member proficient, adaptivity, and proactivity, Organization member proficiency, adaptivity, and proactivity)

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Empowerment, performance, and operational uncertainty: A theoretical integration	Applied Psychology	Wall et al. (2002)	Literature Review	-	-	-
Conceptualizing improvisation in information systems security	European Journal of Information Systems	Njenga and Brown (2012)	Case Study	-	-	-
Entrepreneurial Leadership and Employees' Proactive Behavior: Fortifying Self Determination Theory	Journal of Open Innovation: Technology, Market, and Complexity	Bilal et al. (2021)	Quantitative	Entrepreneurial Leadership; Work Uncertainty	Proactive Personality	Proactive Work Behavior
Work Uncertainty and Extensive Work Effort: The Mediating Role of Human Resource Practices	ILR Review	Avgoustaki (2016)	Quantitative	Task Uncertainty; Schedule Uncertainty	HR Practices: Training, Task Rotation, Teamwork, Productivity pay, Gain sharing, method discretion, schedule discretion	Work Overtime

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
How work redesign interventions affect performance: An evidence-based model from a systematic review	Human Relations	Knight and Parker (2019)	Literature Review	-	-	-
Visions of change as visions of continuity	Academy of Management Journal	Venus et al. (2019)	Quantitative	Vision of continuity; Perceived collective continuity	Work or Environmental Uncertainty	Follower support for change
Job uncertainty and personal control during downsizing: A comparison of survivors and victims	Human Relations	Paulsen et al. (2005)	Quantitative	Job Uncertainty	Personal Control; Job Satisfaction; Emotional Exhaustion	Emotional Exhaustion
Future work design research and practice: Towards an elaborated model of work design	Journal of Occupational and Organizational Psychology	Parker et al. (2001)	Qualitative	-	-	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Three Types of Perceived Uncertainty About the Environment: State, Effect, and Response Uncertainty	Academy of Management Review	Milliken (1987)	Qualitative	-	-	-
Task Uncertainty						
The impact of autonomy and task uncertainty on team performance: A longitudinal field study	Journal of Organizational Behavior	Cordery et al. (2010)	Field Study	-	-	-
Uncertainty, task environment, and organization design: An empirical investigation	Journal of Economic Behavior & Organization	Ben-Ner et al. (2012)	Quantitative	Internal Uncertainty; External Uncertainty	Incentives; Delegation; Monitoring; Internal Labor Market	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Perception of ability-motivation-opportunity oriented HRM practices and organizational commitment: The role of task uncertainty	Journal of Entrepreneurship, Management, and Innovation	Ujma and Ingram (2019)	Quantitative	Human Resource Management Practices (Motivation, Opportunity, and Commitment); Task Uncertainty	Organizational Commitment	-
Automation, Algorithms, and Beyond: Why Work Design Matters More Than Ever in a Digital World	Applied Psychology	Parker and Grote (2020)	Qualitative	-	-	-
Resource Uncertainty						
Beyond Top-Down and Bottom-up Work Redesign: Customizing Job Content through Idiosyncratic Deals	Journal of Organizational Behavior	Hornung et al. (2010)	Two Study Quantitative	Task i-deals; Leader-member; Exchange	**STUDY 1** Personal Initiative **STUDY 2** Work Engagement	**STUDY 1** Work Complexity; Work Control **STUDY 2** Work Complexity; Work Control; Work Stressors

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Does It Matter in the Long Run? Longitudinal Effects and Interactions in the Differentiated Job Demands–Resources Model	European Journal of Work and Organizational Psychology	Schneider et al. (2017)	Longitudinal Quantitative	Job Challenge demands; Job Hindrance Demands; Job Resources; Emotional Exhaustion; Depersonalization; Work Engagement	Job Challenge demands; Job Hindrance Demands; Job Resources; Emotional Exhaustion; Depersonalization; Work Engagement	Job Challenge Demands; Depersonalization
When Do Job Resources Buffer the Effect of Job Demands?	International Journal of Stress Management	Xu and Payne (2020)	Quantitative	Research Task Ambiguity	Well-Being	Research Task Discretion; Job Self-Efficacy; Negative affectivity
The Antecedents and Consequences of Fear at Work	The Cambridge Handbook of Workplace Affect	Jordan et al. (2020)	Literature Review	-	-	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Psychological uncertainty, stress, frustration, and their relationship with counterproductive workplace behavior	Walden University Press	Norwood (2018)	Quantitative	Perceived Employee Uncertainty; Perceived Employee Stress; Perceived Employee Frustration	Counterproductive Work Behaviors	-
Managerial resistance to high performance workplace practices	The Transformation of Work	Taplin (2001)	Case Study	-	-	-
Further evidence on some new measures of job control, cognitive demand and production responsibility	Journal of Organizational Behavior	Wall et al. (1995)	CFA-Two Study Quantitative	Timing Control; Method Control; Monitoring Demand; Problem Solving; Production Responsibility	Job Complexity	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Intrinsic Motivation						
Out of fear or desire? Toward a better understanding of employees' motivation to	Information and Management	Son (2011)	Quantitative	Perceived Deterrent Certainty; Perceived Deterrent Severity; Perceived Legitimacy; Perceived Value Congruence; Computer Self-Efficacy	ISP Compliance	-
User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory	Journal of Management Information Systems	Menard et al. (2017)	Quantitative	Perceived Relatedness; Perceived Competence; Perceived Autonomy	Intention to Comply	Threat Severity; Threat Susceptibility; Self-Efficacy; Response Efficacy; Response Cost; Response Performance; Motivation
Work Incentives, Motivation, And Identity	American Economic Review	Pendergast (2008)	Qualitative	-	-	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Self-Determination Theory-the Iteration of Psychophysiology and Motivation	Psychophysiology	Deci and Ryan (1980)	Literature Review	-	-	-
The empowerment process: Integrating theory and practice	Academy of Management Review	Conger and Kanungo (1988)	Literature Review	Organizational Factors; Supervisory Style; Reward Systems; Job Design	Self-Efficacy Belief	-
Cognitive Elements of Empowerment: An "Interpretive" Model of Intrinsic Task Motivation	Academy of Management Review	Thomas and Velthouse (1990)	Quantitative-Model Development	Interpretative Styles; Interventions; Environmental Events; Behavior Task Assessments; Global Assessments	-	-
Self-determination theory and work motivation	Journal of Organizational Behavior	Gagné and Deci (2005)	Literature Review	Social Environment; Individual Differences	Performance; Psychological Well-being; Organizational Trust and Commitment; Job Satisfaction	Autonomous Work Motivation

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
The Mediating Role of Psychological Empowerment in Information Security Compliance Intention	Journal of the Association of Information Systems	Dhillon et al. (2019)	Quantitative	SETA; Access to Information; Participation in Decision Making	ISP Compliance Intention	Psychological Empowerment
Peers matter: The moderating role of social influence on information security policy compliance	Information Systems Journal	Yazdanmehr et al. (2020)	Quantitative	Command and Control Approach; Self-Regulatory Approach	ISP Compliance	Rules-Oriented Ethical Climate; Susceptibility to Interpersonal Influence
Moderating effects of organization-based self-esteem on organizational uncertainty: Employee response relationships	Journal of Management Information Systems	Hui and Lee (2000)	Quantitative	Anticipated Organizational Change	Job Insecurity; Intrinsic Motivation; Organizational Commitment; Absenteeism	Organizational Based self-esteem

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Perceived Value Congruence						
Protection motivation and deterrence: a framework for security policy compliance in organizations	European Journal of Information Systems	Herath and Rao (2009b)	Quantitative	Perceived Severity of Security Breach; Perceived Probability of Security Breach; Response Cost; Organizational Commitment; Resource Availability; Punishment Severity; Detection Certainty	Security Policy Compliance Intention	Response Efficacy; Security Breach Concern Level; Self-Efficacy; Security Policy Attitude
A conceptual model of information security compliant behavior based on the self-determination theory	Conference on Information Communications Technology and Society	Gangire et al. (2019)	Literature Review	-	-	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Should Authentic Leaders Value Power? A Study of Leaders' Values and Perceived Value Congruence	Journal of Business Ethics	Qu et al. (2019)	Quantitative	Authentic Leadership	Followers Performance	Leaders Values Followers Perceived Value Congruence
Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance	Information Systems Journal	Li et al. (2014)	Quantitative	Procedural Justice Interpersonal Justice Informational Justice Distributive Justice Sanction Severity Sanction Clarity	ISP compliance intention	Personal Ethics
Profiles of fit and misfit: a repeated weekly measures study of perceived value congruence	European Journal of Work and Organizational Psychology	Values et al. (2019)	Quantitative-Cluster Analysis	-	Value Congruence Work Role Behaviors Tenure	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Perceived Self-Efficacy						
Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior	Journal of Information Privacy and Security	Chan et al. (2005)	Quantitative	Coworker Socialization Direct Supervisory Practices Upper Management Practices Self-Efficacy	Information Security Climate	Compliant Behavior
Self-efficacy in information security: Its influence on end users' information security practice behavior	Computers and Security	Rhee et al. (2009)	Quantitative	Computer/Internet Experience Security Breach Incidents General Controllability	Self-Efficacy in Information Security	Security Practice-Technology Intention to Strengthen Security Effort Security Practice-Care Behavior
The Self-Efficacy Variable in Behavioral Information Security Research	Enterprise Systems Conference	He et al. (2014)	Literature Review	-	-	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
How senior management and workplace norms influence information security attitudes and self-efficacy	Behavior and Information Technology	Cuganesan et al. (2018)	Quantitative	Senior Management Support Formal Controls (Specification, Monitoring and Evaluation, Rewards, Sanctions)	Norms	Attitude Self-Efficacy
Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives	Proceeding of the 50th Hawaii International Conference of System Sciences	Nguyen and Kim (2017)	Quantitative	General Technology Awareness Risk Propensity	Self-technical Controllability Information Security Self-Efficacy Information Security Protection Effort Information Security Risk Perception Information Security Reinforcement Intention	Information Security Reinforcement Intention

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Perceived Ownership						
Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions	MIS Quarterly	Anderson and Agarwal (2010)	Quantitative	Concern Regarding Security Threats Perceived Citizen Effectiveness Security Behavior Self-Efficacy Psychological Ownership	Attitude Toward Security Related Behavior	Intentions to Perform Security Related Behavior (Internet) Intentions to Perform Security Related Behavior (One's Own Computer)
Psychological ownership and feelings of possession: three field studies predicting employee attitudes and organizational citizenship behavior	Journal of Organizational Behavior	Dyne and Pierce (2004)	Quantitative	Psychological Ownership		Organizational Commitment Job Satisfaction Organizational Self-Esteem Work Performance

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
When Do Objects Become More Attractive? The Individual and Interactive Effects of Choice and Ownership on Object Evaluation	Personality and Social Psychology Bulletin	Huang et al. (2009)	Experimental Quantitative	-	-	-
Disclosing too much? Situational factors affecting information disclosure in social commerce environment	Electronic Commerce Research and Applications	Sharma and Crossler (2014)	Quantitative	Perceived Surveillance Perceived Linkage Perceived Relevance Perceived Ownership Perceived Enjoyment Privacy Apathy	Perceived Privacy Risk Perceived Usefulness	BINT to Voluntarily Disclose Information
The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination	Computers and Security	Menard et al. (2018)	Quantitative	Collectivism Psychological Ownership	Threat Susceptibility Threat Severity Response Efficacy Self-Efficacy Response Cost	Behavioral Intention Not to Protect Information

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Perceived Effectiveness						
What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors	MIS Quarterly	Boss et al. (2015)	Two Study Review/Quantitative	Perceived Threat Severity Perceived Threat Vulnerability Maladaptive Rewards Response Efficacy Self-Efficacy Response Costs	Fear Protection Motivating	Security-related Behaviors
Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness	Decision Support Systems	Herath and Rao (2009b)	Quantitative	Severity of Penalty Certainty of Detection Normative Beliefs Peer Behavior Perceived Effectiveness	-	Policy Compliance Intentions
An Understanding of Impact of Security Countermeasures on Persistent Policy Compliance	Journal of Digital Convergence	Park and Yim (2012)	Quantitative	Perceived Benefit Security Systems Quality SETA Programs Perceived Security Policies Effectiveness	Information Security Climate Organizational Commitment	Persistent Compliance Intention

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Security Education, Training and Awareness (SETA)						
User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach	Information Systems Research	D'Arcy et al. (2009)	Quantitative	Awareness of: Security Policies, SETA Programs, & Computer Monitoring	Perceived Certainty of Sanctions Perceived Severity of Sanctions	IS Misuse Intention
Leader power and employees' information security policy compliance	Security Journal	Kim et al. (2019)	Quantitative	SETA Program Awareness	Leaders Power Base	ISP Compliance Intention
Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts	Decision Sciences	Burns et al. (2018)	Quantitative	SETA Program Awareness	Security Valence Security Instrumentality Security Expectancy	ISP Compliance Intention Intentions of protect organizational information assets

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
The impact of SETA event attributes on employees' security-related Intentions: An event system theory perspective	Computers and Security	Hu et al. (2021)	Quantitative	SETA Novelty SETA Criticality SETA Disruption	SETA Spatial Dispersion SETA Duration	ISP Compliance Intention Extra-role behavioral Intention
What, I shouldn't have done that?: The influence of training and just-in-time reminders on secure behavior	Thirty-fourth International Conference on Information Systems	Jenkins et al. (2013)	Quantitative	Subjective Norms of Secure Behavior Attitude toward Secure Behavior Perceived Behavioral Control of Secure Behavior SETA Just-in-Time Reminders	Intentions to Behave Securely	Secure Behavior
Proposing SETA program design based on employee motivational fit	AMCIS Proceedings	Menard (2016)	Qualitative	-	-	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance	Decision Support Systems	Yoo et al. (2018)	Quantitative	Flow (Challenge, Feedback, Autonomy, Immersion, Social Interaction)	Psychological Ownership SETA Effectiveness Self-Efficacy	Security Compliance Intention
Security Education, Training, and Awareness Programs: Literature Review	Journal of Computer Information Systems	Hu et al. (2021)	Literature Review	-	-	-
Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach	Hawaii International Conference of System Sciences	Burns et al. (2015)	Quantitative	SETA	Security Valence Security Instrumentality Security Expectancy	Security Precaution Taking Security Psychological Distancing

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Using design-science based gamification to improve organizational security training and compliance	Journal of Management Information Systems	Silic and Lowry (2020)	Quantitative	Perceived ease of use Learning of Policies	Security Response Efficacy Security Self-efficacy Behavioral Intention to follow security policies Immersion	Actual phishing response following security policies
Information Security Policy (ISP) Compliance						
Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness	MIS Quarterly	Bulgurcu et al. (2010)	Quantitative	Information Security Awareness: ISP Awareness General Awareness	Beliefs about Information Security outcomes; Beliefs about overall assessments of non-compliant consequences	Intention to Comply with ISP
Value-focused assessment of information system security in organizations	Information Systems Journal	Dhillon and Torkzadeh (2006)	Qualitative	-	-	-

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Seeing the forest *and* the trees: a meta-analysis of the antecedents to information security policy compliance	MIS Quarterly	Cram et al. (2019)	Literature Review	-	-	-
Employees' adherence to information security policies: An exploratory field study	Information and Management	Siponen et al. (2014)	Quantitative	Severity; Vulnerability; Response efficacy; Self-efficacy; Attitude; Normative beliefs; Rewards	Intention to Comply with ISP	Actual Compliance with ISP
Employees' information security policy compliance: A norm activation perspective.	Decision Support Systems	Yazdanmehr and Wang (2016)	Quantitative	Principle Ethical Climate; ISP Related Awareness of Consequences; ISP Related Ascription of Personal Responsibility	ISP Related Descriptive Norms; ISP Related Injunctive Norms; ISP Related Subjective Norms; ISP Related Personal Norms	ISP Compliance Behavior

Article Title	Journal	Authors (Year)	Study Method	Independent Variable(s)	Moderator/ Mediator	Dependent Variable(s)
Information security policy compliance model in organizations	Computers and Security	Safa et al. (2016)	Quantitative	Individual Involvement: Knowledge Sharing, Collaboration, Intervention, Experience	Attitude toward Compliance with ISP	ISP Compliance Intention
Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory	Computers and Security	Ifinedo (2012)	Quantitative	Threat Appraisal: Perceived vulnerability, Perceived severity; Coping Appraisal: Response efficacy, Response cost, Self-efficacy; Attitude toward ISP compliance; Subjective norms	-	ISP Compliance Intention
Organizations' Information Security Policy Compliance: Stick or Carrot Approach?	Journal of Management Information Systems	Chen et al. (2012)	Quantitative	Punishment; Reward; Certainty of Control	-	ISP Compliance Intention

APPENDIX B: TRANSCRIPTS OF QUALITATIVE INTERVIEWS FOR MODEL DEVELOPMENT

Interview 1

Every work or organization requires strict policies and employee's tactic to be able to Maximize her goals and benefits and when not discussed a lot of frictions and roughage will be experienced during her time of work. One of such instances is when an organization does not have a stipulated punishment as regarding certain offences that are common and found in place of work. For example, we once had a case of theft in our place of work and since the clear out punishment wasn't stated earlier the offenders couldn't be punished under new rules and so although they were laid off, they didn't face extra punishment. This is one of the various issues that can be experienced when policies aren't stipulated. And on the long run companies wouldn't be able to work efficiently and enjoy maximum profit. So therefore, policies and policy security are very much important

Interview 2

As a non-formal educator, I often share information and programs on museum exhibits with students and their teachers. During this process I share pre-written programs that contain content that belongs as intellectual property to the museum. Sometimes teachers will directly as me for my written outline which I know is directly against company policy. Other times I will be asked creative ways to teach content that I feel I can share as a fellow educator as it does not correlate directly to the program I am teaching. It does however make the program I am teaching seem like something anyone can do and not worth paying someone else for. This is a huge gray area in my organization, what is ok to share and what is our intellectual property we can sell as an experience.

Interview 3

Yes, it happened on a specific assignment of a project in our team when I was the leader of 6 employees. as a leader my responsibilities were a great deal. Daily was supposed to communicate with my seniors through the devices provided by my company. but to my utter disappointment I found that every time I was not successful to get communicated due to some organizational policies. in my organization it was predetermined that if you wanted to access any data you need to depend on the others for the code of access. So, it was not possible for me to use the resources whenever I wanted. at this I had to waste a lot of time waiting to get interacted. the task was very crucial for the company and we needed to hand over the project within the time limit. but the hassles regarding organizational information security policies which were inconsistent with the task I was assigned to held us back for quite a long time. it created uncertainty among the team members and specially i was skeptical whether we would be capable to complete the assigned task. The information security policy was totally in congruent with what we were doing that time. it was as if the task had been the rival to it. almost at every step the task was hampered and a sense of uncertainty arose among the employees.

Interview 4

Relay on code of conduct or principles when making direct organizational decisions. It applies to everyone. Everyone has a code of conduct according to their level, and some responsibilities exist according to the organization. The person who will be in that position, his conduct and rules will be governed accordingly. Otherwise, due to violation of organizational code of conduct, one limit after another will be exceeded. Then it will no longer be an organization. Security policy, data secure it also depends on the organization. Organizational policy is essential for performance. There are also some rules for employment. It is one's duty to observe them properly. The law will work equally on everyone under the Employees and Labor Act. It will not be possible to sustain the organization if the jobs of these huge employees and their information are not preserved and their policy making is not done properly. So, it is better to follow the organizational and organizational rules.

Interview 5

With COVID having a huge impact on my work place, we shifted services very quickly to telehealth. This change came with a big learning curve and some unknown policies. Because the shift happened quickly there was not much time for my organization to create new procedures related to information security. We work with a lot of protected health information, so I did not feel very secure in my role at work. Accounts were being shared, which included password sharing. We were also having to believe the telehealth company, when they told us the program we bought, was HIPPA protected. Due to the shift being fast, it was unknown how the system was protected. All staff was encouraged to continue our roles as "normal as possible" although information security policies were either a mess or non-existent in the moment. This created a lot of stress on staff because most of us all have clinical license that we are putting at risk daily.

Interview 6

I am a junior supervisor at my firm, and I have had the opportunity to work in different capacities such as, in replacement of my immediate supervisor, and also worked in charge of the security unit. The security unit was not my original job description, I worked in that office as a result of certain unforeseen events that befell the former security director. I am originally in charge of the sales and marketing department. When I assumed that office, I thought I could do with the normal company rules, and regulations as well as the set policy of the company. I however never considered that there were certain uncertainties as regards that particular job description. And these uncertainties were not stated code of conduct and mode of operations of that position. The inconsistency in policy made it a bit difficult for me to achieve maximum success, as in many ways I find it difficult to describe during our weekly and monthly presentations to our various supervisors. As a result of these uncertainties, I also find it difficult to describe my job duties and to interpret certain organizational procedures as it would warrant me to include those uncertainties that are not consistent with the company's policies. Hence,

this greatly affected distribution of sales and proper accountability of funds in that department. It went on and on until the company found a replacement for that office.

Interview 7

I have experienced many times where I was required to interpret organizational procedures toward information security policies where the rules became insufficient. I work in a warehouse and a lot of the times the rules in place are not the most ideal when trying to finish a job quickly. There are still safe ways to do the procedures that may not be as safe as the rules placed but are a better system. We cut foam in my industry and we work with knives and razors but sometimes the equipment does not have a handle with the knife but it is easier to cut that way so we do not hate time trying to find a knife with a handle. And honestly, we are starting to get completely rid of the knives with handles even though it is not a part of the rules. We also are supposed to wear glasses will working with the machinery but we work with machinery for 8 hours and the glasses are awkward so we do not even bother.

Interview 8

One time during a project work I and my team were working on (about 20 0f us) the project required a lot of attention and strict adherence to company policies, information security and sufficient need to carry out task. We worked on these tasks for a long time and it was very time consuming and stressful, sometimes we even had to take turns to monitor and it also got to a point where we ran out of ideas to complete task. At the long run, the company ran out of information, technological equipment and necessary skills to complete it, it took a while to get back up and this slowed down execution of task. After this my attention was needed to interpret organizational procedure toward information security when it was discovered that some information was wrongly disseminated on the project.

Interview 9

My profession in the insurance industry requires ques from tacit applications of the policy offerings. I used to work from a small insurance office where training was provided comprehensively. A few months ago, I transferred to a larger office where employees are trained with specifications. One employee might do only health another business, and another high value homes. When I first joined this office, this was not made explicit. When clients would call - I would take care of any needs expressed myself rather than pivoting to each individual outside myself. This was seen as "initiative" on my part to step up without being asked. Now that I am aware the new larger office operates differently, I get to choose when to "step up" and assume the needs of clients or pivot out to other staff. This feeling of selectiveness is solely based on my comfortability, interpretation of the office organization, preferred workflow structure, and efficiency to address needs.

Interview 10

I work for a public University. During the entirety of the pandemic policy was constantly hanging and being interpreted by different departments differently. So at times I had to interpret procedures the ways my superiors did, and often those did not align. Especially in terms of leave and work-from-home policies. I just had to comply to whoever has the most power. I was hired during this pandemic with absolutely no policy training (nearly no training at all), so often I have had to go searching and interpreting quickly in order to keep my department running. it is obvious that university systems or at least the one I am in assumes that those hired have prior knowledge or intel on higher academia procedures for both faculty and staff. I have been successful and am completely capable of my job, but it feels like there is bias in unwritten codes. This bias prefers white, older people with ties to higher education.

Interview 11

The company that I work for has a operational gate to gain access to my workplace. There have been multiple occasions where the wrong people who do not belong at my workplace have gained access when they shouldn't of. This happened because of multiple reasons. I work at a very confidential place of business and HIPAA is always something myself and my fellow employees have to follow. We are not allowed to confirm or deny if clients are residing at our place of business. There have been times where someone was not trained correctly and announced to someone at the gate that yes/no the client was indeed there. Sometimes the interface is hard to interpret what the person at the gate is saying due to faulty equipment, so staff will make the mistake of letting the stranger in anyways. This is a high security issue and has been handled. Needless to say it is very difficult to work around.

Interview 12

I work as an auditor for state government. The COVID-19 pandemic recently brought up a lot of uncertainty about the procedures that were in place at the time at my workplace. As an auditor, we can sometimes handle confidential information and we are instructed to use VPNs, secure file transfers, and not take any confidential information home. However, my office went from working in office 100% of the time to working completely remote. Most of our clients were working remotely too. We weren't sure how to access paper versions of documents that were in our offices that we had no access to. We didn't know how to perform our walkthroughs of processes; would the video platform be secure? Was the client recording us? As we continued to work from home, my office came out with more policies and procedures directed at the work-from-home environment. I also learned how to work with what I had access to in the moment, even if it went against our policies that were in place at the time. For a specific example, we typically do not use our client's programs but there were instances where we had to as our agency had not yet implemented a program/software of our own to use.

Interview 13

I have taken extensive hazard material abatement training as required by my employer. I work for a State entity so we have to follow in-house, local, State, and Federal policy's, procedures, and guidelines. As you can imagine we have to follow strict criteria guidelines in order to notify the correct agencies and complete our work. I am constantly on regulated websites where a lack of security and direction is a concern. There are security protocols in effect at my place of employment such as duo factor authentication etc. This is not the case with all information I provide on the internet. I have to trust security measures put in place but I am also aware of what information is pertinent to my request and what information I can use to "bypass" something that is irrelevant. There are a lot of inconsistencies with procedures and mandates in my line of work, primarily because of so many regulated agencies I deal with. I solve this by going above and beyond the requirements and due diligence. If I need clarification I make sure my requests and responses are in writing. I believe this is how all individuals should approach uncertainty about policy, procedures, guidelines, and organizational protocol.

Interview 14

Our workplace was depending on shared credentials for some services for a while. This resulted in passwords being shared in plaintext through shared documents, text files, chats, emails, etc. There was a policy in place to not share passwords, but due to the nature of these accounts, and no proper channels to share passwords securely, this resulted in everyone breaking this policy. This dilemma resulted in the Information Technology team having no way to enforce the password sharing policy.

Eventually due to this, a secure password manager was set up. Due to this policy being overlooked for so long, employees still continued to ignore this policy. Due to the need to ignore this policy for so long, employees did not wish to use the password manager and continued to share passwords insecurely.

Interview 15

While we have specific policies regarding how frequently our password is changed and what it looks like for our personal computers and electronic documentation systems at work, we have very few organizational policies for shared computers. These computers are frequently not updated properly and the untold rule is that whoever is using these devices is the one to ensure they are up-to-date and functioning properly prior to classroom use. For example, when I teach a documentation course at my organization, I know it is my responsibility to ensure each computer is in proper working order and up-to-date. If it is not, it is my responsibility to open a ticket with our IT department to get the issue resolved. It is also my responsibility to ensure the train domain is functioning appropriately as needed for the specific class being taught.

Interview 16

My company was working on a project work that will require a lot of attention, information security, interpretation of organizational procedures, strict adherence to company policy, full inflow of equipment required to fund the project, funds, etc. we worked on the project for months and was having issues completing it due to the information provided. at the long run my skills was needed to detect the problem and that was when I found out that the information disseminated was not valid. lit took a lot of time to discover this thou, i needed to do an overtime on the jo as it requires a lot of attention, also the procedures needed to carry out the task became inconsistent and to be honest it stressed me out but I was heavily compensated for later finding out the problem and solving it.

Interview 17

We have a lot of policies that are black and white and some are confusing and there are plenty times when during and audit we will get a mark against us because it is considered "best practice" but it not written in policy and we will receive a negative mark for that even though it not considered full policy, It is very confusing sometimes for us on following certain policies because of this practice by the company. It hard to know what to do and which one to go by because they contradict each other. Sometimes we have to ask our auditor with new policies about things because we are umbrella company and they want all branches to operate as the same but yet some branches have different rules and regulations and it doesn't make sense to us. When we get new software its also hard to get the work done and understand what rules they want us to follow because sometimes the software doesn't work as expected and causes errors and they blame us for the work getting messed up when we clearly screenshot the errors and forward them and also more than one person is getting the same error. We also have to contact our IT department which is somewhere overseas and the English isn't that great on their end and its sometimes hard to get what is wrong with our computers across to them and have them figure it out and sometimes it is very time consuming and keeping us from helping customers and slowing us down on things we need to be doing instead of waiting on a service technician to come on and help us fix our problem. We also have issues with our back office knowing what each department is doing and its very frustrating when we are told to do things one way by one department and then told to do it another way by another department, so we have to get together with both and let them know what they are both saying and that they don't make sense and its very time consuming to get an answer or we have to wait forever to get an answer back from each department. We have many departments in our company that we have to communicate with

on a daily basis and sometimes it does take them a long time to answer us back, i realize that they have their own jobs to do but our company should either hire more people to help or just have them give us a time on when they can get back to us so that we can let customers know what is going on and let them know when we will be getting back to them about whatever the issue is. We still have very old computer programs that we work on almost like a dos system and it freezes half the time and it is VERY slow and the computer just isn't putting money into upgrading our systems. That makes our jobs very hard and sometimes we have very impatient customers who think that their is something wrong on their end and we have to explain we have very slow technology and there is nothing wrong. As a customer I wouldn't want to sit and wait just because technology is horrible. It is very frustrating for us and the customers when our computers are constantly freezing and shutting down and we have to wait for them to boot back up and start over again. WE also get refurbished scanner and all computer equipment from our company and it doesnt always work when it comes to us. I know tech is expensive but sometimes its better to go for a few new parts instead of buying all used. It is very annoying for all employees.

Interview 18

For my work I have to collect very confidential information from people including their social security numbers, green cards, pay stubs, etc. Even though it was common sense knowledge that this should be kept confidential, the HIPPA laws have never been directly explained to me, and it took a while before directions on how I should keep documents secure were explained. I knew that I should always been my work phone and computer with me, and never leave them in a car or a place where I am not at, in case it gets stolen. I also was recently told a direct way to upload documents from my phone onto my computer, and have been told the importance of always connecting to a VPN when I am working away from the office. Sometimes the system for uploading documents from the phone to computer does not work well, so I need to ask our IT guys again the best way to do this. It is difficult at time balancing time, as I know I should always be deleting documents, but I have other projects to work on so it is hard to find a balance without going too long before deleting documents.

Interview 19

Yes, execution of work task really require attention to organizational policies. even though it is so employees depend sometimes on unwritten code of conduct to bring morality and stability within a working environment. Some time ago we had a little disorganization within the working channel that some information was missing in the building and a delicate information and no on knows how it got missing. at that point I, as supervisor had to interpret organization procedures towards finding security information to recover the missing piece of that information and how it got out of control. there were challenges in the making of the effort for recovery. I had to introduce my own tacit to make the recovery by getting all the security information needed at the point, there was no originally written security policies for such inconsistent and uncertain challenge but had to act or bring in what was needed possibly to get it done.

Interview 20

I work at a nursing home and have come across this often. According to our guidelines given to us by the state health system, we are required to perform tasks a certain way. However, they are often times that we CNA's become so busy that these tasks become to hard to preform. For example, there are many times that we are short staff and are unable to complete our morning routines with residents fully. Often, we have to decide how much time we will spend with a resident, how much effort we can put in for washing them up, or cleaning up their rooms. This would mean that maybe we have to decide to skip brushing their teeth that day, use a short cut for washing them up, or spending enough time with them to talk a little. We become so busy that unfortunately we have to decide whether to follow our procedures or to create short cuts in order for us to have our residents up and dressed in time for breakfast and other daily activities.

Interview 21

In my job, we have to keep the identity of our clients confidential. We can only refer to them over walkie talkies, in e-mails, or in conversations outside of our clinic by first and last name. We collect data daily on their problem behaviors, prompt levels needed to complete tasks, their progress with their protocols, and detailed descriptions of any new behaviors or concerns we observe. We have to use a website to submit our session notes to insurance for billing purposes. Many times we are short staffed and have multiple clients in a single day. Our insurance notes have to be submitted by midnight on the day the session occurred. Our security policy states that we may not send any information over email that could identify the client and that client information should not be viewed on a device where someone else could access it. It does not specifically state that we cannot send ourselves e-mails with data of the client's session to complete the insurance notes at home, since there is often not enough time in the workday to complete them all. Since my laptop is password protected, I live alone, and no one else uses my wifi, I often interpret this to mean that it is okay to send data, with no client identification, to myself over e-mail. I only include the time the session occurred so that I know which client the data belongs to. I know how important a detailed session note is for record keeping and insurance approval, so I believe it is in the best interest for me to e-mail the information to myself. I had previously written it on a piece of paper to keep with me throughout the day, but I realized I could misplace this or someone could get ahold of it much easier than they could my e-mail. I have never had this potential breach in information security mentioned to me in any meeting with my supervisors. They have full access to everything sent through company e-mail or accessed on company Wi-Fi, so I continue to assume I am not breaking any rules.

Interview 22

My organization does not have specific information security policies so I am constantly trying to figure out the best practice. I need to send secure information to third parties and we cannot encrypt emails to third parties so I often have to ask if they have a secure portal to drop files in. For file storage of sensitive information, I mentally keep track of how long its been and delete when I am reminded that it is still on the server. We do not have a formal policy about taking credit cards but I know not to collect that information so I tell customers I cannot process their payments over the phone and they have to use our online portal.

Employees often ask me to share financial information with them but I only do it when I am available and share screen on a virtual call. We have no formal policy on sharing this information but I use my best judgement to not share files and only share it "view only". For sharing personally identifiable information we also do not have a formal policy so I always ask for permission from the individual whose information I need to share.

Interview 23

Information security is dynamic and constantly changing at my workplace. The rules seem to be constantly changing and are difficult to keep up with. My workplace restricts access to personal email, specifically Gmail. On a given day, they required mandatory completion of a COVID-vaccine status confirmation. In order to comply, I needed to access my Gmail account to procure my electronic copy of my vaccine record. I was able to access my account via my phone using my network internet access, and forwarded the information to my work email. I subsequently accessed my work email on my work desktop and accessed the electronic copy of my vaccine record. I was then able to comply with the mandatory requirement. It seemed unreasonable to require immediate and mandatory compliance without allowing the appropriate means or access to comply.

Interview 24

I worked for a non-profit group that put on a week-long summer camp for immigrant and undocumented youth. There were no set rules or procedures about security other than being told to not ask the undocumented youth about their status, where they came from, or anything personal to them being there because they were being held in foster care under another local group. Most of them were also having to deal with the court systems because of their statuses, so sometimes their attendance would be interrupted because they had to go to court some days or half days. A lot of this information about them I learned as the camp went on. There was nothing in writing about how to proceed if a youth told you information or you found out information you maybe weren't supposed to know. There was a big cultural and language barrier, so most of the time, staff couldn't understand the youth, so I think that was a default benefit of being kept out of hearing things we weren't supposed to. But the staff that were picked by the two main organizers were all pretty close friends with good ethics, so I think there was automatic trust to know what not to say or ask youth about their lives.

Interview 25

I work at an accounting firm. I am a receptionist. I have several times where clients ask for copies of previous tax returns. We go have an online portal for clients with accounts where we store their documents. However, not all clients use this dashboard or know how to use it. Some clients will ask me to email a copy of their returns. Tax returns hold sensitive information, that should be kept secure. This is something I believe that clients are aware of when they are asking me for a copy of their return. Because of this, I personally do not have a problem sending returns through email when requested by the client. This could be viewed differently by other people. Some may find this to be risky. There is no official policy in place at the firm where I work regarding emailing returns. I also have never had anything happen when doing this.

Interview 26

Working as a finance officer in my organization, there is a certain project that money is to be paid to the organization account before the commence but it did not go as plan and the client was expecting us to proceed with the task and which is against the rule of the organization but base one trust and longtime relationship the task has to proceed to be able to keep the client and not to lose the client as one of our major customer. The manager on finding it was furious about how things went but I explain everything to him and he said if that is the case client who have long time relationship and who I have known to be people of their words can also be allowed to do business so for the organization/ company not to lose our customer/client to our competitors. As a result of this rules and preceding policy can be step down so others who we have longtime relationship and to allow those who are coming in for business to have a bite of how free and fair the organization is and help us beat our competitors by securing more customers/client. The security of the organization which has to do with the polices and rules governing the organization has to be step down or compromise to meet up to some certain target and tasks

I work as a fifth grade teacher, and often have to use and follow unwritten rules when dealing with privacy or security issues. For example, in emails about specific students, we never use their real names, but just initials instead. Similarly, one simple unwritten rule is to avoid using reply all in emails. This keeps issues pertaining to particular classes, students, or staff private. We are especially attentive to privacy issues when communicating about students requiring outstanding paperwork, accommodations, or other legal matters. It is somewhat of an unwritten rule to keep documentation about all communications between yourself and the parents

of these students for future records. I often wish that, even those this rule was unwritten, there was more consistent formatting for these kinds of documentations.

Interview 27

Yes, I work as a teacher and there is not full transparency on what kind of information is allowed in what places. Especially during times of coronavirus, there is uncertainty on school procedures on who is allowed to share information on employee or student health status, including infection, vaccination, or test status. This happened recently when a coworker had coronavirus and I was not sure whether it was my place to tell their students or parents that information. I decided to not be the one to tell anyone because I didn't want any liability for sharing information, but I also felt it was unethical that students and parents weren't notified about the potential close contact case. This was a situation in which my job duties (teaching and keeping children safe) required me to interpret insufficient organizational procedures on health information security polices.

Interview 28

This was when i was working as a middle supervisor at this particular construction company. The procedures associated with the security policies were very inconsistent for me to perform my work effectively. I was supposed to manage all raw materials and implement necessary for the construction of this road network, but the materials had to be kept on the field without proper security or guide. And if any went missing, i had to account for it. It was a very terrible and scary situation which the company put me. i had two choices. Its either i stay the entire time on the field. Probably sleep in tents at the site to keep an eye on the instruments, or at least i had to find a safe option, that is a very safe place to keep them. The pressure from the management on me was much and i had to deliver well as i had always done. They even expected more. I wrote letters demanding for security measures, but they said it wouldn't fit into the budget, i had to find a way myself to secure the company's properties. It affected those under me too. we made a roster; we took turns to sleep on the site and keep eye on the tools till we were totally completed

Interview 29

I usually consider myself as having a very technical job. As a trained professional in construction in a large private enterprise, I am responsible for training and supervising workers. There are several situations where we are given project works that needs further information which isn't disclosed in the initial debrief. In order for me and my team to get the job done, we need to gain access to company's database to get the necessary information needed to execute the task. This is actually not associated with the security policy but I had to solicit help from one of my superiors in order to gain access and not get queried for doing so. We were able to carry out the task eventually but it would have proven more difficult and straining if we hadn't bent the rules a little as regards the organizational security policy.

Interview 30

I have had several times when computer access/login credentials were required and at the time an individual had not been issued said credentials. I had started a new, fairly independent, position within a company and the in less than a week of training at this new position, the person training me left suddenly left the company. I needed to find ways to contact people when I didn't know who was in charge. There were group chats that I should have been included on, which I wasn't. And there were many permissions for this position that I had not been granted, which I did not even know were permissions that I needed. Due to the nature of this position, many of the on-site managers were not aware of the daily processes of this position and didn't know the person of contact for this position. Eventually, these people were found out, tickets were submitted, and I was able to receive the proper permissions. This was a common process for me during the first couple of months. I easily requested permissions to chatrooms. I was constantly forwarded emails that were what I considered to be outside the purview of my position. Many of these emails were labeled confidential. But at the time seemed to be standard process for managers to send to me in case they wanted to get something done. That's what I did. I got stuff done. Sometimes managers or other assistants shared their login information so others can access the system. However, sharing login information is strictly prohibited whether it be for hand-held devices or laptops. This access occasionally allowed others to view or edit things that wouldn't normally have been available to them. This access was seen by management as a commonplace necessity, regardless of what information security policies in place. Several times, I was asked to train other workers regarding specific systems I worked with. However, they had not been issued login credentials. I showed them how to log in to our systems, without sharing login or password information, then I would train them on how to use these systems. Workers would watch as I

went through the system and showed them how to perform certain tasks. I never allowed them to sit at the keyboard under my credentials. Eventually, many of these workers would gain the proper credentials to access the system. They would have no problems logging into the system. And would often ask for help if they did. However, very often, they would not have received the proper permissions to access different task points and programs within the system. This further delayed their training. Over time, some training programs were created for new employees to learn these systems which made permissions irrelevant for the most part. Some of the training required permissions, which seemed redundant. However, as I progressed with teaching myself the processes needed for my position, I would try to get proper permissions granted to those that required them as needed. I made a list of requirements and eventually requested that anyone coming to work with me, which needed login credentials and permissions, be granted the necessary tools before being assigned to work with me. Unfortunately, as this was not an automated task, so it was on me to make sure that management assigned the proper credentials and permissions. I tried to learn about new trainees as early as possible so that I could hassle management and stay on them about getting these things granted. It worked. Mostly. There was one time during the second of two very important events where we had special air-gapped laptops specifically dedicated to these events. However, they were misplaced and this required me to use two of the laptops that I normally used for these events. I cleared the cache, cookies, and histories from both laptops. I had to log into these laptops with my credentials and allow them to be used by third party contractors. As I knew the processes these computers would be used for, albeit for information that was not available to myself or anyone else within the company, I made the decision to allow their use. I discussed this with management later and management concurred that I had made the correct decision at the time given that I was the only

person really tasked with this event and management had taken a hands-off approach. The notebooks we would have used were not found to my knowledge and I doubt management ever thought about it again. The inconsistencies with these policies often bothered me although nothing seemed to come of it.

Interview 31

If I am understanding the questions correctly, one example of when i have had to deal with this at work would be reviewing certificates of insurance from tenants at work. we are told to look for a few parameters like that certain boxes are checked and that certain language is on the COI, but there are a lot of gray areas and places where things can be confusing on the certificate.

we are told to always ask for the "additional insured endorsement pages", but many tenants and their insurance agencies have not heard of this. so when they send me their COI and additional insured backup, sometimes it says "additional insured blanket policy", or sometimes it has the owner of the property's name (like its supposed to), and other times it has the words "additional insured" but i can't tell if its just explaining what that policy is. most of the times im just looking for the key words, but sometimes i have no idea if the certificate is correct and most people at my office are too busy to be bothered with questions about certificates of insurance, or they dont know. what i do is try my best to make sure the COI is legitimate. first, i ask the person (if they tell me there is no additional insured endorsement page or if their agent doesn't know what it is) for the proof that the policy is "endorsed". sometimes they end of sending me an insurance packet full of about 200 pages and i don't read through everything but i accept that as proof of the policy.

Interview 32

There was this time a few years back, 2015 if I recall correctly when my organization was inconsistent in analysis of her security programming database system. Being a new intern at the protocol and security department at the time, I was a little apprehensive given the fat that I had heard so much about underground cover-ups being carried out in some of these big companies and firms. So I naturally thought somebody had some sinister motives up his or her sleeves. This was coupled with the fact that alot of the men there were actually putting up shady behaviours and some of the female staff acted weird. But I was wrong, as I was about to find out that they only out up a show and a charade to see the stuff I was made of. Alot of the policies in the department ended up bending me in ways I never believed could happen but it all ended up being for the good of my CV and I also got to learn alot practically. I was at the last able to meet up with the working requirements if the company, although I had to work with other departments to be able to. It still ended up being one of the most exhausting tasks I have performed with that department up until this day.

Interview 33

I work at Disneyland in entertainment costuming, and while the company has a decently straightforward policy regarding release of information, it becomes difficult to tell what is appropriate to tell friends who don't work at the company vs friends who do work with the company but in other departments vs people who work in our department but not in the specific venue where new reveals are happening. For example, when costumers know that a certain character is going to be released into the parks. This is often considered "low" impact information, and people share it all the time, but it technically goes against company policy. The same happens when we know that a new show is coming to the parks or an old show/parade is coming back. New information is kept under wraps pretty tightly, but with so many disney fans speculating, it becomes hard to know when/if it's appropriate to confirm theories about new/old shows coming to the parks. It also becomes frustrating when, because of the company's strict information policy, employees find out about significant changes in the work place through media releases to the public rather than the company coming to us as workers.

Interview 34

I was working at a place that had its own software and programs to hold customer information; but it was very very buggy. It would lag, blank out, and close unexpectedly while on call with a customer. So, we would have to open a notepad or some type of internal note program to hold the information while on a call, because the software was so finnicky that we had to temporarily hold the customer information on an outside app. We were told in the beginning of the job that customer info was supposed to only go in one specific software, but as time went on we were told more and more to do something else with the info. We would regularly be checked for having the info, so it would be just a quick delete after the call, but on MacOS it saves automatically, so that would cause issues as well.

Interview 35

I work in logistics and warehousing and am required to operate mobile scanners on a daily basis in order to pick product to be shipped. At work, we recently changed scanner models and there was little to no documentation provided regarding the new equipment. This has led to requiring help from a few selected employees that are sufficiently familiar with the equipment. However, those individuals need our login information in order to help us. That has been a murky area in regards to our personal login security, as no one else is supposed to handle our account information. Hopefully a better way to learn the new equipment will be provided, because as it stands, it poses a significant security risk if one of those trained individuals decided to do something nefarious with our information.

Interview 36

I currently work as a fraud analyst for a major money service business. Keeping customer information private is an essential part of my job, though sometimes the rules are blurred. As a general rule of thumb, disclosing a customer's personal identifying information in Teams chats and emails is prohibited. My job is currently remote and when I have a question about a particular investigation, I raise the issue to my supervisor. It can often be difficult to describe my concerns regarding customer information to my supervisor. For example, if I come across a particular piece of negative news or uncover an extensive criminal history on my customer, it can be difficult to comprehend the impact of this information on my investigation. In one particular instance, I took a screenshot of my customer's criminal history (no PII included, just details of charges) and sent the image to my supervisor. I asked him if I should that classify information as relevant to my investigation. While my supervisor did offer me helpful advice, he informed me that it is against company policy to screenshot that information and send it in a chat. I was unaware of this policy and never made the same mistake. I believe my company's policy should have provided more detailed examples of what activities are forbidden when it comes to communicating about sensitive information. Since then, I have relied on my own judgement regarding sharing information about customer activities.

Interview 37

I have a good one for this. My company is a design/build construction firm that builds large, commercial distribution centers. We rely heavily on all sorts of marketing to build business, and that included LinkedIn, Facebook, Instagram and other social media. Our employee handbook states we should not use social media on company computers and not use social media for personal reasons on our company internet connection. Our company often asks us to go visit posts about the company on social media, or includes links to these things in company emails. In my opinion, it's almost impossible to go on any social media platform and only look at one thing before logging off. My confusion resulting from these opposite orders has both made me feel like I should go look at these links outside of company time, which makes me mad that they are asking me to use personal time for work-related things. It has also made me feel guilty when I looked during company time, then found myself still surfing Facebook ten minutes later. I normally never consume social media on my work computer.

Interview 38

I used to work for a healthcare organization. We were required to follow HIPAA guidelines when it came to protecting client confidentiality. Employees were required to complete online trainings once a year about HIPAA laws, various ways of reporting HIPAA violations as well as the corporate compliance policy and who to report to if we noticed problems with it. I noticed that various co-workers violated HIPAA frequently. I noted that some co-workers would text PHI on non-work phones or sometimes take photos of our clients on their non-work phones, all clear violations of HIPAA. I tried to bring some of these issues to my boss but the issues were ignored. I did what I could to maintain HIPAA myself. However, this was difficult when it seemed that the organization as a whole did not have a clear idea about how to maintain these important privacy laws or have a consistent goal to enforce them.

Interview 39

As an instructor at a college level, I am asked to stay in communication with my students and colleagues. I am also asked to keep professional boundaries. So, for example, we are directed not to give out our personal phone numbers or personal e-mail addresses, but are encouraged to set up a phone app on our computers and use our institutional e-mails to respond to student requests. This is insufficient, at times, because of noncompliance by students, who may use their personal e-mails. I may direct them to use institutional e-mails, but I am not in control of their choice to use the secured platform. I would also suggest that institutional e-mails are more often targets of hacking and spam than my personal e-mail has ever been, in part because mass lists of e-mails are easily found online. I am also responsible for my own personal computer and do not have a work computer. So while I am being asked to use the institution's network and their e-mail, which they can monitor, I am using my personal device. There are also always two options to use for the local network. We are encouraged to use one where we sign in using our institutional e-mail and password, which is then monitored. However, there is a guest system that is open access and often easier to connect to.

Interview 40

I used to work at Starbucks and as a barista, you were expected to answer the store phone when it was heard ringing. There are certain rules about what information you can give out to people over the phone but none of them had been given to me during training. Now of course I understood to not give out information about money or personal information to callers, but that was just common sense. One time, someone called asking when a fellow barista was going to be working and I told them, assuming they just liked when they made their drinks or they were family. My boss overheard me and let me know that we can't give any information about coworkers at all over the phone, especially schedules in case of stalking. Because of uncertainty about the rules, I accidentally gave out information that wasn't supposed to be given.

Interview 41

One of my main projects is to write up operational guidelines and interpret policy gaps for internal procedures. At times this must include collaboration between different team members. There have been different messages relayed by the company security team about which platforms can and cannot be used when accessing and sharing confidential internal policies and procedures. The main issue is the use of Google Docs to collaborate on confidential documentation. In some correspondences, the security team stated in emails that employees cannot use Google Docs at all for. In follow up emails, it was stated that it can be used but only for a limited duration and the document must be deleted after. This made it very difficult to collaborate with multiple teammates, especially those in different international offices.

Interview 42

I work for a healthcare organization. While I usually work in the field directly with patients, the start of covid posed much difficulty in that homecare patients refused in person visits and nursing homes were not allowing contracted workers in. This lead to a very abrupt move to telehealth visits. Telehealth visits with little guidance as to how to utilize the technology and ensure security within that technology. The large company I work for eventually put forth more guidelines but there was a big chunk of time where workers were making it up as we went along. I was not sure how to document patient signatures at first. I was not sure if the visits should be made through a video or over audio only and how to ensure the video would be secure for both the patient and myself. I was also working from home with 2 little kids at home making the matter more complicated.

Interview 43

I am one of the owners of a residential cleaning service and while we do not have a very sophisticated information security policy in place, we do rely on trading very sensitive information between clients and the people that will be placed to work in their homes. I am often having to provide sensitive information over text that involves passwords, door codes, gate codes and addresses. One of the things that we do to combat potential information getting in the hands of the wrong people, is we never provide the person going into the home with the full name of the client. This way, if the workers' phones end up lost or stolen, the recipient will not have an associated address with specific names, codes, passwords, etc to peoples' homes. The people that work for us do not often have access to computers that could potentially protect this information safely by using firewalls or a coded system. Additionally, the educational level of the workers we have does not allow for anything sophisticated or advanced in terms of the information security policies that we put in place. We have lots of rules and procedures that have to be carried out but in the heat of the moment, some of these can easily go by the wayside.

Interview 44

Working in a career field that sees me interacting almost exclusively with large groups of people (teenagers), there are tons of 'unwritten' rules, so to speak, that you learn to utilize and follow while on the job, despite the fact they aren't explicitly outlined in any formal procedures. This is especially true when it comes to information about the students and their grades or accommodations/modifications, as outlined in their IEP and 504 documents. It is a huge violation of FERPA to give this information out, and thus it becomes one of the most closely guarded secrets; however, some accommodations and modifications are extremely obvious to the other students, who will then complain or inquire on to why they do not get the same considerations. Since we are unable to tell them why (the student has special needs and gets to use their notes for this reason, or a separate testing location, or whatever), we have to come up with a lie to parrot back to the kids, which is not something we are ever actually told or given information on. These lies range from teacher to teacher, and yet it is an incredibly common practice, and one of which there is no manual or rules that tell the teachers to do so.

Interview 45

I work at a Toyota dealership in the rental department and we have multiple policies that we have to follow to ensure customer satisfaction and customer security. To put someone in a rental, I am required to obtain a valid US State issued driver license, a debit or credit card, the customers active and valid insurance ID card, two forms of personal contact, their address, and where they are employed at. As one can see, this is a lot of personal information that some people may not want to give. I have ran into issues before where I had a wife trying to get a rental vehicle so her husband could drive it. Most companies, that would be fine. Per Toyota polices and what I have to follow I would not be allowed to do that. In order for him to drive, he had to be there present with his driver license. They were not legally married and he was at work. The customer was trying to email me a picture of the driver license and facetime her husband so I could confirm the information with him. As I stated before, this is not allowed for my job and where I work at. I explained to the couple multiple times why I could not give him authorization to drive and if they continued, I would not be allowed to give them a rental vehicle at all. The manager for the department at the time came as the wife no longer wanted to deal with me. The manager gave them authorization to get the rental and for him to drive the vehicle, as long as she returned it. They were fully responsible and if any damages occurred to the vehicle, they were 100% responsible. I felt very confused because this was not something the corporation allowed and the manager made me look like I was not confident in my job tasks. While that manager was in the position, these things happened quite often. It always made me feel and look dumb and unprofessional in front of the customers. Once the manager left and we got a new one, things were different and she followed every policy and guideline we had so the whole department was

on the same page at all times. That would be the most uncertainty I have had working at this dealership.

Interview 46

I created a new program for my job and it was only me in the department as a caseworker. I knew the policies from headquarters, but at my location there wasn't anything written as we had an entirely new program and the autonomy to create a program that worked best for the area, we were in. As a caseworker I constantly have problems with clients and volunteers come up and I have to navigate based on what I think ethically should happen and write it into the procedures. Some examples of this is how can adult mentors and minor mentees be in a match together, what happens if they are unable to come to the group meeting, and what are topics that we should talk about. Additionally figuring out what contact with mentors looks like after they complete their program and if mentors should have the parents phone numbers.

Interview 47

I used to work at a psychiatric inpatient residential facility for at risk youth. The described situation above, where job duties required me to interpret procedures that were uncertain, happened almost every day. The training for the job was minimal and in order to acquire the job there are very little qualifications. With that being said, a lot of people start work and are put in situations where they are too make judgment calls without any clear direction on how to do this. Over time of working there, and gaining experience through situations, it becomes easier to navigate. However, even then it is still vague and left up to best judgment this leads to an unstable, inconsistent and unsafe working environments, for the staff and the clients.

Interview 48

There was a time I told my coworkers that the security cameras are on in the bathrooms and that against the polices. When i tole everyone they freaked out and I told them to stay calm. I found out what was going on and out a stop to it. the security policy are to be followed at the business at all times .It is my job to take care of that. So the person who was doing it was fired and reported to the police. He is now banded from every entering the building again. This was the first time this has happed under my watch and i will make sure it is the last. It's my job to manage and make sure all the security polices are followed in every inch of this business. If I do not i will be held accountable and possible fired. And i cant let that happen

Interview 49

When working as a departmental trainer it was a task of mine to identify these “unwritten rules”. I was tasked to ask questions as to why the groups did things the way they did even though it was not documented to perform the tasks in the way directed. This included tasks such as underwritten responsibilities of staff, directive from old ways of doing things and so on. I was able to describe why process improvement is imperative for groups to thrive. However, with this conversation it’s also important to note why employees think the way they do so to ask historical questions is also important. Many work groups function to not break the mold or don’t fix something that’s not broken. I however continuously try to think outside the box and to strive for the most efficient way to complete a task. This may involve small improvements over time, or can involvement huge over hauls of process.

Interview 50

In one of my previous roles within my company, I was in a supervisory position as a general manager for a corporate wellness company. The role included overseeing all operations, financials, membership and personal training sales, facility maintenance, health and wellness assessments, etc. Oftentimes, member's and client's cards would be expired or declined for various reasons. If this were to happen towards the end of the month, it would cause a notable hassle for us. The accounting team wanted all transactions from the current month to be processed and paid by the end of the month, so as not to allow a balance on the members account to 'roll over' from the current month into the next month. For example, a client comes to do a scheduled personal training session in the last week of the month. Clients were put onto our schedules using a SAAS company that provided a cloud-based management/scheduling/ payment processing system. We were instructed to process all personal training sessions before the end of each shift. Oftentimes, we would go to 'checkout' the session (therefore processing payment) and we would be notified the card was declined. We would then have to scramble to get in touch with the individual and try to get their CC or ACH details. We were loosely instructed to only take payment information via the cloud-based payment system. Unfortunately, this system would regularly be down for maintenance or not functioning for a multitude of reasons. Therefore, we were often put in a position where we needed to take the CC or ACH information via email, or by writing it down to log into the system later (once it was back up and running). We were constantly reminded that processing all sessions and payments before the end of the month was mandatory and were threatened with write-ups for failing to do so. Due to this, there seemed to be inconsistent policies regarding taking payment info. With the system regularly malfunctioning, we felt forced to break policy and take the payment info by hand or by email, to

then process once the system was up again. We did take precautions by shredding anything written by hand and deleting any emails with payment info. I would describe it as being backed into a corner.

Interview 51

Working in the human resource management field means you have to have a high level of confidentiality. However, when you have a union presence, things can get a bit mucky. For instance, I would never share information such as the last 4 of someone's social security number, their birthday, phone number, shift and rotation they work, etc with another employee. However, we share this information with our union reps on a regular basis. Additionally, the union reps often ask for information such as the results of someone's covid test, the reasoning behind someone's leave, and information regarding someone's termination. It can be tricky to determine just how much information you are able to share. I have made it a point to share as little as possible while still giving the reps the information they need to perform their job. For instance, if they ask about someone who is out with covid, instead of telling them if their results were positive or negative, I will just inform them that the employee can return to work in x amount of days. This is necessary for them to know so that they can assist with getting coverage out on the floor. However, it is often easy to predict what the status of the test was based on how long the employee is going to be out. Many things are a grey area that is hard to determine.

Interview 52

At many retail jobs, the policy is written in that it cannot be violated by customers or by associates working. Many of these policies include things like returns, exchanges, etc. It's difficult to not be able to help customers when there are rules in place that they also must follow in order for things to work properly operationally. There have been several instances in which I had to break procedure in terms of returns in order to leave customers with a positive experience in the store and with the business. Past the 30 days, I've been able to at least issue store credit and get the customers other items in order to better suit their needs. Often times, I have taken initiative to contact the higher up customer service team in order to find better solutions to their issues, all while breaking policy because the customer is unhappy.

Interview 53

Working in higher education, FERPA is a major guiding principle. However, working in athletics at the higher education level, we have tons of parents/guardians who want to have a backdoor view of their students' grades. While the university does offer a FERPA release to students who wish to grant other access to their records, there is no verification policy for when these parents call advisors with questions about their children. In my department, most individuals rely on familiarity with the caller when deciding whether or not to share student information with them. I do not think this is a sustainable practice nor a best practice, and there are easy ways that we could require callers to identify themselves, such as student's birthday or other identifying information. As it is, no such information security policy is in place.

Interview 54

In my previous position there were many unwritten rules, most were common sense and could be figured out by using a moral compass. There were easy ways around job tasks and it was easy to take shortcuts to cheat the system. There were no written rules saying don't do this but you would have to cheat your fellow coworker to achieve this shortcut. There are many situations in jobs that your moral or ethical decision-making skills should just be common knowledge. In other positions I have had, I have had access to databases and files that are of course private. This information could be very valuable. In my position there was not a non-disclosure but of course its common knowledge I wouldn't steal information to take away from work to make financial gain. This information should I have chosen to take it for personal use could have helped me start a competitive business to rival my existing employer. You would think a business would take the private data and have a non disclosure with its employees. I feel that I am a very ethical person and morally I feel this would be very wrong. This would be easy for someone to do without a moral compass or someone who is clearly unethical.

Interview 55

I am not entirely sure I understand this question, but would like to answer to the very best of my abilities. I am a communications specialist for an international company headquartered in the southern United States. In my role I handle public relations and media for the company. Our company serve homeowners associations as part of the property management industry. At my company I have come to understand what kind of information about our company and our relationships with residents can be made public as part of media outreach, and what cannot, because of security and privacy concerns. When handling media requests I have to assess the risk with sharing any information, and the benefit of communicating with media outlets about our company and our business dealings. This changes on a day to day basis, but it is critical to the reputation of our company.

Interview 56

Working in the medical field, there are many policies regarding the security of patient information. I was familiar with HIPAA regulations when I first started this job working in workman's compensation, but in my mind there were a lot of inconsistencies in where information regarding patient's medical health were being sent. I did not have proper training so I was always hesitant in sharing patient information with employers and insurance companies, and it has taken me time to understand where this information can be properly sent, as well as in the methods that this information is sent. I had to question what I knew and the procedures of this company to get a full understanding about the security procedures. I learned that for patients to sufficiently receive worker's compensation, the insurance companies and the employers need to know about the dates of their visits and their current work statuses.

Interview 57

An example that I have faced at several times over the course of my career relates to accessing work information systems on personal devices. For example, there has sometimes been an inconsistency in an organizational policy related to employees accessing their work email accounts on their personal cell phone devices. In one organization that I have worked in, employees were told that the organization's email accounts and files should only be accessed on company phones and/or computers, yet employees were expected to be "on call" and responsive to email messages, for example, virtually around-the clock – despite not all employees having access to a company cell phone. This resulted in a number of employees – the majority, most likely – essentially violating company policy, as employees prioritized the company's insistence that employees be accessible over the stated policy. When this issue was raised with managers, employees were left with the impression that there was an implied understanding that employees were not necessarily expected to comply with the policy.

Interview 58

During COVID everything shut down. And although to many people it may have seem things stop I would argue things speed up. Without the daily necessities of working companies began to focus and where they can change to cut costs and give a better service to their customers. The company that I work for changed all of their security information after they had acquired a new company underneath them. This meant that when I began working with them again after a period of time all of the personal information security information for multiple POS logins needed to be renewed and changed. My first day back I was unable to assist in any customer support because I was on the phone with IT for three hours working to update my personal login information. Including in this the change of employees switching between companies new insights have been put in place as to how the company was run. This lead to new employee numbers new logins time to set up the new employees as well as reset and re-learn an entire new system for past employees. There was much confusion and no very clear way on how to accomplish things I would try to login to one system and be able to login there however I would be unable to login to the other system. Speaking with IT let me to believe they were completely incompetent and unable to assist me in anyway further after resetting the password multiple times and re-entering the same information multiple times they had to do and it was complete new form to fill out for me to be a employee with the company. Once I was finally able to login then I had to go through all of the new forms to show that I was capable and able to work in this capacity. Filling out forms that were dated back from 2019 during which all company policies mixed in with new company policies updated to now. Some of these older forms directly contradicted newer forms sent from the company. This lead to some people following older policies and protocols while mixing in with newer policies and protocols. There

was no clear directive from the higher ups and no clear answers with tech support. Including in this down on the tablets that are used at this work son had the new updates while others had the old past updates. This means that only some more usable while others were inaccessible for us to to work with. The tablets with the updated information still had passed apps that that contain old information. This led to people logging into applications that were not usable anymore and entering client personal information and that was no longer deemed safe for use. Luckily there were no incidences that took place that would lead to a breach in contracts, but it was a security risk all the same. Due to having so many forms that need that were needed to be filled out it was impossible to complete all the forms in one workday even though 90% of them were backdated due to the location being closed from Covid. This meant theoretically we should have been red flagged and received marks on our yearly results. Thankfully due to everything going on those marks were expunged and did not affect our overall reports for the year. This confusion between multiple forms that were old and new, new employees and old employees, difficulty with tablets, and other problems cause things to be extremely difficult to regain a smooth employment there. Although normally I would personally be excited over the growth of the company due to acquirement during a time where a smooth transition process was not able to be worked through with the current employees it led to difficulties distress frustrations breaches of security and many other problems. To this day there are still other issues that have a rose and there are still forms that I currently need to fill out but that technically I am not able to access because they're over three years old. This is become frustrating and and time consuming and there appears to be no end in sight. Currently I am still unable to access my past confidential client information and have no login for that particular system. I am also unable to process transactions even though

having come back from Covid for several months this has affected my income my work status and multiple other things. It has led me to feel frustration and a desire to leave this company.

Interview 59

When working a retail job, I was faced with a few situations where I had no sure fire answer as to what to do in a situation. Very quickly into this job I was promoted to a supervisory position and knew even less as to what to do. I had a few situations where there were things like broken or damaged product that I didn't know what to do with, and therefore I'm fairly certain I damaged out items (i.e. cut up or destroyed products to prevent further use) when they could have otherwise been salvaged and sold at a discounted price. There were also extreme issues where we didn't have a store manager and there were scheduling issues. Myself and another supervisor were tasked with making the schedule for the associates and ourselves without any real training, and unbeknownst to us we were scheduling at least double the hours we were allotted, which messed up the amount we had to schedule the rest of the fiscal year. We also were forced to deal with sanitary issues that were beyond us, as the bathrooms we had in store would back up constantly and we never knew what number to call, or what exact steps we needed to take beyond barring the restroom to make it safe for further customer use. It was a lot of seemingly minor issues that all seemed to arise at once, so during our 4 months without a store manager we were lost.

Interview 60

I worked in an independent retirement living care facility and we were always told to help our residents in any way we could so we often went beyond what our job descriptions were to assist our residents. In one instance, a resident was in the process of moving out of our facility and needed help sending a scan of personal, sensitive documents to their next landlord. However, (as it often happened to be the case) many of our residents were of a much older generation that didn't have good skills with technology; oftentimes, they did not even have a working email. The resident came to me (the concierge) and asked if I would use the company scanner and my company email to scan these personal documents to her next landlord. This put me in a weird situation where I didn't know company policy concerning privacy with company property and email addresses and there was no manager on duty at the time to help me with this situation. As I did not see a security issue with it and was unsure of the policy, I scanned her documents and sent an email outside of the organization as she asked.

Interview 61

Digital transformation played a huge part in the restructure of a tech start-up company where I was formerly an employee. In the beginning of this overhaul, the company held a state of the union type of meeting and informed us of the evolution in company policy and the new changes that were going to be implemented in the future months. The primary issue that was brought up in discussion was increased focus on cyber security, which at the time had been a huge issue for us as an organization. At that point, many of our databases had been corrupted, resulting in the leaking of confidential information. In response to the attack, the company had to outsource forensic / security experts to address the issue. The process was very time consuming and also expensive. We couldn't move on to other projects for about three weeks which was completely devastating to our entire organization. Once we were able to move beyond that roadblock, a team was brought in to demonstrate new procedures and policies as a responsive plan.

Interview 62

I am not exactly sure what you mean by security policy, but for example some of our work passwords and alarm codes are shared with staff and associated rules and procedures are a little unclear. I have heard from colleagues that each of us are supposed to have a unique alarm code, but most of the people on my team all use the same code. I was never assigned a unique code and I use the one my supervisor and colleagues all use, which creates some confusion. The organizational system for sharing account passwords is also inconsistent. Some passwords are printed and placed on our work laptops, and others are not widely shared. Sometimes I have to ask a colleague or supervisor for a password for a specific account, or ask our operations manager, which can be inconvenient.

Interview 63

I work in retail, so there needs to be a lot of organization and procedures to keep the store running smoothly. I worked in costumer service for a long time, so there comes a lot of security when returning items, cashing checks, and sending/receiving money constantly throughout the day. There have been many instances where we were not able to give the information that the costumer wanted due to security policies, so that causes a lot of arguments that made my effort to carry out my work task impossible. It also makes the work space uncomfortable because the manager on the clock has to work with the costumer as best they can, but when security is the topic of the argument, there is little we can do out of the safety of the costumer and the company. I believe that there needed to be a better organizational system when these situations happen so there can more consistent and efficient work.

Interview 64

The best example I can think of is when I was working the night shift for the first time at my company. This was a small crew comprised of only five of us including the supervisor. The supervisor had a rough history with the company, and her husband did as well. He had actually been fired from the company not long before this interaction took place, and he left on very hostile terms. So in our company, we are allowed to listen to any music of our choice, and we all take turns playing what we like over a small Bluetooth speaker system. For some reason, the music choice of the night greatly offended the supervisor, and she made the decision to call her husband to our facility so that he could, "show who was the boss". I was new to the company in general and as stated before, this was my first night shift. I had not been briefed on what to do if situations like this occurred, so at first, I sat back and just stayed out of the way. Her husband had charges pressed against him previously from dangerous behavior and since I didn't really know what to do anyway, I figured it best to basically hide in my corner. However, it quickly became evident that I would have to make a move of some sort, so I ended up sneaking a phone call to the head department supervisor. They then directed me as to what to do, and cops ended up being called. There were no rules/policies in place stating exactly what to do when faced with a situation where someone who is not supposed to be in the building forces their way into the building, so I just did what I could without escalating the situation.

Interview 65

At my old job, I was a math tutor at a local math tutoring place. Kids came for 1 hour sessions to get help with current math needs as well as work on any homework that was needed to be completed. Our policy was that kids were there for the full hour and if they were done with their homework for that day, then they were to continue working on the math worksheets our center provided for them to help them further their understanding of general math concepts. Our goal was for kids to complete 7-8 pages of math worksheets and then any leftover time was spent on homework. One kid had done around 16 pages and kept flying through his worksheets. He also completed all his homework for that day. He had about 10-15 minutes left till it was time for him to pack up but he had asked if he could leave a little bit early that day. I made the executive decision to let him leave early since he had finished all his work and I knew he was the type of kid to come back and keep working hard. It wasn't something that I would let him do every single time but this one time I knew it wasn't a big deal to let him go a few minutes before his session ended.

Interview 66

As a writer and communications professional, I am often working with personal information. I work at a college, and we have a system that holds all the information about an alum or other connection, including phone numbers, addresses, giving information, academic information, and more. I have access to all of this info, which is helpful when scheduling interviews with people or searching for good contacts for certain projects. While I have completed lots of cybersecurity trainings about email phishing and other best practices, I have never received a written procedure about contacts in the system. My own organizational procedure is to never share this information and to update it when I learn new information, like replacing old addresses. I collect class notes regarding promotions and other career updates as well as obituaries, and these also provide information that we can use to update profiles in the system. When going through this information, I often find that there are many inconsistencies in how profiles are kept up. A lot of this is because crucial information is based on the person sending that to us and not us seeking it out. I have never received a lot of instruction on how to keep profiles more consistent.

Interview 67

During my previous job as a web developer, my office provided me with a desktop computer for my work. This was fine for my typical 8 hours of work since, when I started, there was no reason for me to have to be able to work from home. The information security details were pretty lax or nonexistent, so I wasn't concerned when I began bringing my personal laptop to work so I had an additional device to use some of our time tracking software on and for testing some of my work when needed. Soon enough, my boss began sending me messages after hours urging me to make updates because a client wasn't happy with something, there was a misspelling that needed to be fixed, etc. My response of "I don't have access to the website outside of work" was not sufficient. I began using my personal laptop, combined with my personal digital password keeper, to work on website projects outside of work. My bosses never told me this wasn't an authorized procedure and many of the others in the company were doing this as well, so I took their silence as a sign that this was an okay way to work. Right before I left the company, everyone in the office received an email from management stating that personal computers, tablets, etc. were NOT authorized to be used for anything work-related. All employees were asked to discuss with management what devices they would need to continue working the same way they had with their personal devices. I had already put in my 2 weeks by the time this email was sent out, so when I received an urgent email after hours to make an update to a website, I was happy to be able to say I didn't have the authorized equipment to be able to make the change until the next morning when I was back in the office