FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

MANAGERIAL CONTROL EFFECTS ON INFORMATION SECURITY POLICY COMPLIANCE INTENTIONS: CONSIDERATIONS OF FORMAL AND INFORMAL MODES OF CONTROL

A dissertation submitted in partial fulfillment of

the requirements for the degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

Shaun Stewart

2021

To: Interim Dean William Harding
College of Business

This dissertation, written by Shaun Stewart, and entitled Managerial Control Effects on Information Security Policy Compliance Intentions: Considerations of Formal and Informal Modes of Control, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Min Chen

Shen Guo

Yan Chen

George Marakas, Major Professor

Date of Defense: May 14, 2021

The dissertation of Shaun Stewart is approved.

Interim Dean William Harding
College of Business

André G. Gill
Vice President, Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2021

ACKNOWLEDGMENTS

I wish to thank the members of my committee for their support, patience, and infinite assistance in aiding the completion of this project. Their recommendations and kind consideration have been invaluable. In particular, Dr. Yan Chen was extremely helpful in guiding the quantitative research and writing and editing of this dissertation. Additionally, I would like to express my gratitude toward Dr. George Marakas, my co-major professor. From the beginning of this doctoral program, Dr. Marakas has been a steady, guiding hand in ushering our cohort through all of the hurdles of completing professional doctoral studies.

I have found the coursework throughout this DBA program to be well thought out and valuable in equipping us with the tools to take our research into various industries and improve global business processes for the overall betterment of the economy and society. Thank you all.

ABSTRACT OF THE DISSERTATION

MANAGERIAL CONTROL EFFECTS ON INFORMATION SECURITY POLICY COMPLIANCE INTENTIONS: CONSIDERATIONS OF FORMAL AND INFORMAL MODES OF CONTROL

by

Shaun Stewart

Florida International University, 2021

Miami, Florida

Professor George Marakas, Major Professor

With the continued advancement in computer and digital technologies, companies, institutions, and organizations worldwide have leveraged new information technology to increase efficiency and effectiveness for all aspects of their business functions. Oftentimes, the information processed and stored on information systems poses an information security risk to the organization, employees, and clients alike. Therefore, a comprehensive and effective information security management program is essential to protecting data from accidental or intentional exposure to actors who wish to gain access to data to make a profit by selling the information to the highest bidder, utilize the stolen data for their own internal research and development, or use the data to damage a targeted institution for nefarious motives.

Employees' compliance with corporate information security policies is a necessary component to the success of the corporate information security management program. In this study, I adopted the control theory and developed a research model to explain how formal and informal organizational controls affect employees' intentions to

comply with information security policies. To test the model, I collected data from 303 respondents about their perceptions of their organizations' formal and informal control modes along with their respective intentions to comply with information security policies.

SEM-PLS analysis provided results that were only partially in consonance with previous studies and showed some additive effects when control modes were combined into a single model. I found clan control (informal) to have a significant and positive effect. I also found that adding the informal control modes into the model resulted in a different effect by rendering input control (formal) and self-control (informal) insignificant and changing the direction of the relationship of outcome control (formal) and behavior control (formal). In turn, these findings can help organizations set up proper controls to protect themselves from cyber threats and establish the most effective methods of control based on organizational context and control theory to ensure employees' compliance with the established information security policies of their organizations.

TABLE OF CONTENTS

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

FIGURE PAGE

ABBREVIATIONS AND ACRONYMS

SETA	Security Education, Training, and Awareness	32
SRM	Security Risk Management	1

CHAPTER I. INTRODUCTION

Companies in multiple industries rely on the ability to share data among employees and outside of the organizations to further their business interests and to increase the effectiveness of business operations. As a potentially primary means of intellectual property, data can sometimes be commercially sensitive, with the sharing of this data being a requirement to meet commercial needs (Hunt, 2018). Companies may collect data on a wide array of information. For many organizations, information on financial, healthcare, academic, and personal information help drive commercial goals (Roman, 2014). Even with the many similarities of data usage across organizations, the Security Risk Management (SRM) programs of companies vary widely from one company to another and from one industry to another based on local policy, perceived threat, and general security culture (D'Arcy & Hovav, 2007; Guo et al., 2011). Securing Information Technology (IT) systems within an organization is highly complex and requires management to be committed to striking a balance between achieving and maintaining a commercially reasonable level of protection and meeting the research goals of the entity (Roman, 2014).

The risk of doing nothing to protect the critical information system (IS) infrastructure of an organization is too great to ignore. One thousand four hundred and seventy-three data breaches occurred in the United States in 2019, and 164.68 million sensitive personal records were exposed in the country within the same year (Statista, 2020). These numbers have increased from 157 and 66.9 million from 2005, resulting in an 838% increase in data breaches and a 146% increase in sensitive personal data exposure within a 14-year period (Statista, 2020).

The implications of data breaches to organizations are quite striking. Some of the data collected and maintained by organizations must be protected by law. Examples include personal identifiable information (PII) i.e., full name, social security numbers, dates of birth, addresses, driver's license numbers, banking information, etc. Loss of this data caused by a breach could inflict reputational, legal, economic, and operational damage to an organization. Additionally, a data breach could impact future business opportunities as well as prosecution or civil penalties due to mismanagement of secure data. Network attacks could also lead to infrastructure damage that could cripple activities until the network is repaired, thus exacerbating the cost burden resulting from a lax security infrastructure (Hunt, 2018).

Cyber-attacks compromise vast amounts of data for individuals who have contact with compromised organizations. On April 15, 2015, the U.S. Office of Personnel Management (OPM), the U.S. Federal Government's human resource management agency, identified a malicious code incorporated into its IS that had been lingering in the network for approximately one year without being detected due to porous security practices. Consequently, hackers were able to use stolen legitimate credentials from employees to gain access to and infect the network with malware that exfiltrated information on more than 20 million people, many of whom held security clearance and included an unidentified number of background investigations containing personal finances, past substance abuse, psychiatric care, lie detector results, and notes about whether an applicant engages in risky sexual behavior for some of the government's most sensitive jobs and approximately 5.6 million digital images of government employee fingerprints (Koerner, 2016). Large-scale information breaches of this magnitude not

only affect the individuals whose data were compromised, but also affects national security by allowing foreign actors to target individuals with sensitive access to governmental information for nefarious reasons.

In addition to imperiling government organizations due to lax security practices in IS security, the healthcare and insurance industries also face risks due to failing security practices. In February 2015, cyber attackers conducted a massive cyber-attack aiming against health insurer Anthem Inc. The attack affected 78.8 million individuals and cost Anthem $260 million on security-related issues alone, which includes $2.5 million for consultants, $115 million for security improvements, $31 million for initial notification to the public and affected individuals, and $112 million for credit protection to those affected. Ensuing investigations found the attack began with a phishing email sent to an employee containing malicious files that allowed remote access to dozens of systems within the Anthem IS network architecture. Anthem found that the weakest link in an organization's security is human beings (McGee, 2017). Insurance information contains very personal medical, financial, and personal identifiable information data that can be used by nefarious actors to steal identities, gain financial access, or blackmail individuals with the release of information that the targeted individuals may want to remain confidential.

The financial sector has long been a target of hackers wanting to either inflict harm on the U.S. critical financial infrastructure or target individuals for illicit activities. In 2017, state actors targeting the consumer credit bureau Equifax and stole data on nearly 150 million Americans (Krebs, 2020). In a statement on the breach, Equifax announced some of the affected individuals were from the United Kingdom and Canada

but did not provide a specific number. The data extracted included names, social security numbers, birth dates, addresses, and driver's license numbers. Equifax's response to the breach including slow response to patch vulnerabilities, and general haphazard approach to IS security was described as ill-conceived, and a dumpster fire (EPIC, 2021). Data breaches within the credit bureaus could cause companies to deny individuals access to credit cards and/or loans, rent-an-apartments or houses to individuals, charge individuals higher interest rates on credit, or offer employment, and could result in distress and anxiety in the individuals affected.

Data breaches such as these can be very expensive for organizations. In 2016, IBM and the Ponemon Institute conducted a joint study that found IS security breaches cost companies an average of $4 million each in the short-term, which denoted a 29% increase in just three years. In the long-term, these costs could be as much as $7.01 million per company and potentially even higher in the financial services industry accounting for lost customers. This study found that 50% of breaches were caused by malicious or criminal attacks, 27% from system glitches, and 23% from negligent employees, thereby indicating the need for protection against internal and external threats (Champion Solutions Group, 2021). With nearly one-quarter of the breaches stemming from employee negligence, companies have a vested interest to look beyond just the technology and network defense perspective and focus on employee compliance with IS usage and the intention to comply with corporate information security policies (ISPs) to help prevent these breaches from occurring.

Technological solutions have not been enough to reduce the risks posed by information security-related compromises. Empirical evidence points to an increasing

number of increasing security-related incidences even when companies invest more in technological solutions (Bulgurcu et al., 2010). For example, a 2007 study conducted at the University of Maryland was the first to evaluate the near-constant rate of attacks on computers with internet access. The study found that on average, a network is attacked every 39 seconds. Most of these attacks are not targeted specifically to an individual or institution either. Hackers have been observed to employ automated scripts that indiscriminately, and randomly, seek out thousands of computers looking for vulnerabilities. Of the computers observed in the study, each experienced approximately 2,244 attacks per day with a view to inserting undetected entrances into the computers so hackers could create botnets (networks of infected computers) to be used for profit in the form of fraud and identity theft or to disrupt other networks and damage files ("Study: Hackers Attack Every 39 Seconds," 2007). The most successful information security programs are attained when organizations invest in both technological solutions and social solutions (Bulgurcu et al., 2010).

To help industries deal with information security issues both technically and managerially, regulatory bodies have stepped in. As a result, many industries now confront increasing global regulations concentrating on cyber and information SRM practices. These industries have instituted technological and organizational changes in response to privacy and data protection information security legal requirements. More specifically, many industries have organized SRM departments within the larger Enterprise Risk Management (ERM) divisions to manage security. SRM programs can help organizations minimize the risk of security breaches. Hunt (2018) suggested that institutions should take the following steps to manage a SRM program:

- Identify information assets, evaluate vulnerabilities, establish management priorities
- Establish effective oversight and reporting of information risks between the institution's board and the owners, controllers, and users of information assets
- Implement appropriate general and targeted network controls, including sharing and updating awareness of vulnerabilities and practices internally and externally.

These recommendations are great for security risk analysis and the initial implementation of an SRM program. However, the lack of employee adherence to security-related policies and directives is a common SRM issue experienced by firms. This problem results in employees not only failing to secure the cyber network and information but could also add to the risk of exposing sensitive information to nefarious actors. Thus, some of the salient components necessary for an SRM program to be effective are clear, fair, and complete policies that inform employees of the appropriate and legitimate use of IS resources, point out consequences of noncompliance, and provide guidelines as to what employees should do to ensure information security while they use the systems for their job responsibilities (Bulgurcu et al., 2010; D'Arcy & Hovav, 2007). Information Security Policy (ISP) awareness is negatively associated with IS misuse intentions. Similarly, greater awareness of the corporate SRM is negatively associated with IS misuse (D'Arcy & Hovav, 2007); thus, the intention to comply with corporate ISPs is a necessary component to the success of the corporate SRM program.

IS literature has suggested that to improve ISP compliance (ISPC), certain organizational controls are necessary (Chang & Ho, 2006; Eisenhardt, 1985; Hsu et al., 2017; Jaworski, 1988; Keil et al., 2013; Kirsch, 1996, 1997; Kirsch et al., 2002, 2010; Kohli & Kettinger, 2004; Mähring, 2002; Mao et al., 2008; Ouchi, 1979, 1980; Ouchi &

Maguire, 1975; Phillips, 2013; Remus et al., 2016; Sitkin et al., 2020; Vlasic & Yetton, 2004; Wiener et al., 2016). According to several studies, both formal and informal controls influence employee behavior in accordance with organizational goals and create the procedures necessary to influence employee intentions to follow rules and policies such as ISPs (Phillips, 2013). Outcome control, behavior control, and clan control have all been deemed necessary to ensure goal alignment between management and employees to enhance employee compliance (Henderson & Lee, 1992; Kirsch, 1996, 1997; Kirsch et al., 2010). In this context, some research suggests that formal and informal control modes have an additive effect on compliance and intentions to comply with policies and directives (Bateman & Crant, 1993; Buchanan II, 1974; Henderson & Lee, 1992; Jaworski et al., 1993; Kohli & Kettinger, 2004; Waterhouse & Tiessen, 1978). These organizational controls allow organizations to ensure goal alignment between themselves and employees (Henderson & Lee, 1992).

For this study, I used the control theory with behavior control, outcome control, input control, clan control, and self-control to explain factors that affect employees' intentions to comply with ISP to address the research question: To what degree do formal and informal organizational controls affect employees' intentions to comply with ISPs? I found that outcome and behavior control had a significant and negative effect on ISPC intentions, while clan control had a significant and positive effect on ISPC when considered within the context of the hypothesized research model counter to previous studies on formal and informal control effects on ISPC.

CHAPTER II. LITERATURE REVIEW

Internal controls' effects on various outcomes of IT security have been the subject of academic research over the last 50 years (Andress, 2003) and is situated within the broader topic of ERM and Risk Management (RM). SRM has been understood by many practitioners as information risk; however, with the increasing use of IS to store and process data, the old ways of understanding information security were not keeping pace with the rapid technological advancements (Blakley et al., 2001). Further, risk management was viewed as a side-note; an understood function, but one that was not a core business function of many enterprises. It was a function that was to be invested in but had no discernable return on investment (Morgan Stanley, 2017).

More recently, companies have come to understand that although risk management does not make money, it can save money in the long run (Morgan Stanley, 2017). As a result, many in the field of risk management are now recognizing the need to infuse risk management plans into the overall strategies of a company so that the entity's appetite for risk and risk utilization are considered when the company is developing strategic objectives and plans (Edelman et al., 2019).

Over the years, companies have started to realize that their traditional view of risk management (financial risk composed of market, credit, asset and liability, and liquidity) has left lacunae in the risk management strategy (Edelman et al., 2019). Since the 1990s, information risk management has come to be seen as a profession that requires specialized education, an ethical obligation to treat clients appropriately, maintain the integrity and security of client private information, and a professional obligation to report data threats to the proper authorities in order to maintain the integrity of our economic

institutions (Blakley et al., 2001). Additionally, companies have begun incorporating varied structures to address the gap in SRM by developing the position of Chief Risk Officer (CRO) and risk professionals to focus solely on SRM (Edelman et al., 2019).

As a subset of an organization's SRM function, ISPC is a body of research in the IS field that specifically deals with employees' intentions to or actions of complying with an organization's ISP. Multiple theoretical perspectives have been used to assess ISPC including control theory, general deterrence theory, and rational choice theory (Chang & Ho, 2006; D'Arcy et al., 2009a; Dugo, 2007; Guo et al., 2011; Kirsch, 1996, 1997; Kirsch et al., 2002, 2010; Li et al., 2010; Ouchi, 1979, 1980; Ouchi & Maguire, 1975; Phillips, 2013; M. T. Siponen et al., 2010; Vance & Siponen, 2012; Xue et al., 2011). Control theory defines control as organizational actions designed to increase the chances that employees will behave in ways that will support attainment of organizational objectives. Control is a tool that organizations use to formalize the organizational structure. Organizational control, either formal or informal, forms the rules and procedures used to establish the foundation of properly functioning organizations (Phillips, 2013). The more IS-related processes an organization can monitor, the greater the likelihood of the organization identifying deficiencies in IT management and set policies and procedures to model the best practices and mitigate the deficiencies. Therefore, the control theory is an appropriate theory to consider ISPC in terms of using managerial controls to influence employee behavior and enhance organizational outcomes (Phillips, 2013).

IS literature suggests that formal and informal controls for organizational information security programs include implementing good management policy and

oversight (Chang & Ho, 2006; Eisenhardt, 1985; Hsu et al., 2017; Jaworski, 1988; Keil et al., 2013; Kirsch, 1996, 1997; Kirsch et al., 2002, 2010; Kohli & Kettinger, 2004; Mähring, 2002; Mao et al., 2008; Ouchi, 1979, 1980; Ouchi & Maguire, 1975; Phillips, 2013; Remus et al., 2016; Sitkin et al., 2020; Vlasic & Yetton, 2004; Wiener et al., 2016). Formal controls are a subset of internal controls where managers set policy, monitor, and control inputs supplied to employees, outcomes of employee labor, and employee behavior (Hsu et al., 2017; Jaworski, 1988; Keil et al., 2013; Kirsch, 1996, 1997; Kirsch et al., 2002, 2010; Kohli & Kettinger, 2004; Mähring, 2002; Mao et al., 2008; Ouchi, 1979, 1980; Ouchi & Maguire, 1975; Remus et al., 2016; Sitkin et al., 2020; Vlasic & Yetton, 2004; Wiener et al., 2016). While managers have a wide array of controls they could use to influence employees to comply with ISPs, formal sanctions and rewards are two of the formal controls used most often to influence employee behavior concerning the intentions to comply with company's ISP (Vance & Siponen, 2012). These controls, used in conjunction with technology solutions, will provide organizations with a stronger overall IS security (ISS) and SRM program (Chang & Ho, 2006; Phillips, 2013).

Informal controls are another subset that use social pressure from peers to persuade employees to conform with organizational policies (Brief & Aldag, 1981; Choudhury & Sabherwal, 2003; Chua et al., 2012; Henderson & Lee, 1992; Jaworski, 1988; Kirsch, 1996, 1997; Kirsch et al., 2010; Kohli & Kettinger, 2004; Manz et al., 1987; Ouchi, 1980; M. Siponen et al., 2007; M. T. Siponen et al., 2010; Wiener et al., 2016). Research indicates that people in the same workgroup have more influence on employee intention to comply with ISPs than others in the organization. Furthermore, social influence from peer groups has been reported to be a stronger predictor of behavior

than influence from people in other social groups—even in the same organization (Guo et al., 2011). These informal controls can be used to achieve higher levels of control over employees' intentions to comply with ISP (Bateman & Crant, 1993; Buchanan II, 1974; Henderson & Lee, 1992; Jaworski et al., 1993; Kohli & Kettinger, 2004; Waterhouse & Tiessen, 1978).

However, it is still unclear how formal control and informal controls work in unison to influence employees' intentions to comply with ISP. Research indicates that job performance, in addition to sanctions and informal controls, influences employees' intentions to comply with ISPs, and that employees actually care more about job performance than ISS (Guo et al., 2011). Employees utilize a cost-benefit analysis with intentions to comply with ISPs and are more likely to comply when perceived benefits override potential risks from formal sanctions and security threats (Li et al., 2010). In general, research suggests that formal and informal controls can work together to influence both benefits associated with and sanction levied against compliance with ISPs.

The overall purpose of ISPC in an organization is to enhance the effectiveness of the organization's information services both within and external to the organization (Chang & Ho, 2006). Managerial control provides an organization with the ability to target outcomes, reduce costs, and mitigate risks of failure (Phillips, 2013). These managerial controls could take the form of formal or informal control modes or a mixture of the two. Thus, in conjunction with technological solutions companies use to ensure ISS, I believe managerial control is an essential element to an effective ISPC and SRM program. In the following, I discuss the literature related to various formal and informal controls based found in the control theory.

2.1 Input Control

Input control is closely associated with a more traditional resource management within an organization. For the input control mode, the principal specifies, monitors, and manipulates the human, financial, and material resources available to accomplish an activity (Jaworski, 1988; Mähring, 2002). This mode includes funding, labor force, staff recruitment and replacement, training, and other forms of resource allocation (Wiener et al., 2016).

The selection of this type of control mode has been found to be largely contingent on the environment in which the organization finds itself operating. For example, companies in low uncertainty environments will find it more beneficial to adopt a stronger behavior and outcome control mode, whereas companies with high uncertainty environments will find it more advantageous to adopt a higher informal mode (Mao et al., 2008) and input mode (Vlasic & Yetton, 2004) of control.

When using the input control mode, agents are motivated through reward. Rewards are based on the agent's ability to efficiently use the resources the principal provides (Wiener et al., 2016). Unlike rewards, sanctions are also used to motivate agents to ensure efficient use of resources. Agents are more likely to submit to the control of principals when they depend on principals for rewards or are liable to principals for sanctions (Kohli & Kettinger, 2004). This phenomenon is also linked to behavior control and outcome control (Wiener et al., 2016).

2.2 Outcome Control

Outcome controls are managerial performance measures on cost, schedule, target dates, budgets, project milestones, and other expected levels of performance (Vlasic &

Yetton, 2004). Managers can exercise outcome controls by identifying tasks with specific timelines and providing evaluations based on performance and task-completion (Hsu et al., 2017). Notably, both outcome controls and input controls are basal managerial philosophies within organizational control theory, whereby the manager controls the inputs, outcomes, timelines, budgets, manning, hiring, and firing capacities within working teams.

Most research on control antecedents has focused on observing behaviors, measuring outcomes, or transforming inputs to outputs (Kirsch et al., 2010). In the earlier research of antecedents to organizational control, behavior control and outcome control were tested against one another as the two key modes of organizational control. Evidence suggested that outcome control and behavior control are not substitutes for one another and are independent (Ouchi & Maguire, 1975).

When Ouchi developed the first framework for determining which types of control would be most effective, he found that an organization should lean more toward formal controls for the most effective means of control when its ability to effectively and efficiently measure output was high and knowledge of a transformation process was perfect. Contrastingly, informal controls should be selected if the ability to measure outputs is low and knowledge of a transformation process is imperfect (Keil et al., 2013). Ouchi's framework and subsequent tests of formal and informal control on process performance neglected to consider input controls within the formal controls framework as first-order dimensions of control (Keil et al., 2013).

Outcome control places greater emphasis on whether predefined goals are accomplished, to what degree of quality they are accomplished, and if they are

accomplished within a pre-determined timeline. However, it pays attention to how they are accomplished, or the process of accomplishment, which would be more focused on the input mode of control. Outcome control is more appropriate for conditions in which controllers can trust controlees to perform the tasks effectively (Kirsch, 1997).

2.3 Behavior Control

Behavior control refers to the formal control mode that an organization may undertake to accomplish goals most efficiently and effectively. Within the behavior control framework, principals define the steps and procedures for carrying out a specific task and evaluate performance according to agents' adherence to the process and procedures (Kirsch et al., 2002).

For the behavior control mode, group performance is predicated on how closely the group conforms to predefined procedures, methods, and techniques. Performance evaluation is not predicated on high levels of members' effectiveness; however, it does require principals to collect and analyze large copious amounts of data relating to the agents' adherence to the organization's expectations (Hsu et al., 2017). With behavior controls, principals may establish baseline norms with items such as production rules to ensure agents comply with action-based standards that outline the manner in which subordinates should perform tasks. Rewards are often used to reinforce desired behaviors leading to this mode to be most effective with agents who value stable, consistent, and predictable directives that allow for the agent to capture process efficiencies to earn rewards (Sitkin et al., 2020).

Both behavior and outcome controls share the assumption that the principals and agents align goals by providing the agents with appropriate incentives (Kirsch et al.,

2002). This alignment can be reached by either controlling for the process in the case of behavior control or the extent to which predefined goals are achieved. The relationship with the behavior control mode is viewed as dyadic in that a principal exercises control over an agent influencing the behavior for the goal alignment to occur (Remus et al., 2016). Key characteristics of the behavior control mode include the principal specifying and monitoring rules, procedures, and processes while imputing rewards or sanctions based on the agents' adherence to the desired behaviors. Mechanisms for this mode are: mandated IS development methodology, status meetings and conference calls, walkthroughs, and routine/recurring reports (Wiener et al., 2016).

The increasing complexity of tasks and information requirements will eventually render the rules governing behaviors in the behavior control view less effective, which will ultimately lead to the development of clan control systems (Sitkin et al., 2020). Further, in a group setting, individuals will safeguard their group commitment by insisting on equality and full participation to prevent free riding; however, the unintended consequence of this is the creation of boundaries around the group classifying members as either insiders or outsiders further ushering in the clan control mode (Tansey & Rayner, 2009).

2.4 Clan Control

The clan control mode refers to individuals who depend on one another, share a set of common goals, and espouse and promote a common philosophy, values, and beliefs (Ouchi, 1980). This can be best seen in situations where the professional employees and management differ in knowledge, skills, and/or abilities, such as in hospitals, law firms, and other professional firms which may be run by managers who do not have the same

skills as the employees. The clan control mode emphasizes the professional clan and lowers dependence on the organization's management.

Clan control operates when behavior [in a peer group] is motivated by shared values and norms and a common vision (Kirsch et al., 2010). In highly centralized clan environments, lack of principle legitimacy in management results in clan control rather than managerial control, producing higher success in behavioral change (Kohli & Kettinger, 2004). Clans may influence members, and when clans include management-provided information, they may appeal to members' values and beliefs, which can, in turn, lead to greater commitment and compliance from members. This can result in greater goal congruence between the clan and management (Kohli & Kettinger, 2004).

Clan control mechanisms, such as ceremonies and rituals, social sanctioning, and other socialization activities, aim to promulgate and establish shared group norms and values, as well as to identify and enforce commonly accepted behaviors (Kirsch, 1996, 1997; Ouchi, 1980). While clan controls are primarily implemented by the controlees, the controller, who is often outside of the peer group (Chua et al., 2012), can promulgate the development of shared norms and values amongst controlees (e.g., through collocating project team members) (Choudhury & Sabherwal, 2003).

Clan control may be leveraged by controllers and create a positive direct effect on project performance, project cost, and project quality; however, clan control can also have a negative direct effect on project efficiency and project ambidexterity (Wiener et al., 2016). If an organization is using the clan control mechanism, and the clan diverges from the goals, policies, or procedures (behavior control) of the organization, management will eventually need to address a control congruence issue.

Normative beliefs and social disapproval sanctions have a significant direct effect on employees' intention to adhere to IS security policies and procedures (Siponen et al., 2007). Clan mechanisms that control the normative beliefs and social disapproval sanctions for a group will have a strong effect on the group's intentions to comply with policies from management, which would be viewed as lacking legitimacy for the group (Kohli & Kettinger, 2004). Managers must realize when a clan situation has emerged and decide how to best capitalize this control mode in order to inspire employees to follow corporate IS security policies and best practices so that the clan control mode can impart maximum benefits to the organization.

2.5 Self-Control

Manz et al. (1987) defined the self-control mode as a function of intrinsic motivation. Self-control has been further defined as individual standards and objectives (Jaworski, 1988). In this mode, the controlee sets the goals and the actions required to achieve these goals themselves. The controlee further self-monitors his/her behavior and implements all facets of this control mode (Choudhury & Sabherwal, 2003; Henderson & Lee, 1992; Kirsch, 1996).

In this informal control mode, the controller does possess the ability to promote self-control, but cannot directly control this mode with traditional managerial levers or influence. The controller may be able to promote self-control by enabling employees through routine personnel reviews, by encouraging employees through making recommendations for actions or strategic guidance for a project, or by requesting the controlee implement different directions to projects (Brief & Aldag, 1981; Kirsch, 1996; Wiener et al., 2016).

This control mode will work well so long as the controlee's intrinsic motivations, standards, and objectives inherently align with those of the organization. However, this mode will likely be difficult to manage if a divergence begins to emerge in these motivations, standards, and objectives. Managers will have to use a more collaborative approach and less of a directive approach to divergences of standards and objectives while maintaining a focus on responding to the employee' intrinsic motivations (Kirsch, 1996; Wiener et al., 2016).

2.6 ISPC Intentions

SRM comprises an organization identifying potential risks to its ISS posed by both internal and external threats. These threats take the form of compromised sensitive information stored on internal systems, determining the probability of the risks occurring against the IS, prioritizing the risks based on an internal risk/loss calculation, and subsequently developing and incorporating policies, procedures, and training to mitigate risks in accordance with internal risk acceptance/avoidance calculations (Morgan Stanley, 2017).

All major organizations store proprietary and/or sensitive information relating to proprietary information that could be of value to competitors that, if stolen, can be sold on black markets for monetary gain, employee, and/or client information that could be valuable to those interested in stealing personal identities, or internally sensitive/proprietary information that competitors and foreign governments would rather steal than expend their own resources to develop. In recent years, major data breaches have been identified in the banking industry, universities, high-technology companies,

and the government (“Cybersecurity Incidents,” 2020; “The Boeing Breach: How an Employ Slip-Up Cost Colleagues,” 2017; Gatlan, 2019; Roman, 2014; Thomas, 2019).

CHAPTER III. THEORETICAL BACKGROUND

Now that companies realize the need for attention to employees' intentions to comply with information security policies and the overall SRM program, structure and policy have been established to address the issues associated with SRM. Additionally, employees are expected to adapt to the changing environment. Furthermore, measurements of effectiveness must be incorporated to assess whether the current SRM strategy is effective. Deterrence, clarity in policies, and systems auditing are the direct antecedents to security effectiveness (Mishra & Chasalow, 2011). This notwithstanding, control portfolio configuration and control enactment with both formal and informal control modes have shown to significantly affect IS projects in particular (Wiener et al., 2016).

The control mode or blend of modes that an organization exercise over employees who directly take part in SRM may create strengths and weaknesses associated with the effectiveness of a SRM program. Behavior control has demonstrated a positive direct effect for constructs such as project ambidexterity, project performance, and project efficiency. On the other hand, outcome control has shown a positive direct effect on project performance, project efficiency, and project quality. Clan control has shown a negative direct effect on project ambidexterity and project efficiency but has also exhibited a positive effect on project performance, project cost, and project quality; and self-control has demonstrated a positive direct effect on project performance and project quality but also showed a negative direct effect on project performance in certain cases (Wiener et al., 2016). Appropriate blends of control modes will likely have positive effects on project outcomes, and as a consequence, management programs, which

management can use to better control outcomes and overall effectiveness of an RM program.

The overarching theoretical concept addressing these issues resides in organizational control theory. Organizational control theory postulates that control allows a firm to ensure firm goals and employee goals are aligned and that employees adhere to the firm's goals and objectives (Henderson & Lee, 1992). Besides dividing control into formal and informal control modes, control theory further divides formal control into behavior control, outcome control, and input control. Furthermore, it divides informal control into clan control and self-control (Eisenhardt, 1985; Jaworski, 1988; Kirsch, 1996, 1997; Kirsch et al., 2010; Ouchi, 1979; Wiener et al., 2016).

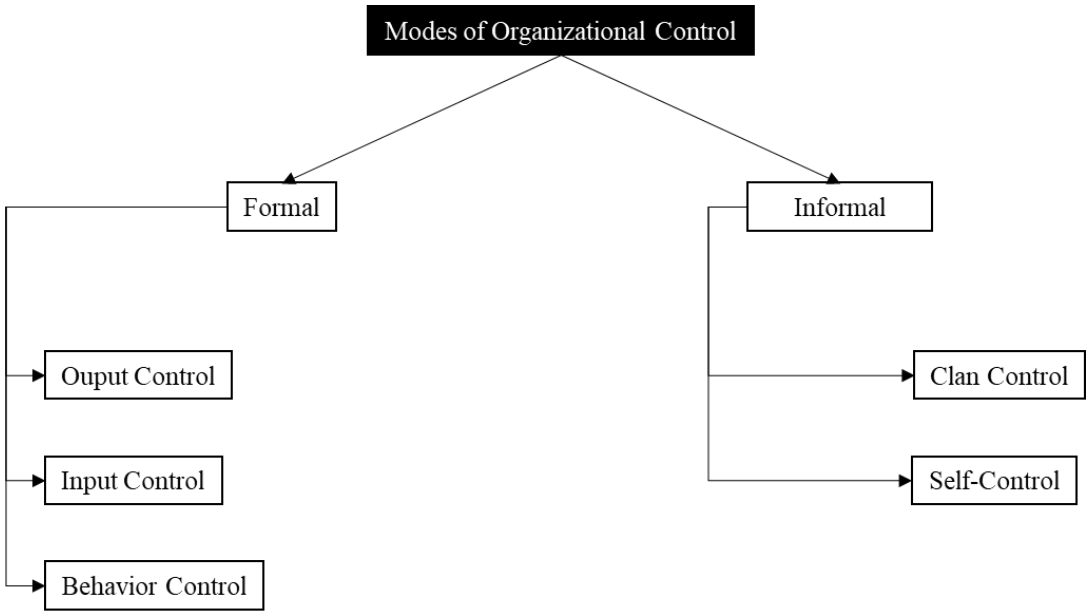


Figure 1: Control Theory (Eisenhardt, 1985; Jaworski, 1988; Kirsch, 1996; Kirsch et al., 2010; Ouchi, 1979; Wiener et al., 2016

Multiple theories underlie organizational control theory. Chief among the underlying theories Principle-Agent Theory where the controller plays the role of the principal and the controlee plays the role of the agent (Wiener et al., 2016). In principal-

agent theory, the principal is someone within the organization that has an ownership interest and who then entrusts an agent with the responsibility of working on his/her behalf to execute operational tasks (Eisenhardt, 1989; Fama & Jensen, 1983). This relationship can then create what is referred to as the fundamental challenge of control: information asymmetries between the principals and agents, risk of moral hazard, and/or time and cost constraints associated with exercising control (Dalton et al., 2007; Fama & Jensen, 1983).

CHAPTER IV. RESEARCH MODEL AND HYPOTHESES

Theories of organizational control consider the processes managers use to influence employee behavior for a given outcome. Research has indicated that formal control mechanisms—input control, outcome control, and behavior control—and informal control mechanisms—clan control and self-control—are the primary factors that will influence the effective implementation of a particular program (Gossett, 2009; Jaworski, 1988; Jaworski et al., 1993; Kirsch, 1996, 1997; Kirsch et al., 2002, 2010; Mähring, 2002; Ouchi, 1979, 1980; Ouchi & Maguire, 1975; Remus et al., 2016).

This study aims to examine the relationships between these control modes and their effects on the employee ISPC intentions in the United States. My first hypothesis considers the relationship between the input control mode and the ISPC intentions.

For the input control mode, the manager sets, monitors, controls, and manipulates all resources available to complete a stated task (Jaworski, 1988; Mähring, 2002). Further, for this control mode, the manager will control the resources that are provided as the *input* for a given product, process, or service. If a controller maintains visibility on the goal of ISPC, he or she will be able to adjust all facets of resources used to create the program directly with a view to achieving this goal. For this reason, I hypothesis the relationship will be direct and ISPC will increase as input control increases.

For the purposes of this study, ISPC is defined as employee intention to comply with corporate ISPs. The goal of effective ISP programs is to mitigate the chances of human error, loss of intellectual property, espionage, information extortion, sabotage or vandalism, theft, software attacks, forces of nature, degraded service quality, hardware

failures, software failures, and/or technological obsolescence (Huang et al., 2010). See figure 2 for the research model and hypotheses.

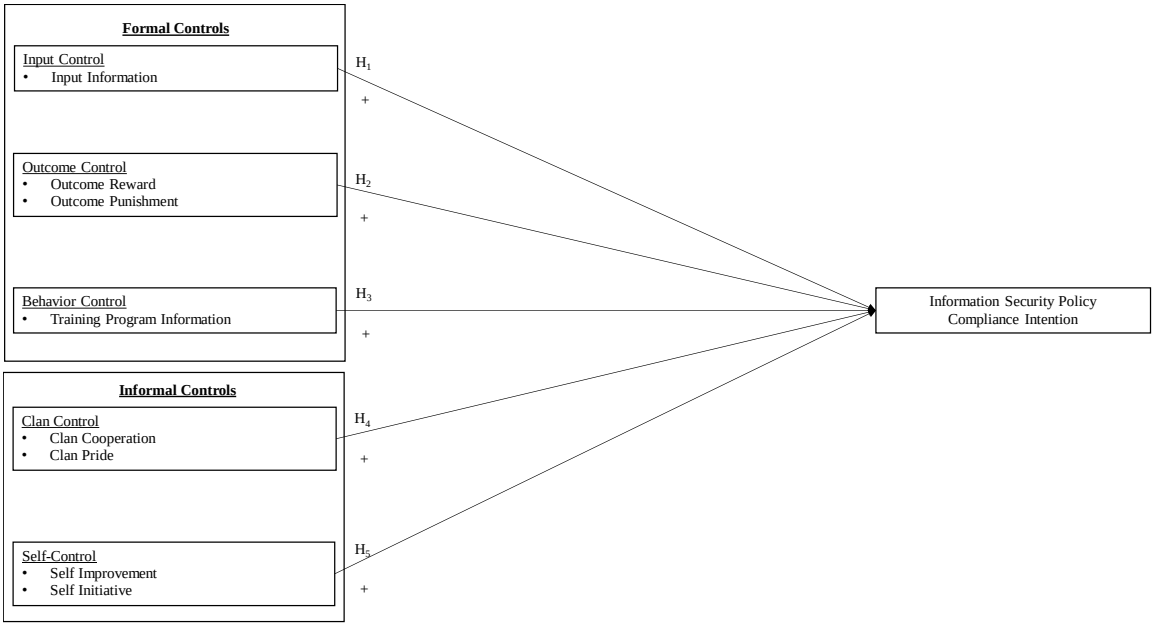


Figure 2: Theoretical model of the hypothetical relationship of formal and informal corporate control modes on ISPC intentions

H_1: *Input control will have a positive, direct effect on ISPC intention*

Challagalla and Shervani (1996) identified three factors reflective of the input control mode of organizational control—information provided to employees from managers regarding the functional effectiveness, rewards provided to employees based on utilization of inputs, and punishments based on deficient use of inputs. Correspondingly, Jaworski (1988) and Mähring (2002) provided evidence that the input control variable will have a positive, direct effect on IS projects.

Hypothesis two considers the relationship between the outcome control mode and ISPC intentions. Ouchi (1975) describes outcome control as the managers' ability to measure and control the output of employees conducting particular tasks. This is closely related to the aforementioned input control mode wherein the controller has the ability to monitor, control, and manipulate the output levels of a task based on the desired results.

This is another classical control mode where the controller possesses unlimited ability to control all aspects of the work function—in this case output.

Within this control mode, if a controller maintains visibility on the goal of executing a successful ISPC program, he or she will successfully manipulate and adjust the output levels, thus controlling the perceived effectiveness of the target organization's SRM program.

H_2: *Outcome control will have a positive, direct effect on ISPC intention*

Jaworski (1993) and Challagalla and Shervani (1996) identified two constructs for outcome control as was found for input control. Information, rewards, and punishments, all of which comprise the outcome control construct. The only difference between input control and outcome control using Jaworski's (1993) conceptualization is what the controller is controlling. The controller will use these three factors to either control the material that goes into a function or control the outcome by controlling the information, rewards, and punishments given to employees.

Ouchi (1975) first elucidated the behavior control mode as a separate mode from outcome control, which to this point had been considered as serving the same purpose and freely substitutable of one another. He found that output measures were important for communicating performance in large organizations, but also observed that this would not be required in smaller, less complex organizations where each person can view the output of all the others. For this reason, he reasoned that behavior control would be the necessary mode for promoting efficiency in the organization and that a manager will rely more on behavior control modes as his or her understanding of the means-ends relationships increases.

The idea that behavior control will have an impact on the performance of a project was later viewed through the lens of organizational citizenship behavior theory. Although this framework was not specifically designed for security-related behaviors, it does lend itself to behaviors of practicing good password management procedures and refraining from risk-related activities, such as downloading illegal software to workplace computers (Stanton et al., 2004).

The more control managers can affect employees' security-related behaviors, by exerting greater control in aligning their behaviors with the SRM program's desired outcomes. The behavior of employees who use the organization's IS is a critical antecedent for the security of these network systems, and constructive behavior will enhance the security effectiveness whereas destructive behaviors will reduce this effectiveness (Stanton et al., 2004). Thus,

H_3: *Behavior control will have a positive, direct effect on ISPC intention.*

Shifting focus from the direct effects exerted by formal control modes to the indirect effects mediated through informal control modes, clan control will exhibit a range of influences on the ISP program of an organization. Unlike the formal control modes, clan control does not allow the controller to directly impact the subordinate employees' activities and behaviors. This mode is best seen in organizations where the employees have a skill set not held by the management, thus reducing managerial influence on the employees, such as a hospital where the management of a hospital does not typically comprise medically-trained doctors (Kohli & Kettinger, 2004).

In such a situation, the controllers lack legitimacy. If clan goals are not aligned with managerial goals, there will be an incongruence as well as lack of efficiency and

effectiveness of the desired outcome. In turn, this will degrade the effectiveness of the formal control modes of input, outcome, and behavior control.

There are situations wherein controllers can use the clan control mode to manipulate the clan to perform in a certain manner in order to achieve a desired end-result. Kohli and Kettinger (2004) found that one such manner is co-opting a respected member of the clan who can exercise direct influence over the clan. By using indirect managerial oversight techniques, controllers will be better situated to influence outcomes, inputs, and behaviors of clan members. This will in effect create a mediated relationship between behavior control and the perceived outcome of ISPC intentions through the clan control mode.

Furthermore, clan control is a control mechanism in its own right. This allows the clan to make decisions, set goals, control behavior, and oversee outcomes internally without the input or direction from outside managers (Kohli & Kettinger, 2004). Depending on the alignment between the clan and that of the management, this will allow the clan to directly affect the perceived effectiveness of ISPC intentions. Allowing the goals of the clan and management to be aligned will have a positive direct effect, whereas misalignment will have a negative direct effect on the program.

H_4: *Clan control will have a positive, direct effect on information security policy compliance intention.*

Empirical research conducted by Buchanan (1974) and Waterhouse and Tiessen (1978) identified seven items with three possible factors that reflected the construct of clan control. Measuring the degree of professional interaction, feedback, and evaluation between marketing professionals, Waterhouse and Tiessen identified five items that

reflected standard-setting and monitoring within the professional domain (Jaworski et al., 1993). Their (1978) research contributed to the empirical research conducted by Buchanan (1974) which identified two professional, cultural control items. Together, the seven items compose three possible factors: cooperation, familiarity, and pride (Jaworski et al., 1993).

Like with clan control, there are techniques managers can use to allow for high self-control with employees on a particular project while still exerting indirect influence over the self-control mode. The combined effect of managerial and self-control will have a positive effect on IS design and performance, thus indicating a mediated relationship between behavior control and ISPC intentions through the self-control mode (Henderson & Lee, 1992).

Self-control is a control mode in its own right. Therefore, self-control allows individuals to make decisions, set goals, control behavior, and oversee outcomes internally without the input or direction from outside managers (Henderson & Lee, 1992). Depending on the alignment of the individual's goals and management's goals, this will allow self-control to have a direct effect on ISPC intentions. Allowing the alignment of the goals of the individual and management will have a positive direct effect, whereas misalignment will have a negative direct effect on intentions.

H_5: *Self-control will have a positive, direct effect on information security policy compliance intention.*

Empirical research conducted by Bateman and Crant (1993) found that individuals possess proactive behavior in that they influence their environments through

intentional alterations of situations in ways other than selection, cognitive restructuring, evocation, or intentional manipulation of social responses.

Clan control will exhibit a range of influences on employees' ISPC intentions. Unlike the formal control modes, clan control does not allow the controller to have a direct impact on the activities and behaviors of subordinate employees. This mode is best observed in organizations where the employees have a skill set not held by the management, thus lowering the managerial influence on the employees, such as a hospital where the management of a hospital does not typically comprise medically-trained doctors (Kohli & Kettinger, 2004).

In such a situation, the controllers lack legitimacy. If clan goals are not aligned with managerial goals, there will be an incongruence and lack of efficiency and effectiveness of the desired outcome. This will in effect degrade the effectiveness of the formal control modes of input, outcome, and behavior control.

In addition to clan control, self-control individual members of a work team may exhibit their own individual control over behavior and outcome. Self-control is the extent to which an individual exercises autonomy in deciding required actions and how to execute activities for projects (Henderson & Lee, 1992). This control mode is akin to clan control in that managers have little direct control on input, outcome, or behavior but differing in that self-control is executed at the individual level and not the group. This mode removes both peer pressure and social control mechanisms used in the clan control mode.

Henderson and Lee (1992) found that this control mode is used more often when managers in an organization have no other choice of control mode, and is typically found

in highly technical fields such as IS design and performance. Although not directed at employee ISPC intentions specifically, Henderson and Lee (1992) found that increases in self-control have a positive effect on IS design and performance.

For this research study, I will consider six demographic responses. I will request the following demographic data along with the collection instrument. I do not hypothesize these demographic points will affect the relationships under observation; however, I will test the demographic data against the results to ensure there is no covariation.

Age may have an effect on employee intentions to comply with ISPs due to life experience, loss of PII, or even situations where the respondent's identity has been stolen due to lax SRM procedures.

Gender may have an effect as there may be a difference in security consciousness between genders. The strata of the organization will also likely have an impact on employees' intentions to comply with ISPs. Those at higher strata may not pay close attention to this facet of the organization as they end up dedicating time to other, higher-priority functions.

Experience working with sensitive information will likely have an effect on employees' intentions to comply with ISPs due to those with higher levels of experience may often have seen security breaches and directly experienced the effects these breaches can have on an organization's reputation, financial position, and level of trust received from clients.

The utilization of security systems will also likely play a role in employees' intentions to comply with ISPs. Those who use security protocol systems are more likely

to have a better outlook on the program than those who sporadically use systems and do not have day-to-day contact with security protocols.

Years of education can also affect ISPC intentions. It can be assumed that those with higher levels of education have worked with more and varied information than those with lower levels of education. Those with graduate degrees have likely engaged in original research where they have had to handle PII and sensitive information personally, whereas undergraduates may not have had these same experiences with data collection, storage, and security. Therefore, increased education level will likely show an increase in intentions to comply with ISPs for an organization.

CHAPTER V. METHODOLOGY

5.1 Instrument Development

For this study, all constructs were measured using existing scales found in the literature with some item modification of item wording to better fit the research model. Each instrument used in this study was utilized as reflective constructs that used a 7-point Likert scale to measure each case.

ISPC was measured using Safa et al.'s ISPC Model (2016). Input Control was measured using Challagalla and Shervani's Dimensions and Types of Supervisory Control measure (1996). Outcome Control, on the other hand, was measured using Bulgurcu et al.'s Outcome Reward and Outcome Punishment two-dimensional scales (2010). Meanwhile, Behavior Control was measured using Bulgurcu et al.'s Security Education, Training, and Awareness (SETA) two-dimensional scale, which measured general information security awareness and information security policy awareness dimensions (2010). Similarly, Clan Control was measured using Jaworski et al.'s clan control scale, which measured clan cooperation and pride (1993). Finally, Self-Control was measured using Bateman and Crant's two-dimensional self-control scale, which measured self-improvement and self-initiative dimensions (1993).

The assessment also included questions related to employee and job characteristic demographics such as gender, age, education, information awareness, industry, job position, company size, and information intensity of the home corporation. This information was used in the pilot study to determine if there was evidence of these demographic groups affecting both independent and dependent variables.

5.2 Study Design, Procedure, and Participants

An employee's willingness to comply with company policy could involve behaviors that are considered unacceptable, and this study required the collection of honest responses while also maintaining anonymity. I relied on an anonymous self-reported cross-sectional survey to meet these requirements while still adequately testing the effect of the research model following a typical practice in organizational psychology and IS security research.

According to Babbie (2016), surveys are useful in describing the characteristics of a large population. This research attempts to describe which characteristics influence employees' intention to comply with their companies' ISP generally, thus the survey methodology was selected to test selected measurable factors' influence on the observed outcome while providing a sample size representative of the age groups, industries, education levels, information security awareness, professional positions, organizational sizes, and information intensities required to make the outcomes of this study reasonably generalizable. Further, IS research has used multiple cross-sectional surveys to study self-reported behaviors (Karahanna et al., 1999; Lankton et al., 2010; Lowry et al., 2016; Moody & Siponen, 2013; Vance et al., 2012; Venkatesh et al., 2012).

Research was conducted for both the pilot and main studies using Amazon's Mechanical Turk platform to recruit respondents and Qualtrics as the survey and data collection platform. I compensated respondents $1.25 per complete survey response for the main study. I determined the compensation amount by dividing the average amount of time to take the survey (10:33) by the United States average minimum wage of $7.25 per hour. The survey was open for a total of 2:44:00 and solicited 466 total cases. In

consonance with the latest literature on the use of Mechanical Turk, in conjunction with the survey features and filtering mechanisms available through Qualtrics, the topic of interest was a good fit for this methodology due to its limited special expertise requirements, reasonable assurances of anonymity, and the ability to reach a large number of people with specific traits e.g. company size, information intensity, and industry (Goodman et al., 2013; Landers & Behrend, 2015; Lowry et al., 2016; Steelman et al., 2014).

Due to the length of the survey, to control for common method bias, and to increase attention to the survey, I incorporated multiple procedural remedies found in the literature (Goodman et al., 2013; Landers & Behrend, 2015; Lowry et al., 2013, 2016; Rouse, 2015; Steelman et al., 2014). I randomized the order of the survey questions, reversed the scaling and anchors of 33% of the instrument questions, explicated the significance of paying attention and the scientific importance of the study, tracked the time spent in completing the surveys and eliminated any that were taken unusually fast compared to the pilot test and other respondents, undertook data validation to improve data accuracy, and provided a marker control variable based on the study conducted by Richardson et al. (2009) that focused on organizational commitment and provided additional evidence for the absence of common method bias.

To control for common method bias, I added social desirability as a control variable measured by Hays et al.'s social desirability scale (1989). Van de Mortel found that the social desirability scale can be used effectively to control for respondents presenting a favorable view of themselves in self-report studies, or, in other words, to control for common method bias (2008). Common method bias could influence the

validity of research conclusions. The social desirability construct is unrelated to the theoretical model used in this study. In accordance with guidance from Lowry et al. (2016), all or most constructs would be highly correlated including the social desirability construct if common method bias was present in the sample. I assessed social desirability in the correlation matrix of all variables. Correlation between social desirability and all of the major constructs in the theoretical model and found little or negative correlations indicating that common method bias is likely not a substantial threat to this study.

The measurement instrument is based on the validated items listed in Chapter III derived from various prior research studies (see Appendix A for measurement instrument). I have made modifications to the questions in order to align better with the design and desired outcomes of this study. Tests for reliability and validity as well as new factor analyses were conducted to ensure the modified questions still measured the constructs in question, internal reliability, while also ensuring that the factors were still a strong enough reflection of the construct under consideration (Rosenthal & Rosnow, 1991).

In accordance with leading practices for Mechanical Turk studies involving lengthy surveys, I employed filters for age, established information security policies at respondents' current job, awareness of regulations prescribed by ISP, country of residence, and primary work language (Lowry et al., 2016). These filters ensured that all respondents were above the age of 18, had an established ISP, had at least a cursory awareness of the ISP, were residents of the United States, and spoke English as their primary language on the job site.

The sample population for both the pilot and main study was recruited from Amazon's Mechanical Turk. This sample allowed for participants in various industries, age groups, education levels, positions, and handling of secure information to identify any gaps in the design and methodology of the study. I restricted the respondents using Amazon Turk's filter function and survey a group of American employees who have some contact with the information security policies within their main employment institutions. Responses were used to test the measurement instruments for reliability, convergent validity, and discriminant validity prior to testing for confirmation of the hypothesized direction and strength of the relationships.

In order to clean the data, I removed respondents who showed no or very little deviation in responses indicating they unengaged responses and had the same response for all responses for the latent variables. Responses that accounted for less than 0.5 standard deviations were closely inspected and responses that were less than 0.35 were considered clearly not engaged at best or malicious at worse. I removed the responses that were clearly not useful to measuring variation in responses while keeping in mind to try and remove as little data as possible to maintain the integrity of the studies.

Next, I examined outliers. Using a 7-point Likert scale, there was not much opportunity for outliers; however, the demographic data points were assessed for outliers e.g., age, gender, education, industry, and position.

Lastly, I analyzed data skewness and kurtosis. I ran skewness and kurtosis tests on all variables. Based on guidance from Gaskin (2016), highly kurtotic items indicated items that were highly centralized around the mean with little variation from different

respondents. I used this information to identify which items to watch in further analysis, specifically the exploratory factor analysis (EFA).

5.3 Informed Pilot Study

I ran an informed pilot study with the instruments prior to executing the pilot study (see Appendix A for the Informed Consent, instructions, and data collection instrument). I worked with colleagues to test the survey instrument in order to test for bias and external validity. Once the instrument was validated through peer review, I began a pilot study using the validated instruments. The informed pilot was designed to indicate any items within the measurement tools that proved difficult to understand by the participants. The informed pilot's sample size was deemed unimportant as the data was not used in any quantitative assessment or analysis nor were the results extrapolated to a larger population. I conducted the informed pilot study with five volunteers from my home office and two family members. This step was conducted to test the understandability and face validity of the instruments only. No adjustments were required.

5.4 Pilot Study

The pilot study was launched in July 2020 using Mechanical Turk and Qualtrics. Utilizing the instrument in Appendix A and Qualtrics as the data collection platform, 45 respondents were collected.

Questions D1-D13 in Appendix A addressed screening questions to determine respondent eligibility to take part in the study and collected basic demographic data for the respondents. Of these respondents, 37 valid cases were collected prior to data screening and cleaning.

Appendix B Table B.2 summarizes the demographics collected for the pilot study. The demographics collected resulted in males representing approximately 70% of respondents and females representing approximately 30%. Approximately 6% of the respondents were between the ages of 18 and 25; 30% between 26 and 35; 30% between the ages of 36 and 45; 15% between the ages of 46 and 55; 15% between the ages of 56 and 65; and 3% between the ages of 66 and 77. Three percent of the respondents held at least a high school diploma; 18% attended some college; 18% had at least a 2-year degree; 39% had at least a 4-year degree; 15% had a professional/ graduate degree; and 6% had a doctorate.

Six percent of the respondents worked in the education field; 9% worked in financial services; 15% were government employees; 9% were in the healthcare industry; 6% were in manufacturing; 3% worked for non-profits; 3% were in the services industry; 15% were in the IT field; 9% worked in the telecommunications industry; 3% worked in the travel industry; 15% worked in wholesale/retail; and 6% reported working of other, non-specified industries. Within these industries, 51% of respondents represented the junior associate/professional position; 39% represented mid-level managers; and 9% represented senior executive positions.

The pilot was open for responses for a total of 95 hours. Forty-five respondents participated in the pilot study. Of the 45 respondents, I retained 33 cases for analysis. Nearly 15.55% of the removed cases were due to respondents not meeting the pre-determined screening criteria, 4.44% of respondents failing to complete the survey, and 6.66% of the respondents providing unengaged responses. This cleaning process allowed for a 73.33% case acceptable use rate of the total number of cases collected.

In order to assess unengaged responses, I calculated the amount of time a respondent took to answer the survey in full compared to the average amount of time taken from all respondents and calculated the standard deviation of responses for the main instrument questions. I set an a priori standard deviation threshold of 0.8 as the discriminator for survey engagement. Using these criteria, three cases were problematic with standard deviations of 0, 0.46, and 0.46, respectively. Of these three, the times to complete were 3:07, 6:26, and 7:22. The average time to complete the full survey was 10:08 minutes.

I analyzed skewness and kurtosis of the collected data looking for kurtotic values over 3 or less than -3 for them to be problematic. Researcher identified six items that exhibited kurtotic issues—BC2, BC5, SC2, SC4, ISPC2, and ISPC3. Data exhibited no skewness issues.

After the data was sufficiently cleaned for the pilot study, I conducted EFA using a principal axis factor analysis for each of the reflective scales with oblique rotation (direct oblimin). Then, I conducted a Kaiser-Meyer-Olkin measure to verify the sampling adequacy for the analysis. Using Eigenvalues and Kaiser's criterion of 1, I determined the actual number of factors to use in the study. I subsequently used a rotation and pattern matrix analysis to determine factor loadings and check the validity of the factor names chosen for the instruments. Finally, I determined Cronbach's alpha scores to assess reliability.

Next, I analyzed initial descriptive statistics on the latent variables—Input Control, Outcome Control, Behavior Control, Clan Control, and Self Control—while

holding the descriptive statistics for the dependent variable—ISPC—in reserve for further analysis.

I analyzed pattern matrices ensuring no cross-loading. Additionally, I determined the adequacy of these factors through KMO and Bartlett's, commonalities, and total variance explained matrices. I determined convergent validity and assessed discriminant validity by ensuring there are no cross-loadings and did not find any correlations between the factors greater than.7. Finally, I determined reliability using Cronbach's Alpha scores.

Following the EFA analysis, I ran an independent-samples t-test to evaluate whether covariates created comparable groups (e.g., age, gender, education, industry, and position) for each construct of input control, outcome control, behavior control, clan control, self-control, or ISPC.

All of the main constructs had Cronbach Alpha scores > 0.7 and Researcher deemed these constructs to be reliable. To assess discriminality reliability, eight components were retained at the 0.6 level, resulting in IC loading on component 1 except for IC4, which did not load on any component, BC loading on component 5 except for BC4, which did not load on any component and BC5, which loaded on component 1, and SC loading primarily on component 4 except for SC1, which did not load, SC2, which loaded on component 2, SC4, which loaded on component 5, and SC5, SC7, and SC10, which all loaded on component 8 (see Appendix B Pilot Study Results for result tables and charts). I aggregated the items in each scale into a single mean scale and ran a statistical description for the demographic and mean variable items.

The mean correlation analysis indicated that OC was significantly correlated with SD and SC; IC was significantly correlated with OUT, BC, and CC; OUT was

significantly correlated with CC; and BC was significantly correlated with CC and SC. OC's correlation with SD and SC was not supported in the factor analysis; however, IC's correlations with OUT, BC, and CC bore out in the factor analysis most strongly with CC on seven items on component one, whereas IC's was only correlated with BC on one item one component one. Factor analysis did not support the correlation with BC and CC but did correlate with one SC item on component five. This correlation analysis indicates that the factors of input control and clan control may not be different variables based on both the loadings of each item reflective of the variable and the correlation of the mean constructs writ large.

I conducted normalcy analysis on all variables under observation. Social desirability, outcome control, behavior control, clan control, and self-control were all tested with a significantly normal distribution. Organizational commitment tested significantly different from that of a normal distribution with both the Kolmogorov-Smirnov and Shapiro-Wilk tests at p=0.012 and p=0.031 respectively. Input Control tested significantly different from that of a normal distribution with the Kolmogorov-Smirnov test at p=0.015; however, the Shapiro-Wilk test was not significant at p=0.060, indicating that the distribution for IC was likely significantly different from that of a normal distribution but only indicated by one test. ISPC also tested significantly different from that of a normal distribution with both the Kolmogorov-Smirnov and Shapiro-Wilk tests at p=0.016 and p=0.001, respectively.

Nonparametric statistics allows for hypothesis testing even when the distribution of variables is not normal (Gibbons, 1993). I chose to use the PLS-SEM technique, which is a nonparametric statistical technique, for the main study.

The pilot study showed that some demographics may have a significant effect on four of the six variables under consideration. The final analysis will have to consider any effects age, position, knowledge, or intensiveness have on IC, OUT, BC, and CC.

The pilot study identified self-control cross-loading on five components and input control and clan control both loading on component one. I analyzed the questionnaire items in both input control and clan control to determine similarities between the two items. I then changed the wording to the seven items in clan control to ensure the two factors, input control, and clan control, were measuring different constructs. In addition to changing the items, I moved the items for clan control to the bottom of the instrument to create the greatest time distance possible to ensure respondents did not inadvertently believe they were answering questions regarding the same topic.

For IC, the principal will specify, monitor, and manipulate the human, financial, and material resources available for an activity (Jaworski, 1988; Mähring, 2002), whereas for the clan control mode, groups of individuals who are dependent on one another, share a set of common goals, endorsing and promoting a common philosophy, values, and beliefs that control the activities of individual members of the group (Ouchi, 1980).

These two factors may load onto the same component due to some possible confusion with the wording in CC e.g. “My department does not,” and “My department encourages,” may elicit the same understanding as “My manager informs,” and “My manager discusses,” found in IC by eliciting an understanding of management influencing aspects of the work environment. In order to better elicit the situation where the group polices the actions and activities of the clan, I removed “department” from all CC items. Further, I changed most “co-worker” terms, a term that could include front-line

and second-line managers, to colleagues, in order to better elicit the understanding of employees other than the respondent who are within the same echelon of the respondent and not a management representative.

Several items in input control, outcome control, behavior control, self-control, and ISPC did not load on a component. I assessed this to be an issue of small sample size and retained these items in the main study.

Additionally, correlation analysis indicated that several constructs – organizational commitment, input control, outcome control, and behavior control – significantly correlated with other factors—specifically self-determination and self-control; outcome control, behavior control, and clan control; clan control; and clan control and self-control respectively. Factor analysis did not indicate cross-loadings on items aside from those previously discussed, so I moved the items in these constructs to other areas of the instrument to create time distance between responses anticipating that this would address the correlation issue.

5.5 Main Study

I launched the main study survey in August 2020 (see Appendix A for the Informed Consent, instructions, and data collection instrument). I removed 163 responses using the same screening procedures I used in the pilot study and eventually collected a total of 303 usable responses for the main study. As shown in Table 2, the sociodemographic data of the 303 cases represented various genders, age groups, education levels, information awareness, industries, positions, company sizes, and company information intensity levels.

The demographics for the main study are depicted in Table 2. Of the data collected, the main study resulted in males representing approximately 62% of respondents, with females representing approximately 37%, and less than 1% reporting gender as “other”. Approximately 15% of the respondents were between the ages of 18 and 25; 41% between 26 and 35; 23% between the ages of 36 and 45; 15.5% between the ages of 46 and 55; and 5% between the ages of 56 and 65. Approximately 2% of the respondents held at least a high school diploma; 4% attended some college; 6% had at least a 2-year degree; 64% had at least a 4-year degree; 23% had a professional/ graduate degree; and less than 1% had a doctorate.

Six percent of the respondents worked in the education field; 21.5% worked in financial services; 1% were government employees; 1% worked in the food/beverage industry; 5% were in the healthcare industry; 17% were in manufacturing; 1% worked for non-profits; 1% were in the medical/biotechnology/pharmacology industry; 1% were in real estate; 2% were in the services industry; 35% were in the IT field; 1% worked in the telecommunications industry; 5% worked in wholesale/retail; and 3% reported working of other, non-specified industries. Within these industries, 26% of respondents represented the junior associate/professional position; 61% represented mid-level managers; and 13% represented senior executive positions.

I requested 410 responses for the main study. After sufficiently cleaning the data for the main study, I conducted a Partial Least Squares Structural Equation Model (PLS-SEM) analysis to test for reliability and validity and to develop measurement and structural models of the data. I used the PLS-SEM approach due to the data not being normally distributed for each of the constructs tested. PLS-SEM is an appropriate method

of analysis when normal distributional assumptions cannot be met (Joe F. Hair et al., 2011). Additionally, PLS-SEM is an appropriate analytical method for soft modeling, which focuses on the prediction of relationships between variables while maximizing covariance between latent variables (Sosik et al., 2009).

During the main study analysis, I considered validity and reliability through confirmatory factor analysis assessing indicator reliability, internal consistency, convergent validity, and discriminant validity using SmartPLS 2.0. Tables 3-5 in chapter six summarize the test results.

Table 1: Demographic Characteristics

Employee Characteristics							
Gender		Age		Education		Information Awareness	
Male	62.0%	18-25	14.9%	High School Graduate	1.7%	Very Low	1.7%
Female	37.3%	26-35	41.3%	Some College	4.3%	Moderately Low	2.0%
Other	0.7%	36-45	23.4%	2-Year Degree	5.6%	Slightly Low	6.9%
		46-55	15.5%	4-Year Degree	64.4%	Neither Low nor High	11.2%
		56-65	5.0%	Professional/Grad Degree	23.4%	Slightly High	28.1%
				Doctorate	0.7%	Moderately High	34.3%
						Very High	15.8%
Job Characteristics							
Industry		Position		Size		Information Intensity	
Education	5.9%	Junior/Professional	26.4%	500-999	37.6%	Slightly Information Intensive	12.5%
Financial Services	21.5%	Mid-Level/Manager	60.7%	1,000-4,999	30.0%	Moderately Information Intensive	34.0%
Government	1.3%	Senior/Executive	12.9%	5,000-10,000	22.1%	Very Information Intensive	43.6%
Food/Beverage	1.3%			> 10,000	10.2%	Extremely Information Intensive	9.9%
Healthcare	5.0%						
Manufacturing	16.8%						
Nonprofit	1.3%						
Med/BioTech/Pharma	1.0%						
Real Estate	1.0%						
Service	2.0%						
InfoTech	34.7%						
Telecommunications	1.0%						
Wholesale/Retail	4.6%						
Other	2.6%						

CHAPTER VI. RESULTS

I used SmartPLS 2.0 to conduct the analysis. I first assessed the measurement model and then tested the structural model. The results are reported below.

6.1 Measurement Model

I tested the measurement quality of all the scales assessing indicator reliability, internal consistency, convergent validity, and discriminant validity through confirmatory factor analysis (CFA) before analyzing the structural model and test the hypotheses (Rahi, 2012).

6.1.1 Indicator Reliability. Indicator reliability is adequate when a variable is consistent with what is intended to be measured (Urbach & Ahlemann, 2010). Chin indicated that indicator loadings should be significant at the 0.05 level and must be ≥ 0.70 (1998). All loadings for the measurement model were significant at the 0.05 level ≥ 0.70 indicating all retained factors adequately reflected the eight independent variables and the control variable and deemed to be reliable (see Table 3).

Table 2: Indicator Reliabiltiy

	IC	OUT_Reward	OUT_Punish	BC_GEN	BC_ISP	SC_Initiative	SC_Improve	CC	SD
IC3	0.906								
IC5	0.927								
OUT1		0.892							
OUT2		0.792							
OUT3		0.861							
OUT6			0.873						
OUT7			0.885						
BC1				0.865					
BC3				0.883					
BC4					0.855				
BC6					0.829				
SC10						0.914			
SC5						0.914			
SC6							0.782		
SC8							0.850		
SC9							0.731		
CC2								0.829	
CC4								0.667	
CC5								0.775	
CC7								0.782	
SD2									0.825
SD3									0.827
SD4									0.766

6.1.2 Internal Consistency. Internal consistency was measured by the composite reliability (CR) suggested by Chin (1998). Nunnally recommended an internal consistency ≥ 0.70 is satisfactory, whereas an internal consistency < 0.60 indicates the lack of reliability (1994). All variables' CR scores were ≥ 0.83 indicating an acceptable level of internal consistency (see Table 4).

6.1.3 Convergent Validity. Fornell and Larcker suggest that convergent validity is achieved when the average variance extracted (AVE) is ≥ 0.50 (1981). Additionally, Chin and Newsted indicated that each latent variable should have the highest loads on one factor and not significantly cross-load onto any other factor (1999). All AVE scores were ≥ 0.62 and expressed the highest loads on the same factor indicating adequate convergent validity (see Table 4).

Table 3: Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF

		Loadings/Cross-Loadings									
Constructs/Items		1	2	3	4	5	6	7	8	9	10
1. BC_GEN	BC1	**0.865**	0.477	0.437	0.030	0.500	0.286	0.250	0.401	-0.013	-0.150
CR = **0.866**	BC3	**0.883**	0.550	0.493	0.022	0.579	0.211	0.310	0.456	-0.002	-0.241
AVE = **0.764**											
VIF = **1.735**											
2. BC_ISP	BC4	0.526	**0.855**	0.552	0.061	0.594	0.204	0.281	0.463	-0.034	-0.236
CR = **0.830**	BC6	0.463	**0.829**	0.493	-0.041	0.481	0.263	0.322	0.390	0.012	-0.141
AVE = **0.709**											
VIF = **1.957**											
3. CC	CC2	0.519	0.552	**0.829**	-0.054	0.590	0.325	0.412	0.531	-0.084	-0.240
CR = **0.849**	CC4	0.259	0.381	**0.667**	-0.150	0.287	0.346	0.504	0.498	-0.254	-0.267
AVE = **0.586**	CC5	0.340	0.458	**0.775**	-0.059	0.460	0.355	0.456	0.493	-0.188	-0.287
VIF = **2.611**	CC7	0.446	0.485	**0.782**	0.004	0.511	0.252	0.428	0.506	-0.062	-0.338
4. IC	IC3	0.014	-0.042	-0.070	**0.906**	0.048	-0.420	-0.354	-0.189	0.579	0.477
CR = **0.913**	IC5	0.038	0.061	-0.059	**0.927**	0.054	-0.393	-0.399	-0.152	0.575	0.476
AVE = **0.840**											
VIF = **2.009**											
5. ISPC	ISPC2	0.537	0.497	0.475	0.068	**0.781**	0.180	0.187	0.373	0.031	-0.132
CR = **0.850**	ISPC4	0.453	0.527	0.502	0.025	**0.822**	0.154	0.170	0.350	0.001	-0.133
AVE = **0.654**	ISPC5	0.510	0.529	0.545	0.042	**0.822**	0.150	0.146	0.421	0.051	-0.182
6. OUT_Reward	OUT6	0.168	0.180	0.270	-0.387	0.068	**0.873**	0.449	0.384	-0.453	-0.427
CR = **0.886**	OUT7	0.325	0.303	0.439	-0.390	0.278	**0.885**	0.487	0.388	-0.418	-0.528
AVE = **0.721**											
VIF = **2.182**											
7. OUT_Punishment	OUT1	0.321	0.300	0.492	-0.327	0.169	0.466	**0.892**	0.500	-0.280	-0.461
CR = **0.872**	OUT2	0.226	0.382	0.529	-0.357	0.181	0.439	**0.792**	0.506	-0.320	-0.410
AVE = **0.773**	OUT3	0.267	0.234	0.429	-0.368	0.178	0.452	**0.861**	0.421	-0.328	-0.469
VIF = **1.854**											
8. SC_Improvement	SC6	0.402	0.400	0.503	-0.220	0.361	0.392	0.438	**0.782**	-0.144	-0.244
CR = **0.832**	SC8	0.360	0.401	0.566	-0.163	0.353	0.354	0.552	**0.850**	-0.147	-0.319
AVE = **0.623**	SC9	0.408	0.405	0.479	-0.046	0.413	0.291	0.319	**0.731**	-0.100	-0.231
VIF = **2.112**											
9. SC_Initiative	SC10	0.035	0.030	-0.114	0.598	0.066	-0.448	-0.297	-0.145	**0.914**	0.515
CR = **0.913**	SC5	-0.048	-0.055	-0.192	0.556	-0.001	-0.459	-0.367	-0.159	**0.919**	0.543
AVE = **0.840**											
VIF = **2.094**											
10. SD	SD2	-0.177	-0.227	-0.297	0.478	-0.158	-0.486	-0.429	-0.347	0.514	**0.825**
CR = **0.848**	SD3	-0.189	-0.243	-0.333	0.368	-0.163	-0.396	-0.493	-0.253	0.380	**0.827**
AVE = **0.650**	SD4	-0.181	-0.044	-0.239	0.415	-0.123	-0.442	-0.333	-0.205	0.523	**0.766**
VIF = **2.011**											

6.1.4 Discriminant Validity. Discriminant validity was measured in accordance with guidelines provided by Fornell and Larcker (1981) and Compeau, Higgins, and Huff (1999). I measured discriminate validity by assessing the correlation between the measures of potential overlapping constructs and assessed the average variance shared between each construct and its measure ensuring this average variance was greater than the variance shared between the constructs and other constructs. Table 4 indicates each construct's correlations with other variables fall below the square root of the AVE of the construct in line with Campeau, Higgins, and Huff (1999). This indicates the measurement model has established the reliability and validity necessary to continue testing the research hypotheses. The bold digits in Table 5 represent the square root of the AVE and are greater than the loadings on all other constructs indicating a valid measurement model.

Table 4: Discriminant Validity of Measurement Model

	1	2	3	4	5	6	7	8	9
1. BC_GEN	**0.874**								
2. BC_ISP	0.589	**0.842**							
3. CC	0.532	0.622	**0.766**						
4. IC	0.029	0.014	-0.070	**0.917**					
5. ISPC	0.618	0.641	0.628	0.056	**0.808**				
6. OUT_Punishment	0.283	0.276	0.406	-0.442	0.199	**0.879**			
7. OUT_Reward	0.321	0.357	0.568	-0.412	0.207	0.533	**0.849**		
8. SC_Improvement	0.491	0.508	0.655	-0.185	0.473	0.439	0.559	**0.917**	
9. SC_Initiative	-0.008	-0.014	-0.168	0.629	0.035	-0.495	-0.363	-0.166	**0.806**

6.2 Structural Model.

6.2.1 Lateral Collinearity. I assessed lateral collinearity by measuring the collinearity statistic VIF. In accordance with Diamantopoulos and Siguaw, VIFs higher than 3.3 would indicate potential collinearity problems (2006). The results of the VIF values can be seen in Table 4. None of the independent variables examined exhibited

lateral collinearity issues as all results were less than the 3.3 threshold indicating lateral multicollinearity is not a concern in this study (Joseph F. Hair et al., 2013).

6.2.2 Coefficient of Determination. The R^2 value is provided in the box of the dependent variable in Figure 3. Overall, outcome control, behavior control, and clan control explained 58% of the variation found in employees' intention to comply with their companies' information security policies.

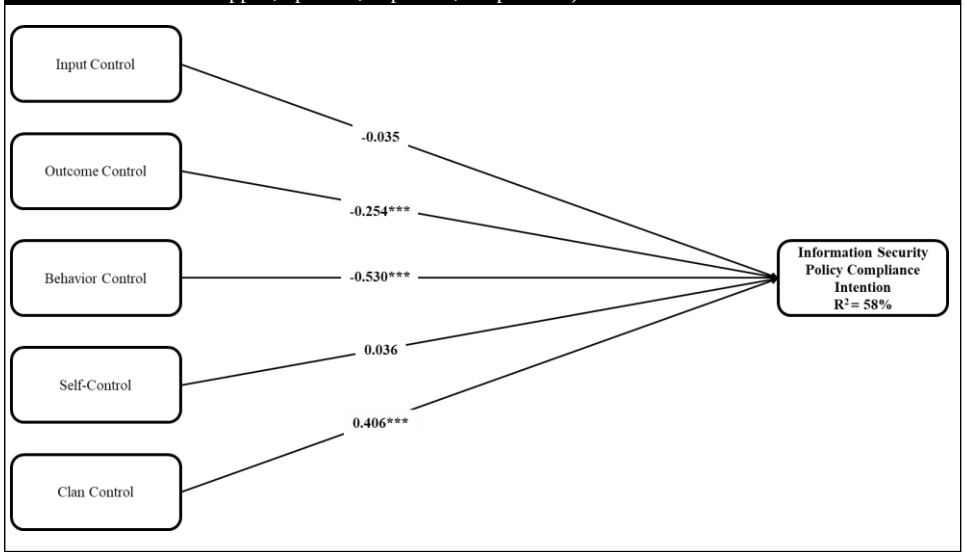
6.2.3 Structural Model Assessment. The hypotheses were tested by running a bootstrapping procedure with a 3,000 case resample. This procedure followed the guidance provided by Hair Jr et al. (2013). The results in Table 6 depict the path coefficients, original sample, mean, standard deviation, standard error, t-value, p-value, as well as the results of the hypothesis test.

Table 5: Results of Structural Model Analysis (Hypothesis Testing)

Hypothesis	Constructs	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	P-Value	Results
H_1	IC -> ISPC	-0.035	0.530	0.528	0.061	0.061	8.76	0.55	Not Supported
H_2	OC -> ISPC	-0.254	0.406	0.406	0.071	0.071	5.70	0.00	Not Supported
H_3	BC -> ISPC	-0.530	-0.035	-0.032	0.059	0.059	0.60	0.00	Not Supported
H_4	CC -> ISPC	0.406	-0.254	-0.254	0.071	0.071	3.58	0.00	Supported
H_5	SC -> ISPC	0.036	0.036	0.039	0.068	0.068	0.53	0.60	Not Supported

Table 6 summarizes the path coefficients that were standardized using the latent variable scores derived from the measurement model. Standardization was used to mitigate any swamping out the effect of the first-order variables used in the theoretical model. The significance level (p-value) was based on t-statistics derived from 3,000-sample bootstrapping in SmartPLS.

Figure 3: Results of testing hypotheses. (Note: Completely standardized estimates; Insignificant interactions were not dropped; *p<0.05, **p<0.01, ***p<0.001)



6.2.4 Hypothesized Relationships. In terms of H_1 concerning the relationship of input control on ISPC intention, the relationship was not significant and failed to indicate a direct relationship between the two constructs. Therefore, H_1 was not confirmed.

The relationship of outcome control on ISPC intention hypothesized in H_2 was negative and significant ($p < 0.001$). Since the relationship was negative, H_2 failed to meet the hypothesized positive relationship with information security policy intention compliance.

With regard to H_3, the relationship between behavior control and ISPC intention was found to be negative and significant ($p < 0.001$). Since the relationship was negative, H_3 failed to meet the hypothesized positive relationship with information security policy intention compliance.

The association between clan control and ISPC intention outlined in H_4 was positive and significant ($p < 0.001$). H_4 confirmed the hypothesized positive relationship between clan control and ISPC. In terms of H_5 concerning the relationship of self-control

on ISPC intention, the relationship was not significant and failed to indicate a direct relationship between the two constructs. Therefore, H_5 was not confirmed.

In summary, H_1, H_2, H_3, and H_5 did not meet the hypothesized relationship with the only H_4, clan control's effects on ISPC, having the hypothesized effect. This resulted in outcome control, behavior control, and clan control having significant effects on employees' intentions to comply with their companies' information security policies explaining 58% of the variance in ISPC with outcome control and behavior control both having a negative effect on ISPC.

6.2.5 Post-hoc Analysis. After conducting the analysis for the main study, I conducted a post-hoc analysis on the data controlling for various industries in the sample to determine if likely industries would cause a significant difference in the outcome of the study. I first segregated Financial Services, Healthcare Services, Information Technology Services, and then the remaining industries. Next, I analyzed the formal-control model and informal-control model using the full sample and the subsamples for each of these industry groups to see if there was any significant difference between these industries concerning those models. I conducted the same reliability and validity tests as with the main test to ensure the modified sample was adequate for the structural analysis. The results follow (please refer to Appendix C for full analysis and results).

6.2.5.1 Results of Formal- and Informal-Control Models with the Full Sample. I found that behavior control ($p<.001$) and outcome control ($p=.021$) both had a significant effect on ISPC in the formal-control model. Input control still had no significant effect on ISPC. Removing the informal control modes did change the direction for both outcome control and behavior control, rendering them both positive and in line with the proposed

hypotheses. For the informal-control model, I found that clan control ($p<.001$) continued to have a significant effect on ISPC and self-control continued to have no significant effect on ISPC (see Tables C.1.C and C.2.C). The findings are the same as in the main study.

6.2.5.2 Results of Formal- and Informal-Control Models with the Financial Services Industry. I found that only behavior control ($p<.001$) had a significant and positive effect on ISPC within the formal-control model, which is the same result when the full sample was used for this model and is in the direction as hypothesized. The results from the informal model show that clan control continued to have a significant effect ($p<.001$), and self-control continued to have no significant effect. Clan control also remained in the positive, hypothesized direction as was found in the main study as well as the full post-hoc model. Keeping in line with the full post-hoc model, the financial services industry indicated behavior control ($p<.001$) and clan control ($p=.014$) were both significant; however contrary to the separate full post-hoc models, outcome control was rendered insignificant in the full financial services model (see Tables C.3.C, C.4.C, and C.5.C).

6.2.5.3 Results of Formal and Informal-Control Models with the Healthcare Services Industry. Results from the formal Healthcare Services model show only behavior control ($p=.010$) significant. This is keeping in line with main study; however, the direction of the effect changed while considering only the Health Services industry to the hypothesized positive direction; however, outcome control was rendered insignificant as was input control. For the informal control modes, the Healthcare Services industry found both clan control and self-control to be insignificant identifying a change from the

main study as well as the full informal post-hoc model. The full Healthcare Services model found behavior control (p=.015) to be the only significant result; however, the direction was in line with the hypothesized direction in the main study (positive) and congruent with the segmented post-hoc findings (see Tables C.6.C, C.7.C, and C.8.C).

6.2.5.4 Results of Formal- and Informal-Control Models with the Information Technology Services Industry. Results from the formal Information Technology Services model show only behavior control (p=.033) being significant. Like with the previous industry models, this result changed from the main study result depicting behavior control having a positive effect on ISPC but rendering outcome control as insignificant. The informal-control model resulted in only clan control (p<.001) as having a significant and positive effect on ISPC. This result is in line with both the main study findings as well as the post-hoc segmented model. The full Information Technology model resulted in only clan control (p=.040) as having a significant effect on ISPC. Combining the formal and informal controls in the Information Technology Services model rendered behavior control insignificant (see Tables C.9.C, C.10.C., and C.11.C).

6.2.5.5 Results of Formal- and Informal-Control Models with All Other Industries Represented in the Collected Data. For the remaining industries, formal controls rendered only behavior control (p<.001) significant and having a positive effect on ISPC. In line with previous findings, the informal control modes rendered clan control (p<.001) as significant in the other industries; however, with the full model, the other services depicted behavior control (p<.001), outcome control (p=.007) [formal controls], and clan control (p<.001) [informal control] as significant. This finding is in line with the main study findings with outcome control continuing to have a negative effect, but changing

the direction of behavior control to the hypothesized positive direction (see Tables C.12.C, C.13.C, and C.14.C).

These findings suggest that there are industrial differences in the effect of formal and informal control on ISPC, though organizations of all types can benefit from some formal controls and informal controls. These findings also indicate that imposing both formal and informal control can increase the complexity in organizational controls and thus render undesirable outcomes. For example, both the post-hoc analysis and the main study show input control or self-control have no significant effect on ISPC. This indicates that future studies should focus on industrial differences and the significant factors, and determine possible moderating variables that could be affecting the significance, strength, and direction of the relationships between the independent and dependent variables.

CHAPTER VII. DISCUSSION

7.1 Discussion of Findings

In this study, I adopted the control theory and developed a research model to study ISPC among employees. The model integrates the informal control modes of clan control and self-control with the more commonly researched formal control modes of input control, outcome control, and behavior control. The empirical results from my research model show striking differences from previous research regarding the direction and magnitude of the relationships between the formal control modes and ISPC intentions. Prior literature indicates that input control, outcome control, and behavior control modes had a significant and positive effect on ISPC intentions (Challagalla & Shervani, 1996; Jaworski, 1988; Jaworski et al., 1993; Lowry et al., 2016; Mähring, 2002; Stanton et al., 2004). Instead, I found the effect of input control was insignificant, whereas the effect of outcome control and behavior control was negative. Furthermore, prior literature shows that clan control and self-control likewise had a significant and positive effect on ISPC intentions (Bateman & Crant, 1993; Buchanan II, 1974; Henderson & Lee, 1992; Jaworski et al., 1993; Kohli & Kettinger, 2004; Waterhouse & Tiessen, 1978). In this study, I only found clan control having a positive and significant effect on ISPC intentions. It appears that the additive effect postulated by combining formal and informal control modes in control theory did not hold in this research. I thus further explored possible reasons and theories to better explain the outcome of this research.

Input control was hypothesized to have a positive, direct effect on ISPC (H_1); however, the result shows that the effect was insignificant. Constituency theory states that

managers must connect with multiple organizational stakeholders to determine the true strategic goals of the organization and nest their organizational strategy within these goals (Connolly et al., 1980). Prior research also suggests that goal-setting theory-based leadership can have a negative effect on motivation if employee values and organizational goals are misaligned (Jensen et al., 2018). If the organization simply states compliance requirements and goals without helping employees internalize them, the effect of such inputs is trivial. This probably explains the insignificant finding related to the input control. Another likely reason behind the insignificant finding is that clans act as agents in a firm whereas managers act as principals creating a conflict or agency problem and further strengthening the resistance to managerial input control (Kohli & Kettinger, 2004; Panda & Leepsa, 2017). These theoretical perspectives help explain the insignificance of input control's effects on ISPC intentions in this study.

Outcome control was hypothesized to have a positive, direct effect on ISPC (H_2). Although significant, the result points to an opposite, negative effect. Outcome control focused on external contingencies—reward and punishment. Reviews of the effectiveness of reward *or* punishment *or* a mixture of the two are mixed in prior research (Chen et al., 2012). Some research indicates that rewards will generate temporary compliance with information security policies but will not create a lasting commitment (Myyry et al., 2009) or entice employees to focus on individual gains rather than larger organizational goals (Nunnally, 1978). Additionally, although the general deterrence theory indicates that when employees are aware of the severity and certainty of punishment, they are less likely to commit a deviant act such as not complying with information security policies (Bloom & Milkovich, 1998; Straub, Jr., 1990), previous research also shows that the

deterrent effect based on punishment is mixed (D'Arcy & Herath, 2011). These findings suggest that the effect of outcome control could depend on contexts or conditions. General outcome control not specific to the context of compliance may not be effective or even lead to an opposite effect.

Additionally, rewards and punishments may have the effect of creating hostility amongst employees by creating the feeling of being controlled or manipulated by managers (Kohn, 1993). This creates a controlling work environment or a very competitive environment among employees through divergence of preferences where employees are not rewarded for the right things and begin to compete with one another (Baker et al., 1988). In such a competitive environment, I contend that employees would focus on the immediate competitive gains against other employees rather than the strategic goals of the organization. This could create the negative effect witnessed in this study. Additionally, agency theory indicates that management may have a different expectation trying to maximize their own interests instead of employees' interests (Panda & Leepsa, 2017). This could be another possible reason for negative outcome control. If management does not properly use rewards and punishments, employees may see this as management maximizing their own interests and thus hostilely act on those controls (Baker et al., 1988).

Behavior control was also hypothesized to have a positive, direct effect on ISPC (H_3), but like with outcome control, the effect was significant but negative. Some reasons for this result may originate from organizational security culture and goal-setting theory. Organizational security culture may not be as strong in some industries such as manufacturing where not as much value is placed on information security as in other

industries, such as finance and healthcare, where information security is more critical to businesses (Chen et al., 2012). If an organization's behavior control—in terms of security training—delivers values against employees' own values, such control may fail to create organizational security culture, but instead, lead to resentment to the control. Additionally, goal-setting theory suggests that in organizations where leadership formulates the strategy of the organization and tells employees what goals to work toward, managers set the tone for the importance of ISPC (Bowers & Seashore, 1966; Price, 1972). However, if the training programs fail to incorporate the goal of ISPC from either the organizational security culture or the goal-setting theory perspectives, behavior control may not be effective. Sometimes, complexity in security technologies or hard-to-reach goals leads to employee rejection.

Another explanation for the results of H_3 could be that sometimes even employees are aware of their responsibilities and policies, but they just do not comply. Proper training of information security policy could aid in employees' compliance intentions; however, if the training curriculum does not utilize methods and tasks that are designed to activate and motivate employees' systematic cognitive information processing, the training may not be effective in influencing intentions to comply with information security policies (Puhakainen & Siponen, 2010). This could have the effect of employees being aware of the policies but not having the motivation to comply with them. Although this was a surprise finding, it may suggest that security training should be designed in such a manner that employees who would misuse IS systems know the company is serious about information security and act per the company's directives. Training programs should provide information on correct and incorrect usage, punishment for

misuse, and knowledge on enforcement. These trainings should be based on the company's information security policy and extend beyond awareness, educating employees about information risks to the organization, recent actions against employees who violated the policy, and raise awareness of responsibilities regarding company IS resources (D'Arcy et al., 2009b). Management can learn from these findings to improve training curricula to include elements beyond simple policy awareness and to strive to improve employee understanding of the risks and punishments associated with non-compliance or misuse of organizational IS systems.

Self-control was hypothesized to have a positive, direct effect on ISPC (H_5), but the effect was insignificant. Self-control is a type of a personal trait. The finding may indicate that under the context of ISPC, such traits may not be directly related to security behaviors or intentions. More specifically, security is not the primary job responsibility for most employees (Chen et al., 2012)—even those who may work in high-security culture organizations. Consequently, even those employees with strong self-control traits may not link their self-control capabilities with the organizational security task because security is not part of their daily tasks.

7.2 Contributions to IS Research

This study adopts the control theory considering both the formal and informal modes of control managers may employ to influence employees' intentions to comply with their companies' information security policies. Studies along these lines have been conducted within the IS field; however, prior research is limited in terms of assessing both formal and informal control modes' effects on ISPC. Most research has focused on the application of formal control modes that have the strongest effect on employee

compliance behavior and considered some informal control modes that take place within an organization that can influence employee compliance (Sitkin et al., 2020). More specifically, prior research in this field focused on formal control concepts such as input control, outcome control, and behavior control and how these concepts affect ISPC (Jaworski, 1988; Jaworski et al., 1993; Kirsch, 1996, 1997; Kirsch et al., 2002; Ouchi, 1979, 1980; Ouchi & Maguire, 1975). Other prior studies focused on informal control concepts such as clan control and self-control without assessing the effect that informal control may have on information security compliance intentions considered along with formal control modes (Bateman & Crant, 1993; Buchanan II, 1974; Henderson & Lee, 1992; Jaworski et al., 1993; Kohli & Kettinger, 2004; Siponen et al., 2007; Siponen et al., 2010; Waterhouse & Tiessen, 1978). This research combines the effects of both formal and informal control modes to assess if there are effects associated with employees' intentions of adhering to information security policies.

By combining the effects of identified formal and informal control modes on employees' intentions to comply with information security policies, this study aims to inform scholars and managers of the effect of both formal and informal control modes and assess whether informal control modes are additive to the formal control modes when considering employee compliance intentions. This research adds to the body of research by considering the effect of formal and informal control modes on information security compliance intentions in a research model and provides managers the ability to better understand their corporate control modes and to create an environment conducive to higher levels of employee ISPC.

This study adds to the theoretical foundations of ISPC intentions in organizations by identifying the relationships between formal and informal organizational controls, management of the SRM function generally, and ISPC specifically. By considering clan control and self-control modes alongside input control, outcome control, and behavior control modes, this research meets Sitkin et al.'s call to consider informal control modes along with the more often studied formal control modes (2020). This study began as a replication of previous studies in control theory using the three well-researched modes of managerial control: input control, outcome control, and behavior control. It then added the two most researched modes of informal control observed in organizations: clan control and self-control. This adds knowledge not only to the theoretical understanding of the factors that contribute to ISPC exercised by employees but also to the practical SRM applications used by organizations. The study was able to identify various formal and informal modes of control and present them in a single model, while empirically testing their effects on ISPC.

The striking findings from this also contribute to the theory in that enforcing all the controls in organizations may not be as effective as expected. Although previous research suggests an additive effect on the formal and informal control modes (Bateman & Crant, 1993; Buchanan II, 1974; Henderson & Lee, 1992; Jaworski et al., 1993; Kohli & Kettinger, 2004; Waterhouse & Tiessen, 1978), this study shows the following effect of outcome control, behavior control, and clan control on ISPC and no effect of input control and self-control:

$$\Upsilon = \boldsymbol{\beta_0} - \mathbf{0.25}(\boldsymbol{OC}) - \mathbf{0.53}(\boldsymbol{BC}) + \mathbf{0.41}(\boldsymbol{CC}) + \boldsymbol{\varepsilon}$$

Organizational theorists may need to carefully reexamine the effect of various combinations of control modes in ISPC.

7.3 Contributions to Practice

This study provides more insights into the practical application of organizational control theory in organizations that attempt to use different organizational control modes for ISPC. Managers can utilize this knowledge to identify the degree to which informal control modes affect their organizations and determine what level of formal control modes are necessary to achieve the desired level of employee compliance with information security policies. Furthermore, managers can use this information to identify proper combinations of control modes to achieve the highest level of effectiveness of employees' intentions of complying with their companies' information security policies.

This study provides managers with three different control modes that show a significant effect on employees' intentions to comply with ISPs. Although this study found a negative effect of outcome control on ISPC, additional research has indicated that managers can exercise outcome control in a manner that elicits positive responses from employees (Guo et al., 2011; Xue et al., 2011). The mixed findings suggest that managers need to more carefully design the assessment for outcome in the ISS field so that rewards and punishments can inspire compliance with ISPs, instead of deterring compliance. For example, prior results indicated that rewards were a more effective method of influencing employees' intentions to comply with ISPs. Managers should provide rewards for employees' compliance with ISPs and incorporate ISPC into job performance objectives. Negative sanctions are outweighed by the importance of job performance (Guo et al., 2011), indicating that incorporating ISPC into job performance may have a stronger

impact on employee behavior than rewards alone. Additionally, managers should formulate formal sanctions insofar as employees see the punishment as a just response to the policy violation (Xue et al., 2011). If employees consider punishments for ISP violations a just means, they may have stronger intentions to comply with ISP. By incorporating ISPC into job performance requirements, tying rewards for compliance to job performance, and ensuring that sanctions are perceived as just and address ISP violations directly and clearly, managers may create a better balance between rewards and punishments and avoid the negative effect of behavior control found in this study.

Managers can influence behavior control with employees through SETA. SETA is an important aspect of compliance intentions (D'Arcy et al., 2009b; Siponen et al., 2010), and has been found to deter IS misuse (D'Arcy et al., 2009b). Results from this study indicated that SETA programs are not always effective. Managers can use this information to ensure that adequate time and effort is dedicated to their employee training programs in order to ensure employees are fully aware of what specific security risks and threats they experience, to ensure they know how to perform specific duties in secure manners, to ensure they are informed why specific security risks or threats exist (Lowry et al., 2015).

Additionally, managers can incorporate the informal control of clan control into their managerial control strategy by instilling pride in all levels of their organizations fostering cooperation within clans (e.g., departments) to help facilitate compliance intentions. Managers can also utilize peers' influence to promote strong ISPC since peer-based social influence is a stronger predictor of individual behaviors (Guo et al., 2011).

For organizations that already have high levels of clan control present such as hospitals, law firms, consulting firms, or organizations with highly skilled technicians conducting IT operations (Kohli & Kettinger, 2004), managers may want to fully incorporate the clan into the formal control strategy by recruiting a confederate within the clan who can champion managerial intentions with other clan members.

7.4 Limitations and Future Research

While this study has theoretical and practical contributions, it is not impervious to limitations. First, the study is limited to the industries represented by the respondents who participated in the study via Amazon's Mechanical Turk. These industries included education, financial services, government, food/beverage, healthcare, manufacturing, nonprofit, medical/bio-technical/pharmaceutical, real estate, services, IT, telecommunications, wholesale/retail, and "other". Although this sample represents a fair section of industries found in the United States, caution must be exercised if researchers attempt to generalize the findings beyond the scope of the industries represented in this sample.

Second, this study ensures the anonymity of respondents to maintain their confidentiality in accordance with the requirements of Institutional Review Board (IRB). The anonymity of respondents was maintained by not collecting personal identifying information outside of the demographic questions, or information that can be used to find personal identifying information. Anonymity helps us prevent social desirability biases in responses and elicit the most honest ones from respondents that they often do not share with organizational management and leadership. However, anonymity may result in respondents being more interested in payment rather than providing the most accurate

self-reporting. Future studies may choose a sample population from an individual industry or even a company where data on employees' actual compliance and organizational controls can be collected.

Additionally, the study was limited in its ability to parse out the differences between industries generally or individual companies specifically. The sample population was very broad in its industrial representation, which may have introduced additional noise into the data. Future studies may use experimental or quasi-experimental designs to isolate organizational and industrial differences in formal and informal control modes and test their outcome (e.g., organizations with higher vs. lower levels of clan control and self-control) to better understand if the specific control is more effective in fostering employees' compliance with information security policies in certain types of organizations and industries.

The pilot study and main study summary statistics both represented similar gender and organizational size profiles; however, the age, education, information awareness, position, and information awareness profiles and industry representations showed significant differences. For this reason, I could not make a generalization from both studies to the general population. The main study represented more industries with higher reported information awareness and moderately higher information intensity indicating and found that age group, ISP awareness, industry, position, company size, and knowledge of computers and IT were all significantly correlated with ISPC. Therefore, future studies may focus on sample populations that better isolate these demographics to parse out any potential differences between groups.

Furthermore, Amazon Mechanical Turk does not verify the truthfulness of respondents. It is possible that respondents who may have otherwise been ineligible for the survey through the initial screening questions to pretend they were eligible i.e., some employees could have been self-employed or unemployed and stated otherwise or may not have worked in the United States and claimed otherwise. This limitation may have altered the outcome of the respondent results if a respondent did not work for an organization with clearly-defined ISP or did not understand the companies' IS environment. Future studies may identify individuals who do understand the ISP within organizations that have clearly defined ISP.

Although this study begins to shed light on how formal and informal control modes in organizations impact employees' ISPC. However, the respondents of this study are regular employees who might not have a full picture of organizational control exercised by managers. Future studies may draw from population pools who have a better understanding of their organizations' levels of input control, outcome control, behavior control, clan control, and self-control and who have a comprehensive understanding of the information security policies, and examine their compliance behaviors and intentions. Additionally, future studies may use secondary data and corresponding analysis tools in order to derive a more comprehensive understanding of employees' ISPC.

Finally, the findings from this study suggest the complexity when both formal and informal controls are in place. Future research can be conducted to validate the findings and to further explore the complex effect of multiple controls.

CHAPTER VIII. CONCLUSION

This research set out to explore the effects informal and formal modes of control have on employees' intentions to comply with corporate information security policies. To answer this question, a sample of 303 respondents from various industries, backgrounds, genders, ages, and stations within their companies was used to collect data concerning their organizations' formal and informal control modes along with their intention to comply with ISP through a survey methodology.

The results from this study are not totally consistent with previous empirical research in which the effect of formal controls and informal controls are additive when combined into a single model (Bateman & Crant, 1993; Buchanan II, 1974; Henderson & Lee, 1992; Jaworski et al., 1993; Kohli & Kettinger, 2004; Waterhouse & Tiessen, 1978). Although hypothesized to be additive, adding the informal control modes resulted in a different effect by rendering one formal control (input control) and one informal control (self-control) insignificant and changing the direction of the relationship of the two remaining formal controls (outcome control and behavior control). The findings are interesting and suggest a complex effect when both formal and informal controls are in place. The knowledge gained from this study can help ensure that organizations set up correct controls to protect themselves from the perils of cybersecurity threats such as corporate espionage, data theft, and myriad phishing attempts.

Future studies can use these findings to validate the model in this study and confirm the complex effects found with formal and informal controls' effects on intentions to comply with ISP. Given that not all professionals have in-depth insight into ISP programs or security controls within their respective organizations, limiting future

samples to those professionals who do have direct insight into ISP programs and security controls may develop better insight into control practices and aid in validating future models of control.

LIST OF REFERENCES

Andress, A. (2003). *Surviving Security: How to Integrate People, Process, and Technology* (2nd ed.). CRC Press, Taylor & Francis Group.

Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2019 (p. 1). (2020). [Statistics Report]. Statista. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Babbie, E. (2016). *The Practice of Social Research* (14th ed.). Cengage Learning.

Baker, G. P., Jensen, M. C., & Murphy, K. J. (1988). Compensation and Incentives: Practice vs. Theory. *The Journal of Finance*, *43*(3), 593–616.

Bateman, T. S., & Crant, J. M. (1993). The Proactive Component of Organizational Behavior: A Measure and Correlates. *Journal of Organizational Behavior*, *14*(2), 103–118.

Blakley, B., McDermott, E., & Geer, D. (2001). Information Security is Information Risk Management. *NSPW '01 Proceedings of the 2001 Workshop on New Security Paradigms*, 97–104. https://doi.org/10.1145/508171.508187

Bloom, M., & Milkovich, G. T. (1998). Relationships Among Risk, Incentive Pay, and Organizational Performance. *Academy of Management Journal*, *41*(3), 283–297.

Bowers, D., & Seashore, S. (1966). Predicting Organizational Effectiveness With a Four-Factor Theory of Leadership. *Administrative Science Quarterly*, *11*(2), 238–263.

Brief, A. P., & Aldag, R. J. (1981). The "Self" in Work Organizations: A Conceptual Review. *The Academy of Management Review*, *6*(1), 75–88.

Buchanan II, B. (1974). Building Organizational Commitment: The Socialization of Managers in Work Organizations. *Administrative Science Quarterly*, *19*(4), 533–546.

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

Challagalla, G. N., & Shervani, T. A. (1996). Dimensions and Types of Supervisory Control: Effects on Salesperson Performance and Satisfaction. *Journal of Marketing*, *60*(1), 89–105.

Champion Solutions Group. (2021, March 10). The Causes and Costs of Data Breaches in the Financial Industry [Data Security]. *Champion Solutions Group*. https://championsg.com/causes-costs-data-breaches-financial-industry

Chang, S., & Ho, C. B. (2006). Organizational Factors to the Effectiveness of Implementing Information Security Management. *Industrial Management & Data Systems*, *106*(3), 345–361.

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

Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In *Modern Methods for Business Research* (pp. 295–336).

Chin, W. W., & Newsted, P. R. (1999). Structural Equation Modeling Analysis with Small Samples Using Partial Least Squares. In *Statistical Strategies for Small Sample Research* (pp. 307–341). SAGE Publications, Inc.

Choudhury, V., & Sabherwal, R. (2003). Portfolios of Control in Outsourced Software Development Projects. *Information Systems Research*, *14*(3), 291–314.

Chua, C. E. H., Lim, W.-K., Soh, C., & Sia, S. K. (2012). Enacting Clan Control in Complex IT Projects: A Social Capital Perspective. *MIS Quarterly*, *36*(2), 577–600.

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study. *MIS Quarterly*, *23*(2), 145–158.

Connolly, T., Conlon, E., & Deutsch, S. (1980). Organizational Effectiveness: A Multiple-Constituency Approach. *The Academy of Management Review*, *5*(2), 211–217.

Cybersecurity Incidents. (2020). [HTML]. *OPM Cybersecurity Resource Center*. https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Dalton, D. R., Hitt, M. A., Certo, S. T., & Dalton, C. M. (2007). The Fundamental Agency Problem and Its Mitigation. *The Academy of Management Annals*, *1*(1), 1–64.

D'Arcy, J., & Herath, T. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. *European Journal of Information Systems*, *20*, 643–658.

D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems Misuse. *Communications of the ACM*, *50*(10), 113–117.

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

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration. *British Journal of Management*, *17*(4), 263–282.

Dugo, T. M. (2007). *The Insider Threat to Organizational Information Security: A Structural Model and Empirical Test* [Dissertation, Auburn University]. http://etd.auburn.edu/handle/10415/1345

Edelman, K., Hurley, B., Devan, P., Bhat, R., & Khan, A. (2019). *Global Risk Management Survey: Reimagining Risk Management to Mitigate Looming Economic Dangers and Nonfinancial Risks* (Assessment 11th Ed.; Deloitte Insights, pp. 1–76). Deloitte & Touche LLP. https://www2.deloitte.com/bg/en/pages/finance/articles/global-risk-management-survey-2019.html

Eisenhardt, K. (1985). Control: Organizational and Economic Approaches. *Management Science*, *31*(2), 134–149.

Eisenhardt, K. (1989). Agency Theory: An Assessment and Review. *The Academy of Management Review*, *14*(1), 57–74.

EPIC. (2021, March 10). Equifax Data Breach [Information]. *Equifax Data Breach*. https://epic.org/privacy/data-breach/equifax/

Fama, E. F., & Jensen, M. C. (1983). Separation of Ownership and Control. *The Journal of Law & Economics*, *26*(2), 301–325.

Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, *18*(3), 382–388.

Gaskin, J. (2016). Gaskin SEM Series [Http]. *Statwiki*. http://youtube.com/Gaskination

Gatlan, S. (2019). Three U.S. Universities Disclose Data Breaches over Two-Day Span [News/Media]. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/three-us-universities-disclose-data-breaches-over-two-day-span/

Gibbons, J. D. (1993). *Nonparametric Statistics—An Introduction* (Vol. 90). SAGE Publications, Inc.

Goodman, J. K., Cryder, C., & Cheema, A. (2013). Data Collection in a Flat World: Strengths and Weaknesses of Mechanical Turk Samples. *Journal of Behavioral Decision Making*, *26*(3), 213–224.

Gossett, L. M. (2009). Organizational Control Theory. In *Encyclopedia of Communication Theory* (.). SAGE Publications, Inc. SAGE Reference Online

Guo, K., Yuan, Y., Archer, N., & Connelly, C. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, *28*(2), 203–236.

Hair, Joe F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152.

Hair, Joseph F., Ringle, C. M., & Sarstedt, M. (2013). Editorial—Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance. *Long Range Planning*, *46*(1–2), 1–12.

Hays, R. D., Hayashi, T., & Stewart, A. L. (1989). A Five-Item Measure of Socially Desirable Response Set. *Educational and Psychological Measurement*, *49*(3), 629–636.

Henderson, J. C., & Lee, S. (1992). Managing I/S Design Teams: A Control Theories Perspective. *Management Science*, *38*(6), 757–777.

Hsu, J. S.-C., Shih, S.-P., & Li, Y. (2017). The Mediating Effects of In-Role and Extra-Role Behaviors on the Relationship Between Control and Software-Project Performance. *International Journal of Project Management*, *35*(8), 1524–1536.

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of Information Security. *Behaviour & Information Technology*, *29*(3), 221–232.

Hunt, G. (2018). Data Breaches—Universities a Growing Target for Data Theft [News/Media]. *TitanHQ Blog*. https://www.titanhq.com/blog/universities-and-the-risk-from-cyber-crime/

Jaworski, B. J. (1988). Toward a Theory of Marketing Control: Environmental Context, Control Types, and Consequences. *Journal of Marketing*, *52*(3), 23–39.

Jaworski, B. J., Stathakopoulos, V., & Krishnan, H. S. (1993). Control Combinations in Marketing: Conceptual Framework and Empirical Evidence. *Journal of Marketing*, *57*(1), 57–69.

Jensen, U. T., Andersen, L. B., & Jacobsen, C. B. (2018). Only When We Agree! How Value Congruence Moderates the Impact of Goal-Oriented Leadership on Public Service Motivation. *Public Administration Review*, *79*(1), 12–24.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. *MIS Quarterly*, *23*(2), 183–213.

Keil, M., Rai, A., & Liu, S. (2013). How User Risk and Requirements Risk Moderate the Effects of Formal and Informal Control on the Process Performance of IT Projects. *European Journal of Information Systems*, *22*(6), 650–672.

Kirsch, L. J. (1996). The Management of Complex Tasks in Organizations: Controlling the Systems Development Process. *Organization Science*, *7*(1), 1–21.

Kirsch, L. J. (1997). Portfolios of Control Modes and IS Project Management. *Information Systems Research*, *8*(3), 215–239.

Kirsch, L. J., Ko, D.-G., & Haney, M. H. (2010). Investigating the Antecedents of Team-Based Clan Control: Adding Social Capital as a Predictor. *Organization Science*, *21*(2), 469–489.

Kirsch, L. J., Sambamurthy, V., Ko, D.-G., & Purvis, R. L. (2002). Controlling Information Systems Development Projects: The View from the Client. *Management Science*, *48*(4), 484–498.

Koerner, B. I. (2016, October 23). Inside the Cyberattack That Shocked the US Government [Business Security]. *Wired*. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

Kohli, R., & Kettinger, W. J. (2004). Informating the Clan: Controlling Physicians' Costs and Outcomes. *MIS Quarterly*, *28*(3), 363–394.

Kohn, A. (1993). Why Incentive Plans Cannot Work. *Harvard Business Review*, *71*(5), 54–62.

Krebs, B. (2020, February 10). U.S. Charges 4 Chinese Military Officers in 2017 Equifax Hack [Security Blog]. *KrebsOnSecurity*. https://krebsonsecurity.com/2020/02/u-s-charges-4-chinese-military-officers-in-2017-equifax-hack/#more-50492

Landers, R. N., & Behrend, T. S. (2015). An Inconvenient Truth: Arbitrary Distinctions Between Organizational, Mechanical Turk, and Other Convenience Samples. *Industrial and Organizational Psychology*, *8*(2), 142–164.

Lankton, N. K., Wilson, E. V., & Mao, E. (2010). Antecedents and Determinants of Information Technology Habit. *Information & Management*, *47*(5–6), 300–307.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory. *Decision Support Systems*, *48*(4), 635–645.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" Science in Traditional Organization and Information Systems Survey Research: A Case for Using Nontraditional Methods of Data Collection, Including Mechanical Turk and Online Panels. *Journal of Strategic Information Systems*, *25*(3), 232–240.

Lowry, P. B., Moody, G. D., Galletta, D. F., & Vance, A. (2013). The Drivers in the Use of Online Whistle-Blowing Reporting Systems. *Journal of Management Information Systems*, *30*(1), 153–190.

Lowry, P. B., Posey, C., Bennett, R. (Becky) J., & Roberts, T. L. (2015). Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust. *Information Systems Journal*, *25*(3), 193–273.

Mähring, M. (2002). *IT Project Governance*. Stockholm School of Economics. https://books.google.com/books?hl=en&lr=&id=gkdZdB7z_CQC&oi=fnd&pg=PR1&dq=IT+Project+Governance&ots=r4znssV8RN&sig=E2CvcTFRL4GpIKdAL_hNCx-bs8U#v=onepage&q=IT%20Project%20Governance&f=false

Manz, C. C., Mossholder, K. W., & Luthans, F. (1987). An Integrated Perspective of Self-Control in Organizations. *Administration and Society*, *19*(1), 3–24.

Mao, J.-Y., Zhang, X., & Song, W. (2008). Information Systems Development in a Low Maturity Environment: An Exploratory Case Study on Control Modes. *PACIS 2008 Proceedings*, *263*, 1–12.

McGee, M. K. (2017, January 10). A New In-Depth Analysis of Anthem Breach [Banking Security]. *BankInfo Security*. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Mishra, S., & Chasalow, L. (2011). Information Security Effectiveness: A Research Framework. *Issues in Information Systems*, *12*(1), 246–255.

Moody, G. D., & Siponen, M. (2013). Using the Theory of Interpersonal Behavior to Explain Non-Work-Related Personal Use of the Internet at Work. *Information & Management*, *50*(6), 322–335.

Morgan Stanley Annual Report (Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 For the Year Ended December 31, 2017 No. 1–11758; FORM 10-K, p. 185). (2017). United States Securities and Exchange Commission.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study. *European Journal of Information Systems*, *18*(2), 126–139.

Nunnally, J. C. (1978). *Psychometric Theory*. McGraw-Hill.

Ouchi, W. G. (1979). A Conceptual Framework for the Design of Organizational Control Mechanisms. *Management Science*, *25*(9), 833–848.

Ouchi, W. G. (1980). Markets, Bureaucracies, and Clans. *Administrative Science Quarterly*, *25*(1), 129–141.

Ouchi, W. G., & Maguire, M. A. (1975). Organizational Control: Two Functions. *Administrative Science Quarterly*, *20*(4), 559–569.

Panda, B., & Leepsa, N. M. (2017). Agency Theory: Review of Theory and Evidence on Problems and Perspectives. *Indian Journal of Corporate Governance*, *10*(1), 74–95.

Phillips, B. (2013). Information Technology Management Practice: Impacts upon Effectiveness. *Journal of Organizational and End User Computing*, *25*(4), 50–74.

Price, J. (1972). The Study of Organizational Effectiveness. *The Sociological Quarterly*, *13*(1), 3–15.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757–778.

Rahi, S. (2012). *Structural Equation Modeling Using SmartPLS* (1st ed.). CreateSpace Independent Publishing Platform.

Remus, U., Wiener, M., Saunders, C., Mähring, M., & Kofler, M. (2016). Control Modes Versus Control Styles: Investigating ISD Project Control Effects at the Individual Level. *Managing IS Projects and IS Development*, 1–21. https://aisel.aisnet.org/icis2016/ManagingIS/Presentations/4/

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A Tale of Three Perspectives: Examining Post Hoc Statistical Techniques for Detection and

Correction of Common Method Variance. *Organizational Research Methods*, *12*(4), 762–800.

Roman, J. (2014). University Breaches: A Continuing Trend [News/Media]. *Data Breach Today*. https://www.databreachtoday.asia/university-breaches-continuing-trend-a-6660

Rosenthal, R., & Rosnow, R. L. (1991). *Essentials of Behavioral Research: Methods and Data Analysis* (2nd ed.). McGraw-Hill, Inc.

Rouse, S. V. (2015). A Reliability Analysis of Mechanical Turk Data. *Computers in Human Behavior*, *43*, 304–307.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security*, *56*, 1–13.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2007). Employees' Adherence to Information Security Policies: An Empirical Study. *New Approaches for Security, Privacy and Trust in Complex Environments*, *232*.

Siponen, M. T., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, *43*(2), 64–71.

Sitkin, S. B., Long, C. P., & Cardinal, L. B. (2020). Assessing the Control Literature:

Looking Back and Looking Forward. *Annual Review of Organizational Psychology and Organizational Behavior*, *7*, 339–368.

Sosik, J. J., Kahai, S. S., & Piovoso, M. J. (2009). Silver Bullet or Voodoo Statistics? A Primer for Using the Partial Least Squares Data Analytic Technique in Group and Organization Research. *Group & Organization Management*, *34*(1), 5–36.

Stanton, J. M., Mastrangelo, P. R., Stam, K. R., & Jolton, J. (2004). Behavioral Information Security: Two End Users Survey Studies of Motivation and Security Practices. *AMCIS 2004 Proceedings*, 1–8.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data Collection in the Digital Age: Innovative Alternatives to Student Samples. *MIS Quarterly*, *38*(2), 355–378.

Straub, Jr., D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 2270347.

Study: Hackers Attack Every 39 Seconds. (2007). [Academic]. *University of Maryland A. James Clark School of Engineering*. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

Tansey, J., & Rayner, S. (2009). *Cultural Theory and Risk from: Handbook of Risk and Crisis Communication*. Routledge.

The Boeing Breach: How an Employ Slip-Up Cost Colleagues. (2017). [HTML]. *CyberPolicy*. https://www.cyberpolicy.com/cybersecurity-education/the-boeing-breach-how-an-employee-slip-up-cost-colleagues

Thomas, B. (2019, October 1). Financial Data Breaches 2019: Captial One, First American, Desjardins, More. *BITSIGHT The Standard in Security Ratings*. https://www.bitsight.com/blog/financial-data-breaches-2019-capital-one-first-american-desjardins-more

Urbach, N., & Ahlemann, F. (2010). Structural Equation Modeling in Information Systems Research Using Partial Least Squares. *Journal of Information Technology Theory and Application*, *11*(2), 5–40.

Van de Mortel, T. F. (2008). Faking it: Social Desirability Response Bias in Self-Report Research. *Australian Journal of Advanced Nursing*, *25*(4), 40–48.

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

Vance, A., & Siponen, M. T. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing*, *24*(1), 21–41.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, *36*(1), 157–178.

Vlasic, A., & Yetton, P. (2004). Effective Project Control: Insights from the Australian Construction Industry. *PACIS 2004 Proceedings*, 1–15.

Waterhouse, J. H., & Tiessen, P. (1978). A Contingency Framework for Management Accounting Systems Research. *Accounting, Organizations and Society*, *3*(1), 65–76.

Wiener, M., Mähring, M., Remus, U., & Saunders, C. (2016). Control Configuration and Control Enactment in Information Systems Projects: Review and Expanded Theoretical Framework. *MIS Quarterly, WP Version*, 1–84.

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, Justice, and Compliance in Mandatory IT Settings. *Information Systems Research, 22*(2), 400–414.

APPENDIX A

Informed Consent and Online Survey

ADULT ONLINE CONSENT TO PARTICIPATE IN A RESEARCH STUDY
Managerial Control Effects on Information Security Policy Compliance Intentions: Considerations of Formal and Informal Modes of Control

SUMMARY INFORMATION

Things you should know about this study:

- **Purpose:** The purpose of this study is to examine the relationships between formal organizational control methods defined as input control, outcome control, and behavior control, and informal organizational control methods defined as clan control and self-control and their effects on employee intentions to comply with information security policy.
- **Procedures**: If you choose to participate, you will be asked to respond to a survey that will measure your perceptions of the above concepts relating to your daily job.
- **Duration:** This survey will take approximately 10 minutes to complete.
- **Risks**: The main risk or discomfort from this research is psychological discomfort. The survey will ask you to think about situations at your current job and provide your feelings and opinions which may cause some psychological discomfort for some.
- **Benefits:** There are no direct benefits to you from this research. There may be potential indirect benefits in the way of improvements in information security risk management and data protection.
- **Alternatives:** There are no known alternatives available to you other than not taking part in this study.
- **Participation:** Taking part in this research study is voluntary. You may withdraw at any time.

Please carefully read the entire document before agreeing to participate.

PURPOSE OF THE STUDY

The purpose of this study is to determine how, and to what degree, formal and informal organizational control mechanisms impact employee intention to comply with his/her organization's information security policy.

For the purposes of this study, formal control mechanisms will be defined as how managers exercise control over the material and labor input of a project or operation, how managers exercise control over the outcomes of a project or operation, and how managers exercise control over the behavior of employees working on a project or operation. Informal control mechanisms will be defined as how employees exercise group or clan control over their project or operation, and self-control will be how individual employees exercise their own individual will over a project or operation. Information security policy will be defined as policies instituted by an organization designed to protect sensitive information such as proprietary information, personal identifiable information, financial information, etc. that resides or is transmitted across electronic media and connected external communications terminals leaving it vulnerable to hacking and theft.

NUMBER OF STUDY PARTICIPANTS

If you decide to be in this study, you will be one of approximately 440 people total with approximately 40 respondents for the pilot study and an additional 400 respondents for the main study.

DURATION OF THE STUDY

Your participation will involve approximately 10 minutes of your time to complete.

PROCEDURES

If you agree to be in the study, we will ask you to do the following thing:

After acknowledging this informed consent form, you will be asked to complete a survey that will open for you and ask several demographic questions and then a series of questions designed to measure your perception of organizational input control, outcome control, behavior control, clan control, and self-control regarding networked computer systems containing sensitive or proprietary information within your institution. At no time will you be asked to divulge any privileged information owned or controlled by your organization.

RISKS AND/OR DISCOMFORTS

The study has the following possible risks to you:

There are minimal risks to you associated with this study. Answering questions pertaining to perceptions of formal and informal control methods within your organization, your intentions to comply with your organization's information security policies, and demographic information is personal in nature and could cause mild psychological discomfort.

This risk is mitigated by the use of survey questions that have been used in prior studies that measure these perceptions in the least intrusive manner.

Additionally, unless contacted by you for additional questions pertaining to this informed consent form, the study will be conducted blind, and researchers will not have access to your identity meaning they cannot make your responses, perceptions or comments public. By asking for certain demographic information, it may be possible to extrapolate your identity; however, these data points are required for control of certain factors that may influence the results or the study. Researchers will keep all personal identifying information confidential to the fullest extent possible while still meeting the requirements of the study design.

BENEFITS

The study has the following possible benefits to you:

There are no direct benefits to you associated with this study. Indirectly, you along with other workers in your organization may experience potential positive changes within your organization that could increase your organization's information security risk management processes and procedures and ensure private data remains secure whereby your organization can reduce the risk of public embarrassment and loss of revenue.

ALTERNATIVES

There are no known alternatives available to you other than not taking part in this study.

CONFIDENTIALITY

The records of this study will be kept private and will be protected to the fullest extent provided by law. In any report that may be published, researchers will not include any information that will make it possible to identify you. Research records will be stored securely and only the researchers will have access to the records. However, your records may be inspected by authorized University or other agents who will also keep the information confidential.

USE OF YOUR INFORMATION

Your information collected as part of the research will not be used or distributed for future research studies even if identifiers are removed.

COMPENSATION & COSTS

As a contracted respondent for this study, I am offering $1.25 for the completion of this survey, which will be paid through the Amazon Mechanical Turk platform. This amount is commensurate with the average national minimum wage and accounts for the length of time that will be required to respond to the survey questions.

RIGHT TO DECLINE OR WITHDRAW

Your participation in this study is voluntary. You are free to participate in the study or withdraw your consent at any time during the study. Receipt of payment for completion of the survey is contingent on your completion of the survey in its entirety; however, you will not lose any other benefits if you decide to not participate, or if you quit the study early. The researcher reserves the right to remove you without your consent at such time that he/she feels it is in the best interest of the study.

RESEARCHER CONTACT INFORMATION

If you have any questions about the purpose, procedures, or any other issues relating to this study, you may contact Shaun Stewart at Florida International University, Miami, Florida, sstew042@fiu.edu.

IRB CONTACT INFORMATION

If you would like to talk with someone about your rights of being a subject in this research study or about ethical issues with this research study, you may contact the FIU Office of Research Integrity by phone at 305-348-2494 or by email at ori@fiu.edu.

PARTICIPANT AGREEMENT

I have read the information in this consent form and agree to participate in this study. I have had a chance to ask any questions I have about this study, and they have been answered for me. By clicking on the "consent to participate" button below I am providing my informed consent.

Do you consent to the previous online consent form?

- ○ Yes
- ○ **No**

Please select from the following items the selection that best describes you:

1. What is your age group?
   - ○ **Less than 18**
   - ○ 18-25
   - ○ 26-35
   - ○ 36-45

- 46-55
- 56-65
- 66-75
- > 75

2. What is your country of residence?
   - United States
   - **Canada**
   - **Great Britain**
   - **Australia**
   - **Other**
3. What is your primary work language?
   - English
   - **German**
   - **French**
   - **Spanish**
   - **Chinese**
   - **Other**
4. Has your employer established information security policies?
   - Yes
   - **No**
5. To what extent are you aware of the regulations prescribed by the information security policy (ISP) of your organization?
   - **Not at all aware**
   - **Slightly aware**
   - Moderately aware
   - Very aware
   - Extremely aware
6. In order to receive compensation for this survey, please provide your Amazon Mechanical Turk identification number below.

   _____
7. With which gender do you best identify?
   - Male
   - Female
   - Other
8. What is your highest education Level?
   - Less than High School
   - High School Graduate
   - Some College
   - 2 Year Degree
   - 4 Year Degree
   - Professional/Graduate Degree
   - Doctorate
9. Which selection best identifies your current industry of employment?
   - Education
   - Financial Services

- Government
- Food/Beverage/CPG
- Health Care
- Manufacturing
- Nonprofit
- Medical, Bio-Technology, Pharmacology
- Real Estate
- Services
- Information Technology
- Telecommunications
- Travel
- Wholesale/Retail
- Other

10. Which selection best identifies your current position in your organization?
    - Junior/Professional
    - Mid-Level/Manager
    - Senior/Executive
11. Which selection best identifies the approximate size of your organization?
    - 500-999
    - 1,000-4,999
    - 5,000-10,000
    - More Than 10,000
12. How would you best describe your knowledge of computers and information technology?
    - Very low
    - Moderately low
    - Slightly low
    - Neither low nor high
    - Slightly high
    - Moderately high
    - Very high
13. How would you best describe the information intensiveness of your company?
    - Not at all Information Intensive
    - Slightly Information Intensive
    - Moderately Information Intensive
    - Very Information Intensive
    - Extremely Information Intensive

To what degree do the following statements accurately represent you and your current work organization?

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
14. I am willing to put in a great deal of effort, beyond what is normally expected, in order to help my organization be successful	○	○	○	○	○	○	○
15. I really care about the fate of my organization	○	○	○	○	○	○	○
16. For me, my organization is the best of all possible organizations to work for	○	○	○	○	○	○	○
17. I am always courteous even to people who are disagreeable	○	○	○	○	○	○	○
18. There have been occasions when I took advantage of someone	○	○	○	○	○	○	○
19. I sometimes try to get even rather than forgive and forget	○	○	○	○	○	○	○
20. I sometimes feel resentful when I don't get my way	○	○	○	○	○	○	○
21. No matter who I'm talking to, I'm always a good listener	○	○	○	○	○	○	○
22. My manager informs me about the information security policy compliance activities I am expected to perform	○	○	○	○	○	○	○
23. My manager discusses the requirements of information security policy compliance with me	○	○	○	○	○	○	○
24. My manager does not discuss with me whether I meet his/her expectations on information security policy compliance	○	○	○	○	○	○	○
25. If my manager feels I need to adjust my information security policy compliance activities, s/he tells me about it	○	○	○	○	○	○	○
26. My manager does not evaluate my information security policy compliance activities	○	○	○	○	○	○	○

For the following responses, please select the option that best completes the following statement:
_____ I comply with the requirements of information security policies (ISP).

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
27. My pay raises and/or promotions depend on whether...	○	○	○	○	○	○	○
28. I will receive personal mention in oral or written assessment reports if...	○	○	○	○	○	○	○
29. My receiving tangible or intangible rewards are tied to whether...	○	○	○	○	○	○	○

For the following responses, please select the option that best completes the following statement:
_____ I don't comply with the requirements of the ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
30. I will probably be punished or demoted if...	○	○	○	○	○	○	○
31. I will not receive personal reprimand in oral or written assessment reports if...	○	○	○	○	○	○	○
32. I will incur monetary or non-monetary penalties if...	○	○	○	○	○	○	○
33. My facing tangible or intangible sanctions is tied to whether...	○	○	○	○	○	○	○

To what degree do the following statements accurately represent you and your current work organization?

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
34. Overall, I am aware of the potential security threats and their negative consequences	○	○	○	○	○	○	○
35. I do not have sufficient knowledge about the cost of potential security problems	○	○	○	○	○	○	○
36. I understand the concerns regarding information security and the risks they pose in general	○	○	○	○	○	○	○

37. I know the rules and regulations prescribed by the ISP of my organization	○	○	○	○	○	○	○
38. I do not understand the rules and regulations prescribed by the ISP of my organization	○	○	○	○	○	○	○
39. I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization	○	○	○	○	○	○	○
40. My department does not encourage cooperation to achieve ISP compliance among co-workers	○	○	○	○	○	○	○
41. My department encourages job-related discussions to achieve ISP compliance among co-workers	○	○	○	○	○	○	○
42. Co-workers in my department are not familiar with each other's performance on ISP compliance	○	○	○	○	○	○	○
43. Most co-workers in my department are able to provide accurate appraisals of each other's work on ISP compliance	○	○	○	○	○	○	○
44. My department fosters an environment where co-workers respect each other's work on ISP compliance	○	○	○	○	○	○	○
45. The work environment does not encourage co-workers to feel a part of the department	○	○	○	○	○	○	○
46. The work environment encourages co-workers to feel a sense of pride in their ISP compliance work	○	○	○	○	○	○	○
47. I am constantly on the lookout for new ways to improve my life	○	○	○	○	○	○	○
48. If I see something I do not like, I fix it	○	○	○	○	○	○	○
49. When I have a problem, I tackle it head-on	○	○	○	○	○	○	○
50. I do not look for better ways to do things	○	○	○	○	○	○	○
51. I prefer to not challenge the status quo	○	○	○	○	○	○	○
52. I feel driven to make a difference in my community, and maybe the world	○	○	○	○	○	○	○
53. I tend to let others take the initiative to start new projects	○	○	○	○	○	○	○
54. Wherever I have been, I have been a powerful force for constructive change	○	○	○	○	○	○	○

55. I love being a champion for my ideas, even against others' opposition	○	○	○	○	○	○	○
56. I do not enjoy facing and overcoming obstacles to my ideas	○	○	○	○	○	○	○
57. I am certain I will not adhere to information security policies	○	○	○	○	○	○	○
58. I intend to continue to comply with information security policies	○	○	○	○	○	○	○
59. I will not comply with information security policies to protect information assets	○	○	○	○	○	○	○
60. I am not likely to follow information security policies in the future	○	○	○	○	○	○	○
61. I will follow information security policies whenever possible	○	○	○	○	○	○	○

Note[1]: The following questions correspond with the constructs used in this study:

Organizational Commitment: Q14-Q16

Social Desirability: Q17-Q21

Input Control: Q22-Q26

Outcome Control (Reward): Q27-Q29

Outcome Control (Punishment): Q30-Q33

Behavior Control (General IS Awareness): Q34-Q36

Behavior Control (ISP Awareness): Q37-Q39

Clan Control (Cooperation): Q40-Q46

Clan Control (Pride): Q44-Q46

Self-Control (Improvement): Q47-Q51

Self-Control (Initiative): Q52-Q56

ISP Compliance Intentions: Q57-Q61

Note[2]: Informed consent, exclusionary data, Mechanical Turk Identification, and Demographic data collected in Q1-Q13.

APPENDIX B

Pilot Study Results

Following data cleaning, Researcher retained 33 cases for pilot analysis resulting in a 73.33% usability rate of the collected data. Based on a selection of responses identified in Appendix A, the following questions were designed to screen and collect demographics for the respondents. D1 is both a demographic and a discriminator; D2-D6 indicate only discriminator questions. D7-D13 are demographic questions only.

Of the demographic data collected, a total of 33 cases were used in the pilot study. As shown in Table B.2, the sociodemographic data of these 33 cases represented various genders, age groups, education levels, information awareness, industries, positions, company sizes, and company information intensity levels.

Table B.1: Demographic Questions

D1	What is your age range?
D2	What is your country of residence?
D3	What is your primary language at work?
D4	Does your employer have established information security policies?
D5	To what extet are you aware of the regulations prescribed by the information security policy (ISP) of your organization?
D6	In order to receive compensation for this survey, please provide your Amazon Mechanical Turk identification number below.
D7	With which gender do you best identify?
D8	What is your highest education level?
D9	Which selection best identifies your current industry of employment?
D10	Which selection best identifies your current position in your organization?
D11	Which selection best identifies the approximate size of your organization?
D12	How would you best describe your knowledge of computers and information technology?
D13	How would you best describe the information intensiveness of your company?

Table B.2: Demographic Characteristics							
Employee Characteristics							
Gender		Age		Education		Information Awareness	
Male	69.7%	18-25	6.1%	High School Graduate	3.0%	Slightly Low	3.0%
Female	30.3%	26-35	30.3%	Some College	18.2%	Neither Low nor High	6.1%
		36-45	30.3%	2-Year Degree	18.2%	Slightly High	36.4%
		46-55	15.2%	4-Year Degree	39.4%	Moderately High	39.4%
		56-65	15.2%	Professional/Grad Degre	15.2%	Very High	15.2%
		66-77	3.0%	Doctorate	6.1%		
Job Characteristics							
Industry		Position		Size		Information Intensity	
Education	6.1%	Junior/Professional	51.5%	500-999	54.5%	Slightly Information Intensive	3.0%
Financial Services	9.1%	Mid-Level/Manager	39.4%	1,000-4,999	12.1%	Moderately Information Intensive	36.4%
Government	15.2%	Senior/Executive	9.1%	5,000-10,000	6.1%	Very Information Intensive	27.3%
Healthcare	9.1%			> 10,000	27.3%	Extremely Information Intensive	33.3%
Manufacturing	6.1%						
Nonprofit	3.0%						
Service	3.0%						
InfoTech	15.2%						
Telecommunications	9.1%						
Travel	3.0%						
Wholesale/Retail	15.2%						
Other	6.1%						

Table B.3: Kurtosis	
BC2	4.831
BC5	6.012
SC2	4.687
SC4	6.528
ISPC2	4.857
ISPC3	5.577

Exploratory Factor Analysis. Items IC3, IC5, OUT5, BC2, BC5, CC1, CC3, CC6, SC4, SC5, SC7, SC10, ISPC1, and ISPC3 are reverse coded on the instrument in Appendix A. For reliability analysis, Researcher re-coded these items and considered the Cronbach Alpha scores. The control variable analysis on social desirability (SD) resulted in a Cronbach Alpha score of -0.897. The value was negative due to a negative average covariance among items violating reliability model assumptions. This factor had no reverse coded items from literature; however, SD2, SD3, and SD4 could have been reverse coded based on the wording of the questions. Researcher reverse coded SD2, SD3, and SD4 in order to re-run the reliability analysis. Following recoding, SD

produced a Cronbach Alpha score of 0.854. Following this result, Researcher deemed the control variable social desirability reliable.

Following reliability analysis, Researcher conducted discriminality analysis by conducted a Rotated Component Matrix analysis using both the 0.5 and 0.6 threshold. At the 0.5 level, the data exhibited a significant cross-loading on multiple items. Input Control and Clan Control significantly cross-loaded on component 1. Organizational Commitment (control variable) and Self-Control slightly cross-loaded on component 2 with two Self-Control items. Behavior Control Cross-loaded slightly with Input Control on one item on component 4. Input Control cross-loaded slightly with Self-Control with one item on component 8, and Behavior Control cross-loaded with Self-Control slightly on one item on component 9.

At the 0.6 level, the data still exhibited significant cross-loading noted at the 0.5 level between Input Control and Clan Control on component 1. At the 0.6 level, 8 factors resulted with a few outliers on components 9, 10, and 11 for Input Control, Behavior Control, and Self-Control, but only two items for component 9, and one item for component 11. Adjusting to reflect eight components allowed for a cleaner rotated component matrix.

Table B.4: Rotated Component Matrix								
	Component							
	1	2	3	4	5	6	7	8
OC1	0.053	**0.804**	-0.144	0.222	0.062	0.129	0.180	0.132
OC2	0.147	**0.781**	-0.006	0.212	0.076	0.121	0.191	0.195
OC3	0.067	**0.751**	0.158	0.266	-0.208	0.121	0.244	-0.028
SD1	0.081	0.113	-0.079	0.112	0.069	-0.079	**0.890**	-0.249
SD2	0.116	-0.159	0.140	-0.105	-0.167	0.072	**0.789**	0.029
SD3	-0.283	0.458	-0.076	-0.061	0.251	-0.055	**0.628**	0.254
SD4	-0.108	0.276	-0.093	0.145	-0.119	-0.195	**0.682**	0.317
SD5	-0.066	0.215	-0.171	0.131	0.104	0.053	**0.821**	-0.193
IC1	**0.741**	0.035	0.285	-0.042	0.233	-0.051	-0.018	0.233
IC2	**0.745**	-0.011	0.328	-0.004	0.128	0.034	0.035	0.234
IC3	**0.859**	0.022	0.047	-0.096	-0.029	0.109	0.145	0.283
IC4	0.378	0.193	0.230	-0.018	0.379	0.234	-0.104	0.347
IC5	**0.696**	0.239	0.045	-0.177	0.178	-0.138	-0.204	0.453
OUT1	0.224	0.141	**0.840**	-0.063	-0.094	-0.129	-0.082	-0.202
OUT2	0.410	0.035	**0.721**	0.118	-0.249	0.067	0.052	0.027
OUT3	0.109	-0.184	**0.850**	0.119	0.011	-0.159	-0.028	0.111
OUT4	0.460	0.049	0.508	-0.066	0.215	-0.111	-0.071	-0.270
OUT5	0.061	0.459	0.488	0.032	0.024	-0.089	0.057	0.145
OUT6	0.116	-0.195	**0.760**	-0.277	0.040	-0.008	-0.109	0.054
OUT7	0.578	0.156	0.465	-0.277	0.137	0.103	-0.116	-0.158
BC1	0.351	0.365	0.146	0.173	**0.655**	0.327	-0.034	-0.089
BC2	0.039	-0.223	-0.052	0.139	**0.808**	0.065	0.028	0.122
BC3	0.193	0.431	0.022	0.185	**0.628**	0.317	0.008	-0.178
BC4	0.392	0.508	0.081	0.043	0.462	0.270	0.074	-0.112
BC5	**0.679**	-0.059	0.207	0.060	0.442	-0.045	0.148	-0.130
BC6	0.380	0.397	0.106	0.063	0.562	0.169	-0.088	-0.126
CC1	**0.829**	0.091	0.085	-0.010	0.098	0.205	0.148	0.062
CC2	**0.698**	0.060	0.193	0.333	0.010	0.038	0.024	-0.308
CC3	**0.873**	-0.016	0.070	0.055	-0.072	0.056	-0.021	-0.073
CC4	**0.856**	0.010	0.055	0.209	0.019	0.040	-0.048	-0.246
CC5	**0.696**	0.112	0.048	0.397	0.241	-0.083	-0.070	-0.232
CC6	**0.760**	0.219	-0.174	0.051	0.082	0.204	-0.148	0.106
CC7	**0.836**	-0.004	0.151	0.264	-0.004	0.223	-0.109	-0.160
SC1	0.149	0.254	-0.151	0.552	0.374	-0.220	0.127	-0.165
SC2	0.034	**0.689**	-0.206	0.380	0.124	-0.116	-0.254	0.299
SC3	0.277	0.327	-0.036	**0.700**	0.224	-0.013	0.040	0.140
SC4	0.036	-0.104	-0.157	0.270	**0.771**	0.009	0.009	0.234
SC5	0.052	0.161	0.067	0.383	0.015	-0.169	-0.220	**0.721**
SC6	-0.032	0.385	-0.235	**0.637**	0.136	0.013	0.091	0.231
SC7	0.002	0.154	-0.226	0.463	0.026	0.233	-0.037	**0.724**
SC8	0.092	0.191	-0.056	**0.786**	0.076	0.020	0.121	0.213
SC9	0.091	0.070	0.197	**0.789**	0.194	0.304	-0.049	0.192
SC10	-0.129	0.381	0.120	0.343	0.145	0.142	0.165	**0.605**
ISPC1	-0.177	-0.432	0.284	-0.038	-0.055	**0.621**	0.077	0.291
ISPC2	0.135	0.082	-0.211	0.254	0.294	**0.742**	-0.032	-0.043
ISPC3	0.320	0.069	-0.051	-0.147	-0.007	**0.837**	-0.002	-0.149
ISPC4	0.042	0.273	-0.148	0.076	0.532	**0.540**	-0.055	0.050
ISPC5	0.153	0.206	-0.213	0.076	0.209	**0.791**	-0.074	0.152

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
Rotation converged in 20 iterations.

Within-Group Analysis. Researcher conducted Independent-Samples Kruskal-Wallis and Mann-Whitney U tests to determine whether the population medians on the independent variables and the dependent variable were the same across all levels of the demographic groups of age, gender, education level, position, company size, knowledge of computers and technology, and information intensiveness. The nonparametric Kruskal-Wallis and Mann-Whitney U tests were conducted in lieu of an ANOVA analysis due to the non-normal distribution found in Input Control and Internet Security Policy Compliance. For this test, the null hypothesis that the distribution of the independent and dependent variables is the same across categories of the demographics. Significant findings indicated that the distribution of the independent and dependent variables are different across age and position for input control, intensiveness for outcome control, knowledge for behavior control, and position and intensiveness for clan control.

Table B.5: Within-Group Analysis

K-test	Age	Gender	Education	Industry	Position	Size	Knowledge	Intenseiveness
IC	**significant**	not sig	not sig	not sig	**significant**	not sig	not sig	not sig
OUT	not sig	not sig	not sig	not sig	not sig	not sig	not sig	**significant**
BC	not sig	not sig	not sig	not sig	not sig	not sig	**significant**	not sig
CC	not sig	not sig	not sig	not sig	**significant**	not sig	not sig	**significant**
SC	not sig	not sig	not sig	not sig	not sig	not sig	not sig	not sig
ISPC	not sig	not sig	not sig	not sig	not sig	not sig	not sig	not sig

The two-way contingency table analysis was significant for the distribution of Input Control across Age and Position with $K(5, N=33) = 11.95$, $p=0.04$ and $K(2, N=33) = 7.69$, $p=0.02$ respectively. Follow-up tests were conducted to evaluate pairwise differences among the six age groups. The results indicated three of the fifteen pairwise differences were significant; however, the adjusted significance using the Bonferroni correction for multiple tests did not result in a significant difference in Input Control

based on the age demographics. Junior/Professional – Mid-Level Manager remained significant across Bonferroni's adjustment indicating there is a difference in mean for Input Control across the Junior/Professional – Mid-Level Manager demographics.

Table B.6: IC Pairwise Comparisons of Age

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
18-25-56-65	-2.800	8.061	-0.347	0.728	1.000
18-25-66-75	-4.500	11.800	-0.381	0.703	1.000
18-25-26-35	-8.550	7.463	-1.146	0.252	1.000
18-25-36-45	-12.400	7.463	-1.662	0.097	1.000
18-25-46-55	-20.400	8.061	-2.531	**0.011**	0.171
56-65-66-75	-1.700	10.554	-0.161	0.872	1.000
56-65-26-35	5.750	5.277	1.090	0.276	1.000
56-65-36-45	9.600	5.277	1.819	0.069	1.000
56-65-46-55	17.600	6.094	2.888	**0.004**	0.058
66-75-26-35	4.050	10.105	0.401	0.689	1.000
66-75-36-45	7.900	10.105	0.782	0.434	1.000
66-75-46-55	15.900	10.554	1.506	0.132	1.000
26-35-36-45	-3.850	4.309	-0.894	0.372	1.000
26-35-46-55	-11.850	5.277	-2.246	**0.025**	0.371
36-45-46-55	-8.000	5.277	-1.516	0.130	1.000

Table B.7: IC Pairwise Comparisons of Position

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
Senior/Executive-Junior/Professional	0.098	6.034	0.016	0.987	1.000
Senior/Executive-Mid-Level/Manager	9.603	6.171	1.556	0.120	0.359
Junior/Professional-Mid-Level/Manager	-9.505	3.550	-2.677	**0.007**	0.022

The two-way contingency table analysis was significant for the distribution of outcome control across information intensiveness with $K(3, N=33) = 10.60$, $p=0.01$. Follow-up tests were conducted to evaluate pairwise differences among the four information intensity groups. The results indicated two of the six pairwise differences were significant; however, the adjusted significance using the Bonferroni correction for

multiple tests resulted in only moderately information intensive – very information intensive remaining significant across Bonferroni's adjustment indicating there is a difference in mean for Outcome Control across the moderate to very information intensive organizations.

Table B.8: OUT Pairwise Comparisons of Intensiveness					
Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test	Sig.	Adj. Sig.[a]
Moderately information intensive-Extremely	-9.140	4.029	-2.269	**0.023**	0.140
Moderately information intensive-Very information	-12.847	4.256	-3.019	**0.003**	0.015
Moderately information intensive-Slightly	13.458	10.046	1.340	0.180	1.000
Extremely information intensive-Very information	3.707	4.338	0.855	0.393	1.000
Extremely information intensive-Slightly information	4.318	10.081	0.428	0.668	1.000
Very information intensive-Slightly information	0.611	10.174	0.060	0.952	1.000

The two-way contingency table analysis was significant for the distribution of Behavior Control across Knowledge of Computers and Information Systems with K(4, N=33) = 12.09, p=0.02. Follow-up tests were conducted to evaluate pairwise differences among the five knowledge groups. The results indicated three of the ten pairwise differences were significant; however, the adjusted significance using the Bonferroni correction for multiple tests resulted in only neither low nor high – very high knowledge remaining significant across Bonferroni's adjustment indicating there is a difference in mean for Behavior Control across the neither low nor high – very high knowledge of computers and information technology.

Table B.9: BC Pairwise Comparisons of Knowledge					
Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
Neither low nor high-Slightly	-9.375	7.333	-1.279	0.201	1.000
Neither low nor high-Slightly	15.250	11.758	1.297	0.195	1.000
Neither low nor high-	-16.250	7.292	-2.228	**0.026**	0.259
Neither low nor high-Very	-22.950	8.032	-2.857	**0.004**	0.043
Slightly high-Slightly low	5.875	9.993	0.588	0.557	1.000
Slightly high-Moderately high	-6.875	3.843	-1.789	0.074	0.736
Slightly high-Very high	-13.575	5.110	-2.656	**0.008**	0.079
Slightly low-Moderately high	-1.000	9.963	-0.100	0.920	1.000
Slightly low-Very high	-7.700	10.517	-0.732	0.464	1.000
Moderately high-Very high	-6.700	5.052	-1.326	0.185	1.000

The two-way contingency table analysis was significant for the distribution of clan control across position and information intensity with $K(2, N=33) = 12.73$, $p<0.01$ and $K(3, N=33) = 9.06$, $p=0.03$ respectively. Follow-up tests were conducted to evaluate pairwise differences among the three position groups and four intensity groups. The results indicated two of the three pairwise differences within the position groups were significant for both initial significance as well as with the Bonferroni correction for multiple tests indicating there is a difference in mean for Clan Control across the Senior Executive – Mid-Level Manager and Junior/Professional – Mid-Level Manager demographics. Further, the results indicated two of the four pairwise differences within the intensity groups were significant for the initial significance but not with the Bonferroni correction for multiple tests indicating there is no difference in mean for Clan Control Across the information intensity demographics.

Table B.10: CC Pairwise Comparisons of Position					
Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
Senior/Executive-	5.480	6.045	0.907	0.365	1.000
Senior/Executive-Mid-	16.526	6.183	2.673	**0.008**	0.023
Junior/Professional-Mid-	-11.045	3.557	-3.106	**0.002**	0.006

Table B.11: CC Pairwise Comparisons of Intensiveness					
Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test	Sig.	Adj. Sig.[a]
Moderately information intensive-Very information	-9.847	4.257	-2.313	**0.021**	0.124
Moderately information intensive-Extremely	-10.534	4.030	-2.614	**0.009**	0.054
Moderately information intensive-Slightly	14.125	10.048	1.406	0.160	0.959
Very information intensive-Extremely information	-0.687	4.339	-0.158	0.874	1.000
Very information intensive-Slightly information	4.278	10.176	0.420	0.674	1.000
Extremely information intensive-Slightly information	3.591	10.083	0.356	0.722	1.000

Table B.12: Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
D1	33	2	7	4.12	1.269
D7	33	1	2	1.30	0.467
D8	33	2	7	4.64	1.220
D9	33	1	15	8.21	4.891
D10	33	1	3	1.58	0.663
D11	33	1	4	2.06	1.321
D12	33	3	7	5.58	0.936
D13	33	2	5	3.91	0.914
OC	33	1.67	7.00	4.9394	1.57994
SD	33	1.00	6.60	3.9879	1.54995
IC	33	2.40	7.00	5.2364	1.13518
OUT	33	1.86	6.71	4.0043	1.19495
BC	33	4.00	7.00	5.9697	0.71133
CC	33	2.00	6.86	4.8398	1.27413
SC	33	3.40	7.00	5.3121	1.01512
ISPC	33	3.60	7.00	6.1758	0.79806
Valid N (listwise)	33				

Table B.13: Correlations

		OC	SD	IC	OUT	BC	CC	SC	ISPC
OC	Pearson Correlation	1	**.388***	0.199	0.039	0.292	0.189	**.530****	0.068
	Sig. (2-tailed)		0.025	0.268	0.830	0.099	0.293	0.002	0.706
	N	33	33	33	33	33	33	33	33
SD	Pearson Correlation	**.388***	1	-0.071	-0.113	0.076	-0.078	0.152	-0.049
	Sig. (2-tailed)	0.025		0.695	0.532	0.673	0.667	0.399	0.788
	N	33	33	33	33	33	33	33	33
IC	Pearson Correlation	0.199	-0.071	1	**.460****	**.498****	**.723****	0.238	0.146
	Sig. (2-tailed)	0.268	0.695		0.007	0.003	0.000	0.183	0.418
	N	33	33	33	33	33	33	33	33
OUT	Pearson Correlation	0.039	-0.113	**.460****	1	0.208	**.398***	-0.106	-0.009
	Sig. (2-tailed)	0.830	0.532	0.007		0.244	0.022	**0.558**	**0.959**
	N	33	33	33	33	33	33	33	33
BC	Pearson Correlation	0.292	0.076	**.498****	0.208	1	**.531****	**.357***	**0.329**
	Sig. (2-tailed)	0.099	0.673	0.003	0.244		0.001	0.041	0.062
	N	33	33	33	33	33	33	33	33
CC	Pearson Correlation	0.189	-0.078	**.723****	**.398***	**.531****	1	0.179	0.197
	Sig. (2-tailed)	0.293	0.667	0.000	0.022	0.001		0.320	0.271
	N	33	33	33	33	33	33	33	33
SC	Pearson Correlation	**.530****	0.152	0.238	-0.106	**.357***	0.179	1	0.143
	Sig. (2-tailed)	0.002	0.399	0.183	0.558	0.041	0.320		0.427
	N	33	33	33	33	33	33	33	33
ISPC	Pearson Correlation	0.068	-0.049	0.146	-0.009	**0.329**	0.197	0.143	1
	Sig. (2-tailed)	0.706	0.788	0.418	0.959	0.062	0.271	0.427	
	N	33	33	33	33	33	33	33	33

*. Correlation is significant at the 0.05 level (2-tailed).
**. Correlation is significant at the 0.01 level (2-tailed).

Table B.14: Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
OC	0.174	33	0.012	0.928	33	0.031
IC	0.171	33	0.015	0.938	33	0.060
ISPC	0.170	33	0.016	0.864	33	0.001

Table B.15: Pre-Pilot Items	
IC	**CC**
My manager informs me about the information security policy compliance activities I am expected to perform	My department does not encourage cooperation to achieve information security policies compliance among co-workers
My manager discusses the requirements of information security policy compliance with me	My department encourages job-related discussions to achieve information security policies compliance among co-workers
My manager does not discuss with me whether I meet his/her expectations on information security policy compliance	Co-workers in my department are not familiar with each other's performance on information security policies compliance
If my manager feels I need to adjust my information security policy compliance activities, s/he tells me about it	Most co-workers in my department are able to provide accurate appraisals of each other's work on information security policies compliance
My manager does not evaluate my information security policy compliance activities	My department fosters an environment where co-workers respect each other's work on information security policies compliance
	The work environment does not encourage co-workers to feel a part of the departmental effort in information security policies compliance
	The work environment encourages co-workers to feel a sense of pride in their information security policies compliance activities

Table B.16: Post-Pilot Items	
IC	**CC**
My manager informs me about the information security policy compliance activities I am expected to perform	~~My department does not~~ **My colleagues do not** encourage cooperation to achieve information security policy compliance. ~~among co-workers~~
My manager discusses the requirements of information security policy compliance with me	~~My department~~ **My colleagues** encourage job-related discussions to achieve information security policy compliance ~~among co-workers~~
My manager does not discuss with me whether I meet his/her expectations on information security policy compliance	~~Co-workers~~ **Colleagues** in my ~~department~~ **work center** are not familiar with each other's performance on information security policy compliance
If my manager feels I need to adjust my information security policy compliance activities, s/he tells me about it	Most ~~co-workers~~ **colleagues** in my ~~department~~ **work center** are able to provide accurate appraisals of each other's work on information security policy compliance
My manager does not evaluate my information security policy compliance activities	My ~~department~~ **colleagues** foster an environment where ~~co-~~workers respect each other's work on information security policy compliance
	~~The work environment~~ **My colleagues** do not encourage co-workers to feel a part of the ~~departmental~~ **organization's** effort in information security policy compliance
	~~The work environment~~ **My colleagues** encourage co-workers to feel a sense of pride in the~~ir~~ **organization's** information security policy compliance activities

Organizational Commitment

Table B.17: OC Tests of Normality

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
OC	0.174	33	0.012	0.928	33	0.031
a. Lilliefors Significance Correction						

Figure B.1: OC Histogram and Normal Curve

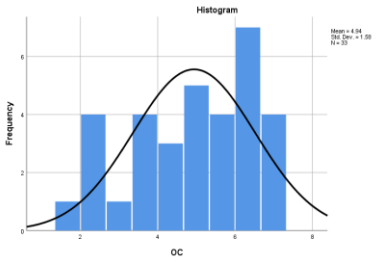


Figure B.2: OC Boxplot

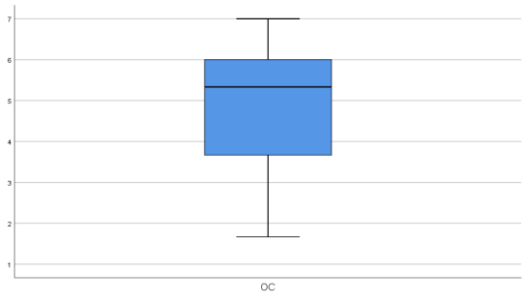
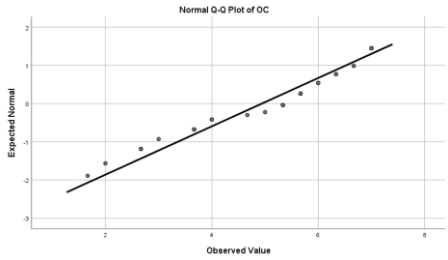


Figure B.3: OC Normal Q-Q Plot



Input Controls

Table B.18: IC Tests of Normality

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
IC	0.171	33	0.015	0.938	33	0.060

a. Lilliefors Significance Correction

Figure B.4: IC Histogram and Normal Curve

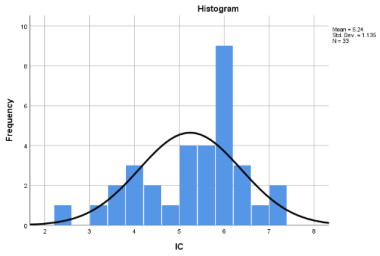


Figure B.5: IC Boxplot

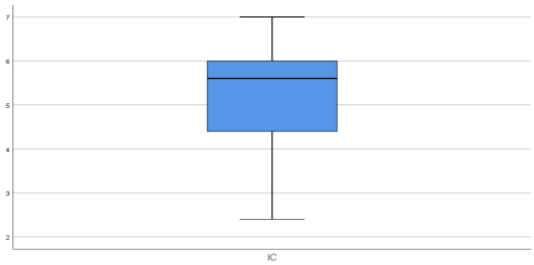
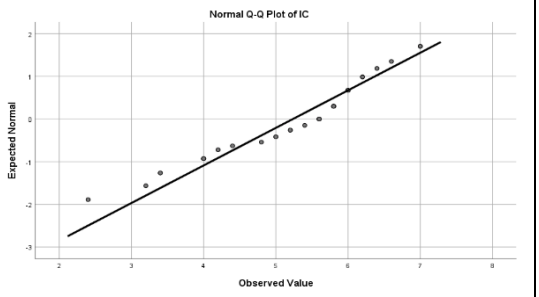


Figure B.6: IC Normal Q-Q Plot



Internet Security Policy Compliance

Table B.19: ISPC Tests of Normality

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
ISPC	0.170	33	0.016	0.864	33	0.001

a. Lilliefors Significance Correction

Figure B.7: ISPC Histogram and Normal Curve

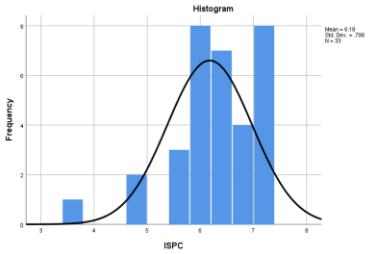


Figure B.8: ISPC Boxplot

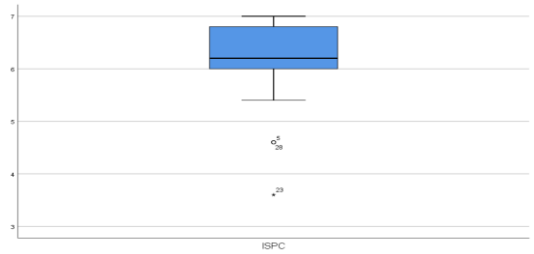
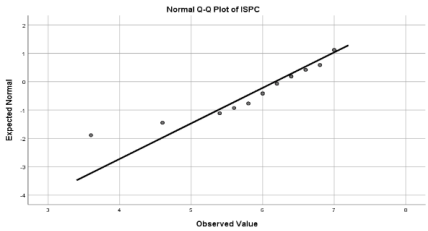


Figure B.8: ISPC Normal Q-Q Plot



APPENDIX C

Post-Hoc Analysis

Table C.1.A: Full Formal Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings					
Constructs/Items			1	2	3	4	5	6
1. BC_GEN								
CR	**0.856**	**BC1**	**0.944**	0.477	0.030	0.503	0.285	0.228
α	**0.692**	**BC3**	**0.780**	0.549	0.021	0.582	0.210	0.308
AVE	**0.750**							
VIF	**1.691**							
2. BC_ISP								
CR	**0.830**	**BC4**	0.499	**0.848**	0.059	0.593	0.204	0.308
α	**0.590**	**BC6**	0.453	**0.836**	-0.041	0.481	0.263	0.336
AVE	**0.709**							
VIF	**1.706**							
3. IC								
CR	**0.913**	**IC3**	0.016	-0.042	**0.909**	0.050	-0.420	-0.361
α	**0.811**	**IC5**	0.039	0.059	**0.924**	0.055	-0.393	-0.395
AVE	**0.841**							
VIF	**1.437**							
4. ISPC								
CR	**0.849**	**ISPC2**	0.515	0.496	0.068	**0.805**	0.179	0.186
α	**0.735**	**ISPC4**	0.433	0.525	0.026	**0.806**	0.153	0.168
AVE	**0.653**	**ISPC5**	0.493	0.529	0.042	**0.813**	0.150	0.152
5. OUT_Punishment								
CR	**0.872**	**OUT6**	0.186	0.182	-0.388	0.068	**0.875**	0.449
α	**0.706**	**OUT7**	0.326	0.303	-0.390	0.280	**0.883**	0.480
AVE	**0.773**							
VIF	**1.756**							
6. OUT_Reward								
CR	**0.876**	**OUT1**	0.322	0.300	-0.327	0.172	0.466	**0.836**
α	**0.805**	**OUT2**	0.200	0.382	-0.357	0.181	0.439	**0.891**
AVE	**0.702**	**OUT3**	0.250	0.235	-0.367	0.177	0.451	**0.782**
VIF	**1.849**							

Table C.1.B: Full Formal Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6
BC_GEN	**0.866**					
BC_ISP	0.752	**0.842**				
IC	0.174	0.108	**0.917**			
ISPC	0.773	0.799	0.240	**0.808**		
OUT_Punishment	0.541	0.526	0.665	0.447	**0.879**	
OUT_Reward	0.537	0.618	0.643	0.457	0.727	**0.838**

Table C.1.C: Full Formal Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.480	0.480	0.483	0.050	0.050	9.669	**0.000**
IC -> ISPC	0.097	0.097	0.094	0.062	0.062	1.572	0.117
OUT -> ISPC	0.150	0.150	0.147	0.065	0.065	2.328	**0.021**

Table C.2.A: Full Informal Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings			
Constructs/Items			1	2	3	4
1. CC						
CR	**0.849**	**CC2**	**0.829**	0.591	-0.084	0.531
α	**0.769**	**CC4**	**0.668**	0.288	-0.254	0.498
AVE	**0.586**	**CC5**	**0.775**	0.460	-0.188	0.493
VIF	**1.866**	**CC7**	**0.782**	0.510	-0.062	0.506
2. ISPC						
CR	0.654	**ISPC2**	0.475	**0.773**	0.031	0.373
α	**0.735**	**ISPC4**	0.502	**0.826**	0.001	0.350
AVE	**0.654**	**ISPC5**	0.545	**0.825**	0.051	0.421
3. SC_Initiative						
CR	**0.913**	**SC10**	-0.114	0.066	**0.914**	-0.145
α	**0.810**	**SC5**	-0.192	-0.001	**0.919**	-0.159
AVE	**0.840**					
VIF	**1.073**					
4. SC_Improvement						
CR	**0.832**	**SC6**	0.503	0.361	-0.144	**0.782**
α	**0.695**	**SC8**	0.566	0.353	-0.147	**0.850**
AVE	**0.623**	**SC9**	0.479	0.413	-0.100	**0.731**
VIF	**1.855**					

Table C.2.B: Full Informal Model Discriminant Validity of Measurement

	1	2	3	4
CC	0.766			
ISPC	0.793	**0.808**		
SC_Improvement	**0.809**	0.688	**0.789**	
SC_Initiative	0.410	0.187	0.407	**0.917**

Table C.2.C: Full Informal Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Error	t-value	p-value
CC -> ISPC	0.642	0.642	0.640	0.063	10.186	**0.000**
SC -> ISPC	-0.022	-0.022	-0.012	0.075	0.294	0.769

Table C.3.A: Formal Financial Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings					
Constructs/Items			1	2	3	4	5	6
1. BC_GEN								
CR	**0.863**	**BC1**	**0.871**	0.582	0.265	0.591	0.543	0.503
α	**0.683**	**BC3**	**0.872**	0.589	0.173	0.555	0.479	0.525
AVE	**0.760**							
VIF	**2.139**							
2. BC_ISP								
CR	**0.867**	**BC4**	0.533	**0.863**	0.143	0.521	0.496	0.461
α	**0.692**	**BC6**	0.638	**0.886**	0.158	0.532	0.496	0.518
AVE	**0.765**							
VIF	**2.093**							
3. IC								
CR	**0.918**	**IC3**	0.267	0.189	**0.928**	0.136	0.487	0.551
α	**0.821**	**IC5**	0.193	0.126	**0.914**	0.125	0.407	0.468
AVE	**0.848**							
VIF	**1.567**							
4. ISPC								
CR	**0.823**	**ISPC2**	0.414	0.359	-0.037	**0.691**	0.293	0.177
α	**0.681**	**ISPC4**	0.546	0.402	0.143	**0.792**	0.329	0.227
AVE	**0.609**	**ISPC5**	0.563	0.610	0.183	**0.849**	0.398	0.345
5. OUT_Punishment								
CR	**0.876**	**OUT6**	0.538	0.505	0.455	0.376	**0.898**	0.742
α	**0.717**	**OUT7**	0.495	0.495	0.403	0.404	**0.867**	0.589
AVE	**0.779**							
VIF	**2.633**							
6. OUT_Reward								
CR	**0.849**	**OUT1**	0.430	0.466	0.451	0.195	0.649	**0.873**
α	**0.730**	**OUT2**	0.538	0.528	0.373	0.310	0.555	**0.695**
AVE	**0.654**	**OUT3**	0.480	0.384	0.516	0.311	0.633	**0.847**
VIF	**3.011**							

Table C.3.B: Formal Financial Services Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6
BC_GEN	**0.871**					
BC_ISP	0.820	0.765				
IC	0.501	0.415	**0.921**			
ISPC	0.811	**0.776**	0.376	**0.780**		
OUT_Punishment	0.766	0.753	0.698	0.664	**0.882**	
OUT_Reward	0.768	0.749	0.745	0.576	0.871	**0.809**

Table C.3.C: Formal Financial Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.768	0.768	0.766	0.134	0.134	5.732	**0.000**
IC -> ISPC	0.036	0.036	0.028	0.139	0.139	0.257	0.798
OUT -> ISPC	-0.130	-0.130	-0.114	0.224	0.224	0.580	0.564

Table C.4.A: Informal Financial Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings			
Constructs/Items			1	2	3	4
1. CC						
CR	**0.869**	**CC2**	**0.853**	0.711	0.564	0.179
α	**0.802**	**CC4**	**0.757**	0.527	0.501	0.266
AVE	**0.624**	**CC5**	**0.729**	0.401	0.562	0.335
VIF	**1.891**	**CC7**	**0.817**	0.547	0.518	0.162
2. ISPC						
CR	**0.821**	**ISPC2**	0.412	**0.684**	0.361	0.086
α	**0.681**	**ISPC4**	0.512	**0.781**	0.324	0.164
AVE	**0.607**	**ISPC5**	0.693	**0.862**	0.509	0.144
4. SC_Improvement						
CR	**0.846**	**SC6**	0.673	0.503	**0.899**	0.163
α	**0.720**	**SC8**	0.590	0.323	**0.844**	0.196
AVE	**0.651**	**SC9**	0.335	0.437	**0.656**	0.252
VIF	**1.844**					
3. SC_Initiative						
CR	**0.946**	**SC10**	0.240	0.144	0.214	**0.944**
α	**0.885**	**SC5**	0.291	0.179	0.256	**0.950**
AVE	**0.897**					
VIF	**1.099**					

Table C.4.B: Informal Financial Services Model Discriminant Validity of Measurement Model

	1	2	3	4
CC	0.790			
ISPC	**0.844**	**0.779**		
SC_Improvement	0.821	0.722	**0.807**	
SC_Initiative	0.530	0.414	0.498	**0.947**

Table C.4.C: Informal Financial Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
CC -> ISPC	0.693	0.693	0.693	0.113	0.113	6.153	0.000
SC -> ISPC	0.031	0.031	0.045	0.103	0.103	0.298	0.766

Table C.5.A: Full Financial Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings								
Constructs/Items			1	2	3	4	5	6	7	8	9
1. BC_GEN											
CR	**0.760**	**BC1**	**0.871**	0.582	0.588	0.265	0.591	0.542	0.458	0.479	0.297
α	**0.863**	**BC3**	**0.872**	0.589	0.497	0.173	0.555	0.480	0.412	0.444	0.215
AVE	**0.683**										
VIF	**2.154**										
2. BC_ISP											
CR	**0.765**	**BC4**	0.533	**0.863**	0.606	0.144	0.522	0.495	0.373	0.459	0.204
α	**0.867**	**BC6**	0.638	**0.886**	0.614	0.158	0.533	0.496	0.441	0.517	0.183
AVE	**0.692**										
VIF	**2.459**										
3. CC											
CR	**0.653**	**CC4**	0.620	0.602	**0.803**	0.169	0.526	0.544	0.575	0.405	0.266
α	**0.849**	**CC5**	0.461	0.546	**0.766**	0.142	0.401	0.641	0.438	0.504	0.335
AVE	**0.736**	**CC7**	0.426	0.545	**0.853**	0.094	0.544	0.503	0.390	0.414	0.162
VIF	**3.068**										
4. IC											
CR	**0.848**	**IC3**	0.267	0.189	0.162	**0.928**	0.137	0.487	0.515	0.424	0.592
α	**0.918**	**IC5**	0.193	0.126	0.142	**0.913**	0.125	0.407	0.459	0.317	0.608
AVE	**0.821**										
VIF	**2.477**										
5. ISPC											
CR	**0.608**	**ISPC2**	0.414	0.359	0.371	-0.037	**0.688**	0.293	0.132	0.322	0.085
α	**0.822**	**ISPC4**	0.546	0.402	0.446	0.143	**0.788**	0.327	0.215	0.280	0.164
AVE	**0.681**	**ISPC5**	0.563	0.610	0.587	0.183	**0.854**	0.398	0.279	0.494	0.144
6. OUT_Punishment											
CR	**0.779**	**OUT6**	0.538	0.505	0.589	0.455	0.377	**0.901**	0.710	0.606	0.470
α	**0.875**	**OUT7**	0.495	0.495	0.624	0.403	0.403	**0.863**	0.522	0.579	0.421
AVE	**0.717**										
VIF	3.479										
7. OUT_Reward											
CR	**0.830**	**OUT1**	0.430	0.466	0.548	0.451	0.196	0.650	**0.912**	0.520	0.337
α	**0.907**	**OUT3**	0.480	0.384	0.506	0.516	0.312	0.634	**0.910**	0.393	0.458
AVE	**0.795**										
VIF	**2.355**										
8. SC_Improvement											
CR	**0.630**	**SC8**	0.505	0.437	0.551	0.400	0.320	0.565	0.581	**0.761**	0.195
α	**0.772**	**SC9**	0.348	0.451	0.319	0.253	0.436	0.506	0.239	**0.825**	0.253
AVE	0.413										
VIF	**2.238**										
9. SC_Initiative											
CR	**0.897**	**SC10**	0.253	0.202	0.261	0.626	0.144	0.487	0.388	0.244	**0.945**
α	**0.946**	**SC5**	0.302	0.216	0.312	0.608	0.179	0.471	0.437	0.294	**0.949**
AVE	**0.885**										
VIF	**2.039**										

Table C.5.B: Full Financial Services Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6	7	8	9
BC_GEN	0.871								
BC_ISP	**0.905**	0.874							
CC	0.888	**0.914**	0.808						
IC	0.708	0.645	0.638	**0.921**					
ISPC	0.900	0.881	0.885	0.615	0.780				
OUT_Punishment	0.875	0.868	**0.910**	0.836	0.815	0.882			
OUT_Reward	0.840	0.826	0.872	0.853	0.726	**0.916**	**0.911**		
SC_Improvement	0.853	0.865	0.856	0.798	**0.833**	0.905	0.841	**0.793**	
SC_Initiative	0.736	0.685	0.742	0.898	0.643	0.843	0.813	0.730	**0.947**

Table C.5.C: Full Financial Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.562	0.562	0.537	0.150	0.150	3.741	**0.000**
CC -> ISPC	0.374	0.374	0.405	0.148	0.148	2.522	**0.014**
IC -> ISPC		0.079	0.081	0.186	0.186	0.425	0.672
OUT -> ISPC		-0.301	-0.285	0.210	0.210	1.434	0.155
SC -> ISPC		0.054	0.040	0.192	0.192	0.283	0.778

Table C.6.A: Formal Healthcare Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings					
Constructs/Items			1	2	3	4	5	6
1. BC_GEN								
CR	**0.910**	**BC1**	**0.916**	**0.828**	-0.159	0.716	0.337	0.518
α	**0.802**	**BC3**	**0.911**	0.756	0.101	0.700	0.369	0.491
AVE	**0.834**							
VIF	**2.093**							
2. BC_ISP								
CR	0.639	**BC4**	0.201	0.348	0.045	0.373	0.039	0.208
α	0.117	**BC6**	0.862	**0.957**	-0.094	0.560	0.392	0.513
AVE	0.519							
VIF	**1.793**							
3. IC								
CR	**0.831**	**IC3**	0.044	-0.056	**0.921**	-0.242	0.147	0.314
α	**0.617**	**IC5**	-0.153	-0.080	**0.759**	-0.145	-0.101	0.151
AVE	**0.713**							
VIF	**1.102**							
4. ISPC								
CR	**0.825**	**ISPC2**	0.622	0.464	0.044	**0.731**	0.405	0.372
α	**0.680**	**ISPC4**	0.551	0.557	-0.512	**0.735**	-0.077	0.219
AVE	**0.612**	**ISPC5**	0.645	0.451	-0.028	**0.873**	0.405	0.436
5. OUT_Punishment								
CR	**0.932**	**OUT6**	0.399	0.393	0.032	0.361	**0.941**	0.651
α	**0.854**	**OUT7**	0.319	0.311	0.089	0.174	**0.928**	0.534
AVE	**0.873**							
VIF	**1.522**							
6. OUT_Reward								
CR	**0.867**	**OUT1**	0.691	0.630	0.249	0.474	0.648	**0.944**
α	**0.769**	**OUT2**	0.452	0.472	-0.149	0.348	0.229	**0.715**
AVE	**0.687**	**OUT3**	0.218	0.249	0.519	0.248	0.622	**0.812**
VIF	**1.997**							

Table C.6.B: Formal Healthcare Services Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6
BC_GEN	0.913					
BC_ISP	**0.932**	0.720				
IC	0.185	0.274	**0.844**			
ISPC	0.880	**0.796**	0.488	**0.782**		
OUT_Punishment	0.621	0.616	0.251	0.539	**0.934**	
OUT_Reward	0.743	0.736	0.542	0.657	0.798	**0.829**

Table C.6.C: Formal Healthcare Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.699	0.699	0.654	0.245	0.245	2.853	**0.010**
IC -> ISPC	-0.219	-0.219	-0.178	0.239	0.239	0.916	0.370
OUT -> ISPC	0.074	0.074	0.126	0.278	0.278	0.267	0.792

Table C.7.A: Informal Healthcare Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings			
Constructs/Items			1	2	3	4
1. CC						
CR	**0.898**	**CC2**	**0.808**	0.481	0.579	0.325
α	**0.831**	**CC5**	**0.892**	0.587	0.603	0.396
AVE	**0.747**	**CC7**	**0.890**	0.630	0.579	0.205
VIF	**1.976**					
2. ISPC						
CR	**0.893**	**ISPC2**	0.603	**0.892**	0.610	0.047
α	**0.760**	**ISPC5**	0.584	**0.904**	0.642	0.230
AVE	**0.806**					
4. SC_Improvement						
CR	**0.770**	**SC6**	0.428	0.471	**0.782**	0.102
α	**0.551**	**SC8**	0.617	0.677	**0.654**	0.218
AVE	**0.529**	**SC9**	0.437	0.387	**0.741**	0.312
VIF	**1.895**					
3. SC_Initiative						
CR	**0.899**	**SC10**	0.219	0.045	0.167	**0.879**
α	**0.778**	**SC5**	0.397	0.219	0.346	**0.927**
AVE	**0.816**					
VIF	**1.143**					

Table C.7.B: Informal Healthcare Services Model Discriminant Validity of Measurement Model

	1	2	3	4
CC	**0.864**			
ISPC	0.813	**0.898**		
SC_Improvement	0.823	0.835	**0.727**	
SC_Initiative	0.593	0.397	0.543	**0.903**

Table C.7.C: Informal Healthcare Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
CC -> ISPC	0.485	0.485	0.499	0.237	0.237	2.047	0.053
SC -> ISPC	0.261	0.261	0.269	0.249	0.249	1.047	0.307

Table C.8.A: Full Healthcare Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings								
Constructs/Items			1	2	3	4	5	6	7	8	9
1. BC_GEN											
CR	**0.910**	**BC1**	**0.916**	**0.829**	0.330	-0.160	0.708	0.337	0.517	0.616	0.150
α	**0.802**	**BC3**	**0.911**	**0.756**	0.469	0.100	0.708	0.369	0.491	0.555	0.078
AVE	**0.834**										
VIF	**2.311**										
2. BC_ISP											
CR	0.639	**BC4**	0.202	0.347	0.109	0.045	0.362	0.039	0.208	0.239	-0.111
α	0.117	**BC6**	**0.862**	**0.958**	0.398	-0.094	0.554	0.392	0.512	0.579	0.036
AVE	**0.519**										
VIF	**2.063**										
3. CC											
CR	**0.896**	**CC2**	0.356	0.309	**0.773**	0.239	0.317	0.720	0.638	0.574	0.325
α	**0.831**	**CC5**	0.511	0.482	**0.907**	-0.027	0.557	0.790	0.589	0.603	0.397
AVE	**0.743**	**CC7**	0.266	0.252	**0.899**	0.030	0.556	0.608	0.575	0.575	0.206
VIF	4.751										
4. IC											
CR	**0.831**	**IC3**	0.044	-0.056	0.069	**0.919**	-0.211	0.147	0.314	0.066	0.397
α	**0.617**	**IC5**	-0.153	-0.080	0.027	**0.763**	-0.128	-0.101	0.152	0.193	0.428
AVE	**0.713**										
VIF	**1.488**										
5. ISPC											
CR	**0.827**	**ISPC2**	0.622	0.464	0.596	0.043	**0.759**	0.405	0.372	0.607	0.048
α	**0.680**	**ISPC4**	0.551	0.556	0.155	-0.511	**0.695**	-0.077	0.219	0.388	0.012
AVE	**0.616**	**ISPC5**	0.645	0.451	0.597	-0.028	**0.889**	0.405	0.436	0.637	0.232
6. OUT_Punishment											
CR	**0.932**	**OUT6**	0.399	0.393	0.805	0.031	0.383	**0.941**	0.651	0.467	0.321
α	**0.854**	**OUT7**	0.319	0.312	0.695	0.087	0.198	**0.928**	0.535	0.383	0.337
AVE	**0.873**										
VIF	3.405										
7. OUT_Reward											
CR	**0.867**	**OUT1**	0.691	0.630	0.597	0.248	0.480	0.648	**0.944**	0.711	0.478
α	**0.769**	**OUT2**	0.452	0.472	0.381	-0.149	0.326	0.229	**0.714**	0.509	0.169
AVE	**0.687**	**OUT3**	0.218	0.248	0.674	0.519	0.275	0.622	**0.812**	0.601	0.359
VIF	**2.628**										
8. SC_Improvement											
CR	**0.770**	**SC6**	0.700	0.694	0.422	0.250	0.465	0.323	0.750	**0.784**	0.104
α	**0.551**	**SC8**	0.306	0.107	0.601	0.050	0.596	0.378	0.437	**0.643**	0.218
AVE	**0.529**	**SC9**	0.394	0.513	0.449	0.000	0.469	0.302	0.436	**0.748**	0.313
VIF	3.343										
9. SC_Initiative											
CR	**0.898**	**SC10**	-0.113	-0.256	0.212	0.552	-0.078	0.289	0.224	0.167	**0.876**
α	**0.778**	**SC5**	0.288	0.200	0.400	0.337	0.266	0.341	0.514	0.347	**0.929**
AVE	**0.816**										
VIF	**1.824**										

Table C.8.B: Full Healthcare Services Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6	7	8	9
BC_GEN	0.913								
BC_ISP	**0.932**	0.720							
CC	0.661	0.637	0.862						
IC	0.188	0.274	0.248	**0.845**					
ISPC	0.880	0.791	0.759	0.457	**0.785**				
OUT_Punishment	0.621	0.616	**0.897**	0.249	0.562	**0.934**			
OUT_Reward	0.743	0.736	0.825	0.542	0.663	0.798	0.829		
SC_Improvement	0.801	**0.783**	0.819	0.365	0.835	0.676	**0.860**	**0.728**	
SC_Initiative	0.354	0.045	0.593	0.689	0.358	0.593	0.654	0.545	**0.903**

Table C.8.C: Full Healthcare Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.612	0.612	0.549	0.230	0.230	2.659	**0.015**
CC -> ISPC	0.511	0.511	0.480	0.290	0.290	1.764	0.092
IC -> ISPC	-0.225	-0.225	-0.160	0.204	0.204	1.100	0.284
OUT -> ISPC	-0.551	-0.551	-0.424	0.379	0.379	1.455	0.160
SC -> ISPC	0.387	0.387	0.338	0.266	0.266	1.457	0.160

Table C.9.A: Formal Information Technology Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings					
Constructs/Items			1	2	3	4	5	6
1. BC_GEN								
CR	**0.888**	**BC1**	**0.884**	0.368	-0.033	0.408	0.260	0.248
α	**0.748**	**BC3**	**0.903**	0.455	-0.036	0.572	0.218	0.426
AVE	**0.798**							
VIF	**1.486**							
2. BC_ISP								
CR	**0.800**	**BC4**	0.425	**0.845**	-0.152	0.459	0.083	0.253
α	**0.503**	**BC6**	0.325	**0.788**	-0.009	0.405	0.048	0.138
AVE	**0.667**							
VIF	**1.317**							
3. IC								
CR	**0.894**	**IC3**	-0.107	-0.053	**0.917**	-0.199	0.421	0.219
α	**0.763**	**IC5**	0.051	-0.142	**0.880**	-0.167	0.459	0.332
AVE	**0.808**							
VIF	**1.480**							
4. ISPC								
CR	**0.837**	**ISPC2**	0.522	0.394	-0.191	**0.811**	0.181	0.254
α	**0.709**	**ISPC4**	0.349	0.418	-0.200	**0.760**	0.046	0.137
AVE	**0.631**	**ISPC5**	0.427	0.458	-0.096	**0.811**	0.166	0.130
5. OUT_Punishment								
CR	**0.846**	**OUT6**	0.060	-0.010	0.512	-0.068	**0.821**	0.245
α	**0.639**	**OUT7**	0.365	0.134	0.343	0.318	**0.889**	0.382
AVE	**0.733**							
VIF	**1.506**							
6. OUT_Reward								
CR	**0.859**	**OUT1**	0.367	0.129	0.171	0.189	0.293	**0.854**
α	**0.752**	**OUT2**	0.199	0.375	0.314	0.156	0.331	**0.747**
AVE	**0.671**	**OUT3**	0.361	0.110	0.260	0.203	0.297	**0.851**
VIF	**1.397**							

Table C.9.B: Formal Information Technology Services Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6
BC_GEN	**0.893**					
BC_ISP	0.680	**0.817**				
IC	0.196	0.323	**0.899**			
ISPC	0.743	0.728	0.453	**0.794**		
OUT_Punishment	0.516	0.286	0.698	0.413	**0.856**	
OUT_Reward	0.617	0.494	0.548	0.473	0.611	**0.819**

Table C.9.C: Formal Information Technology Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.568	0.568	0.539	0.263	0.263	2.160	**0.033**
IC -> ISPC	-0.218	-0.218	-0.188	0.256	0.256	0.854	0.395
OUT -> ISPC	0.130	0.131	0.150	0.287	0.287	0.454	0.650

Table C.10.A: Informal Information Technology Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement

			Loadings/Cross-Loadings			
Constructs/Items			1	2	3	4
1. CC						
CR	**0.824**	**CC2**	**0.868**	0.667	0.414	-0.023
α	**0.684**	**CC5**	**0.812**	0.538	0.439	0.205
AVE	**0.613**	**CC7**	**0.653**	0.407	0.383	0.091
VIF	**1.414**					
2. ISPC						
CR	**0.837**	**ISPC2**	0.529	**0.774**	0.282	-0.114
α	**0.709**	**ISPC4**	0.493	**0.763**	0.225	-0.103
AVE	**0.632**	**ISPC5**	0.639	**0.845**	0.406	-0.072
4. SC_Improvement						
CR	**0.788**	**SC6**	0.280	0.158	**0.741**	0.347
α	**0.601**	**SC8**	0.463	0.339	**0.833**	0.266
AVE	**0.556**	**SC9**	0.449	0.423	**0.651**	0.077
VIF	**1.533**					
3. SC_Initiative						
CR	**0.901**	**SC10**	0.102	-0.118	0.320	**0.910**
α	**0.780**	**SC5**	0.084	-0.096	0.273	**0.900**
AVE	**0.819**					
VIF	**1.102**					

Table C.10.B: Informal Information Technology Services Model Discriminant Validity of Measurement

	1	2	3	4
CC	0.783			
ISPC	**0.838**	**0.795**		
SC_Improvement	0.722	0.625	**0.745**	
SC_Initiative	0.321	0.344	0.573	**0.905**

Table C.10.C: Informal Information Technology Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
CC -> ISPC	0.746	0.746	0.695	0.178	0.178	4.205	**0.000**
SC -> ISPC	-0.109	-0.109	-0.029	0.258	0.258	0.423	0.673

Table C.11.A: Full Information Technology Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings								
Constructs/Items			1	2	3	4	5	6	7	8	9
1. BC_GEN											
CR	**0.888**	**BC1**	**0.884**	0.368	0.386	-0.032	0.406	0.260	0.248	0.253	-0.055
α	**0.748**	**BC3**	**0.903**	0.455	0.520	-0.034	0.565	0.218	0.426	0.361	0.004
AVE	**0.798**										
VIF	**1.718**										
2. BC_ISP											
CR	**0.800**	**BC4**	0.425	**0.845**	0.452	-0.152	0.462	0.083	0.253	0.417	0.123
α	**0.503**	**BC6**	0.325	**0.788**	0.300	-0.009	0.406	0.048	0.138	0.249	-0.119
AVE	**0.667**										
VIF	**1.514**										
3. CC											
CR	**0.824**	**CC2**	0.432	0.429	**0.868**	-0.085	0.666	0.206	0.165	0.414	-0.023
α	**0.684**	**CC5**	0.327	0.361	**0.810**	0.060	0.533	0.243	0.316	0.439	0.205
AVE	**0.613**	**CC7**	0.464	0.287	**0.656**	-0.009	0.411	0.201	0.469	0.383	0.091
VIF	**1.864**										
4. IC											
CR	**0.894**	**IC3**	-0.107	-0.053	-0.017	**0.914**	-0.192	0.421	0.219	0.209	0.620
α	**0.763**	**IC5**	0.051	-0.142	-0.023	**0.884**	-0.167	0.459	0.332	0.170	0.537
AVE	**0.808**										
VIF	**0.192**										
5. ISPC											
CR	**0.837**	**ISPC2**	0.522	0.394	0.530	-0.190	**0.787**	0.181	0.254	0.282	-0.114
α	**0.709**	**ISPC4**	0.349	0.418	0.493	-0.200	**0.764**	0.046	0.137	0.225	-0.103
AVE	**0.632**	**ISPC5**	0.427	0.458	0.639	-0.097	**0.833**	0.166	0.130	0.406	-0.072
6. OUT_Punishment											
CR	**0.846**	**OUT6**	0.060	-0.010	0.051	0.512	-0.065	**0.821**	0.245	0.265	0.583
α	**0.639**	**OUT7**	0.365	0.134	0.381	0.344	0.314	**0.889**	0.382	0.296	0.393
AVE	**0.733**										
VIF	**1.776**										
7. OUT_Reward											
CR	**0.859**	**OUT1**	0.367	0.129	0.242	0.172	0.180	0.293	**0.854**	0.286	0.210
α	**0.752**	**OUT2**	0.199	0.375	0.370	0.314	0.158	0.331	**0.747**	0.441	0.400
AVE	**0.671**	**OUT3**	0.361	0.110	0.299	0.261	0.197	0.297	**0.851**	0.296	0.285
VIF	**1.559**										
8. SC_Improvement											
CR	**0.788**	**SC6**	0.230	0.230	0.279	0.295	0.155	0.253	0.231	**0.741**	0.347
α	**0.601**	**SC8**	0.247	0.340	0.463	0.144	0.338	0.258	0.446	**0.833**	0.266
AVE	**0.556**	**SC9**	0.324	0.387	0.449	-0.010	0.421	0.222	0.226	**0.651**	0.077
VIF	**1.702**										
9. SC_Initiative											
CR	**0.901**	**SC10**	-0.058	0.015	0.101	0.598	-0.119	0.515	0.341	0.320	**0.910**
α	**0.780**	**SC5**	0.011	0.008	0.084	0.571	-0.098	0.492	0.311	0.273	**0.900**
AVE	**0.819**										
VIF	**2.187**										

Table C.11.B: Full Information Technology Services Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6	7	8	9
BC_GEN	**0.893**								
BC_ISP	0.680	**0.817**							
CC	0.714	0.682	**0.783**						
IC	0.192	0.324	0.149	**0.899**					
ISPC	0.739	0.730	0.837	0.448	**0.795**				
OUT_Punishment	0.516	0.286	0.522	0.698	0.411	**0.856**			
OUT_Reward	0.617	0.494	0.607	0.549	0.467	0.611	**0.819**		
SC_Improvement	0.588	0.644	0.722	0.461	0.623	0.573	0.642	**0.745**	
SC_Initiative	0.165	0.112	0.320	0.804	0.346	0.746	0.601	0.573	**0.905**

Table C.11.C: Full Information Technology Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.334	0.334	0.293	0.278	0.278	1.202	0.231
CC -> ISPC	0.526	0.526	0.478	0.253	0.253	2.079	**0.040**
IC -> ISPC	-0.137	-0.137	-0.124	0.231	0.231	0.595	0.553
OUT -> ISPC	-0.005	-0.005	0.031	0.280	0.280	0.017	0.987
SC -> ISPC	-0.048	-0.046	-0.024	0.285	0.285	0.161	0.873

Table C.12.A: Formal Other Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings					
Constructs/Items			1	2	3	4	5	6
1. BC_GEN								
CR	**0.871**	**BC1**	**0.880**	0.594	0.043	0.577	0.288	0.300
α	**0.703**	**BC3**	**0.876**	0.577	0.061	0.554	0.192	0.249
AVE	**0.771**							
VIF	**1.842**							
2. BC_ISP								
CR	**0.849**	**BC4**	0.598	**0.868**	0.149	0.696	0.330	0.354
α	**0.646**	**BC6**	0.547	**0.851**	0.180	0.561	0.363	0.423
AVE	**0.738**							
VIF	**2.068**							
3. IC								
CR	**0.892**	**IC3**	0.070	0.198	**0.997**	0.123	0.508	0.470
α	**0.851**	**IC5**	-0.043	0.086	**0.787**	0.014	0.451	0.479
AVE	**0.807**							
VIF	**1.531**							
4. ISPC								
CR	**0.870**	**ISPC2**	0.544	0.618	0.140	**0.845**	0.230	0.203
α	**0.775**	**ISPC4**	0.520	0.644	0.077	**0.839**	0.245	0.255
AVE	**0.690**	**ISPC5**	0.541	0.565	0.066	**0.807**	0.189	0.167
5. OUT_Punishment								
CR	**0.872**	**OUT6**	0.212	0.277	0.405	0.123	**0.876**	0.564
α	**0.706**	**OUT7**	0.268	0.429	0.499	0.344	**0.882**	0.580
AVE	**0.773**							
VIF	**1.958**							
6. OUT_Reward								
CR	**0.914**	**OUT1**	0.311	0.432	0.431	0.238	0.551	**0.897**
α	**0.859**	**OUT2**	0.287	0.434	0.454	0.281	0.607	**0.876**
AVE	**0.780**	**OUT3**	0.230	0.327	0.394	0.145	0.565	**0.877**
VIF	**2.064**							

Table C.12.B: Formal Other Services Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6
BC_GEN	**0.878**					
BC_ISP	0.816	**0.859**				
IC	0.243	0.437	**0.899**			
ISPC	0.803	0.857	0.338	**0.831**		
OUT_Punishment	0.523	0.635	0.717	0.516	**0.879**	
OUT_Reward	0.559	0.671	0.695	0.501	0.807	**0.883**

Table C.12.C: Formal Other Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.787	0.788	0.786	0.045	0.045	17.581	**0.000**
IC -> ISPC	0.057	0.057	0.052	0.076	0.076	0.748	0.455
OUT -> ISPC	-0.092	-0.092	-0.088	0.066	0.066	1.399	0.164

Table C.13.A: Informal Other Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings			
Constructs/Items			1	2	3	4
1. CC						
CR	**0.873**	**CC2**	**0.825**	0.571	0.586	0.192
α	**0.811**	**CC4**	**0.741**	0.311	0.620	0.304
AVE	**0.632**	**CC5**	**0.777**	0.462	0.528	0.133
VIF	**2.196**	**CC7**	**0.833**	0.602	0.601	0.075
2. ISPC						
CR	**0.870**	**ISPC2**	0.570	**0.854**	0.467	0.042
α	**0.775**	**ISPC4**	0.507	**0.832**	0.462	0.101
AVE	**0.690**	**ISPC5**	0.513	**0.805**	0.391	-0.021
4. SC_Improvement						
CR	**0.856**	**SC6**	0.602	0.477	**0.806**	0.146
α	**0.748**	**SC8**	0.552	0.363	**0.835**	0.145
AVE	**0.665**	**SC9**	0.623	0.461	**0.805**	0.141
VIF	**2.153**					
3. SC_Initiative						
CR	**0.903**	**SC10**	0.144	0.028	0.162	**0.907**
α	**0.784**	**SC5**	0.217	0.062	0.158	**0.906**
AVE	**0.822**					
VIF	**1.053**					

Table C.13.B: Informal Other Services Model Discriminant Validity of Measurement Model

	1	2	3	4
CC	0.795			
ISPC	0.800	**0.830**		
SC_Improvement	**0.852**	0.728	**0.816**	
SC_Initiative	0.446	0.222	0.420	**0.907**

Table C.13.C: Informal Other Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
CC -> ISPC	0.606	0.606	0.606	0.093	0.093	6.506	**0.000**
SC -> ISPC	0.048	0.049	0.058	0.100	0.100	0.486	0.627

Table C.14.A: Full Other Services Model Loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and VIF of Measurement Instruments

			Loadings/Cross-Loadings								
Constructs/Items			1	2	3	4	5	6	7	8	9
1. BC_GEN											
CR	**0.871**	**BC1**	**0.880**	0.594	0.457	0.044	0.578	0.288	0.300	0.539	0.073
α	**0.703**	**BC3**	**0.876**	0.577	0.421	0.062	0.554	0.192	0.249	0.475	0.037
AVE	**0.771**										
VIF	**2.061**										
2. BC_ISP											
CR	**0.849**	**BC4**	0.598	**0.868**	0.583	0.150	0.696	0.330	0.354	0.530	0.081
α	**0.646**	**BC6**	0.547	**0.851**	0.556	0.180	0.560	0.363	0.423	0.514	0.103
AVE	**0.738**										
VIF	**2.453**										
3. CC											
CR	**0.873**	**CC2**	0.434	0.582	**0.825**	0.253	0.571	0.376	0.479	0.586	0.192
α	**0.811**	**CC4**	0.279	0.380	**0.741**	0.357	0.310	0.423	0.595	0.620	0.304
AVE	**0.632**	**CC5**	0.374	0.475	**0.777**	0.209	0.462	0.352	0.538	0.528	0.133
VIF	**2.743**	**CC7**	0.454	0.608	**0.833**	0.102	0.602	0.289	0.396	0.601	0.075
4. IC											
CR	**0.890**	**IC3**	0.070	0.198	0.271	**0.998**	0.123	0.508	0.470	0.256	0.595
α	**0.851**	**IC5**	-0.043	0.086	0.140	**0.784**	0.013	0.451	0.479	0.163	0.647
AVE	**0.805**										
VIF	**2.071**										
5. ISPC											
CR	**0.870**	**ISPC2**	0.544	0.618	0.570	0.141	**0.849**	0.230	0.203	0.467	0.042
α	**0.775**	**ISPC4**	0.520	0.644	0.507	0.077	**0.834**	0.245	0.255	0.462	0.101
AVE	**0.690**	**ISPC5**	0.541	0.565	0.513	0.067	**0.809**	0.189	0.167	0.391	-0.021
6. OUT_Punishment											
CR	**0.872**	**OUT6**	0.212	0.277	0.298	0.404	0.122	**0.876**	0.564	0.423	0.463
α	**0.706**	**OUT7**	0.268	0.429	0.469	0.499	0.344	**0.882**	0.580	0.396	0.506
AVE	**0.773**										
VIF	**2.171**										
7. OUT_Reward											
CR	**0.914**	**OUT1**	0.311	0.432	0.518	0.430	0.237	0.551	**0.897**	0.548	0.378
α	**0.859**	**OUT2**	0.287	0.434	0.646	0.454	0.282	0.607	**0.876**	0.601	0.406
AVE	**0.780**	**OUT3**	0.230	0.327	0.437	0.393	0.143	0.565	**0.877**	0.515	0.413
VIF	**2.770**										
8. SC_Improvement											
CR	**0.856**	**SC6**	0.478	0.570	0.602	0.226	0.477	0.394	0.525	**0.806**	0.146
α	**0.748**	**SC8**	0.398	0.434	0.552	0.218	0.362	0.367	0.541	**0.835**	0.145
AVE	**0.665**	**SC9**	0.538	0.484	0.623	0.175	0.461	0.379	0.471	**0.805**	0.141
VIF	**2.888**										
9. SC_Initiative											
CR	**0.903**	**SC10**	0.011	0.056	0.144	0.568	0.027	0.504	0.394	0.162	**0.907**
α	**0.784**	**SC5**	0.103	0.139	0.217	0.545	0.062	0.496	0.426	0.158	**0.906**
AVE	**0.822**										
VIF	**2.091**										

Table C.14.B: Full Other Services Model Discriminant Validity of Measurement Model

	1	2	3	4	5	6	7	8	9
BC_GEN	**0.878**								
BC_ISP	0.816	**0.859**							
CC	0.707	0.815	0.795						
IC	0.245	0.438	0.514	**0.897**					
ISPC	0.803	0.856	**0.799**	0.340	**0.831**				
OUT_Punishment	0.523	0.635	0.661	0.717	0.516	**0.879**			
OUT_Reward	0.559	0.671	0.778	0.694	0.500	0.807	**0.883**		
SC_Improvement	0.760	0.779	0.852	0.503	0.728	0.682	0.793	**0.816**	
SC_Initiative	0.251	0.327	0.446	0.783	0.221	0.743	0.672	0.420	**0.907**

Table C.14.C: Full Other Services Model Results of Structural Model Analysis

Construct	β	Original Sample	Sample Mean	Standard Deviation	Standard Error	t-value	p-value
BC -> ISPC	0.614	0.614	0.607	0.080	0.080	7.699	**0.000**
CC -> ISPC	0.376	0.376	0.384	0.097	0.097	3.870	**0.000**
IC -> ISPC	0.064	0.064	0.064	0.072	0.072	0.885	0.378
OUT -> ISPC	-0.24	-0.240	-0.247	0.088	0.088	2.737	**0.007**
SC -> ISPC	-0.006	-0.005	0.003	0.110	0.110	0.044	0.965

VITA

SHAUN STEWART

EDUCATION AND PROFESSIONAL EXPERIENCE

2018-2021	Deputy Operations Branch Chief U.S. Southern Command Miami, FL
2021-	U.S. Navy Reserve Officer U.S. Navy Reserve, U.S. Southern Command Miami, FL
2015-2018	Program Manager U.S. Department of Defense Washington, D.C.
2013	Master of Business Administration (MBA) FLORIDA INTERNATIONAL UNIVERSITY Miami, FL
2009	B.S. in Liberal Studies (Emphasis: Persian Studies) EXCELSIOR COLLEGE Albany, NY
2007-2018	Project Manager U.S. Department of Defense Multiple global locations
2007	A.A.S. in Military Operations COCHISE COLLEGE Sierra Vista, AZ
2006-2007	Tug and Barge Operations Technician Moran Towing Savannah, GA
2006	A.A. in Persian Farsi DEFENSE LANGUAGE INSTITUTE Monterey, CA
1999-2006	U.S. Government Cryptologic Linguist U.S. Navy Augusta, GA