ASSESSMENT OF INFORMATION SECURITY CULTURE IN HIGHER EDUCATION

by

HENRY W. GLASPIE, IV
B.A. Hampton University, 1992
B.S. University of Cincinnati, 2001
M.S. University of Central Florida, 2005
M.S. University of Central Florida, 2014

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Modeling and Simulation
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Summer Term
2018

Major Professor: Waldemar Karwowski

ABSTRACT

Information security programs are instituted by organizations to provide guidance to their users who handle their data and systems. The main goal of these programs is to protect the organization's information assets through the creation and cultivation of a positive information security culture within the organization. As the collection and use of data expands in all economic sectors, the threat of data breach due to human error increases. Employee's behavior towards information security is influenced by the organizations information security programs and the overall information security culture. This study examines the human factors of an information security program and their effect on the information security culture. These human factors consist of stringency of organizational policies, behavior deterrence, employee attitudes towards information security, training and awareness, and management support of the information security programs. A survey questionnaire was given to employees in the Florida College System to measure the human aspects of the information security programs. Confirmatory factor analysis (CFA) and Structural Equation Modeling (SEM) were used to investigate the relationships between the variables in the study using IBM® SPSS® Amos 24 software. The study results show that management support and behavior deterrence have a significant positive relationship with information security. Additionally, the results show no significant association between information security culture and organization policies, employee commitment and employee awareness. This suggests a need for further refinement of the model and the survey tool design to properly assess human factors of information security programs and their effects on the organizational security culture.

Dedicated to my parents, my children, and all my family and friends who have mentored me since birth.

ACKNOWLEDGMENTS

First, I would like to thank my lord and savior, Jesus Christ, who blessed me with opportunities and placed people in my life who have helped me at every stop along my journey.

I would like to give a special thanks to Dr. Waldemar Karwowski, my advisor, dissertation chair and chair of the Department of Industrial Engineering & Management Systems, for providing me motivation and direction through this dissertation process. I would also like to thank my dissertation committee: Dr. Thomas Wan, Dr. Peter Hancock, and Dr. Bruce Caulkins. Each played an important part in shaping the direction of my research.

Additionally, I would like to thank my parents, children, extended family, and friends who were extremely supportive throughout my education and career. Their mentorship, enthusiastic attitude towards my goals, and love gave me a foundation to stand upon when I felt like I could stand no longer.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS/ACRONYMS

CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CIO	Chief Information Officer
C.R.	Critical Ratio
df	Degrees of Freedom
FCS	Florida College System
FERPA	Family Educational Rights and Privacy Act
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
IRB	Institutional Review Board
ISP	Information Security Program
M.I.	Modification Indices
RMSEA	Root Mean Square Error of Approximation
SEM	Structural Equation Modeling
TLI	Tucker and Lewis Index

UCF	University of Central Florida

CHAPTER ONE: INTRODUCTION

1.1 Background

In today's environment, organizations collect, transmit, and use data to perform a variety of business-related functions. These functions affect communications, finance, commerce, higher education, and government. Their proliferation of data makes them fertile targets for cyber criminals. The cyber criminals (or hackers) could be working independently, for other organizations, or nation-state actors (Adams & Makramalla, 2015). The threat of cyber-attack has resulted in large investments in secure data storage, networks, and cyber-defense systems (Safa et al., 2015). Even with these investments, cyber-crime is still very prevalent with massive breaches being reported almost daily in the news media. Over the past few years, cyber-crime and information security incidents have seen an exponential annual increase. According to the 2015 IBM Cyber Security Intelligence Index, there were nearly twice as many cyber security incidents than in 2014 (IBM, 2015).

Despite the significant budgetary expenditures in tools and systems to fight cyber-attacks, there is very little comparative investment in human factors and security culture. Information security is not solely a technical issue. An organization's investment in just technology does not eliminate the many security challenges. Among cyber security practitioners, it is well known that humans are the weak link in information security (Acuña, 2016) and many human factors affect information security management (Alavi, Islam, Jahankhani, & Al-Nemrat, 2013). Information system user's undesirable behavior is a direct reflection of the culture of information security in the organization (Öğütçü, Testik, & Chouseinoglou, 2016). The aforementioned IBM report states that 9 out of 10 information security incidents were caused by some sort of human error.

This is a 10% increase in human involvement reported over a two-year span (IBM, 2013). In spite of this, organizations have still continued to focus their cybersecurity investments in the area of technology infrastructure (Herschberger, 2014). There is an obvious gap in information security among organizations that only consider technology aspects of security and forego the human aspects.

1.2 Statement of the Problem

Human errors can be the result of negligence, accident, or deliberate action. Because of this, organizations need to invest in building an information security culture that is inclusive of all personnel and leadership (Guo, 2013). Organizations that have a security culture minimize the risk posed to information privacy (Da Veiga, & Martins, 2015a). Prevalent research highlights that a positive security culture can increase security policy compliance, strengthen the overall information security posture, and reduce the financial loss due to security breaches.

Over the last few years there has been a significant increase in information security breaches among higher education institutions (Grama, 2014). Data from the Privacy Rights Clearinghouse reveals that since 2005 there have been 788 publicly disclosed data breaches in higher education resulting in 14.8 million records compromised. Of these breaches, 30% were the result of human error (Privacy Rights Clearinghouse, 2017). Higher education organizations are ripe for cybersecurity incidents due to their vast amounts of research, student, and financial data used and stored on their computer systems.

In higher education and many other industries, there is a necessity to assess the information security programs that directly influence the overall information culture. Currently, there is a need to research the effects of the human aspects of information security programs and their causal effect on organizational information security culture. Information security programs that enhance the overall information security culture in an organization are necessary to decrease the human error that leads to this type of data loss.

1.3 Research Objectives

Information security culture has been found to have a positive effect on employee adherence to policy and security behavior (Hu, Xu, Dinev, & Ling, 2011; Parsons et al., 2015; Tang & Zhang, 2016). Alhogail, and Mirza (2014) define information security culture as the "collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in an organization with the aim of influencing employees' security behavior to preserve information security''. These interactions result in either acceptable or unacceptable in actions taken by employees who use the organization's data and systems. With the intent of cultivating a positive information security in higher education institutions, the study has the following goals:

- To develop a model that assesses and evaluates current perceptions of information security culture
- To identify the relationships between human factors in information security and information security culture

- To assist the higher education organizations in evaluating the performance of information security awareness programs

Prior works have focused solely on behavior (Abraham, 2011) or human behavioral theories (Lebek et al., 2014). None of these studies have specifically analyzed the factors that influence the overall information security culture and the challenges that leadership faces in cultivating the culture. Additionally, a conceptual model is created from the relevant literature to highlight each factor's role and its contributions. This quantitative study identifies the correlations that exist between the human aspects of an information security program and information security culture. The outcome of this research can be used to improve information security management programs in organizations and by professionals and researchers for conducting further research in this area.

CHAPTER TWO: LITERATURE REVIEW

2.1 Information Security Culture Model

In synthesizing the research, a theoretical model was developed of the factors that influence information security culture and how they weave together as the fabric of the culture. The model, based on the literature (Alavi, R., Islam, S., Jahankhani, H., & Al-Nemrat, A., 2013; AlHogail, 2015; Badie, N., & Lashkari, A. H., 2012; Knapp, K. J., & Ferrante, C. J., 2014), includes the following factors of: 1) information security policy; 2) behavior deterrence and incentives; 3) attitudes and involvement (employee commitment); 4) training and awareness; 5) management support (see Figure 1).

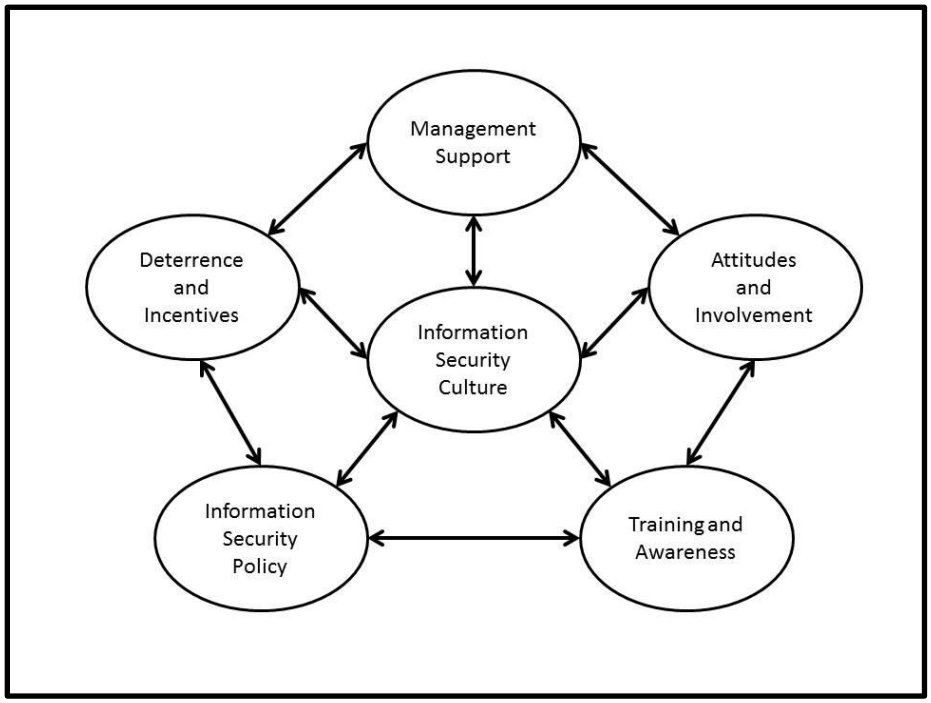


Figure 1: Factors that influence and cultivate an information security culture.

2.2 Information Security Policy

As the focus of information security measures shift from technology to human factors, many authors have investigated the influence and effect that information security policies have on the overall information security culture. Most organizations are required to have some sort of information security policy in place in the organization. This is usually mandated by a regulatory authority (federal, state, local, accreditation, or auditor) as a condition of certification. The policies set mandatory guidelines to influence favorable organizational behavior when using systems or working with data (D'Arcy, Hovav, & Galletta, 2009). All information security policies should comply with and emphasize the organization's objectives (Sari, 2012).

Security policies are created to communicate security protocols, assign clear roles and responsibilities, and provide employees with guidance for acceptable usage to ensure security behaviors during the performance of their jobs (Bulgurcu, Cavusoglu, & Benbasat, 2010). The roles, responsibilities, and guidelines also give clarity to who should be contacted and how information security incidents are handled (Sari 2012). Emphasizing the roles and responsibilities of the users provides a personalization to compliance and promotes ownership. Personalization gives the user an active role in compliance and mitigates the restrictive connotation (Ahlan, Lubis, & Lubis, 2015). By doing this, a reference is provided for training users based on their job function.

The policies should be easily accessible, reviewed periodically, and are applicable to all members, partners, and agents of the organization (Singh et al., 2013). When policies are complex, ambiguous, complicated, vague, or difficult for users to understand, attitudes towards

compliance are negatively affected. Organizations should make their policies as understandable, relevant, and accessible as possible to all employees (Renaud, 2012).

It is organizational management's responsibility to support the information security policy construction process. In their study, Flowerday and Tuyikeze (2016) explain that there is a comprehensive structured methodology for the development of an effective security policy and provides a framework called the "Information Security Policy Development Lifecycle". The authors state that it is essential that management must be highly involved in this process to ensure the proper human and capital resources are allocated. They found that this support is directly correlated to the success of the policy implementation process. Karlsson, Goldkuhl, and Hedström, (2017) propose a list of 8 criteria for policy development. Among these they recommend that security policies be developed in a way that aligns the policy with current work practices and processes. This removes confusion from the employee and eliminates situations where choices are made between policy compliance and task completion.

The research by Haeussinger and Kranz (2013) shows that the creation and promotion information security policies is the foundational element of any information security management program and has a positive influence on employee awareness. Research by Safa et al. (2012) also notes that an organization's information security policy has an enormous influence on security conscious care behavior. Choi, Levy, and Hovav (2013) examined how user awareness of security policies contributed to their initiative skill and action skill, and computer skill related to security. The results showed that awareness of security policies showed a significant effect on "action skill" or compliance with policies and procedures.

Having a security policy alone does not ensure employee compliance. An organization must have a comprehensive information security policy in order to have a meaningful impact on information security culture. A comprehensive security policy assimilates technology systems security and security culture (Acuña, 2016). This is supported in research by Chen, Ramamurthy, and Wen (2015) showing that awareness alone contributes little to the organization security culture.

Hu et al. (2012) noted that a stronger positive attitude towards information security compliance, leads to an increased intention towards policy compliance. Organizations that actively encourage their employees to comply with their policies see an increase in overall information security (Chen & Li, 2014). Therefore, management must make sure that employees fully understand the policies and favorably perceive them. Additionally, organizational management must take an active role in motivating their users towards policy compliance. Siponen et al (2014), states that employee's attitudes toward information security threats have a significant impact on their compliance with information security policies. Therefore, management that works to actively promote compliance among their employees see an increase in positive security behavior (Tang & Zhang, 2016). This can be achieved by understanding the forces that lead to accountable and compliant behavior. Those employees who readily exhibit compliance behavior can be "security allies" who help shape the compliant culture in the organization (Crossler et al., 2013).

Research by Han, Kim, & Kim (2017), shows that perceived benefits affect employee policy compliance. Organizations that deliver awareness and training that focuses on the benefits of security policy compliance will see more positive outcomes. This idea is further supported in

the Box and Pottas (2014) research. The authors also suggest that management should employ the compliance promoting actions of outlining the benefits of policy compliance, and presenting messages to users that stimulate their sense of achievement in compliance and a sense of teamwork or common purpose. These actions build a feeling of organizational trust by the employee and a positive attitude towards compliance.

Policy compliance has also been found to be greatly influenced by social pressure. Findings in Cheng et al. (2013) suggested that perceptions of fellow employees or immediate supervisors are influential on intentions towards policy violations. This is mirrored in a study by Ifinedo (2014) that found that users form social bonds with other employees and use them as role models. These role models then influence what is perceived as beliefs and behaviors as well as attitudes towards compliance. Management can leverage these relationships as informal control mechanisms in security awareness program activities. Teambuilding and other exercises that enhance workplace relationships would then be incorporated to bring about positive security behaviors.

2.3 Deterrence and Incentives

Most information security policies contain language that informs the applicable parties about the penalties of noncompliance. This is the formal deterrence against negative employee behavior. In many organizations, this punishment could range from remediation to termination. Several studies have discussed the link between an employee's willingness towards security policies compliance and their perceived benefit or cost of compliance versus noncompliance. Results from a study by Parsons et al. (2015), reveals that organizations with higher severity in

punishments for noncompliance were more likely to have a healthy information security culture. Without clear and consistent consequences for noncompliance, users are likely to demonstrate risky or noncompliant behavior.

Moreover, it has been shown that these perceptions are based on expected outcomes or assessment of consequences. The employees' beliefs about benefit of compliance and the cost of noncompliance impact their intentions to comply (Bulgurcu et al., 2010). But differing opinions have been presented on how to motivate employees to comply with the organization's security policies. Chen, Ramamurthy, and Wen (2012), showed that both the severity level of punishment and the level of reward significantly affect compliance intention. This is reinforced when there is a high level of certainty that the reward or punishment will be enforced. Also, the impact of punishment on intention to comply is greater when there is low reward.

Aside from severity of punishment and formal sanctions for noncompliance, there have been studies on the effect that informal sanctions have on compliance intention. D'Arcy and Devaraj (2012) reported on the informal sanctions, or social and self-imposed costs, as the need for social approval and acceptance through culturally appropriate and acceptable behavior. The authors also presented evidence that these self-imposed costs are significant determinants of compliance intention and are shown to have more significance than formal sanctions. This shows that moral beliefs and social pressures are considered when employees make compliance decisions. Results from research by Hu et al. (2011) contradict the notion of deterrence as the biggest factor in policy compliance. Their findings suggest that deterrence has no influence on an individual's intent to comply with policy. The authors further state that perceived benefits and

intrinsic satisfactions are more influential in compliance decision making. In their study population, reward or benefit is a larger motivating force.

In studying how rewards or incentives contribute to the information security culture, Farahmand, Atallah, and Spafford (2013) point out that not all incentives positively influence performance and caution against using incentives that are not efficient. Efficient incentives persuade a large number of heterogeneous users to act for the common cause. Acting with a common purpose or in an organizationally prosocial context is the basis of research by Thomson and van Niekerk (2012). In this work, the authors state that when prosocial behavior is cultivated in an organization, the need for punishments or rewards to influence compliance is eliminated. In a prosocial environment, employees are not apathetic to the organizations policies. The organizational goals of information security are accepted without the thought of consequences or expectations of rewards. Vance, Siponen, and Pahnila (2012) stated that rewards can have a negative effect on compliance intention if the perceived benefit of noncompliance is greater than the perceived incentive from the organization. Employees that see intrinsic incentives, such as saving time or ease of use, as a benefit of policy noncompliance, are more likely to exhibit inappropriate security behavior. In conclusion, regardless of deterrence or incentives, adherence to information security policy is a major factor in cultivating an information security culture.

2.4 Attitudes and Involvement

Positive employee attitudes about information security compliance and their involvement in the process is another factor that impacts the information security culture in an organization. Ifinedo (2014) defines attitude as the employee's positive or negative feelings towards a

behavior. Research has shown that user's experience and involvement influences their perceptions or attitudes about information security (Safa et al., 2015). Lebek et al. (2014) highlights the fact that there is a direct relationship between attitude and behavioral intent. Furthermore, an employee's attitude towards organizational compliance and the perceptions of their colleagues in their workplace greatly affects secure behavior (Ifinedo, 2012).

When employees participate in activities that are focused on a commitment to the organization's security goals and engage with like-minded colleagues in such matters, there is a positive effect on information security compliance (Ifinedo, 2014). This emphasizes the importance of active employee involvement. Parsons, et al. (2014b) state that employee knowledge, attitudes, and behaviors are influenced by organizational factors. They draw a conclusion that increased knowledge of policy and procedure is highly correlated with a positive attitude towards the organization's policy and procedure. Safa, et al. (2016) extend this theme with findings that show that the sharing of information security knowledge, security collaboration, and mediation, between the organization and its employees, greatly effects compliance.

Employee attitudes and involvement are also influenced by experience. The research presented in Chen and Zahedi (2016) shows that once users perceive, or have experienced a cyber threat, they are more likely to take protective actions. Results from a study by Öğütçü et al., (2016) confirm these findings by highlighting that the more users perceive threats and increase their awareness of the technology, the more productive their security-focused behavior becomes. Awareness and perception is a positive result of comprehensive information security training. The user's own personal experience or knowledge of incidents that happen to familiar

environments eliminates the thought that it “won’t happen here” or “won’t happen to me” (Davinson, and Sillence, 2010).

Guo, Yuan, Archer, and Connelly (2011) demonstrated that attitudes towards security behavior are also influenced by the effect of job performance, workgroups norms, and perceived identity match. Most users that want to achieve advantages to increase job performance will engage in any action that improves productivity and efficiency. In the same way they avoid actions that are seen as hindrances. With respect to workgroup norms, employees will adopt the attitudes, opinions, and practices of their work teams in the absence of expertise. In this way group attitudes drive the behavior of individuals. Perceived identity match influences security behaviors based on self-identity. If users believe that following policies is an important part of their self-image in their profession, they will more likely adhere to the policies. Employee attitudes can also be influenced by changes to information systems; workspace, regulatory and compliance rules; and job roles or responsibilities. All of these changes can affect employee satisfaction. Failure of organizational management to recognize these changes and how they affect employees could lead to a negative security culture (Dhillon, Syed, & Pedron, 2016).

When users evaluate an information system, satisfaction is the most commonly used measurement. Shropshire, Warkentin, and Sharma (2015), note that information system satisfaction is equated to perceived ease of use and system usefulness. The research shows this to be a significant predictor of system security intention. Montesdioca and Maçada (2015) concluded that user dissatisfaction with security practices can be a risk for information system security. The authors assert that one way to change the negative relation is through user involvement in developing security practices. Developing consistent policies, systems that meet

users' needs, and training in how to use the systems efficiently, can increase employee productivity and satisfaction.

2.5 Training and Awareness

When information security is viewed as an inconvenience or a barrier to task completion, users can be deterred from following security rules and policy compliance. Management can mitigate this risk by properly training their employees on the computers and data systems with which they operate to complete tasks. Research has shown that computer skills and level of experience can affect a user's potential security behavior (Badie & Lashkari, 2012).

Training and awareness is a foundational piece of all thriving information security cultures. It provides employees with the requisite knowledge needed for proper use of systems, compliance with policies, and handling of data. Information security managers must implement training and awareness programs focused on policies, roles, and responsibilities. Employees that lack proper awareness and training can expose the organization to security risks. Organizations need to devote resources towards building information security skills across all levels of personnel and management (Adams et al., 2015). Those that receive training have been shown to demonstrate a more positive information security culture (Da Veiga, Martins, 2015b). No matter the hardware or software system investment, the untrained or unaware employee becomes the vector for cyber-attack (Badie & Lashkari 2012). Inadequate skills and awareness can lead to intentional or unintentional error that can be a liability to security. Computer users who possess the adequate knowledge of information security concepts, exhibit more positive attitude towards information security, which then results in more positive behavior (Parsons, McCormac,

Pattinson, Butavicius, & Jerram, 2014a). Organizations need to provide employee information system and security training that is sufficient to eliminate errors.

While organizations invest heavily in their hardware or software systems, inconvenience, schedules, and business needs often leave employees informally trained or not trained at all. As a result, the unfortunate users become a security liability (Parsons et al., 2014a). Inadequate training in the organizations systems often lead to errors that can place the data and systems at risk. Computer users who possess the adequate knowledge of information security concepts are more comfortable in their use and can contribute to the security awareness program through knowledge sharing. This, in turn, results in positive security behaviors (Anwar et al., 2017). It is incumbent upon management to make sure employees receive the necessary training on the specific systems and their proper use to reduce the organization's security exposure.

Lack of awareness of cyber-attacks against the human factors of information security contributes significantly to breaches caused by human behavior. Management has the responsibility to make sure their awareness programs benefit employees by promoting consistent review and understanding of the importance of handling data and systems and the prevalence of threats against them. Also, the content of the training needs to be constantly reviewed (Alavi et al. 2013). The awareness programs should be customized using the language and jargon specific to the business objectives and environment (Metalidou et al., 2014).

Information security training should not be delivered to users in a "technocratic" or fact-based broadcast. This type of training fails to bridge the gap between the organizations security policies and business objectives and the needs of the audience. Information security training should be focused on the formation of habits in relation to the user's perceptions and the

procedural options available to them. Immersive and scenario-based skills training in incident response can provide users with "hands-on" experience to increase their security knowledge with relevance to their daily tasks. Research by Chen and Zahedi (2016) shows that once users' have experienced a cyber threat, they are more likely to have a protective attitude towards security. Also, Öğütçü et al., (2016) confirms this by accentuating that increased awareness and threat perception leads to more security-focused behavior. Threat awareness and perception are the result of the focused security skills training and help to eliminate laissez faire attitude towards security and awareness. Training that provides relevant and immersive activities to show the steps involved in information security or the impacts of an incident, are shown to be effective in increasing awareness. They give the employee an avenue to retain the experience, rather than the procedural information.

The awareness training should be delivered in a wide variety of modalities to include classroom training, online training via web-based delivery systems and video, newsletters, posters, and fliers. An organization benefits from this variety because it allows the content to be delivered multiple times and in multiple ways. Results from research by Abawajy (2014) show that even though video-based training was preferred modality, all the training methods that were evaluated showed an increase in information security understanding.

McBride, Carter, and Warkentin (2012), noted that training scenarios illicit different reactions among employees with different personality traits. Because of this, the authors imply that information security training must be varied to accommodate individual employee personality types. The data from this study show that different personality types also react differently to threats and sanctions. As a result, organizations must maintain a nuanced and

tailored approach so that their training and awareness programs reflect those differences. Furthermore, organizations under specific regulatory authority should take special care to increase employee awareness of the authority's policies. These trainings should be on a regular recurring basis to keep up with changes in business processes, standards and regulations (Hipsky & Younes, 2015). Information security awareness and training should be included in risk assessment strategies to enhance mitigation. Research has shown that despite the threats of cybercrime and insider breach that organizations face, the employee awareness levels are still lacking. Adoption of comprehensive information security awareness programs fosters a culture of security compliance in an organization (Chan & Mubarak, 2012).

Finally, security awareness must be monitored and measured on a regular basis. Kritzinger and Smith (2008) propose an Information Security Retrieval and Awareness model for the enhancement of security awareness among employees. In this model, the measuring and monitoring dimension provides an assessment to each employee based on security issues relevant to their work processes. The results are then immediately known to management to determine any knowledge gaps and to execute the proper remediation. From these assessments, the organization can determine the information security awareness status and ensure that new and developing security concerns can be integrated and then evaluated in a timely manner.

2.6 Management Support

Management support is an important factor in cultivating an information security culture even though there has not been a lot of research in this area. Consistent top management support is essential to creating a supportive environment in the organization and providing the necessary

support. This support includes budget, technology, and human capital. Support and leadership from management are key contributors to successful implementation of information security efforts. Fazlida and Said (2015) state that organization management must give importance to the promotion of security awareness rather than treating information security as a technology issue. This is necessary to avoid policy rejection or impediments to compliance.

Additionally, consistent support and participation creates an affirming environment which is essential to achieve a positive organization security culture. A study by Alavi et al. (2013) highlights this by showing that management must be a visible and vocal advocate for the security program's policies and goals. This advocacy and participation has been shown to be fostered by management's strong belief in the program objectives and that positive results for the organization can be achieved. Organizational leadership's commitment to promote awareness and to entice their staff to exhibit positive security behaviors directly influences employee's attitudes towards information security threats (Flores & Ekstedt, 2016). Barton et al. (2016) adds to this by showing that the extent of management's belief in information security leads to their increased participation in information security programs. The increased participation in turn leads to greater overall acceptance of security policies and practices within the organization.

Top management must advocate and deliver a clear message of its information policies and goals to the rest of the organization (Alavi et al. 2013). In order for an information security management program to be effective, management must define the organization's information security goals and objectives. It is imperative that managers formulate the strategy for protecting assets and formulate budgets that incorporate information security to negate the risk of damage caused by possible attacks (Montesdioca et al., 2015). Senior management must be actively

involved in the planning and decision-making processes. It is also at this level that the policies and guidelines are developed (Narain Singh, Gupta, & Ojha, 2014). When management is engaged in the process, employees have more positive attitudes towards compliance. The emphasis that leadership places on information security drives the culture (Dhillon et al., 2016). According to research by Said, Abdullah, Uli, and Mohamed (2014), top management support makes the strongest contribution to information security knowledge sharing.

The leadership must think strategically about developing the policies, objectives, and plans that make up the information security strategy. It is then their responsibility to convey clarity and consistency in messages to employees about acceptable behavior and the sanctions for negative actions (Alhogail, 2015). There are correlations between management support and security awareness which is strengthened by the security culture (Knapp & Ferrante, 2014). It is further stated that in environments where the employee tasks are highly dependent upon other employees, management needs to emphasize security awareness and training programs as these employees tend to police each other. In organizations where this type of task dependence doesn't exist, lack of co-worker monitoring and poor attitudes towards compliance may be prevalent. Therefore, management needs emphasize and closely monitor security policy and attitudes for compliance.

The group dynamic is also emphasized in research by Safa et al., 2016. The authors found that management can affect compliance attitudes by facilitating cross-training, knowledge sharing, and security collaboration. Employees who share security knowledge raise awareness on a whole and those who work together on common security goals show a positive attitude towards compliance. Finally, management plays an important role in building proper organizational

structures to support the culture. This structure makes sure that the business strategy and the security function remains aligned. Employee attitudes can be negative towards security if the policies and programs are seen as a hindrance to the employees' task function. This can lead to noncompliance out of the necessity to efficiently complete tasks (Flores, Antonsen, & Ekstedt, 2014).

Further, it has been found that in organizations with a hierarchical structure, employees in management positions (or persons of authority) can have a productive influence on the security aware behavior of coworkers, subordinates, and others in lower positions. Research by Dang-Pham, Pittayachawan, & Bruno (2017) showed that these staff are seen to have power in the workplace and are therefore more likely to affect the security behaviors of others. This outcome was also seen in a study highlighting security behavior influence. The authors suggested that this influence should be maximized to foster organizational trust where management is viewed by subordinate staff as "security champions" and are available to give advice (Dang-Pham, Pittayachawan, & Bruno, 2016). In this role, the senior employees are a reference point for behavior in the absence of IT personnel. This effect is invaluable in creating positive habits and behaviors regarding information security. Another study by Aurigemma and Mattson (2017) suggests that employees in management positions should have separate security awareness trainings and that highlight the impact that their status has on the information security attitudes and behaviors of others. Additionally, management should also participate in combined security awareness trainings with all employees so that they can see how their influence affects the conduct and practice.

As business processes are shaped and redesigned by management, this also influences an organization's security behaviors. Management must also acknowledge the importance of evaluating the information security policies and controls and how they impact users and daily business processes (Flores, Antonsen, & Ekstedt, 2014). Within this alignment of processes and security, the aspects of policy development, acquisition of hardware and software, security awareness and skills training, and data handling controls are essential elements (Young & Windsor, 2010). Consequently, management must have a deep understanding the organization's business processes and how any designs or changes can affect information security. After the thorough analysis, it is then necessary to incorporate these in to the security awareness program content to ensure an understanding among employees (Dhillon, Syed, & Pedron, 2016).

While evaluating the processes and promoting information security awareness programs in the organization, management must take care to avoid the "burn-out" or stress that comes with compliance. In the study by Lee, Lee, & Kim (2016), this stress is defined as the point at which the technology and job demands exceed the employee's ability to comply with information security policies and productivity demands. Management needs to consider the proper ways to raise awareness and protection of information security while minimizing the stress level of task completion under the rules of compliance.

Along with general information security awareness, management should specifically shape employee's skills and attitudes towards the organization's data and assets. Proper security management controls can be implemented to restrict employee's use of systems and information and thus, removing abuse opportunity. Moreover, organizations should provide training in

business ethics, privacy, and other relevant moralities. The research has shown that this has had a positive effect on controlling misbehavior (Kim, Park, & Baskerville, 2015).

CHAPTER THREE: METHODOLOGY

3.1 Introduction

This study assesses the human factors inherent to a successful security awareness program and how they correlate to a healthy information security culture in higher education. Additionally, the study measures how the human factors correlate with each other as they form a causal relationship with security culture. The research starts with a thorough literature review, which is in the previous chapter, and is followed by development of the research model, development of the survey instrument, model validation, and discussion of results. The developed model highlights human factors as independent and dependent variables in the causal relationship with each other. The hypotheses express these relationships verbally. Further, the development of the survey instrument was based on the study variables and validated survey questions from previous studies on information security. Model validation occurs through statistical analysis using descriptive statistics, confirmatory factor analysis (CFA), and Structural Equation Modeling (SEM).

3.2 Proposed Research Model, Research Questions, and Hypotheses

The focus of this research is assessment of the human aspects of an information security program and the organizational security culture. Measuring the security culture was based on employee perceptions of the information security program and culture in their higher education institution. Consequently, the research addressed the following questions:

- What are the human aspects that influence and cultivate an information security culture?

- How do organizational security policies and sanctions affect an information security culture?
- What effect does employee commitment to information security have on the security culture?
- How does organizational management affect the information security culture?
- How does employee security awareness affect the information security culture?

Based on the literature (Alavi, R., Islam, S., Jahankhani, H., & Al-Nemrat, A., 2013; AlHogail, 2015; Badie, N., & Lashkari, A. H., 2012; Knapp, K. J., & Ferrante, C. J., 2014), the research questions, and the goals of the study a proposed model was constructed. This model evaluated the relationships between negative behavior deterrence, organizational policies, employee commitment to security, employee training and awareness, organizational management support (the independent variables) and information security culture (the dependent variable). Figure 2 illustrates the proposed model of the human elements of an information security program (ISP) and the information security culture.

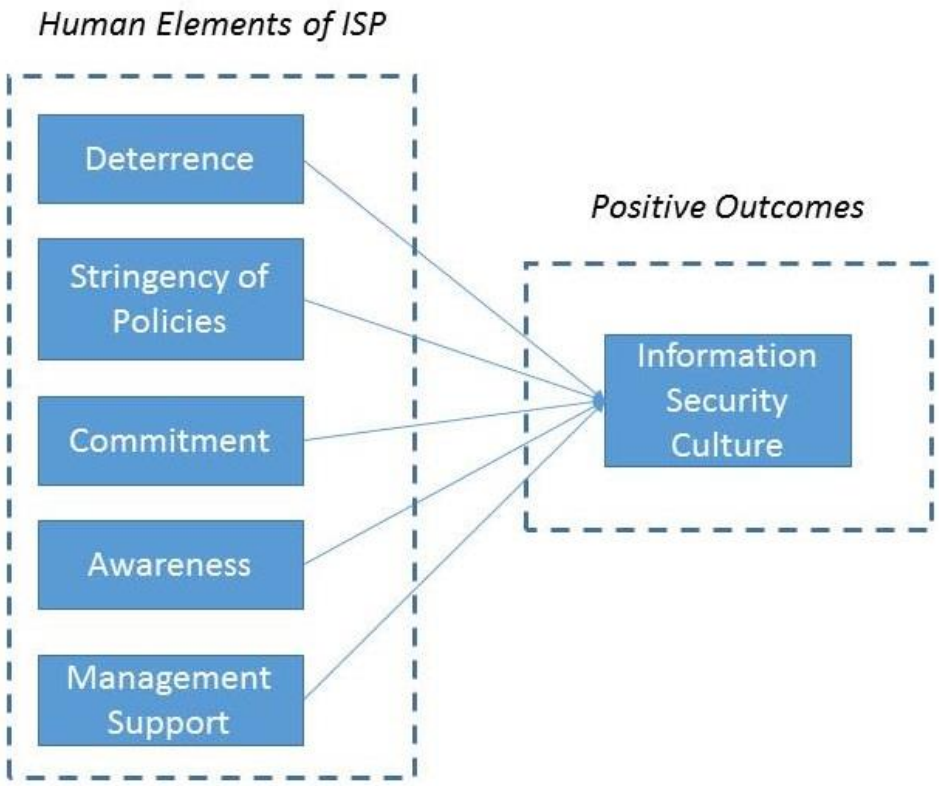


Figure 2: Proposed model of Human Elements of ISP and Information Security Culture

The variables in the model were measured by the indicators (questions) in the survey instrument. Each indicator was validated from previous studies in the literature with modifications to meet a specific research focus. The analysis of the variables and their relationships were conducted using Structural Equations Modeling (SEM). The following hypotheses are proposed to test the relationships between the variables in the model.

- H1: Behavior Deterrence positively contributes to the information security culture.
- H2: Stringency of Information Security Policies positively contributes to the information security culture.

- H3: Employee Commitment to Information Security Programs positively contributes to the information security culture.
- H4: Employee Information Security Awareness positively contributes to the information security culture.
- H5: Management Support of Information Security Programs positively contributes to the information security culture.

3.3 Survey Instrument

The questionnaire was developed and distributed to the employees in two of the Florida College System (FCS) schools (see Appendix A). The FCS is made up of 28-member colleges that provide undergraduate and workforce education to over 800,000 students in the state of Florida (Florida College System, 2017). The study was conducted using a web-based survey tool due to the conveniences it presents to the interviewer and the respondents. Use of a web based survey was advantageous based on the wide geography of the state of Florida, low cost and simplicity of administration, and efficiency in data gathering and analysis when using statistical software. The disadvantages of using a web-based survey tool are the lower response rates and the inability to clarify questions or encourage honest and accurate answers.

The target population of the survey was the specific employees that handle sensitive data or use systems that contain information of high value in the eyes of cyber criminals. These employees were more likely to be subject to state and federal regulations such as the Family Educational Rights and Privacy Act (FERPA) which protects the privacy student records, the Health Insurance Portability and Accountability Act (HIPAA) which protects the privacy of

medical records, and the Gramm-Leach-Bliley Act (GLBA) which protects the privacy of financial information.

The survey contains 7 sections and a total of 28 questions. The first section collected demographic data, which included the respondent characteristics of gender, age, education level (highest education attained), and employment rank (management or staff). The next 5 sections collected data pertaining to the human aspects of the information security program and the final section collected data pertaining to the perceptions of the information security culture. All of the questions outside of the demographic section were answered on a slider that was labeled with a 7-point Likert scale with the range of: Strongly disagree, Disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Agree, and Strongly agree.

The web-based survey was delivered using the Qualtrics® survey software. The software allows users to create customized web-based surveys and conduct statistical analysis. The 7-point Likert scale questions used the slider questions type. The slider question is more interactive to the respondent. Instead of selecting a scale point, it allows the respondent to move the bar to their preference level. This allows for recording of fractional responses.

3.4 Study Variables

The study variables in this research are factors measuring the human aspects of information security and the security culture. The human aspects are the exogenous latent (independent) variables containing the following five dimensions: 1) Behavior Deterrence, 2) Stringency of Policies, 3) Employee Commitment, 4) Employee Awareness, and 5) Management

Support. Information Security Culture is the endogenous latent variable and the demographic data of Gender, Age, Education level and Employment rank are the control variables. The operational definitions are listed in Table 1.

3.4.1 Behavior Deterrence

Behavior deterrence refers to the ability of an organization to prevent or control a user's actions or behavior using fear of retribution or punishment. It is usually prevalent in organizational policies as the consequence of not following an established set of rules. The behavior deterrence factor is measured by 4 questions which define how respondent perceives that the organization observes, controls, and assesses their activities while at work along with the likelihood of punishment. For example: "If I were caught violating my college's information security policies, I would be punished."

3.4.2 Stringency of Policies

Stringency of policies reflects whether the organization's information security policies exist, employees are aware of them, and their perceived impact on the user. Policies are ineffective if they are not known to exist and are not accessible for reference. The survey contains four questions that address the organizations policies as they relate to information security and whether they are acknowledged by the user. For example: "At my college, Information security policies have been adequately explained to employees."

3.4.3 Employee Commitment

Employee Commitment refers to the employee's overall attitudes towards the organization's information security program and their involvement in protecting its assets. A user's perception of information security has a great influence on their security behaviors. Four questions measure the user's attitude towards information security policies and propensity to take personal responsibility in information security. For Example: "If I do not comply with the information security policies, it would be harmful to my college."

3.4.4 Employee Awareness

The awareness factor addressed the training and overall understanding of the sensitive nature of the data handled by the employee in the execution of their work-related tasks. These four questions measure the user's perception of the security training they were given, the modalities of training received, and their importance in the overall security program. For example: "I have received different methods of training (courses, presentations, self-study, etc.) in information security from my college."

3.4.5 Management Support

Management support reflects the organizational management's commitment to information security program and the importance given to the promotion of security awareness. If employees do not feel that their management is attentive to information security then the organizational information security culture will reflect that. In the survey assessment, four

questions measure the user's opinions on their management's involvement and investment in the protection of data and assets and the overall information security of the organization. Example: "The management and supervisors in my department adhere to the information security policies."

3.4.6 Information Security Culture

Information security culture is a reflection of the organization as a whole and their acknowledgment, behavior, and perceptions towards protecting their data and assets and the overall importance of information security. Information security culture is expected to be positively influenced by the 5 observed exogenous variables. It is measured in four questions based on the user's opinions of the business practices, co-worker attitudes, and overall organizational environment. Example: "Practicing good security of information and computer systems is the accepted way of doing business at my college."

Table 1. Operationalization of Study Variables

Variable	Data Type	Role	Attribute	Operational Measurement
Behavior Deterrence	Ordinal	Exogenous	1: Strongly disagree 2: Disagree 3: Neither agree nor disagree 4: Agree 5: Strongly agree	Four items that measuring perception of assessment, likelihood and severity of sanctions
Stringency of Policies	Ordinal	Exogenous	1: Strongly disagree 2: Disagree 3: Neither agree nor disagree 4: Agree 5: Strongly agree	Four items measuring the existence, awareness, and impact of security policies

Variable	Data Type	Role	Attribute	Operational Measurement
Employee Commitment	Ordinal	Exogenous	1: Strongly disagree 2: Disagree 3: Neither agree nor disagree 4: Agree 5: Strongly agree	Four items measuring the commitment to information security
Employee Awareness	Ordinal	Exogenous	1: Strongly disagree 2: Disagree 3: Neither agree nor disagree 4: Agree 5: Strongly agree	Four items measuring the existence of training and awareness of responsibility for security
Management Support	Ordinal	Exogenous	1: Strongly disagree 2: Disagree 3: Neither agree nor disagree 4: Agree 5: Strongly agree	Four items measuring the perceived importance and involvement of management in information security
Information Security Culture	Ordinal	Endogenous	1: Strongly disagree 2: Disagree 3: Neither agree nor disagree 4: Agree 5: Strongly agree	Four items measuring the perception of the organization's information security culture
Gender	Ordinal	Control	0: Female 1: Male	Gender of respondent
Age	Ordinal	Control	1: 18-29 2: 30-39 3: 40-49 4: 50-59 5: 60+	Age group of respondents
Education Level	Ordinal	Control	1: High School 2: Associates 3: Bachelors 4: Masters 5: Ph.D.	Highest level attained (High School to Ph.D.)
Employment Rank	Ordinal	Control	0: Staff 1: Management	Staff or management position in organization

3.5 Procedures

To conduct the survey at the Florida State Colleges, approval was sought by the leadership at the institutions. A presentation was made to their Information Technology representatives and the members of the Florida College System Consortium Cybersecurity Task Force along with a cover letter explaining the reason for the study, its goals, and the assurance of respondent confidentiality. Once approval was granted at the institutions, the survey link was given to the Chief Information Officers (CIOs) of the respective colleges and an introductory email was sent to individual faculty and staff requesting their participation. The link to the survey questionnaire was provided in the email.

3.5.1 Institutional Review Board (IRB)

In addition to the approval from the institutions, the questionnaire was also reviewed and accepted by the Institutional Review Board (IRB) of the University of Central Florida (UCF) (see Appendix B). The IRB at UCF is a committee established to protect the rights and welfare of human participants involved in research and to ensure that ethical principles are followed. Upon IRB approval at UCF, the same IRB approval was sought at each college that agreed to participate. Once the college's IRB approved and accepted, volunteer participants were recruited. The first page of the survey provided the respondents with an informed consent as well as an invitation to participate. Participation in the survey was voluntary and completely anonymous to ensure receipt of candid and honest responses. The survey collected only limited personal demographic information needed for data analysis. No names or other personally identifiable information was requested. All participants had the right to discontinue the survey at any time.

3.5.2 Pilot Survey

The original survey was distributed to the CIOs and other executive leadership at each institution that chose to participate. These recipients approved the dissemination of the survey and provided feedback. The result of their feedback is the final survey that was distributed. A copy of the final survey can be found in Appendix A.

3.5.3 Participants

To complete the survey, respondents were recruited from the colleges that agreed to participate. The potential respondents were employees of the college who are 18 years of age or older and have access to the college's sensitive information while conducting their college duties.

3.6 Sampling

The targeted population for this study included the employees of the Florida College System. According to the Florida College System 2016 Fact Book, the population consists of 45,294 employees. This total includes full-time and part-time faculty and staff. As part of the process, individual colleges were contacted and asked to participate in the study.

Specific participation in the study was sought from each college individually due to the sensitive nature of the subject and the confidential nature of each institutions information security posture. Initially, 10 of the 29 state colleges in Florida verbally agreed to participate in the study. Once the study was ready to start, only 2 schools were willing to have their employees

surveyed. The sensitive nature of the subject has made it difficult to convince institutions of higher education to participate in this kind of research. Organizations that collect higher education security data, such as the Privacy Rights Clearinghouse and Gemalto, do so only from published reports and voluntary disclosure by the institutions. While it is only recently that the Department of Education has required colleges and universities to report security and data breach information, many higher education institutions are hesitant to share their security information (Tassi, 2018). Based on the colleges that were still willing to participate, the survey link was sent to 326 Florida College System employees. Out of the 326, 179 complete and usable responses were received resulting in a 54.9% response rate.

3.6.1 Sample Size

In the literature, sample size is an important factor in analyzing and drawing statistical inferences about populations. However, there is very little agreement on the proper sample size for SEM and how it should be determined. The generally accepted minimum sample size is 100 to 150 responses (Ding, Velicer, & Harlow, 1995). Klein (2010) and Boomsma and Hoogland (2001) state that as a rule as thumb researchers should use the recommended sample size of 5 to 10 cases per parameter and a minimum sample size of 200 is needed to reduce biases to an acceptable level. Wolf, E. J., Harrington, K. M., Clark, S. L., & Miller, M. W. (2013) have shown that samples sizes can vary based on the model construction and that small sample sizes are sufficient. Using the suggested ratio of 5:1, the minimum sample size for this study would be 120. With the amount of requested participation, the 179 completed responses on the survey meets the requirement.

3.7 Statistical Analysis

The statistical analysis in this study was achieved by performing descriptive statistics, confirmatory factor analysis (CFA), structural equation modeling (SEM), and hypothesis testing. The following subsections provide a description of each analysis.

3.7.1 Descriptive Statistics

The initial data analysis was performed by reviewing the data for missing values, outliers, multivariate normality, reliability, and validity of scales. In addition, an analysis was performed to eliminate potential multicollinearity. Multicollinearity exists when predictor variables are highly correlated. This common research problem results in large standard errors and difficulty in producing statistically significant results. Kline (2010) suggests that a correlation of 0.85 or greater shows evidence of multicollinearity and Schumacker & Lomax (2016) show that using Spearman's correlation matrix is appropriate for detecting multicollinearity for each latent variable when the data is ordinal.

3.7.2 Confirmatory Factor Analysis

Confirmatory factor analysis (CFA) is an extension of factor analysis that determines whether a set of factors fit a construct (Schumacker & Lomax, 2016). CFA was used to confirm the reliability and validity of the measurement model at each latent construct (Kline, 2010). IBM® SPSS® Amos 24.0.0 software was utilized to complete the CFA.

Goodness of fit indices were used to determine how well the constructed model fit the collect research data. The literature recommends that multiple goodness of fit statistics be used to support the fit of a model to a data set. In this analysis, four fit indices (Chi-square, Tucker and Lewis index (TLI), comparative fit index (CFI), and root mean square error of approximation (RMSEA) were used to determine model fitness (Byrne, 2010).

The first index used was the Chi-square ($\chi 2$) statistic which tests the closeness of fit between the model and a saturated or perfect fit model. A low Chi-square value is considered a better fit to the model data but the index can be easily affected by sample size which can consequently inflate its score. Previous studies have recommended using a ratio of Chi-square to degrees of freedom of less than four as an acceptable fit (Hu & Bentler, 1999; Hooper, Coughlan, & Mullen, 2008).

The TLI is less sensitive to sample size and is used to compare a single model or alternative models to the null model. HU & Bentler (1999) suggest that a value greater than 0.90 is considered an acceptable fit. Any value less than 0.90 requires model restructuring.

The CFI compares the hypothesized model with the null model. Like the TLI, the CFI is less sensitive because of its ability to adjust to sample size. Its similarity to the TLI continues as its index value above 0.9. is considered acceptable (Hu & Bentler, 1999).

The RMSEA is one of the most frequently used measures of model fit. This index can account for the complexity of the model. Lower values suggest less manipulation of the model fit exists. An RMSEA index value of less than 0.08 is considered and acceptable fit and values greater than 0.10 are considered a poor fit to the data (Hooper, Coughlan, & Mullen, 2008).

3.7.3 Structural Equation Modeling

Structural equation modeling (SEM) is large set of statistical methodologies that specifies causal relationships among latent and observed variables (Byrne, 2010). Its purpose in this study is to estimate and test the relationships among the model constructs and determine if the hypotheses are supported by the sample data. Using the IBM® SPSS® Amos 24.0.0 software, the CFA was conducted to validate the measurement models and each resulting construct was used to build the structural model. The composite structure model was then analyzed to test the relationships between the human factors in an information security program (the dependent variables) and information security culture (the independent variable).

CHAPTER FOUR: FINDINGS

This chapter presents the findings of the statistical analysis used in the study to analyze the data and for discovery of normality and extreme or missing values. Descriptive statistics were performed by creating frequency tables of the control variables. After the initial analysis, data with missing values were eliminated and only completed responses were used. A Spearman's Rho correlation matrix was used to detect problems with multicollinearity for each latent variable.

The study used structural equation modeling (SEM) to determine and analyze the effects that stringency of policies, behavior deterrence, employee commitment, employee awareness, and management support on organizational information security culture. The initial step in this process was to analyze the validity of the measurement model (Hu & Bentler, 1999). Using confirmatory factor analysis (CFA), the construct of each latent variable was validated. Upon completion, a CFA was completed to validate the structural model with all exogenous and endogenous variables included. This structural model was then adjusted to improve model fit and remove negative relationships between the exogenous and endogenous variables. This chapter concludes by testing the hypothesis and exploring the overall model fit using the SEM and path analysis.

4.1 Descriptive Statistics

4.1.1 Missing Data

In conducting the data analysis, the data was examined for any missing values. The survey was distributed to 326 employees at 2 institutions in the Florida State College System. The survey was completely voluntary with no completion incentives given to the respondents. There were no termination points in the survey and the only requirement was that the respondents must be 18 years of age of older. This requirement was explained in the disclosure statement at the beginning of the survey and as a part of the age question, Q2 ("What is your age?"). Question 2 was the only required question on the survey. The respondents had the option to give no response to any other question. If the respondent was not at least 18 years old, the survey was terminated and no data was collected. Some of the respondents, though they met the requirement, did not complete the entire survey and those responses were eliminated. As a result, 179 state college employees completed the entire survey with only 2 of the completed surveys missing data.

The missing data was from the gender demographic question, Q1 ("Which gender do you identify with?" (Male/Female)). It is possible that the question was missed by the respondent or they felt that answering the question could possibly remove anonymity when combined with the other demographic questions, or that they did not identify with the gender choices given. The population of respondents who identified with female as their gender was 104 out of 179, or 58.1%. To complete the analysis with the 2 missing values, the gender responses were recoded to Female and Non-Female. The Non-Female category consisted of the 2 missing values and the 73 male responses.

4.1.2 Outliers

The survey respondent's scores were checked for outliers or responses that were abnormal or exceptional. While examining the data it was found that all responses fell within the expected ranges. The 24 questions that had responses given on a 7-point Likert scale were expected to be with in a minimum of 0 and a maximum of 10. All answers within this range were considered normal and not an outlier. The age question provided values that were within the expected range and the other demographic questions were categorized as multiple choice. Therefore, all data values were kept and used in the analysis.

4.1.3 Normality

The skewness and kurtosis was examined for each observed variable to discover if univariate normality exists in the data (see Appendix D). As the data is analyzed using statistical techniques such as Analysis of Variance (ANOVA), linear regression, and t-tests, approximate normality is relied upon (Oppong & Agbedra, 2016).

The behavior deterrence indicators have a slightly negative skewness with absolute values between .595 and 1.33. The kurtosis for these indicators range from -.759 to 1.621. This indicates an approximate normal distribution of the data. The skewness and kurtosis of the variables: employee awareness, management support, and information security culture all follow the same with a slightly negative skewness and kurtosis values with the acceptable range of normal data distribution. The stringency of policies and employee commitment indicators both showed a highly negative skewness with absolute values between 1.31 and 2.496 and kurtosis values ranging up to 8.597. These values are extreme and outside the range of an approximate

normal distribution. These results imply that the statistical assumptions may be biased and further analysis may result in removal of the variables from the model.

4.1.4 Multicollinearity

Multicollinearity can occur when two measured variables are highly inter-correlated or inter-associated and can give similar results in measurements. The existence of multicollinearity can result in the statistical analysis being inaccurate and unreliable. Since ordinal data was used in the analysis, Spearman's rho is used to illustrate the correlations between the indicators (Schumacker & Lomax, 2016). The Spearman's rho correlation matrix was conducted for each indicator of each variable in the study using the IBM® SPSS® 24 software (see Appendix E). Correlations of 0.85 or greater were used to indicate multicollinearity and potential problems in the data (Kline, 2010).

The variable, stringency of policies, had four indicators (Questions 5-8) that were analyzed. There were moderate to strong relationships between the indicators which were statistically significant at 0.01. The highest correlation was between Question 5 and 6 at 0.700, but below the 0.85 level. As a result, no multicollinearity problems were found among all indicators of stringency of policies.

Behavior deterrence was comprised of four indicators (Questions 9-12) and tested for potential multicollinearity. The indicator correlations showed a weak to moderate relationships between the indicators. Therefore, no multicollinearity problems we identified between the behavior deterrence indicators.

The employee commitment indicators were Questions 13-16. All correlations of this factor revealed a moderate to strong relationship between the indicators and were statistically significant at the 0.01 level. The highest correlation was 0.678, which was found between Question 13 and Question 16. As this was below the threshold of 0.85, no multicollinearity problems were found.

Variables representing employee awareness, management support, and information security culture contained the indicators Questions 17-20, Questions 21-24, and Questions 24-28 respectfully. Each of the indicators in their corresponding factors identified a moderate to strong correlation with the highest correlation at 0.793. All were significant at 0.01 and below the multicollinearity threshold of 0.85.

4.2 Frequency Analysis

The respondents in the study were recruited from the employee pool of 2 institutions in the Florida State College System. The only requirement was that they be 18 years of age or older. A total 326 employees were recruited for the survey and 198 individuals started the web-based survey. Of the 326 respondents, 19 were found to be incomplete or unfinished surveys and were excluded from the data. Therefore, of 179 out of 326 state college employees completed the web-based survey which resulted in a 54.9% response rate. The 179 completed surveys were used in the data analysis.

4.2.1 Demographic Information

The demographic information collected in the survey illustrates the characteristics of the respondent population. Four pieces of demographic information was collected from the respondents: gender, age, educations level, employment type. This section details the responses obtained for Questions 1 through 4 (see Appendix C for more details).

The first piece of demographic information collected was the gender of the respondents. The responses were coded as Female and Non-Female. A total of 104 survey completers identified their gender as female (58.1 %) and 75 as non-female (41.9%). This aligns closely with the gender demographic numbers presented in the 2017 Florida College System Fact Book which stated that 56% of the college system employees identified as female and 44% identified as non-female (Florida College System, 2017).

The second demographic factor investigated was the age of the respondent. This question was mandatory and was a termination point, as being 18 years or older was requirement to participate in the survey. The average (mean) age of the respondents were 51 years old with a standard deviation of 11.87 years and the respondent ages ranged from 20 to 76 years old. Based on the 179 respondents, 51 (28.5%) of the employees were of young adult age (18-44 years old), 110 (61.5%) were middle age adults (45-64 years old), and 18 (10%) were senior age adults (65 years of age and older). The age responses were recoded for analysis purposes.

The next survey question determined the highest educational level of the respondents. The analysis shows that 28 (15.6%) of the respondents selected high school diploma as their highest education level, 36 (20.1%) had an associates degree, 37 (20.7) had a bachelors degree, and 78 (43.6%) had a graduate level degree.

The last demographic question inquired about the employment level of the respondent. Most of the respondents listed their employment level as staff (114 out of 179 responses, 63.7%) with 18 choosing management (10.1%), 7 choosing faculty (3.9%), and 40 choosing dean, director, or above (22.3%). The faculty response numbers are believed to be low because the survey was distributed during the summer semester operations of the institutions. Most Florida College System faculty are not on contract during the summer semester or take vacation and some institutions decrease operations to 4 days a week.

4.3 Confirmatory Factor Analysis

To start the SEM analysis, a CFA was conducted to verify the validity and reliability of each measurement model. Using maximum likelihood estimation, the models of stringency of policies, behavior deterrence, employee commitment, employee awareness, management support and information security culture were evaluated to assess how well the observed variables describe the hypothesized model. Using the AMOS® 24 software, the six individual models were evaluated by completing the SEM steps of model specification, identification, estimation, evaluation, and modification (Hoyle, 1995; Kline, 2010, Schumacker & Lomax, 2016).

Specifying the initial measurement model is the first step of CFA. This is accomplished by for each latent variable by evaluating its uniformity to the respective observed indicators. This relationship between the observed variables and the corresponding latent variable is the factor loading and determines how strongly the relationship exists.

The following step used maximum likelihood estimation to confirm whether the model was properly identified. The results of the software analysis determined whether each parameter in the model could be estimated from the covariance matrix.

The next step was testing of the specified model the evaluation of the goodness-of-fit statistics. The goodness-of-fit statistics were generated from the software and used to determine of the specified model was supported by the observed data. In this analysis, four fit indices (Chi-square, Tucker and Lewis index (TLI), comparative fit index (CFI), and root mean square error of approximation (RMSEA) were used to determine model fitness.

The final step of the CFA analysis evaluated the need to make modifications to improve the overall model fit. Modifications to the specified model consisted of three steps to improve the initial model fitness. The initial step was to certify that each factor loading in the latent construct were statistically significant and had a critical ratio (C.R.) of ± 1.96 or higher (Schumaker & Lomax, 2016). Indicators that did not meet this condition were removed from the model. Review of the modification indices (M.I.) were next which determine the anticipated decrease in the Chi-square value that decrease if the model included the covariance between error terms. The AMOS 24 generated M.I. statistics that were used to improve the model fit of each initial model. M.I. values that were greater than 4.0 ($p < 0.05$) required determination of model adjustment. The third step was the calculation of Cronbach's alpha to also determine model reliability. An α measurement of 0.70 is the threshold for ensuring strong internal consistency (Nunnally, 1978).

4.3.1 Confirmatory Factor Analysis of Stringency of Policies

Stringency of Policies is the first latent endogenous variable considered in this model. The original model used four indicators (survey questions 5 through 8) to measure the factor. Figure 3 depicts the initial measurement model and its standardized estimates or factor loadings.

With the degrees of freedom equal to 9 and greater than zero (14 observations minus the 12 distinct parameters estimated), the model was determined to be overidentified. The Chi-square statistic of 29.942 is above the threshold of three times of the degree of freedom equaling 27. These calculations are significant at $p < 0.05$. This results in a significant difference between the model and the saturated model.

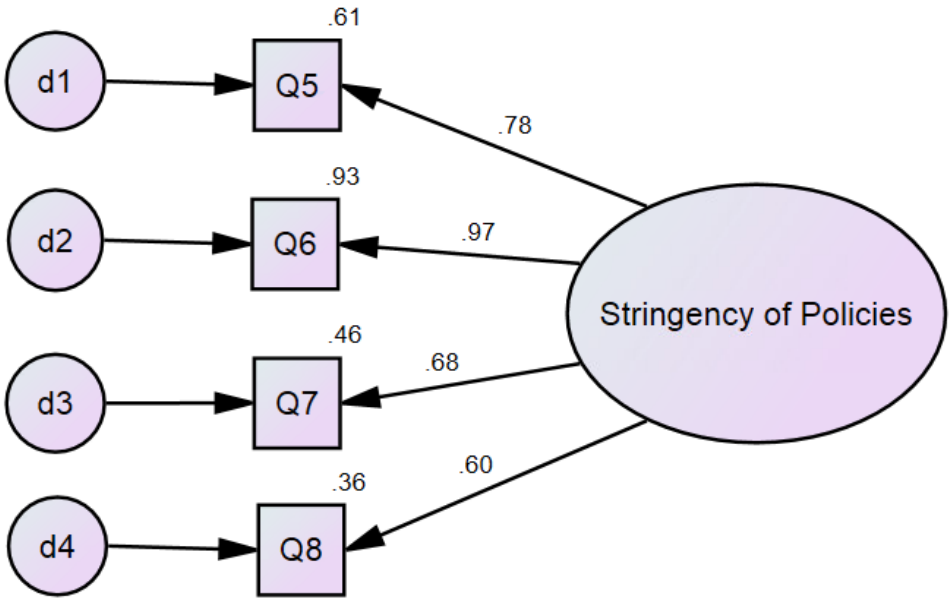


Figure 3: Initial Stringency of Policies measurement model

The goodness-of-fit statistics of the model showed a need for improvement. The CFI was slightly above the acceptable fit limit of 0.90, but the TLI was below that limit, the Chi-square ratio with degrees of freedom ($\chi 2/df$) was above the acceptable level of 4, and the RMSEA value of .280 was significantly higher than the acceptable limit of 0.08. As a result, it was determined that the model was not a good fit with the data.

The indicators have a strong relationship with the latent variable, stringency of policies. This can be seen in their relatively high factor loadings. Table 2 shows that the indicators, questions 5, 7, and 8 have a moderate correlation with the latent variable with question 6 having a strong correlation. All factor loadings are significant at the 0.05 level as their C.R. is greater than 1.96. Therefore, no indicators were removed in the improved model.

For further model improvement, the M.I.s were measured for the purpose of decreasing the Chi-square value of the improved model. The error terms were correlated in the revised model for any covariances with modification indices above 10.

Table 2: Parameter estimates for the Stringency of Policies measurement model

	Initial Model				**Revised Model**			
Indicator	**Std. Estimate**	**S.E**	**C.R.**	**P**	**Std. Estimate**	**S.E**	**C.R.**	**P**
Stringency of Policy Q5	0.783	0.143	8.342	***	0.742	0.162	7.668	***
Stringency of Policy Q6	0.967	0.172	8.803	***	1.030	0.240	7.437	***
Stringency of Policy Q7	0.678	0.179	7.543	***	0.639	0.156	8.989	***
Stringency of Policy Q8	0.601				0.544			

Note: *** means $p < 0.001$

The revised stringency of policies measurement model contains the same indicators as the initial model. The error terms d3 and d4 were correlated based on the measurements of the M.I.s from the initial model (see Figure 4).

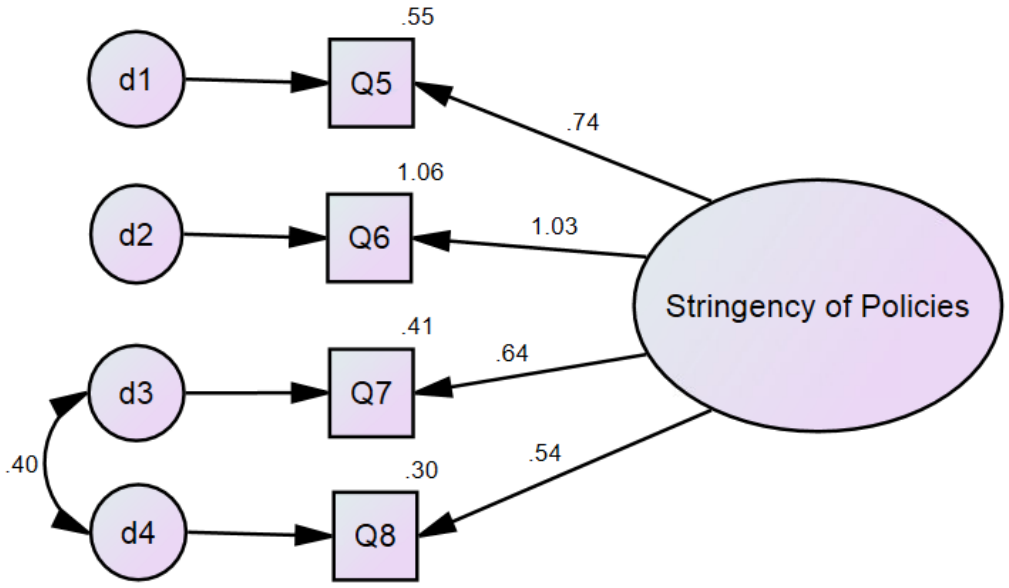


Figure 4: Revised Stringency of Policies measurement model

The improved model has a lower degree of freedom (1) than the initial model (9), which is still greater than zero and therefore overidentified. The Chi-square value was considerably lowered to 3.672 and the $\chi 2/df$ ratio is below 4 indicating a good model fit. The probability level is 0.05 indicating that these results are statistically significant.

The goodness-of-fit measurements of CFI and TLI are above the threshold of 0.9 and very close to 1.0, indicating a good model fit. In contrast, the RMSEA lowered to 0.123, but is

still above the 0.08 level. The goodness-of-fit indices for the both the initial and improved models are shown in Table 3.

The standardized estimates of the indicators, Questions 5, 7, and 8 had only slightly decreased factor loadings that in the initial model. Question 6 had an increase of the already strong estimate and overall the loadings continued to remain strong.

Table 3: Goodness-of-fit indices for Stringency of Policies

	Fit Criteria			
Index	**Good Fit**	**Acceptable Fit**	**Initial Model**	**Revised Model**
$\chi 2$	$0 \leq \chi 2 \leq 2df$	$2df < \chi 2 \leq 3df$	29.942	3.672
p value	$.05 < p \leq 1.00$	$.01 \leq p \leq .05$	0.000	0.05
$\chi 2$ / df	$0 \leq \chi 2/df \leq 2$	$2 < \chi 2/df \leq 3$	14.971	3.672
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < .95$	0.920	0.992
TLI*	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < .95$	0.761	0.954
RMSEA	$0 \leq RMSEA \leq .05$	$.05 < RMSEA \leq .08$	0.280	0.123

Note: * The "non-normed" index, on occasion, can be larger than 1 or slightly below 0.

The indicators in the improved model have critical values greater than 1.96 and are significant at the 0.05 level. Because of this, all indicators were maintained in the model. The revised model shows improvement in model fit with most fit statistics measuring in the acceptable ranges. Cronbach's alpha was used to evaluate the improved model construct. The measurement was found to be 0.848. This is above the generally accepted threshold of 0.70 and indicates that the measurement model is reliable.

4.3.2 Confirmatory Factor Analysis of Behavior Deterrence

The next latent endogenous variable considered in this model is behavior deterrence. The original model used four indicators (survey questions 9 through 12) to measure the factor. Figure 4 depicts the initial measurement model and its standardized estimates or factor loadings.

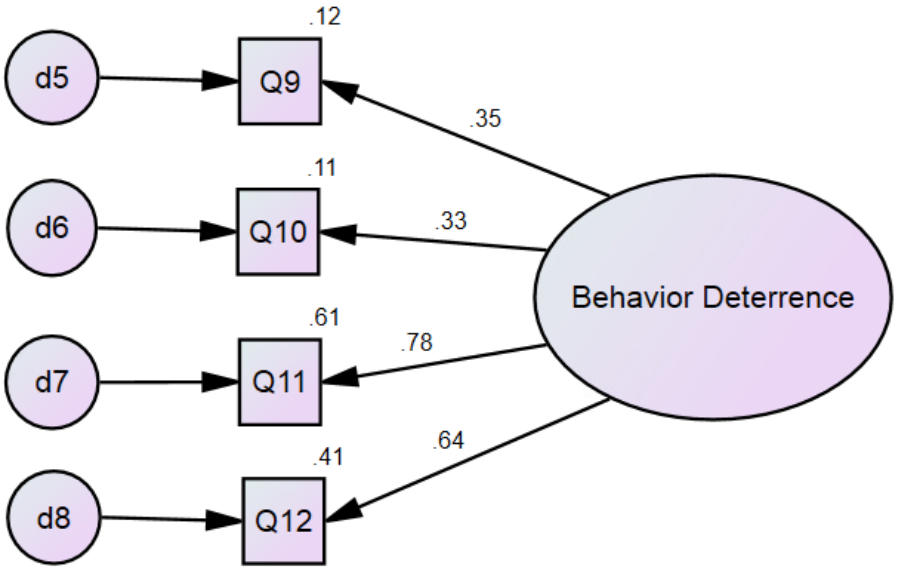


Figure 4: Initial measurement model for Behavior Deterrence

With the degree of freedom equal to 2, which is greater than zero (10 observations minus 8 parameters to be estimated, the behavior deterrence model was overidentified. The Chi-square statistic of 19.498 is above the threshold of three times of the degree of freedom. These calculations are significant at $p < 0.05$. This results in a significant difference between the initial and the saturated models.

The values of the goodness-of-fit indices CFI and TLI are below 0.90 and the RMSEA value of 0.222 is above the acceptable limit of 0.08. Additionally, the Chi-square ratio with

degrees of freedom ($\chi 2/df$) was above the acceptable level of 4. All indices show a poor model fit.

Two of the indicators of behavior deterrence, Question 11 and Question 12, have a moderately strong relationship with the latent variable. The indicators, Question 9 and Question 10, have weak relationships with behavior deterrence (see Table 4). All indicators are significant at the 0.05 level as their C.R. is greater than 1.96. Therefore, no indicators were removed in the improved model. Further, the M.I.s for those indicators show a covariance of 16.955, which is above the threshold of 10. This suggests a need to correlate the error terms of Question 9 an Question 10.

Table 4: Parameter estimates for the Behavior Deterrence measurement model

	Initial Model				**Revised Model**			
Indicator	**Std. Estimate**	**S.E**	**C.R.**	**P**	**Std. Estimate**	**S.E**	**C.R.**	**P**
Behavior Deterrence Q9	0.351	0.139	3.671	***	0.298	0.138	3.340	***
Behavior Deterrence Q10	0.333	0.216	3.506	***	0.263	0.214	2.986	.003
Behavior Deterrence Q11	0.783	0.305	4.256	***	0.867	0.496	3.095	.002
Behavior Deterrence Q12	0.638				0.597			

Note: *** means $p < 0.001$

The improved behavior deterrence model contained the same indicators as the original model with indicators of Question 9 and 10 correlated (see Figure 5).

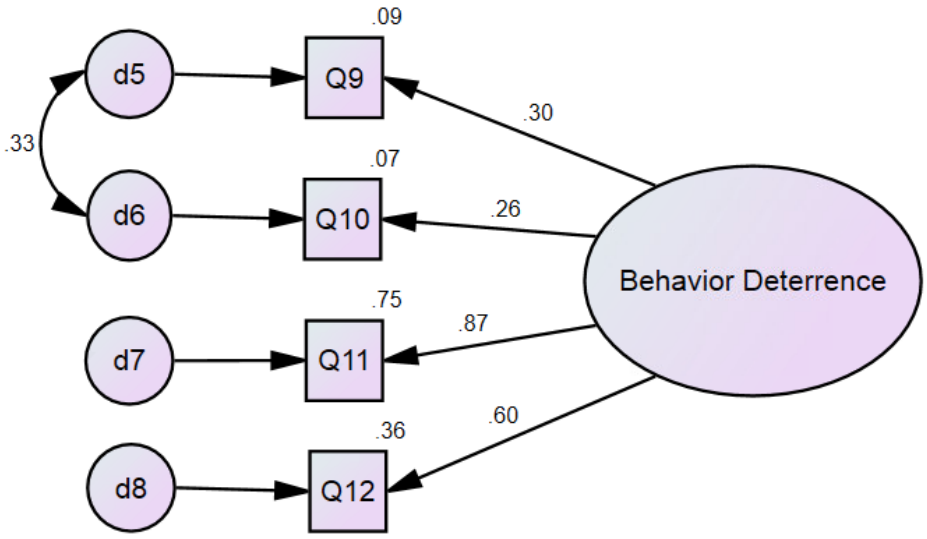


Figure 5: Revised behavior deterrence measurement model

With a degree of freedom of 1 (14 observations minus 13 parameters to be estimated), the revised model is overidentified because the degree of freedom is greater than zero. The Chi-square value was significantly lowered from 19.498 in the initial model to 1.083 in the improved model and the Chi-square ratio with degrees of freedom ($\chi 2/df$) is lower than 2 and the probability level (0.298) is higher than 0.05, indicating no statistical significance. Consequently, there are no significant differences between the improved and saturated models.

Also, the goodness-of-fit statistics of CFI (0.999) and TLI (0.995) are very close to 1.0 and the RMSEA of 0.022 is less than 0.05, signifying that the model fits well. Table 5 illustrates the goodness-of-fit indices of the initial and revised behavior deterrence measurement models

The standardized estimates of the indicator, Question 7, had only slightly increase in the factor loadings of the improved model. The other indicators had a decrease in their already weak

estimates. With critical values greater than 1.96, all indicators show significance at the 0.05 level and deemed important to the model. Therefore, all indicators will remain in the model. The Cronbach's alpha for the behavior deterrence construct was 0.617 which is slightly lower than the recommended level of 0.70. This does not necessarily mean that the measurement model is unreliable. Although 0.70 is a widely known measurement level for good model fit, recent studies have shown that measurements above 0.50 can be acceptable (Teo. Mohamad, & Ramayah, 2011). Thus, the model is deemed to be reliable.

Table 5: Goodness-of-fit indices for behavior deterrence

	Fit Criteria			
Index	**Good Fit**	**Acceptable Fit**	**Initial Model**	**Revised Model**
$\chi 2$	$0 \leq \chi 2 \leq 2df$	$2df < \chi 2 \leq 3df$	19.498	1.083
p value	$.05 < p \leq 1.00$	$.01 \leq p \leq .05$	0.000	0.298
$\chi 2$ / df	$0 \leq \chi 2/df \leq 2$	$2 < \chi 2/df \leq 3$	9.749	1.083
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < .95$	0.816	0.999
TLI*	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < .95$	0.447	0.995
RMSEA	$0 \leq RMSEA \leq .05$	$.05 < RMSEA \leq .08$	0.222	0.022

Note: * The "non-normed" index, on occasion, can be larger than 1 or slightly below 0.

4.3.3 Confirmatory Factor Analysis of Employee Commitment

The initial measurement model for the exogenous latent variable, employee commitment, had the indicators that consisted of Questions 13 through 16. The initial measurement model and its standardized estimates are shown in Figure 6.

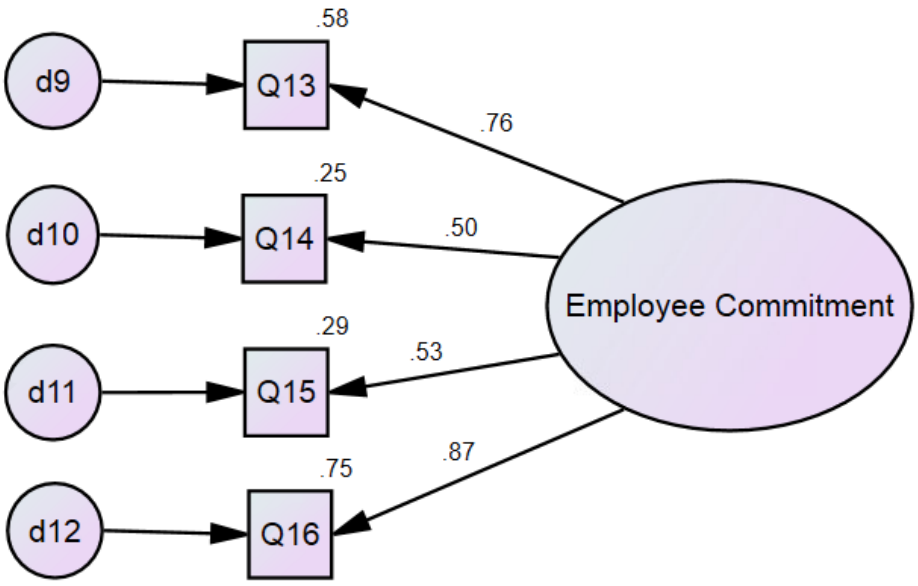


Figure 6: Initial employee commitment measurement model

The initial employee commitment model was overidentified with a degree of freedom of 2, which is greater than zero (14 observations minus the 12 distinct parameters estimated). The Chi-square statistic of 4.313 is below the threshold of three times of the degree of freedom equaling 6. The probability level (0.116) is higher than 0.05, indicating no statistically significant difference between the model and the saturated model.

The CFI and TLI were above the good fit level of 0.95 and the RMSEA value of 0.081 is on the cusp of the acceptable fit range so it is deemed a good model fit. Table 6 presents the goodness-of-fit indices for the measurement model.

The indicators, Question 13 and 16, have a strong relationship with the latent variable, employee commitment. But the indicators, Question 14 and 15 were found to have a moderate

correlation with the latent variable (see Table 7). All indicators are significant at the 0.05 level as their C.R. is greater than 1.96. Therefore, no indicators were removed in the improved model.

The M.I.s were measured to decrease the Chi-square value of the improved model. There were no covariances in the measured modification indices. It was decided that the model needed no revisions.

The internal consistency of the employee commitment construct was determined by Cronbach's alpha. The Cronbach's alpha was measured at 0.762, which is above the recommended level of 0.70 and indicates that the model is reliable.

Table 6: Goodness-of-fit indices for employee commitment

	Fit Criteria			
Index	**Good Fit**	**Acceptable Fit**	**Initial Model**	**Revised Model**
$\chi 2$	$0 \leq \chi 2 \leq 2df$	$2df < \chi 2 \leq 3df$	4.313	N/A
p value	$.05 < p \leq 1.00$	$.01 \leq p \leq .05$	0.116	N/A
$\chi 2$ / df	$0 \leq \chi 2/df \leq 2$	$2 < \chi 2/df \leq 3$	2.156	N/A
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < .95$	0.988	N/A
TLI*	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < .95$	0.963	N/A
RMSEA	$0 \leq RMSEA \leq .05$	$.05 < RMSEA \leq .08$	0.081	N/A

Note: * The "non-normed" index, on occasion, can be larger than 1 or slightly below 0.

Table 7: Parameter estimates for the Employee Commitment measurement model

Indicator	Initial Model				Revised Model			
	Std. Estimate	S.E	C.R.	P	Std. Estimate	S.E	C.R.	P
Employee Commitment Q13	0.761	0.133	8.526	***	N/A	N/A	N/A	N/A
Employee Commitment Q14	0.502	0.170	6.548	***	N/A	N/A	N/A	N/A
Employee Commitment Q15	0.535	0.229	6.152	***	N/A	N/A	N/A	N/A
Employee Commitment Q16	0.868				N/A			

Note: *** means $p < 0.001$

4.3.4. Confirmatory Factor Analysis of Employee Awareness

The measurement model for the exogenous latent variable, employee awareness, was comprised of the indicators: Questions 17 through 20. The initial measurement model and its standardized estimates are shown in Figure 7.

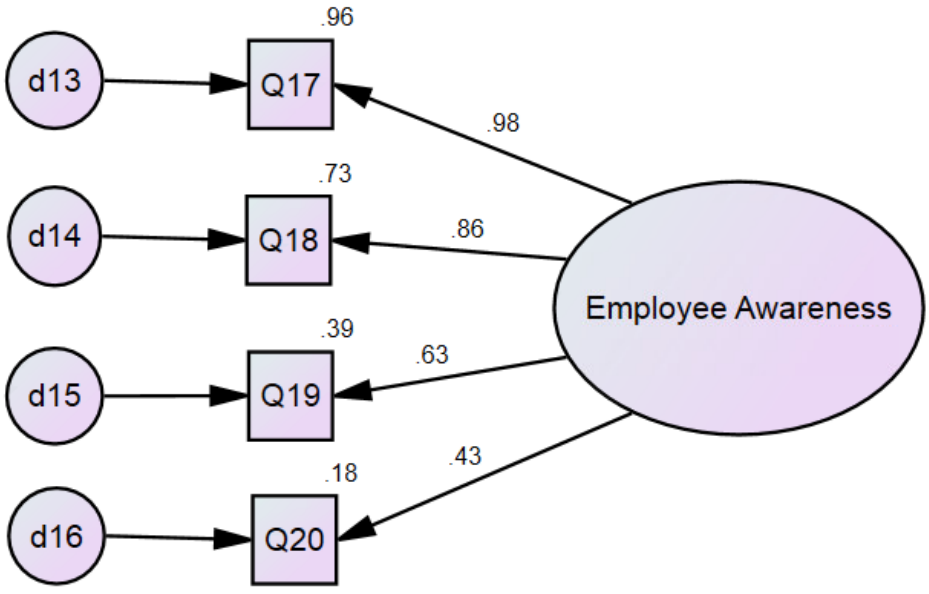


Figure 7: Initial employee awareness measurement model

The initial employee awareness model was overidentified with a degree of freedom of 2, which is greater than zero (14 observations minus the 12 distinct parameters estimated). The Chi-square statistic of 2.604 is below the threshold of three times of the degree of freedom equaling 6. The probability level (0.272) is higher than 0.05, indicating no statistically significant difference between the model and the saturated model.

The CFI and TLI were above the good fit level of 0.95 and very close to 1.0. The RMSEA value is below the good fit range so it is a good model fit. The goodness-of-fit indices for the measurement model is presented in Table 8.

The indicators, Question 17 and 18, have a strong relationship with the latent variable, employee awareness. But the indicators, Question 19 and 20 were found to have only a moderate correlation with the latent variable (see Table 9). All indicators are significant at the 0.05 level as their C.R. is greater than 1.96. Therefore, no indicators were removed in the improved model.

The M.I.s were measured to decrease the Chi-square value of the improved model. There were no covariances in the measured modification indices. It was decided that the model needed no revisions.

The internal consistency of the employee awareness construct was determined by Cronbach's alpha. The Cronbach's alpha was measured at 0.811, which is above the recommended level of 0.70 and indicates that the model is reliable.

Table 8: Goodness-of-fit indices for employee awareness

Index	Fit Criteria		Initial Model	Revised Model
	Good Fit	Acceptable Fit		
$\chi 2$	$0 \leq \chi 2 \leq 2df$	$2df < \chi 2 \leq 3df$	2.604	N/A
p value	$.05 < p \leq 1.00$	$.01 \leq p \leq .05$	0.272	N/A
$\chi 2$ / df	$0 \leq \chi 2/df \leq 2$	$2 < \chi 2/df \leq 3$	1.302	N/A
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < .95$	0.988	N/A
TLI*	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < .95$	0.995	N/A
RMSEA	$0 \leq RMSEA \leq .05$	$.05 < RMSEA \leq .08$	0.041	N/A

Note: * The "non-normed" index, on occasion, can be larger than 1 or slightly below 0.

Table 9: Parameter estimates for the Employee Awareness measurement model

Indicator	Initial Model				Revised Model			
	Std. Estimate	S.E	C.R.	P	Std. Estimate	S.E	C.R.	P
Employee Awareness Q17	0.981	0.437	5.941	***	N/A	N/A	N/A	N/A
Employee Awareness Q18	0.857	0.382	5.951	***	N/A	N/A	N/A	N/A
Employee Awareness Q19	0.627	0.332	5.340	***	N/A	N/A	N/A	N/A
Employee Awareness Q20	0.427				N/A			

Note: *** means $p < 0.001$

4.3.5 Confirmatory Factor Analysis of Management Support

The exogenous latent variable, management support, consists of 4 indicators, Questions 21 through 24. The initial measurement model and its standardized estimates are shown in Figure 8.

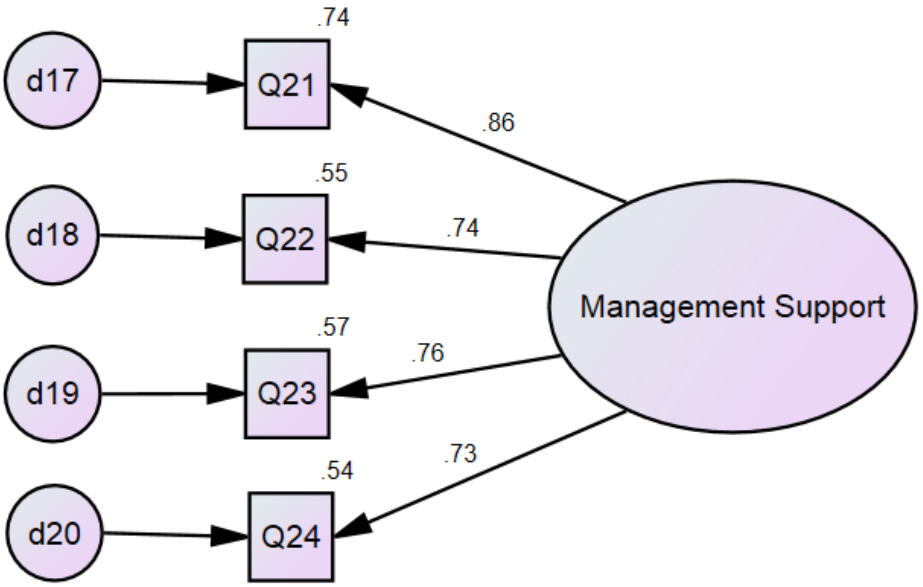


Figure 8: Initial management support measurement model

The management support model was overidentified with a degree of freedom of 2, which is greater than zero (14 observations minus the 12 distinct parameters estimated). The Chi-square statistic of 15.860 is well above the threshold of three times of the degree of freedom (6). The probability level (0.000) is lower than 0.05, indicating that there is a statistically significant difference between the model and the saturated model.

The CFI was above the good fit level of 0.95. The TLI was below the acceptable fit range of 0.90 and the RMSEA value was above the acceptable fit range so the model was not a good fit.

The indicators have a strong relationship with the latent variable, management support (see Table 10). All indicators are significant at the 0.05 level as their C.R. is greater than 1.96. All indicators are significant at the 0.05 level as their C.R. is greater than 1.96. Therefore, no

indicators were removed in the improved model. In addition, the M.I.s for the error terms of the indicators, Question 19 and Question 20, show a covariance of 10.746, which is slightly above the threshold of 10. This suggests a need to correlate the error terms of Question 9 and Question 10.

Table 10: Parameter estimates for the Management Support measurement model

Indicator	Initial Model				Revised Model			
	Std. Estimate	S.E	C.R.	P	Std. Estimate	S.E	C.R.	P
Management Support Q21	0.858	0.102	10.329	***	0.914	0.144	8.678	***
Management Support Q22	0.739	0.105	9.208	***	0.747	0.128	8.484	***
Management Support Q23	0.756	0.096	9.414	***	0.685	0.092	9.930	***
Management Support Q24	0.733				0.660			

Note: *** means $p < 0.001$

The revised management support measurement model contained the same indicators as the original model with indicators of Question 9 and 10 correlated (see Figure 9).

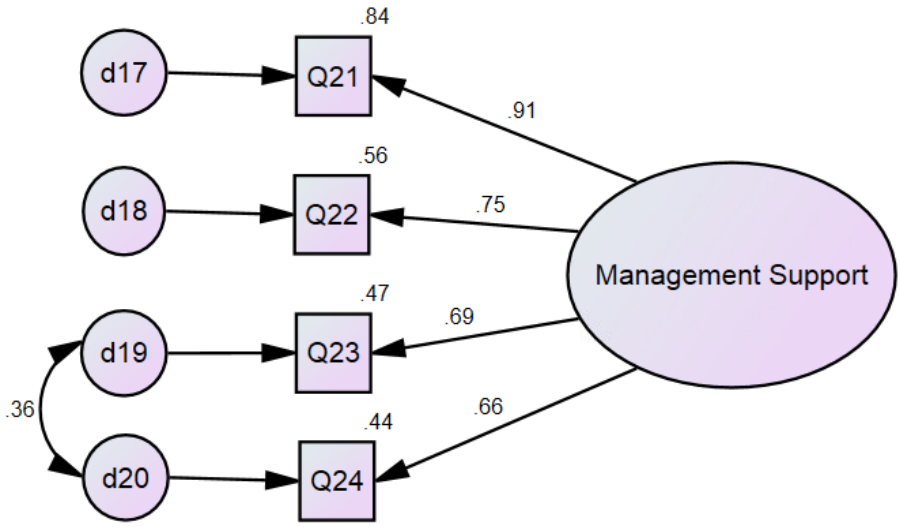


Figure 9: Revised management support measurement model

The improved model has a degree of freedom of 1 (14 observations minus 13 parameters to be estimated) and is overidentified because the degree of freedom is greater than zero. The Chi-square value was significantly lowered from 15.860 in the initial model to 0.031 in the improved model and the Chi-square ratio with degrees of freedom ($\chi 2/df$) is lower than 2 and the probability level (0.861) is higher than 0.05, indicating no statistical significance. Consequently, there are no significant differences between the improved and saturated models.

The goodness-of-fit statistics of CFI and TLI are at the optimal level of model fit. The RMSEA of 0.000 is less than 0.05, further signifying that the model fits well. Table 11 illustrates the goodness-of-fit indices of the initial and revised behavior deterrence measurement models

The standardized estimates of the indicator, Question 21, had a small increase in the factor loadings of the improved model. The other indicators, Question 23 and 24, had a small

decrease but maintained their moderately strong relationships with the latent variable. With critical values greater than 1.96, all indicators show significance at the 0.05 level and deemed important to the model. Therefore, all indicators will remain in the model. The Cronbach's alpha for the management support construct was 0.854 which is higher than the recommended level of 0.70. Therefore, the measurement model is reliable.

Table 11: Goodness-of-fit indices for management support

	Fit Criteria			
Index	**Good Fit**	**Acceptable Fit**	**Initial Model**	**Revised Model**
$\chi 2$	$0 \leq \chi 2 \leq 2df$	$2df < \chi 2 \leq 3df$	15.860	0.031
p value	$.05 < p \leq 1.00$	$.01 \leq p \leq .05$	0.000	0.861
$\chi 2$ / df	$0 \leq \chi 2/df \leq 2$	$2 < \chi 2/df \leq 3$	7.930	0.031
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < .95$	0.956	1.000
TLI*	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < .95$	0.869	1.018
RMSEA	$0 \leq RMSEA \leq .05$	$.05 < RMSEA \leq .08$	0.197	0.000

Note: * The "non-normed" index, on occasion, can be larger than 1 or slightly below 0.

4.3.6 Confirmatory Factor Analysis of Information Security Culture

The last CFA was conducted on the endogenous latent variable, information security culture. This measurement model consisted of 4 indicators, Questions 25 through 28. The initial measurement model and its standardized estimates are shown in Figure 11.

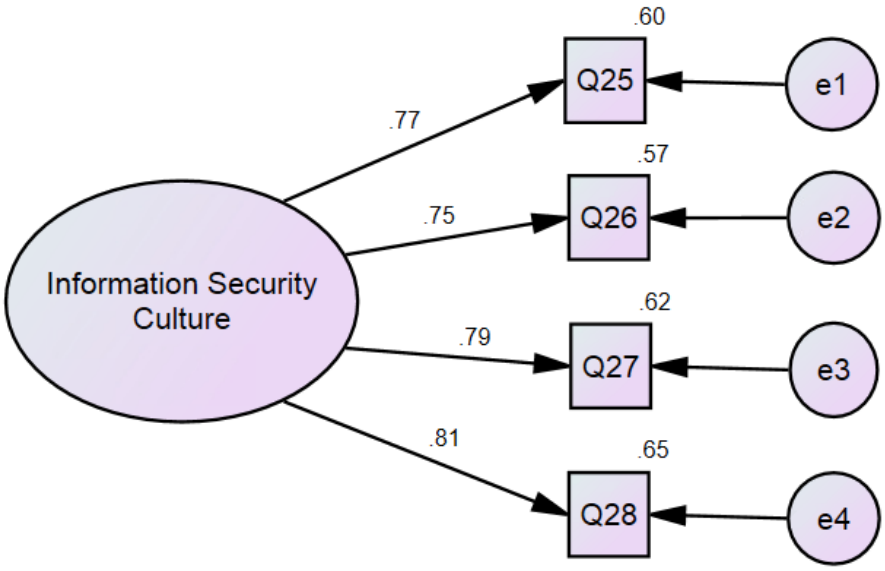


Figure 10: Initial management information security culture measurement model

The initial information security culture measurement model was overidentified with a degree of freedom of 2, which is greater than zero (14 observations minus the 12 distinct parameters estimated). The Chi-square statistic of 6.068 is slightly above the threshold of three times of the degree of freedom equaling 6. The probability level (0.048) is lower than 0.05 and indicates that there is a statistically significant difference between the model and the saturated model.

The CFI and TLI were above the good fit level of 0.95 and very close to 1.0. Even though the RMSEA value of 0.107 is above the acceptable fit range, the model is deemed a good fit. Table 12 presents the goodness-of-fit indices for the measurement model.

Table 12: Goodness-of-fit indices for information security culture

Index	Fit Criteria		Initial Model	Revised Model
	Good Fit	Acceptable Fit		
$\chi 2$	$0 \leq \chi 2 \leq 2df$	$2df < \chi 2 \leq 3df$	6.068	N/A
p value	$.05 < p \leq 1.00$	$.01 \leq p \leq .05$	0.048	N/A
$\chi 2$ / df	$0 \leq \chi 2/df \leq 2$	$2 < \chi 2/df \leq 3$	3.034	N/A
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < .95$	0.987	N/A
TLI*	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < .95$	0.961	N/A
RMSEA	$0 \leq RMSEA \leq .05$	$.05 < RMSEA \leq .08$	0.107	N/A

Note: * The "non-normed" index, on occasion, can be larger than 1 or slightly below 0.

All indicators have a moderately strong relationship with the latent variable, information security culture (see Table 13). The indicators are significant at the 0.05 level as their C.R. is greater than 1.96. Therefore, no indicators were removed in the improved model.

Table 13: Parameter estimates for the Information Security Culture measurement model

Indicator	Initial Model				Revised Model			
	Std. Estimate	S.E	C.R.	P	Std. Estimate	S.E	C.R.	P
Information Security Culture Q25	0.807	0.109	10.467	***	N/A	N/A	N/A	N/A
Information Security Culture Q26	0.789	0.111	10.268	***	N/A	N/A	N/A	N/A
Information Security Culture Q27	0.752	0.093	9.789	***	N/A	N/A	N/A	N/A
Information Security Culture Q28	0.772				N/A			

Note: *** means $p < 0.001$

The M.I.s were measured to decrease the Chi-square value of the improved model. There were no covariances in the measured modification indices. It was decided that the model needed no revisions.

The internal consistency of the information security culture construct was determined by Cronbach's alpha. The Cronbach's alpha was measured at 0.861, which is above the recommended level of 0.70 and indicates that the model is reliable. The reliability results for tests of Cronbach's alpha for all models is listed in Table 14.

Table 14: Cronbach alpha statistics for all constructs

Model	Items	Cronbach's alpha (α)
Stringency of Policies	Q5 through Q8	0.848
Behavior Deterrence	Q9 through Q12	0.617
Employee Commitment	Q13 through Q16	0.762
Employee Awareness	Q17 through Q20	0.811
Management Support	Q21 through Q24	0.854
Information Security Culture	Q25 through Q28	0.861

4.4 Structural Equation Modeling

Once the individual measurement models were validated, the research hypotheses were tested from the developed structural equation model. The full model consisted of five exogenous latent variables: stringency of policies, behavior deterrence, employee commitment, employee awareness, and management support; and one endogenous latent variable (information security culture). The asserted variable relationships in the model are supported from the research presented in the literature review. The Figure 12 depicts the full hypothesized structural equation model.

The proposed model is overidentified with 244 degrees of freedom resulting from 324 observation points and 80 unknown parameters. The Chi-square statistic of 915.672 and the Chi-square ratio with degrees of freedom ($\chi 2/df$) denotes an unacceptable model fit. The probability level is less than 0.05 suggesting that there is a significant difference between the initial and saturated models.

The goodness-of-fit indices of CFI and TLI are lower than 0.90 and the RMSEA is above 0.80 resulting in an unacceptable model fit.

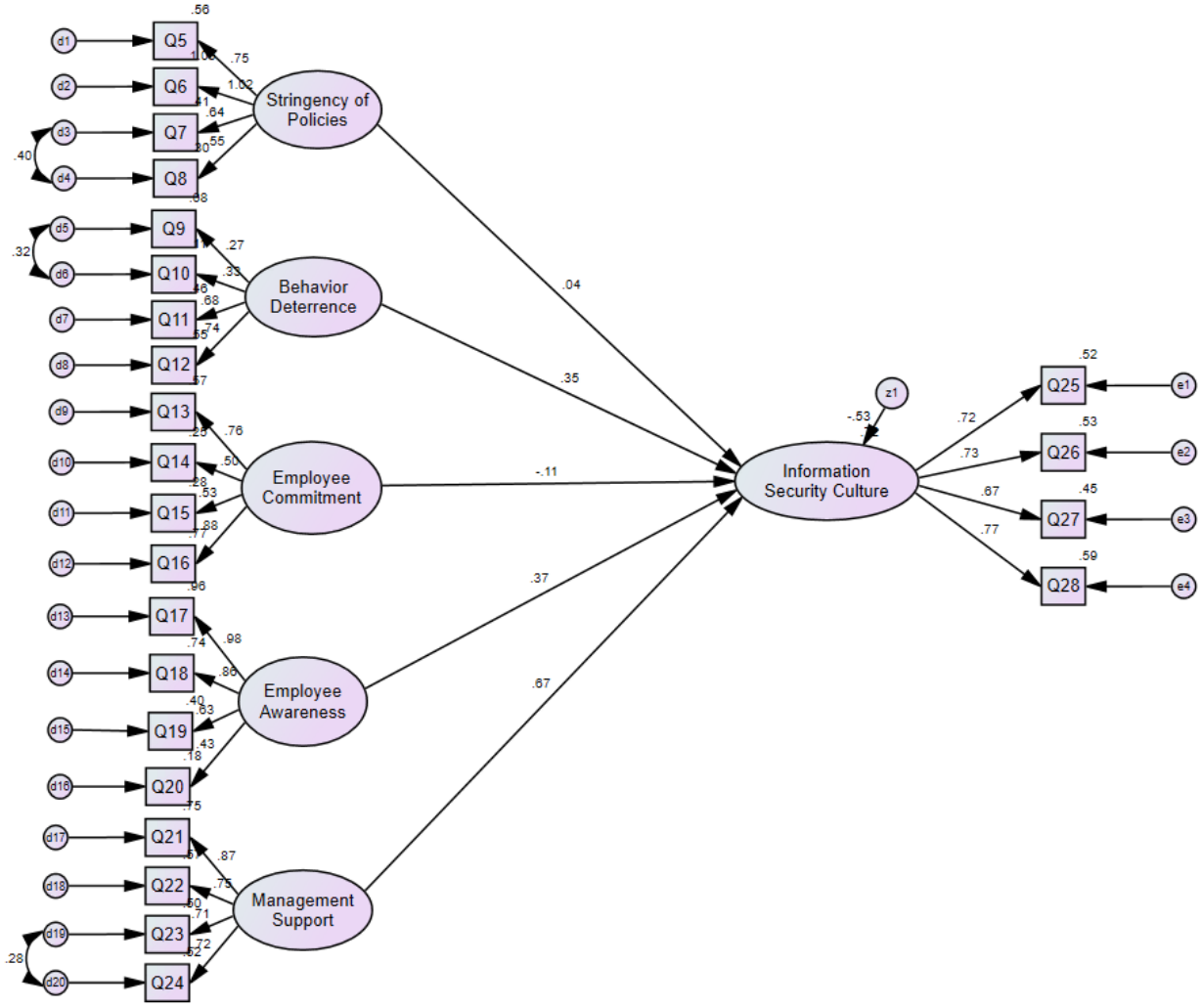


Figure 11: Initial hypothesized structural equation model

The path coefficient of the exogenous latent variable, stringency of policies, were low (less than 0.15) and suggest a very weak relationship with the endogenous latent variable, information security culture. Additionally, the variable was not significant at the 0.05 significance level, as its critical value is lower than 1.96. Because of this, and its minimal influence on information security culture, the latent variable, stringency of policies was removed in the revised model (see Table 14).

Table 15: Parameter estimates for the initial structural model

Indicator	Initial Model			
	Std. Estimate	S.E.	C.R.	P
Information Security Culture ← Stringency of Policies	0.037	0.070	0.648	0.517
Information Security Culture ← Behavior Deterrence	0.351	0.083	4.029	***
Information Security Culture ← Employee Commitment	-0.111	0.100	-1.714	0.087
Information Security Culture ← Employee Awareness	0.374	0.126	4.219	***
Information Security Culture ← Management Support	0.666	0.089	7.128	***
Q5 ← Stringency of Policies	0.748	0.161	7.743	***
Q6 ← Stringency of Policies	1.023	0.233	7.532	***
Q7 ← Stringency of Policies	0.642	0.155	8.997	***
Q8 ← Stringency of Policies	0.549			
Q9 ← Behavior Deterrence	0.274	0.118	2.915	0.004
Q10 ← Behavior Deterrence	0.332	0.188	3.454	***
Q11 ← Behavior Deterrence	0.682	0.197	4.947	***
Q12 ← Behavior Deterrence	0.740			
Q13 ← Employee Commitment	0.757	0.130	8.567	***
Q14 ← Employee Commitment	0.497	0.227	6.113	***
Q15 ← Employee Commitment	0.532	0.168	6.535	***
Q16 ← Employee Commitment	0.876			
Q17 ← Employee Awareness	0.977	0.427	6.015	***
Q18 ← Employee Awareness	0.859	0.379	5.971	***
Q19 ← Employee Awareness	0.632	0.331	5.365	***
Q20 ← Employee Awareness	0.429			
Q21 ← Management Support	0.867	0.108	10.068	***
Q22 ← Management Support	0.753	0.109	9.176	***
Q23 ← Management Support	0.711	0.083	10.397	***
Q24 ← Management Support	0.720			
Q25 ← Information Security Culture	0.724			
Q26 ← Information Security Culture	0.668	0.106	8.890	***
Q27 ← Information Security Culture	0.730	0.127	8.175	***
Q28 ← Information Security Culture	0.724	0.124	9.305	***

Note: *** means $p < 0.001$

The modification indices (M.I.) were also evaluated for possible improvements to the model's fit by decreasing the Chi-square statistic and freeing up parameters. Covariances with M.I. over 5.0 were reviewed and considered for correlation in the revised model. The following correlations error terms were made: e1 and e3, d5 and d6, d6 and d12, d6 and d13, d7 and d11, d7 and d12, d7 and d14, d7 and d16, d8 and d11, d8 and d18, d9 and d15, d9 and d18, d10 and d19, d12 and d17, d16 and d18, and finally d19 and d20 (see Figure 13). In addition, correlations were made between all the exogenous latent variables based on the M.I. and covariances.

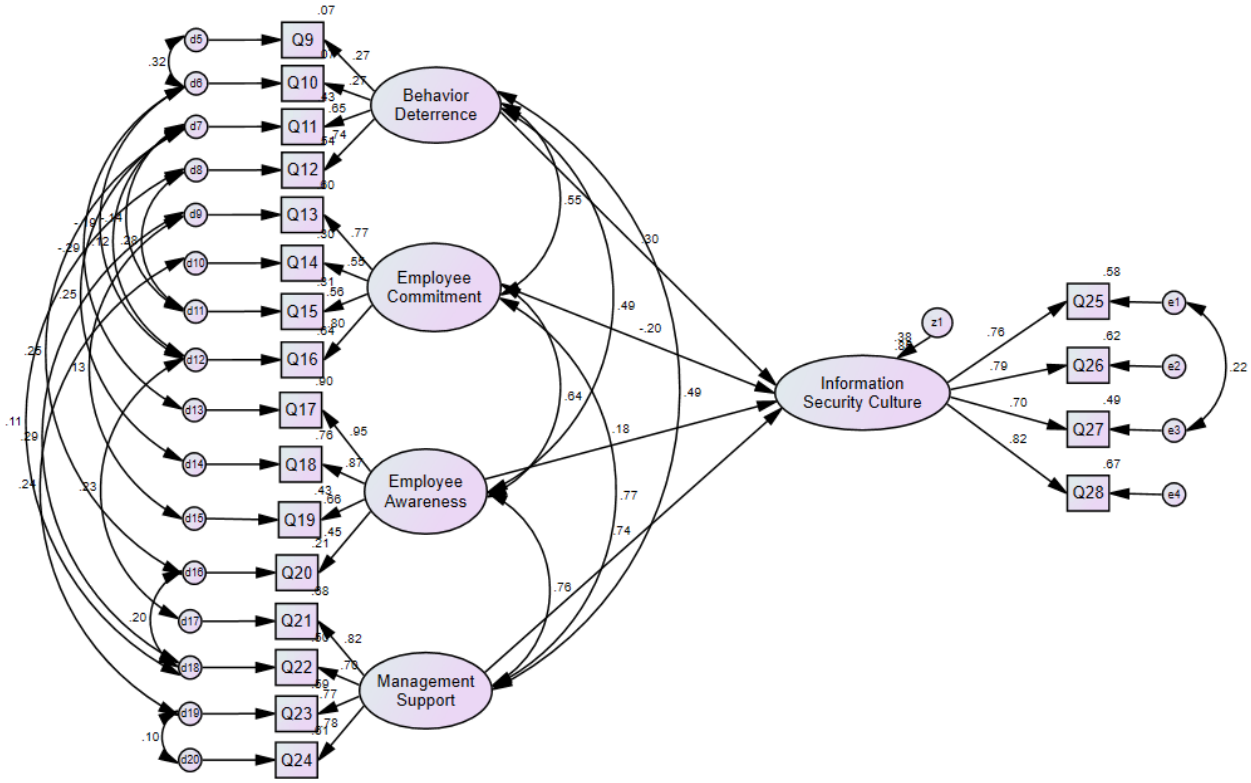


Figure 12: First revised structural equation model

The improved model contains the endogenous latent variable, information security culture and the exogenous latent variables: behavior deterrence, employee commitment, employee awareness, and management support. The latent variable, stringency of policies was removed due to its low path coefficient and it weak impact and information security culture.

The revised model has degrees of freedom of 144 (230 observations minus 86 parameters to be estimated) which makes the model overidentified. The Chi-square value decreased significantly from the initial model to 278.429. The Chi-square ratio with degrees of freedom ($\chi 2/df$) is below 2.0 suggesting a good model fit. The probability level is close to zero, which means less than 0.05. This implies that there is a significant difference between the improved and saturated models.

The values of the goodness-of-fit indices CFI and TLI are above 0.90 which is the level of acceptable model fit. The RMSEA value is was reduced to below 0.80 also indicating acceptable model fit. Table 15 compares the goodness-of-fit indices of the initial and improved structural models.

Table 16: Goodness-of-fit indices for the initial and revised structural models

Index	**Fit Criteria**		**Initial Model**	**First Revised Model**
	Good Fit	**Acceptable Fit**		
$\chi 2$	$0 \leq \chi 2 \leq 2df$	$2df < \chi 2 \leq 3df$	915.672	278.429
p value	$.05 < p \leq 1.00$	$.01 \leq p \leq .05$	0.000	0.000
$\chi 2$ / df	$0 \leq \chi 2/df \leq 2$	$2 < \chi 2/df \leq 3$	3.753	1.934
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < .95$	0.723	0.929
TLI*	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < .95$	0.687	0.906
RMSEA	$0 \leq RMSEA \leq .05$	$.05 < RMSEA \leq .08$	0.124	0.072

Note: * The "non-normed" index, on occasion, can be larger than 1 or slightly below 0.

In the evaluation of the indicators in the first revised model, it was noted that the relationship between the variable employee commitment and information security culture was negative, weak and not significant as its critical value is less than 1.96. Therefore, the indicator was removed from the revised model. Also, the indicator employee awareness, was weak and not significant and it too was removed.

The second revised model contains the endogenous latent variables, behavior deterrence and management support, and the exogenous latent variable information security culture (see Figure 14).

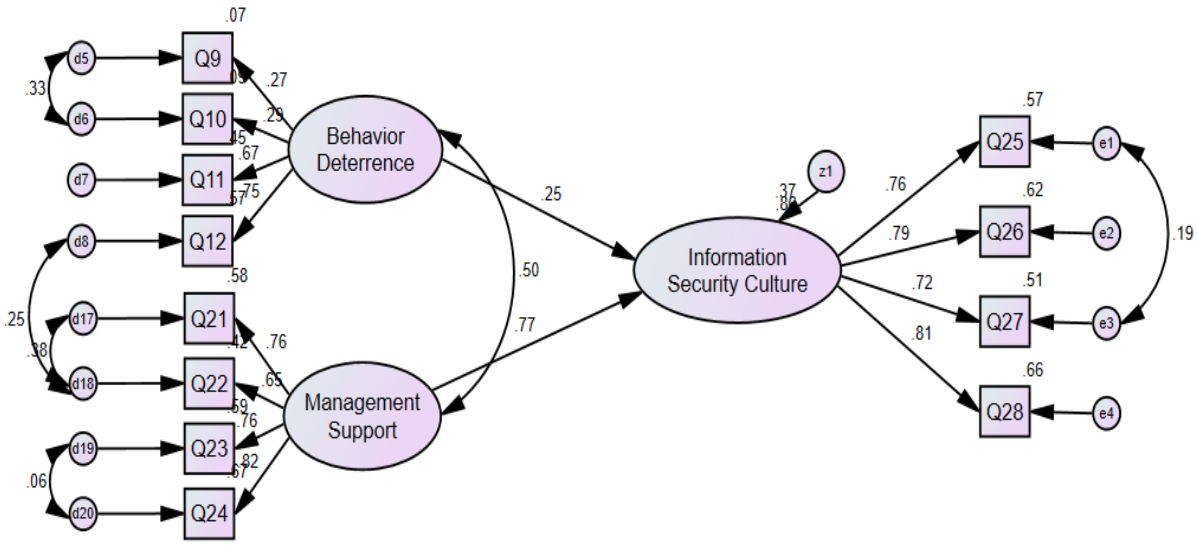


Figure 13: Second revised structural equation model

The second revised model is overidentified with a degrees of freedom value of 46, which is greater than zero (90 observation minus 44 parameters). The Chi-square value was again lowered substantially to 78.245 and the Chi-square ratio with degrees of freedom ($\chi 2/df$) is 1.701

suggesting a good model fit. The probability level is close .002, which is lower than 0.05 denoting a statistical significance between the revised and saturated models.

The goodness-of-fit indices of CFI and TLI and risen above and 0.95 and the RMSEA still remaining below 0.8 all indicating a good model fit. The goodness-of-fit indices of the first and second revised models are compared in Table 16.

Table 17: Goodness-of-fit indices for the first and second revised structural models

Index	Fit Criteria		First Revised Model	Second Revised Model
	Good Fit	Acceptable Fit		
$\chi 2$	$0 \leq \chi 2 \leq 2df$	$2df < \chi 2 \leq 3df$	278.429	78.245
p value	$.05 < p \leq 1.00$	$.01 \leq p \leq .05$	0.000	0.002
$\chi 2$ / df	$0 \leq \chi 2/df \leq 2$	$2 < \chi 2/df \leq 3$	1.934	1.701
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < .95$	0.929	0.966
TLI*	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < .95$	0.906	0.952
RMSEA	$0 \leq RMSEA \leq .05$	$.05 < RMSEA \leq .08$	0.072	0.063

Note: * The "non-normed" index, on occasion, can be larger than 1 or slightly below 0.

The modifications in the second revised model caused some significant changes in the factor loadings. However, the factor loadings for management support and information security culture remained moderately strong and the factors loading for behavior deterrence and information security culture remained in the weaker relationship range (see Table 17).

Table 18: Parameter estimates for the first and second revised structural model

Indicator	First Revised Model				Second Revised Model			
	Std. Estimate	S.E.	C.R.	P	Std. Estimate	S.E.	C.R.	P
Information Security Culture ← Stringency of Policies	Removed				Removed			
Information Security Culture ← Behavior Deterrence	0.304	0.103	3.245	***	0.253	0.091	3.007	0.003
Information Security Culture ← Employee Commitment	-0.196	0.235	-1.650	0.099	Removed			
Information Security Culture ← Employee Awareness	0.183	0.161	1.777	0.001	Removed			
Information Security Culture ← Management Support	0.737	0.151	4.936	***	0.774	0.097	7.714	***
Q5 ← Stringency of Policies	Removed				Removed			
Q6 ← Stringency of Policies	Removed				Removed			
Q7 ← Stringency of Policies	Removed				Removed			
Q8 ← Stringency of Policies	Removed				Removed			
Q9 ← Behavior Deterrence	0.268	0.113	2.988	0.003	0.269	0.111	3.007	0.003
Q10 ← Behavior Deterrence	0.270	0.174	3.025	0.002	0.292	0.174	3.246	0.001
Q11 ← Behavior Deterrence	0.653	0.148	6.208	***	0.674	0.157	6.065	***
Q12 ← Behavior Deterrence	0.738				0.754			
Q13 ← Employee Commitment	0.772	0.128	9.861	***	Removed			
Q14 ← Employee Commitment	0.552	0.241	7.040	***	Removed			
Q15 ← Employee Commitment	0.556	0.178	7.156	***	Removed			
Q16 ← Employee Commitment	0.798				Removed			
Q17 ← Employee Awareness	0.947	0.362	6.495	***	Removed			
Q18 ← Employee Awareness	0.875	0.342	6.376	***	Removed			
Q19 ← Employee Awareness	0.659	0.308	5.751	***	Removed			
Q20 ← Employee Awareness	0.453				Removed			
Q21 ← Management Support	0.824	0.084	11.438	***	0.764	0.082	10.248	***
Q22 ← Management Support	0.704	0.088	9.618	***	0.649	0.090	8.495	***
Q23 ← Management Support	0.767	0.767	0.767	***	0.765	0.073	11.152	***
Q24 ← Management Support	0.781			***	0.818			
Q25 ← Information Security Culture	0.759				0.757			
Q26 ← Information Security Culture	0.787	0.092	10.560	***	0.788	0.094	10.431	***
Q27 ← Information Security Culture	0.698	0.097	10.522	***	0.717	0.100	10.611	***
Q28 ← Information Security Culture	0.820	0.107	11.030	***	0.815	0.109	10.799	***

Note: *** means $p < 0.001$

The indicators in the second revised model had critical values greater than 1.96 and are therefore significant and remain in the model. The path coefficient between management support and information security culture was moderately high ($\beta = 0.774$, $p < 0.001$) and suggests a strong positive relationship between the latent variables. This supports the assertion from the literature that management support has great influence on the information security culture. The path coefficient between behavior deterrence and information security culture remained low ($\beta = 0.253$, $p = 0.003$) suggesting a weak relationship between the two. This is also supported in the literature as not all computer users respond positively to consequence and negative reinforcement. The degree of explained variance (R2) in the model was determined by using the zeta residual associated with information security culture from the model. This calculation revealed that the two-remaining exogenous latent variables, management support and behavior deterrence, account for 86.31% of the variance in the variable, information security culture. The internal consistency of the second revised structural model was determined by Cronbach's alpha. The Cronbach's alpha was measured at 0.766, which is above the recommended level of 0.70 and indicates that the model is reliable.

4.5 Hypothesis Testing

Hypothesis testing is the final step in the statistical analysis process. The second revised structural model was used to test the research hypotheses (see Figure 14). The study included five hypotheses which were tested using the revised structural model in AMOS® 24. The five study hypotheses are as follows:

- H1: Behavior Deterrence positively contributes to the information security culture.
- H2: Stringency of Information Security Policies positively contributes to the information security culture.
- H3: Employee Commitment to Information Security Programs positively contributes to the information security culture.
- H4: Employee Information Security Awareness positively contributes to the information security culture.
- H5: Management Support of Information Security Programs positively contributes to the information security culture.

The first hypothesis (H1) was supported. Behavior deterrence had a small but statistically significant effect on information security culture ($\beta = 0.253$, $p = 0.003$). This was as predicted from the literature review. The second hypothesis (H2) was not supported. Stringency of policies did not have a statistically significant on information security culture ($\beta = 0.311$, $p > 0.05$). This lack of significance implies that a mediating effect could better explain how organizational security policies effect the overall security culture. The third hypothesis (H3) was not supported. Employee commitment did not have statistically significant effect on information security culture ($\beta = -0.196$, $p > 0.05$). This means that employee's attitudes and commitment toward information security and its direct effect on overall security culture could be better explained through a mediating effect. The fourth hypothesis (H4) was not supported. Employee awareness did not have a statistically significant effect on information security culture ($\beta = 0.183$, $p > 0.05$). The direct effect of employee awareness and training on information security culture was not

significant which implied that mediating effect could better explain how employee security awareness can affect the security culture. The fifth hypothesis (H5) was supported. Management support had a statistically significant positive effect on information security culture ($\beta = 0.774$, $p < 0.001$). As employees recognize management's involvement in the organizational information security programs, their personal involvement will increase.

CHAPTER FIVE: CONCLUSION

The focus of this study was to examine the human factors of an information security program and their effect on the information security culture. The age, education level, and level of employment were considered when attempting to analyze their potential influence on the results. A model for assessing information security culture by substantiating the human factor relationships was developed. This validation was used to confirm the importance of the human factors on the overall information security culture. This chapter includes a discussion of the study results and its implications. Study conclusions, limitations, and recommended areas for future research will also be discussed.

5.1 Discussion

A survey assessment was used to collect data on participant characteristics and their perceptions of information security. It was hypothesized that information security culture was positively influenced by the organizational human factors of stringency of policies, behavior deterrence, employee commitment, employee awareness, and management support. Employees of two institutions in the Florida College System were given the web-based survey and the data received was relevant to the modeled relationships.

The first hypothesis tested was the impact that behavior deterrence has on the information security culture. It was determined through the results that behavior deterrence had a significant positive effect on information security culture. The more employees expected that their computer usage would be monitored and that inappropriate actions would be punished, the more they adhere to information security rules. This is consistent with the research of Parsons et al. (2015)

and Bulgurcu, Cavusoglu, and Benbasat (2010), that organizations with known severity in punishment for non-compliant user behavior, are more likely to have positive information security culture.

The next hypothesis analyzed the influence that stringency of policies had on information security culture. The study results indicated that effects of stringency of policies were not statistically significant on the information security culture. This was surprising as all information security compliance regulations and subsequent audits require the organization to have security policies specific to the organization and the type of sensitive data that it handles, stores, and transmits. Studies show that if these policies don't exist in the organization, or they exist only to meet compliance regulations and are not understood by the users, then they can be easily dismissed or not followed (Cox, 2012). This type of user behavior is contrary to a positive information security culture and places organizational information assets at risk.

The third hypothesis evaluated the effect that employee commitment and attitudes towards their organization's information security program had on the overall information culture. The study results indicated that these effects had a negative and insignificant result on the security culture. This is contrary to the prior research studies by Safa et al. (2016), Chen and Zahedi (2016), and Ifinedo (2014) that show that positive employee attitudes towards information security result in positive impacts on the culture and compliance. Further refinement to the model and the survey instrument is necessary to make sure that the influence of employee commitment is properly accounted for.

The fourth hypothesis examined the effect that employee awareness and training had on information security culture. Findings showed that employee awareness did not have a

significant effect on information security culture. This again is contradictory to prior research and industry standards. Training and awareness is the foundation of any information security program and research has shown that users who receive training are more likely to adhere to policy and regulations and exhibit a more positive information security culture (Da Veiga & Martins, 2015b; Parsons et al., 2014a). Again, improvements to the model and the survey instrument may lead to a more accurate assessment of the impact of employee awareness and training.

The final hypothesis appraised the importance that management support has on the information security culture. The results indicated that management support has significant positive effects on information security culture. The more visible, vocal, and supportive organizational management is towards information security, the more healthy and positive the security culture will be. This is supported in prior studies by Alavi et al. (2013), Barton et al. (2016), and Fazlida and Said (2015), which state that consistent support and participation from management creates an environment that is necessary to support the organization's information security goals.

Overall, most survey respondents believed that their organization had a positive information security culture and that this culture was supported by management. The average response to the security culture indicators (Questions 25 to 28) was between "Somewhat agree" and "agree". This held true for the respondents who did not identify as being in a management position (114 out of 179 or 63.7%). Their response is a clear reflection of the organization's information security program.

5.2 Conclusion

Data and information systems are the driving factors in today's business organizations. The security of these factors can have negative implications on a business' revenue, business to business relationships, customer privacy and trust, intellectual property, and compliance with local, state, and federal laws and regulations (Schatz & Bashroush, 2016). The systems and the data contained within them are valuable commodities that are subject to cyber-crime, insider-threats, and data loss. Because of this, organizations invest heavily in technological controls to safeguard their data and information. The human factor has shown to be the most critical in information security. This is due to the roles users play in data breaches and policy compliance (Acuña, 2016; Mitnick & Simon, 2011). As part of normal business operations, users handle the data and operate the systems that support the organization. Therefore, an emphasis is placed on information security culture and awareness programs based on their effectiveness in strengthening user's security aptitude and behavior (Soomro, Shah, & Ahmed, 2016). A sound information security culture demonstrates an organization's overall attitude towards information security and compliance. Therefore, it should be treated with the same level of importance as the strategic plan and with the same level of investment as any technical security control.

This research study utilized SEM to analyze and assess the relationships between stringency of policies, behavior deterrence, employee commitment, employee awareness, management support, and information security culture. A total of 179 employees from two institutions in the Florida College System voluntarily completed the survey instrument and represented a 54.9% response rate. Confirmatory factor analysis was conducted to validate each measurement model in the study and structural equation modeling was used to test the research hypotheses. The results illustrated that management support is a highly influential part of an

organizations information security culture. In addition, behavior deterrence was also revealed to be a factor in a healthy security culture. The findings in the research show that management support and behavior deterrence represented 86.31% of the variance in respondent perceptions about information security culture. The research results further emphasize the role that the human factors play in the formation of the organizational security culture. Management must pay more attention to these factors to build more robust information security programs and identify ways to use them to foster a positive information security culture in the organization.

5.3 Research Contribution

The present study is significant for both research and organizations that wish to mitigate risk and protect information assets. The developed model and the accompanying survey instrument offer a foundation for assessing the human factors present in an information security program and the overall organizational information security culture. Additionally, the model serves as an important contribution to understanding the impacts of the human factors on the security culture. The survey instrument and model indicators were constructed for use on a universal scale and are agnostic to any type of organization. This survey explored intricate human factors that exist in information security programs including training modalities, punishment severity, and task completion versus security-focused behaviors. Also, the research makes a significant contribution to the body of knowledge by highlighting the elements of the security awareness program that focuses on the roles that humans assume in the security of data and assets outside of information technology departments. Organizations benefit from

management and staff who understand the importance of protecting sensitive information and are as equal a security defense as the as the technological controls.

5.4 Research Limitations

This section highlights the study limitations and the areas that could be improved for future research. The study provides an understanding of the human factors of an information security program, how they influence the information security culture, and a theoretical model and survey instrument. Both the model and survey instrument are based on extracted literature and personal training and knowledge of information security programs. While the literature search and training has been extensive, it is does not encompass the complete body of knowledge.

A survey instrument was developed and used in the data collection process and was distributed to two higher education institutions in the Florida College System. Despite information security being world-wide practice, organization type, geographic location, the type of data handled, differences in geographic laws and regulatory compliance, and general computer experience all represent potential study limitations. The collected data reflected the participants perceptions of the information security programs and information security culture within their respective organizations. These perspectives are subjective and may not represent the experiences and realities in other organizations around the world. There may have also been bias in the respondents' answers as they may have chosen answers that were correct based on their information security knowledge and not based on their personal perceptions and experiences. Furthermore, information security effects all organizations that handle sensitive data across the

globe. Therefore, the number of responses used in this survey is small compared to the affected global community. A diverse and larger sample could allow for a more vigorous analysis and a more accurate assessment.

5.5 Future Research

The research examined the effect of stringency of policies, behavior deterrence, employee commitment, employee awareness, and management support on information security culture. Study findings show that behavior deterrence and management support have a direct effect on information security culture. Nevertheless, the association between behavior deterrence and information security culture was found to be weak. Previous studies have confirmed that there is an influence on information security culture by both behavior deterrence and incentive (Chen, Ramamurthy, &Wen, 2012). Further research is needed to explore the hypothesis developed in the study and for continued refinement of the model.

Future research should also facilitate the analysis of the impact that stringency of policies, employee commitment, and employee awareness have on information security culture. The current study could not substantiate the influence of the relationship between these factors and organizational security culture. The survey instrument could be analyzed and refined to determine if more meaningful responses and results could be achieved.

Additionally, further improvement of the model can be validated by repeating this study with the inclusion of the refined human factor models. The CFA performed on large data samples could be used to improve the model validation and using data samples across industries

and geographies could improve the model analysis. Also, higher education institutions have historically been cultures that rely on collaboration, open-mindedness, and open access to information for the advancement of academia and overall human enrichment (Kurdi, El-Haddadeh, & Eldabi, 2018). This operational model is not always compatible with the restrictions of information security. Further research could analyze the data from government or commercial industries that have a more closed mindset on information sharing. Finally, bootstrapping and cross-validation can also be used for more accurate data analysis and to determine sample bias.

APPENDIX A: SURVEY INSTRUMENT

UNIVERSITY OF CENTRAL FLORIDA

Title of Project: Assessing Information Security Culture in Higher Education

Principal Investigator: Henry Glaspie, Doctoral Candidate, Ph.D. in Modeling and Simulation

Faculty Supervisor: Waldemar Karwowski, PhD

You are being invited to take part in a research study. Whether you take part is up to you.

The purpose of this research is identify and analyze the relationship between elements of a higher education organizations information security culture and their employees perceptions of the information security practices. Information security culture is a collection of attitudes and assumptions that guides a user's interaction with technology. For the purposes of this survey, any use of the term "my college" means the college at which you are employed.

Participants in this study will be asked to answer a 28 question survey on information security and programs in their workplace.

The survey is expected to take approximately 20 minutes.

Your identity will be kept confidential.

This is the only request that will be made if you agree to participate in this study.

Your survey responses will be stored in a secure database and no identifying information about you will be shared in the study results. The survey results may be used later as a reference source in the event that any discrepancies arise. The survey results will be destroyed approximately five years after this study is completed based on UCF IRB standard recommendations.

You must be 18 years of age or older to take part in this research study.

Study contact for questions about the study or to report a problem:

If you have questions, concerns, or complaints: Henry Glaspie, Graduate Student, Modeling and Simulation Program, College of Graduate Studies, (321) 202-4370 or by email at hank@knights.ucf.edu; or Dr. Waldemar Karwowski, Faculty Supervisor, Department Industrial Engineering & Management Systems at (407) 823-2204 or by email at wkar@ucf.edu.

IRB contact about your rights in the study or to report a complaint:

Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (UCF IRB). This research has been reviewed and approved by the IRB. For information about the rights of people who take part in research, please contact: Institutional Review Board, University of Central Florida, Office of Research & Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246 or by telephone at (407) 823-2901.

We greatly appreciate your consideration of this request.

→

UNIVERSITY OF CENTRAL FLORIDA

Which gender do you identify with?

Male

Female

What is your age? (You must be 18 years of age or older to take part in this research study)

What is your highest education level attained?

High School
Associates Degree
Bachelors Degree
Graduate Degree

What is your employment type?

Staff
Management
Faculty
Director, Dean, or Above

→

My college has specific guidelines that govern what employees a can do with information and computer resources.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

At my college, the information security policies are written in a manner that is clear and understandable.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

UNIVERSITY OF CENTRAL FLORIDA

At my college, information security policies have been adequately explained to employees.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

At my college, the information security policies are readily available for my reference.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

I believe that employee computing activities are monitored by my college.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

I believe that my college monitors the content of employees' e-mail messages.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

UNIVERSITY OF CENTRAL FLORIDA

I believe that my college conducts periodic audits to detect the use of unauthorized software on its computers.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

If I were caught violating my college's information security policies, I would be punished.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

Complying with my college's information security policies is important to me.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

Complying with the requirements of my college's information security policies is **NOT** time consuming or burdensome for me.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

If I do not comply with my college's information security policies, it would be harmful to my college.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

I believe that I have a responsibility regarding the protection of my college's information and computer resources.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

My college trains employees on their computer security responsibilities.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

My college's information security training explains what is expected of employees from the start of employment.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

I have received different methods of training (courses, presentations, self-study, etc.) in information security from my college.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

The information that I transmit, receive, or access in my daily work is such that it is imperative to ensure confidentiality and maintain privacy.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

UNIVERSITY OF CENTRAL FLORIDA

The management at my college is committed to information security in order to protect sensitive data.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

The management and supervisors in my department adhere to the information security policies.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

UNIVERSITY OF CENTRAL FLORIDA

The information security controls implemented by my college support the school's mission.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

My college has the necessary information security controls in place in order to protect sensitive data.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

Employees at my college comply with the information security policies.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

Practicing good security of information and computer systems is the accepted way of doing business at my college.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

UNIVERSITY OF CENTRAL FLORIDA

At my college, employees will **NOT** take security risks with information and computer systems just to accomplish their work.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

The overall environment at my college fosters information security-minded thinking in all of our actions.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

Use the slider bar to indicate your level of agreement with the statement

→

We thank you for your time spent taking this survey.
Your response has been recorded.

APPENDIX B: IRB APPROVAL LETTER

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Determination of Exempt Human Research

From: **UCF Institutional Review Board #1**
FWA00000351, IRB00001138

To: **Henry Glaspie**

Date: **March 12, 2018**

Dear Researcher:

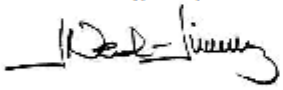
On 03/12/2018, the IRB reviewed the following activity as human participant research that is exempt from regulation:

Type of Review:	Exempt Determination – Category 2 – Adult Participants Online Survey; n=500
Project Title:	Assessing Information Security Culture in Higher Education - Qualtrics survey
Investigator:	Henry Glaspie
IRB Number:	SBE-18-13718
Funding Agency:	
Grant Title:	
Research ID:	N/A

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request in iRIS so that IRB records will be accurate.

In the conduct of this research, you are responsible to follow the requirements of the Investigator Manual.

This letter is signed by:



Signature applied by Jennifer Neal-Jimenez on 03/12/2018 09:50:14 PM EDT

Designated Reviewer

APPENDIX C: SURVEY RESPONSES

Respondent	Gender Q1	Age Group Q2	Education Level Q3	Employment Type Q4	Policy Q5	Policy Q6	Policy Q7	Policy Q8
1	0	2	1	1	8.5	7.5	8.5	10.0
2	1	1	2	0	10.0	10.0	8.5	10.0
3	1	2	1	0	9.5	9.5	9.0	10.0
4	1	2	3	2	8.5	7.0	7.0	9.0
5	0	3	3	3	10.0	10.0	8.5	8.5
6	0	2	3	3	9.5	9.5	9.5	8.5
7	0	1	2	0	8.5	8.5	8.5	8.5
8	1	2	3	3	10.0	10.0	8.5	10.0
9	1	1	2	0	8.5	6.5	7.5	8.5
10	1	2	2	0	8.5	10.0	8.5	8.5
11	1	1	1	0	8.5	8.0	6.5	6.0
12	1	2	3	0	7.5	6.0	5.0	6.5
13	1	3	2	0	8.5	8.5	7.0	8.5
14	0	3	3	3	10.0	10.0	10.0	10.0
15	1	1	3	1	9.5	10.0	8.5	8.5
16	0	2	1	0	10.0	10.0	6.5	10.0
17	0	1	1	0	10.0	10.0	10.0	10.0
18	0	2	2	3	7.5	6.5	7.5	7.0
19	1	1	2	0	10.0	10.0	10.0	10.0
20	0	2	2	0	8.5	8.5	8.5	8.5
21	0	2	3	0	5.0	8.5	8.5	8.5
22	0	3	1	0	8.5	7.0	8.5	9.0
23	0	3	3	1	0.0	0.0	0.0	0.0
24	1	1	1	0	9.5	9.0	9.5	9.5
25	1	1	3	3	7.0	7.5	8.5	9.0
26	0	3	1	0	10.0	10.0	8.5	10.0
27	1	2	2	0	10.0	10.0	10.0	10.0
28	1	1	3	0	9.5	8.5	9.5	8.5
29	0	2	0	0	4.0	4.5	5.0	6.5
30	1	1	1	0	10.0	10.0	8.5	10.0
31	1	1	3	1	3.5	7.0	1.5	10.0
32	0	2	2	0	7.0	6.5	6.5	3.5
33	1	2	1	0	6.5	3.5	1.5	3.5
34	1	2	3	3	10.0	10.0	10.0	10.0
35	1	1	2	0	10.0	7.0	6.5	8.5
36	1	2	3	3	8.5	8.5	8.5	7.0
37	1	1	3	0	10.0	10.0	10.0	8.5
38	1	2	3	0	10.0	10.0	10.0	10.0

Respondent	Gender Q1	Age Group Q2	Education Level Q3	Employment Type Q4	Policy Q5	Policy Q6	Policy Q7	Policy Q8
39	0	1	2	0	10.0	8.5	8.5	8.5
40	0	1	1	0	1.5	1.5	1.5	8.5
41	0	2	0	0	10.0	10.0	10.0	10.0
42	1	1	3	1	10.0	10.0	10.0	8.5
43	0	2	1	3	8.5	8.5	8.5	8.5
44	1	2	3	0	10.0	10.0	10.0	10.0
45	0	2	0	0	10.0	10.0	10.0	10.0
46	1	1	1	0	8.5	8.5	8.5	8.5
47	1	2	3	0	8.5	7.0	5.0	5.0
48	0	2	3	1	10.0	8.5	8.5	7.0
49	1	1	2	1	8.5	10.0	8.5	8.5
50	1	2	1	0	8.5	8.5	8.5	8.5
51	0	2	3	3	10.0	10.0	10.0	8.5
52	1	2	0	0	10.0	10.0	10.0	10.0
53	0	2	3	3	10.0	10.0	10.0	10.0
54	1	1	1	0	9.5	9.5	9.5	8.5
55	1	3	3	0	10.0	10.0	10.0	10.0
56	1	2	2	0	10.0	10.0	10.0	10.0
57	1	2	3	1	10.0	8.5	8.5	8.5
58	0	2	0	1	10.0	10.0	5.0	5.0
59	1	2	3	0	7.0	6.5	6.5	7.0
60	1	3	2	0	8.5	7.0	7.0	8.5
61	0	2	3	3	10.0	8.5	10.0	10.0
62	1	2	2	1	9.0	8.5	8.5	9.5
63	1	2	1	0	8.5	8.5	6.5	6.5
64	0	2	3	0	10.0	10.0	10.0	10.0
65	1	2	0	0	10.0	8.5	10.0	10.0
66	1	2	1	0	8.5	8.5	8.5	8.5
67	1	2	1	0	8.5	5.0	5.0	5.0
68	1	1	3	3	10.0	8.5	4.0	6.5
69	1	2	0	0	8.5	8.5	8.5	8.5
70	0	2	0	0	6.5	1.5	1.5	8.5
71	0	1	3	3	10.0	8.5	7.0	8.5
72	1	2	2	0	8.5	8.5	6.5	6.5
73	1	2	2	0	8.5	6.5	8.5	8.5
74	0	1	3	3	8.5	8.5	8.5	8.5
75	1	2	0	0	10.0	8.5	8.5	7.0
76	1	2	3	2	7.5	8.0	8.5	3.0

Respondent	Gender Q1	Age Group Q2	Education Level Q3	Employment Type Q4	Policy Q5	Policy Q6	Policy Q7	Policy Q8
77	0	2	2	1	7.0	5.0	6.5	6.5
78	0	2	2	0	8.5	8.5	8.5	8.5
79	1	2	0	0	10.0	10.0	10.0	10.0
80	1	1	3	1	8.5	6.5	6.5	7.0
81	1	2	0	0	8.5	7.0	8.5	7.0
82	0	3	3	3	10.0	10.0	10.0	10.0
83	1	2	1	0	8.5	8.5	6.5	5.0
84	1	1	3	0	8.5	6.5	3.5	3.5
85	1	3	1	0	8.5	8.5	8.5	8.5
86	1	1	2	0	10.0	10.0	10.0	10.0
87	1	2	0	0	10.0	10.0	10.0	10.0
88	0	2	1	0	8.5	8.5	7.0	5.0
89	1	2	0	0	8.5	9.0	5.0	5.0
90	1	2	1	0	8.5	7.0	5.0	5.0
91	0	1	1	0	6.5	5.0	6.5	3.5
92	0	1	1	1	8.0	6.5	10.0	8.5
93	0	3	0	1	5.0	8.5	6.5	6.5
94	0	2	3	0	9.0	9.0	8.0	9.0
95	1	1	3	0	8.5	8.5	8.5	8.5
96	1	2	1	0	10.0	10.0	10.0	10.0
97	1	2	3	2	0.0	5.0	10.0	5.0
98	0	2	3	0	6.5	6.5	3.0	3.0
99	1	2	2	0	0.0	0.0	10.0	10.0
100	0	2	1	1	7.0	9.0	7.0	8.5
101	1	2	3	3	5.0	7.0	1.5	7.0
102	0	1	0	0	5.0	5.0	5.0	5.0
103	1	1	1	0	10.0	10.0	10.0	10.0
104	0	3	1	0	8.5	6.5	5.0	6.5
105	1	2	3	2	8.5	8.5	8.5	8.5
106	0	2	1	0	9.0	8.0	8.5	8.5
107	0	2	0	1	10.0	10.0	8.5	8.5
108	0	2	1	0	8.5	8.5	8.5	8.5
109	1	2	1	0	9.0	9.0	9.0	8.5
110	0	1	3	0	8.5	8.5	10.0	8.5
111	1	2	2	0	10.0	8.5	8.5	8.5
112	1	2	3	3	8.5	8.5	8.5	9.0
113	1	2	3	3	8.5	8.0	7.0	6.0
114	1	2	3	3	7.5	7.0	7.5	9.5

Respondent	Gender Q1	Age Group Q2	Education Level Q3	Employment Type Q4	Policy Q5	Policy Q6	Policy Q7	Policy Q8
115	1	2	3	3	10.0	10.0	10.0	5.5
116	0	2	1	0	8.5	10.0	10.0	10.0
117	1	2	1	0	8.0	7.0	7.5	5.0
118	1	1	2	0	10.0	10.0	10.0	10.0
119	1	2	0	0	10.0	10.0	10.0	10.0
120	1	1	1	0	7.0	5.0	7.0	5.0
121	0	2	3	3	10.0	8.5	9.0	9.0
122	1	3	3	3	10.0	7.0	5.0	7.5
123	0	1	3	3	7.0	6.5	7.0	8.5
124	1	2	0	0	10.0	9.0	10.0	10.0
125	1	2	3	3	10.0	6.5	1.5	10.0
126	0	1	3	0	8.5	6.5	1.5	5.0
127	0	2	2	0	10.0	8.5	8.5	8.5
128	1	2	2	0	10.0	9.0	8.5	10.0
129	0	1	2	0	10.0	9.0	3.5	8.5
130	0	2	3	3	7.0	7.0	3.5	8.5
131	0	3	3	0	8.5	8.5	8.5	10.0
132	1	2	0	0	7.0	5.0	3.5	7.0
133	0	2	3	3	10.0	8.5	9.0	9.0
134	1	3	3	3	10.0	7.0	5.0	7.5
135	0	1	3	3	7.0	6.5	7.0	8.5
136	1	2	0	0	10.0	9.0	10.0	10.0
137	1	2	3	3	10.0	6.5	1.5	10.0
138	0	1	3	0	8.5	6.5	1.5	5.0
139	0	2	2	0	10.0	8.5	8.5	8.5
140	1	2	2	0	10.0	9.0	8.5	10.0
141	0	1	2	0	10.0	9.0	3.5	8.5
142	0	2	3	3	7.0	7.0	3.5	8.5
143	0	3	3	0	8.5	8.5	8.5	10.0
144	1	2	0	0	7.0	5.0	3.5	7.0
145	1	1	3	3	10.0	10.0	8.5	10.0
146	0	2	3	1	10.0	7.0	3.5	5.0
147	0	2	3	0	10.0	8.5	8.5	10.0
148	1	1	3	3	8.5	7.0	8.5	8.5
149	1	2	0	0	9.5	9.5	10.0	10.0
150	0	3	2	3	10.0	6.5	6.5	6.5
151	0	2	3	0	1.5	1.5	0.0	0.0
152	0	2	2	0	8.5	8.5	6.5	8.5

Respondent	Gender Q1	Age Group Q2	Education Level Q3	Employment Type Q4	Policy Q5	Policy Q6	Policy Q7	Policy Q8
153	0	2	2	0	9.0	8.5	10.0	8.5
154	0	2	3	3	9.0	8.5	8.5	8.5
155	1	1	3	3	10.0	8.5	7.0	8.5
156	0	2	3	0	7.5	10.0	10.0	10.0
157	1	2	0	0	8.5	8.5	5.0	5.0
158	1	2	2	1	10.0	10.0	5.0	5.0
159	1	1	3	0	8.5	8.5	7.0	8.5
160	1	2	3	3	7.0	3.5	3.5	3.5
161	0	1	3	3	8.5	8.5	6.5	8.5
162	1	1	0	0	10.0	10.0	10.0	10.0
163	1	1	0	0	10.0	8.5	8.5	8.5
164	1	2	1	0	8.5	5.0	3.5	3.5
165	1	2	0	0	8.5	8.5	7.5	7.5
166	1	1	2	0	8.5	8.5	8.5	8.5
167	1	2	3	3	9.5	6.5	7.0	6.5
168	0	1	0	0	10.0	10.0	10.0	10.0
169	1	2	3	0	7.0	7.0	5.0	3.5
170	1	2	2	0	8.5	7.0	8.5	6.5
171	0	1	1	0	10.0	8.5	5.0	10.0
172	1	2	3	2	9.0	9.5	7.5	10.0
173	1	2	0	0	10.0	10.0	8.5	8.5
174	0	2	3	0	10.0	10.0	8.5	5.0
175	1	2	2	0	10.0	10.0	10.0	10.0
176	0	3	3	2	8.5	6.5	6.5	7.0
177	1	2	3	2	10.0	8.5	9.5	10.0
178	0	2	3	3	8.5	8.5	8.5	8.5
179	0	1	3	0	6.5	6.5	8.5	8.5

Respondent	Deterrence Q9	Deterrence Q10	Deterrence Q11	Deterrence Q12
1	10.0	0.0	8.5	8.5
2	10.0	10.0	10.0	10.0
3	9.5	2.5	9.5	9.5
4	7.0	1.5	5.0	8.5
5	8.5	8.5	10.0	10.0
6	9.5	1.5	9.5	10.0
7	8.5	8.5	8.5	7.0
8	10.0	1.5	8.5	8.5
9	8.5	10.0	8.5	10.0
10	10.0	7.0	8.5	10.0
11	9.5	7.5	9.5	9.0
12	10.0	5.0	10.0	8.5
13	8.5	8.5	8.5	8.5
14	10.0	1.5	8.5	8.5
15	8.5	1.5	8.0	3.5
16	3.5	5.0	7.0	8.5
17	10.0	10.0	10.0	10.0
18	8.5	5.0	5.0	5.0
19	8.5	8.5	7.0	3.5
20	8.5	5.0	8.5	8.5
21	5.0	7.0	8.5	8.5
22	8.5	5.0	6.5	7.0
23	10.0	5.0	10.0	5.0
24	9.5	8.5	9.0	10.0
25	3.0	3.0	6.5	8.5
26	2.0	2.0	10.0	10.0
27	10.0	9.5	10.0	10.0
28	8.5	8.5	8.5	8.5
29	5.0	4.0	5.0	5.0
30	10.0	8.5	10.0	10.0
31	3.0	1.5	8.5	9.0
32	8.5	7.0	8.5	5.0
33	5.0	5.0	5.0	5.0
34	5.0	5.0	10.0	10.0
35	10.0	10.0	6.5	5.0
36	8.5	6.5	8.5	8.5
37	10.0	8.5	10.0	10.0
38	10.0	10.0	9.0	8.5

Respondent	Deterrence Q9	Deterrence Q10	Deterrence Q11	Deterrence Q12
39	7.5	6.5	3.5	5.0
40	6.5	7.0	5.0	5.0
41	8.5	8.5	10.0	10.0
42	10.0	10.0	5.0	6.5
43	5.0	5.0	5.0	8.5
44	8.5	8.5	8.5	10.0
45	5.0	3.5	6.5	5.0
46	6.5	5.0	5.0	5.0
47	7.0	5.0	5.0	9.0
48	10.0	2.0	3.5	2.0
49	8.5	5.0	5.0	8.5
50	5.0	8.5	5.0	5.0
51	10.0	5.0	10.0	8.5
52	10.0	10.0	10.0	10.0
53	8.5	3.5	10.0	10.0
54	9.5	9.5	9.0	10.0
55	8.5	8.5	10.0	10.0
56	6.5	1.5	5.0	8.5
57	9.5	9.5	7.5	9.0
58	10.0	10.0	8.5	8.5
59	5.0	5.0	5.0	8.5
60	10.0	10.0	10.0	10.0
61	10.0	10.0	8.5	7.0
62	7.0	3.0	9.0	10.0
63	8.5	8.5	8.5	10.0
64	8.5	8.5	8.5	10.0
65	8.5	8.5	8.5	10.0
66	8.5	8.5	5.0	8.5
67	7.0	3.5	6.5	5.0
68	8.5	5.0	6.0	6.5
69	5.0	6.5	8.5	8.5
70	8.5	8.5	8.5	8.5
71	10.0	10.0	8.5	8.5
72	8.5	8.5	6.5	6.5
73	8.5	6.5	8.5	8.5
74	8.5	8.5	9.0	8.5
75	7.0	1.5	8.5	6.0
76	10.0	8.5	8.5	6.5

Respondent	Deterrence Q9	Deterrence Q10	Deterrence Q11	Deterrence Q12
77	5.0	7.0	3.0	5.0
78	10.0	10.0	10.0	10.0
79	10.0	1.5	10.0	10.0
80	8.5	8.5	10.0	6.5
81	7.5	7.0	8.5	9.0
82	10.0	10.0	10.0	10.0
83	8.5	8.5	8.5	8.5
84	8.5	6.5	6.5	9.0
85	8.5	8.5	8.5	3.5
86	10.0	10.0	10.0	10.0
87	10.0	8.5	7.0	7.0
88	10.0	5.0	8.5	8.5
89	8.5	5.0	8.0	9.5
90	7.0	5.0	8.5	8.5
91	10.0	10.0	3.5	6.5
92	10.0	10.0	10.0	10.0
93	5.0	5.0	8.5	7.0
94	8.5	1.5	5.0	5.0
95	8.5	8.5	8.5	8.5
96	10.0	5.0	5.0	10.0
97	10.0	0.0	10.0	1.5
98	8.5	8.5	8.5	8.5
99	10.0	10.0	10.0	8.5
100	7.0	7.0	5.0	5.0
101	8.5	10.0	8.5	8.5
102	6.0	8.5	5.0	8.5
103	10.0	8.5	10.0	10.0
104	8.5	8.5	6.5	5.0
105	9.5	9.0	9.5	7.0
106	8.0	8.0	8.0	7.5
107	10.0	1.5	8.5	8.5
108	8.5	6.5	8.5	8.5
109	8.5	7.5	7.5	9.0
110	5.0	5.0	7.0	10.0
111	8.5	7.0	10.0	8.5
112	8.5	8.5	8.5	9.0
113	10.0	10.0	8.5	9.0
114	8.5	6.5	8.5	9.5

Respondent	Deterrence Q9	Deterrence Q10	Deterrence Q11	Deterrence Q12
115	10.0	10.0	10.0	10.0
116	10.0	10.0	10.0	10.0
117	8.5	8.5	8.5	8.5
118	10.0	6.5	8.5	10.0
119	10.0	10.0	10.0	10.0
120	10.0	8.5	8.5	8.5
121	9.0	1.5	3.5	8.0
122	8.0	4.5	10.0	6.5
123	7.0	10.0	10.0	8.5
124	10.0	10.0	10.0	5.0
125	7.0	3.5	5.0	5.0
126	8.5	10.0	5.0	5.0
127	7.0	7.0	8.0	8.5
128	10.0	10.0	10.0	10.0
129	8.5	1.5	8.5	9.0
130	8.5	8.5	1.5	3.5
131	8.5	3.5	8.5	8.5
132	7.0	7.0	7.0	7.0
133	9.0	1.5	3.5	8.0
134	8.0	4.5	10.0	6.5
135	7.0	10.0	10.0	8.5
136	10.0	10.0	10.0	5.0
137	7.0	3.5	5.0	5.0
138	8.5	10.0	5.0	5.0
139	7.0	7.0	8.0	8.5
140	10.0	10.0	10.0	10.0
141	8.5	1.5	8.5	9.0
142	8.5	8.5	1.5	3.5
143	8.5	3.5	8.5	8.5
144	7.0	7.0	7.0	7.0
145	7.0	6.5	10.0	10.0
146	3.5	1.5	8.5	7.0
147	10.0	8.5	8.5	10.0
148	10.0	6.5	6.5	3.5
149	7.5	3.5	3.0	7.0
150	6.5	5.0	3.5	8.5
151	10.0	10.0	10.0	10.0
152	9.0	9.0	8.5	8.0

Respondent	Deterrence Q9	Deterrence Q10	Deterrence Q11	Deterrence Q12
153	5.0	5.0	8.5	8.5
154	1.5	1.5	8.5	8.5
155	8.5	1.0	10.0	10.0
156	5.0	5.0	9.5	5.0
157	7.0	7.0	7.0	7.0
158	10.0	10.0	8.5	10.0
159	8.5	8.5	8.5	8.5
160	8.5	7.0	3.5	5.0
161	8.5	1.5	5.0	6.5
162	10.0	10.0	10.0	10.0
163	8.5	5.0	8.5	8.5
164	10.0	7.0	8.5	8.5
165	5.0	5.0	8.5	8.5
166	8.5	9.0	9.0	8.5
167	10.0	6.5	10.0	6.5
168	10.0	10.0	10.0	10.0
169	8.5	7.0	5.0	8.5
170	10.0	7.0	10.0	10.0
171	10.0	10.0	5.0	10.0
172	10.0	10.0	10.0	10.0
173	8.5	5.0	8.5	8.5
174	8.5	7.0	10.0	8.5
175	10.0	5.0	10.0	8.5
176	8.5	7.0	8.5	5.0
177	6.5	9.0	10.0	9.0
178	8.5	7.0	10.0	8.5
179	6.5	8.5	10.0	8.5

Respondent	Commitment Q13	Commitment Q14	Commitment Q15	Commitment Q16
1	10.0	9.0	10.0	10.0
2	10.0	7.0	10.0	10.0
3	10.0	9.0	10.0	10.0
4	10.0	5.0	10.0	10.0
5	10.0	10.0	10.0	10.0
6	10.0	10.0	10.0	10.0
7	10.0	8.5	8.5	8.5
8	10.0	8.5	10.0	10.0
9	10.0	10.0	10.0	10.0
10	8.0	8.0	10.0	10.0
11	8.5	8.5	6.0	8.5
12	10.0	9.0	8.5	10.0
13	8.5	8.5	8.5	8.5
14	10.0	10.0	10.0	10.0
15	1.5	8.5	8.5	9.0
16	10.0	4.0	10.0	10.0
17	10.0	10.0	10.0	10.0
18	5.0	3.5	6.5	6.5
19	8.5	8.5	10.0	10.0
20	8.5	8.5	8.5	8.5
21	10.0	8.5	10.0	10.0
22	8.5	3.5	7.0	8.5
23	10.0	10.0	10.0	10.0
24	9.5	2.0	9.5	9.0
25	8.5	3.5	8.5	9.5
26	10.0	8.5	10.0	10.0
27	10.0	10.0	10.0	10.0
28	10.0	10.0	10.0	10.0
29	5.0	5.0	5.0	7.0
30	10.0	8.5	8.5	8.5
31	8.5	5.0	8.5	9.0
32	7.0	8.5	8.0	8.5
33	10.0	5.0	8.5	10.0
34	10.0	8.5	10.0	10.0
35	7.0	8.5	8.5	10.0
36	8.5	8.5	8.5	10.0
37	8.5	7.0	8.5	8.5
38	10.0	0.0	10.0	10.0

Respondent	Commitment Q13	Commitment Q14	Commitment Q15	Commitment Q16
39	9.0	8.0	8.0	9.0
40	8.5	5.0	5.0	5.0
41	10.0	10.0	10.0	10.0
42	10.0	10.0	10.0	10.0
43	10.0	3.0	10.0	10.0
44	10.0	10.0	10.0	10.0
45	8.5	8.5	10.0	10.0
46	5.0	5.0	5.0	5.0
47	10.0	9.0	7.0	10.0
48	10.0	9.0	6.5	10.0
49	8.5	8.5	8.5	8.5
50	8.5	8.5	8.5	10.0
51	10.0	10.0	0.0	10.0
52	10.0	10.0	10.0	10.0
53	8.5	3.0	7.0	10.0
54	10.0	9.5	10.0	10.0
55	10.0	10.0	10.0	10.0
56	10.0	10.0	10.0	10.0
57	9.0	8.5	8.5	8.5
58	10.0	10.0	10.0	10.0
59	8.5	3.5	8.5	8.5
60	10.0	10.0	10.0	10.0
61	8.5	8.5	10.0	10.0
62	10.0	3.5	10.0	10.0
63	10.0	10.0	10.0	10.0
64	10.0	10.0	10.0	10.0
65	10.0	10.0	10.0	10.0
66	8.5	8.5	8.5	9.0
67	8.5	8.5	7.0	8.5
68	9.5	6.0	8.5	9.5
69	10.0	8.5	10.0	10.0
70	3.5	3.5	7.0	7.0
71	10.0	5.0	7.0	8.5
72	10.0	5.0	10.0	10.0
73	10.0	10.0	10.0	10.0
74	8.5	8.5	9.0	8.5
75	9.5	8.0	9.0	9.5
76	8.5	8.5	7.0	8.5

Respondent	Commitment Q13	Commitment Q14	Commitment Q15	Commitment Q16
77	8.5	6.5	8.5	8.5
78	10.0	3.5	10.0	10.0
79	10.0	10.0	10.0	10.0
80	8.5	8.5	6.5	8.5
81	10.0	10.0	10.0	10.0
82	10.0	10.0	10.0	10.0
83	10.0	8.5	8.5	8.5
84	7.0	8.5	8.5	8.5
85	8.5	8.5	8.5	8.5
86	10.0	10.0	10.0	10.0
87	10.0	10.0	10.0	10.0
88	8.5	8.5	7.0	10.0
89	8.5	9.0	9.5	9.5
90	10.0	8.5	5.0	8.5
91	6.0	3.5	8.0	7.0
92	10.0	1.5	8.5	8.5
93	8.5	8.5	8.5	8.5
94	8.5	8.5	8.5	9.5
95	8.5	8.5	8.0	8.5
96	10.0	10.0	10.0	10.0
97	10.0	8.5	10.0	10.0
98	8.5	4.5	8.5	10.0
99	10.0	10.0	10.0	10.0
100	8.5	3.5	5.0	8.5
101	10.0	8.5	10.0	10.0
102	5.0	0.0	3.5	5.0
103	10.0	10.0	10.0	10.0
104	8.5	6.5	5.0	8.5
105	9.0	7.5	6.5	9.0
106	7.5	8.5	8.0	8.0
107	10.0	5.0	10.0	10.0
108	8.5	3.0	6.5	10.0
109	9.5	9.5	9.5	9.5
110	10.0	9.0	9.0	10.0
111	10.0	8.5	8.5	10.0
112	8.5	8.5	10.0	10.0
113	10.0	8.5	7.0	8.5
114	8.5	6.5	7.0	10.0

Respondent	Commitment Q13	Commitment Q14	Commitment Q15	Commitment Q16
115	10.0	10.0	10.0	10.0
116	10.0	10.0	10.0	10.0
117	8.0	5.0	8.0	7.0
118	10.0	8.5	10.0	10.0
119	10.0	10.0	8.5	10.0
120	7.0	5.0	7.0	8.5
121	8.5	3.5	10.0	9.0
122	9.0	8.5	6.5	10.0
123	10.0	5.0	8.5	10.0
124	10.0	5.0	0.0	10.0
125	7.0	5.0	6.5	7.0
126	8.5	5.0	8.5	8.5
127	8.5	8.5	9.0	8.5
128	10.0	9.0	10.0	10.0
129	10.0	8.5	8.5	10.0
130	10.0	10.0	8.5	10.0
131	10.0	9.0	10.0	10.0
132	9.0	7.0	9.0	8.0
133	8.5	3.5	10.0	9.0
134	9.0	8.5	6.5	10.0
135	10.0	5.0	8.5	10.0
136	10.0	5.0	0.0	10.0
137	7.0	5.0	6.5	7.0
138	8.5	5.0	8.5	8.5
139	8.5	8.5	9.0	8.5
140	10.0	9.0	10.0	10.0
141	10.0	8.5	8.5	10.0
142	10.0	10.0	8.5	10.0
143	10.0	9.0	10.0	10.0
144	9.0	7.0	9.0	8.0
145	10.0	10.0	10.0	10.0
146	10.0	3.5	5.0	8.5
147	10.0	8.5	10.0	10.0
148	8.5	0.0	8.5	10.0
149	10.0	9.5	10.0	10.0
150	10.0	6.5	10.0	10.0
151	8.5	5.0	8.5	8.5
152	10.0	8.5	9.0	10.0

Respondent	Commitment Q13	Commitment Q14	Commitment Q15	Commitment Q16
153	10.0	10.0	8.5	10.0
154	10.0	8.5	9.0	10.0
155	10.0	10.0	10.0	10.0
156	10.0	10.0	8.5	10.0
157	8.5	8.5	8.5	10.0
158	10.0	5.0	8.5	10.0
159	10.0	8.5	8.5	8.5
160	6.5	3.5	5.0	8.5
161	8.5	10.0	10.0	10.0
162	10.0	10.0	10.0	10.0
163	10.0	8.5	10.0	10.0
164	7.0	1.5	5.0	8.5
165	10.0	10.0	10.0	10.0
166	8.5	8.5	8.5	8.5
167	10.0	5.0	10.0	10.0
168	10.0	5.0	10.0	10.0
169	10.0	5.0	10.0	10.0
170	8.5	8.5	10.0	10.0
171	8.5	7.0	10.0	7.0
172	10.0	7.0	10.0	10.0
173	10.0	8.5	7.5	10.0
174	10.0	10.0	10.0	9.0
175	10.0	10.0	8.5	10.0
176	8.5	3.5	7.0	8.5
177	10.0	9.0	10.0	10.0
178	10.0	7.0	8.5	10.0
179	10.0	10.0	10.0	10.0

Respondent	Awareness Q17	Awareness Q18	Awareness Q19	Awareness Q20
1	9.5	10.0	7.5	8.5
2	10.0	10.0	7.0	10.0
3	9.5	9.5	8.5	8.5
4	7.0	5.0	7.0	10.0
5	9.0	7.0	6.5	10.0
6	10.0	8.5	7.0	7.0
7	8.5	8.5	8.5	10.0
8	8.5	8.5	1.5	6.5
9	8.5	8.5	5.5	7.0
10	9.0	9.5	8.0	10.0
11	7.0	7.0	7.0	8.0
12	3.5	5.0	3.5	6.5
13	6.5	7.0	3.5	8.5
14	7.0	8.5	10.0	10.0
15	8.5	8.5	1.5	8.5
16	6.5	8.5	8.5	10.0
17	10.0	10.0	10.0	10.0
18	5.5	7.0	5.0	5.0
19	8.5	8.5	10.0	10.0
20	8.5	8.5	8.5	8.5
21	8.5	8.5	8.5	9.0
22	7.0	5.0	6.5	6.5
23	10.0	10.0	10.0	10.0
24	9.0	9.0	9.0	9.5
25	6.5	3.5	4.0	7.5
26	9.0	10.0	10.0	10.0
27	5.0	5.0	0.0	10.0
28	7.0	7.0	7.0	8.5
29	5.0	5.0	1.5	5.0
30	8.5	10.0	8.5	6.5
31	1.0	1.0	0.5	9.5
32	3.5	3.5	1.5	7.0
33	1.5	0.0	0.0	8.5
34	10.0	5.0	8.5	8.5
35	8.5	8.5	10.0	3.5
36	8.5	8.5	8.5	8.5
37	9.0	9.5	9.5	10.0
38	10.0	10.0	10.0	10.0

Respondent	Awareness Q17	Awareness Q18	Awareness Q19	Awareness Q20
39	8.5	8.5	5.5	1.5
40	3.5	3.0	3.0	5.0
41	8.5	8.5	8.5	10.0
42	10.0	10.0	8.5	10.0
43	8.5	8.5	5.0	8.5
44	10.0	10.0	10.0	10.0
45	8.5	10.0	8.5	7.0
46	5.0	5.0	5.0	5.0
47	3.5	4.0	3.0	6.5
48	5.0	5.0	0.0	0.0
49	8.5	8.5	8.5	8.5
50	5.0	5.0	5.0	10.0
51	10.0	10.0	10.0	10.0
52	10.0	10.0	10.0	10.0
53	10.0	10.0	10.0	6.5
54	9.0	9.0	5.0	10.0
55	10.0	10.0	10.0	10.0
56	10.0	10.0	8.5	10.0
57	7.0	8.5	6.0	9.0
58	8.5	8.5	8.5	8.5
59	6.5	6.5	6.5	10.0
60	7.0	7.0	8.5	10.0
61	8.5	10.0	7.0	8.5
62	6.5	6.5	7.0	10.0
63	8.5	8.5	8.5	10.0
64	8.5	8.5	8.0	10.0
65	8.5	10.0	9.0	10.0
66	8.5	9.5	8.5	8.5
67	5.0	5.0	5.0	8.5
68	6.0	3.5	4.0	9.5
69	10.0	10.0	8.5	10.0
70	1.5	2.0	1.5	3.0
71	10.0	6.5	6.5	8.5
72	5.0	5.0	5.0	5.0
73	8.5	8.5	8.5	10.0
74	8.5	8.5	8.5	9.0
75	7.5	7.5	1.5	6.5
76	7.0	7.0	3.0	8.5

Respondent	Awareness Q17	Awareness Q18	Awareness Q19	Awareness Q20
77	6.5	5.0	6.5	8.5
78	5.0	8.5	8.5	10.0
79	10.0	10.0	6.5	10.0
80	7.0	7.0	7.0	8.5
81	7.0	7.0	3.5	10.0
82	8.5	8.5	8.0	8.5
83	3.5	5.0	6.5	7.0
84	1.5	3.5	1.5	8.5
85	3.5	3.5	1.5	8.5
86	10.0	10.0	10.0	10.0
87	10.0	10.0	8.5	10.0
88	6.5	6.5	8.5	5.0
89	8.5	10.0	5.0	5.0
90	5.0	5.0	3.5	6.5
91	4.0	4.0	0.0	1.0
92	1.5	5.0	2.0	7.0
93	7.0	6.5	7.0	8.5
94	5.0	5.0	5.0	5.0
95	8.5	9.0	8.5	8.5
96	8.5	8.5	10.0	10.0
97	8.5	9.0	9.0	9.0
98	1.5	1.5	3.0	10.0
99	10.0	10.0	10.0	10.0
100	5.0	5.0	5.0	5.0
101	6.5	6.5	1.5	8.5
102	5.0	5.0	1.5	6.5
103	8.5	10.0	10.0	10.0
104	5.0	8.5	6.5	8.5
105	8.5	8.5	9.0	9.0
106	8.5	8.0	8.0	9.0
107	5.0	5.0	5.0	10.0
108	8.5	5.0	5.0	8.5
109	9.0	9.5	2.0	9.0
110	8.5	10.0	1.5	7.0
111	8.5	8.5	5.0	10.0
112	10.0	10.0	8.5	9.0
113	7.0	7.5	6.5	8.5
114	6.5	7.5	5.0	9.5

Respondent	Awareness Q17	Awareness Q18	Awareness Q19	Awareness Q20
115	10.0	10.0	10.0	10.0
116	8.5	10.0	8.5	10.0
117	2.0	2.0	7.0	7.0
118	6.5	10.0	5.0	5.0
119	10.0	10.0	8.5	10.0
120	5.0	5.0	6.5	8.5
121	7.5	8.5	5.0	8.5
122	8.0	10.0	3.5	10.0
123	6.5	6.5	7.0	7.0
124	3.5	9.5	5.0	5.0
125	1.5	1.5	6.5	7.0
126	0.0	0.0	6.5	1.5
127	8.5	8.5	8.5	9.0
128	7.0	7.0	7.0	10.0
129	8.5	6.5	8.5	10.0
130	7.0	3.5	8.5	8.5
131	9.0	5.0	8.5	10.0
132	7.0	6.5	6.5	9.0
133	7.5	8.5	5.0	8.5
134	8.0	10.0	3.5	10.0
135	6.5	6.5	7.0	7.0
136	3.5	9.5	5.0	5.0
137	1.5	1.5	6.5	7.0
138	0.0	0.0	6.5	1.5
139	8.5	8.5	8.5	9.0
140	7.0	7.0	7.0	10.0
141	8.5	6.5	8.5	10.0
142	7.0	3.5	8.5	8.5
143	9.0	5.0	8.5	10.0
144	7.0	6.5	6.5	9.0
145	10.0	10.0	10.0	10.0
146	3.5	5.0	5.0	8.5
147	8.5	8.5	8.5	10.0
148	8.5	7.0	10.0	1.5
149	10.0	9.5	9.0	8.5
150	8.5	8.5	10.0	1.5
151	0.0	0.0	0.0	7.0
152	8.5	8.0	5.0	5.0

Respondent	Awareness Q17	Awareness Q18	Awareness Q19	Awareness Q20
153	10.0	8.5	8.5	2.0
154	8.5	9.0	8.5	7.0
155	8.5	8.5	6.5	10.0
156	10.0	9.0	8.0	10.0
157	8.5	8.5	7.0	10.0
158	5.0	5.0	6.5	10.0
159	6.5	6.5	5.0	8.0
160	3.5	3.5	1.5	5.0
161	7.0	6.5	6.5	6.5
162	10.0	10.0	10.0	10.0
163	8.5	8.5	8.5	8.5
164	3.5	2.0	7.0	5.0
165	7.5	7.5	7.5	8.5
166	8.5	8.5	8.5	8.5
167	3.5	6.5	7.0	6.5
168	10.0	10.0	10.0	5.0
169	1.5	3.5	8.5	8.5
170	5.0	5.0	8.5	10.0
171	3.5	5.0	1.5	3.0
172	7.5	8.0	8.5	10.0
173	8.5	5.0	10.0	8.5
174	10.0	10.0	8.5	10.0
175	10.0	8.5	10.0	10.0
176	3.5	5.0	5.0	7.0
177	10.0	10.0	7.0	10.0
178	10.0	9.0	8.5	8.5
179	8.5	8.0	8.5	10.0

Respondent	Support Q21	Support Q22	Support Q23	Support Q24	Culture Q25	Culture Q26	Culture Q27	Culture Q28
1	9.0	10.0	8.5	9.0	5.0	6.0	2.0	6.5
2	10.0	10.0	5.0	10.0	8.5	10.0	7.0	10.0
3	10.0	10.0	9.5	9.0	8.0	9.5	9.5	9.0
4	8.5	8.5	8.5	8.5	7.0	7.0	7.0	8.5
5	8.5	8.5	10.0	10.0	8.5	10.0	8.5	8.5
6	10.0	10.0	10.0	10.0	9.0	10.0	8.5	10.0
7	8.5	8.5	9.0	8.5	8.5	8.5	8.5	8.5
8	10.0	10.0	8.5	8.5	3.5	7.0	3.0	8.5
9	8.5	8.5	8.5	8.5	6.5	8.5	8.5	5.0
10	7.5	8.0	9.0	5.5	5.0	5.0	5.0	6.5
11	7.0	3.5	8.5	7.5	6.5	7.5	4.0	5.5
12	6.5	8.5	7.5	6.5	6.5	9.0	8.5	8.0
13	8.5	8.5	8.5	7.0	7.0	8.5	6.5	6.5
14	10.0	10.0	10.0	10.0	8.5	10.0	7.0	7.0
15	8.5	2.0	8.5	9.0	6.5	9.0	3.0	3.5
16	10.0	10.0	8.5	8.5	8.5	10.0	5.0	7.0
17	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
18	6.5	7.0	6.5	6.5	5.0	5.0	5.0	5.0
19	10.0	10.0	8.5	8.5	8.5	10.0	8.5	10.0
20	8.5	8.5	8.5	8.5	5.0	8.5	8.5	8.5
21	10.0	10.0	8.5	8.5	8.5	9.0	8.5	9.0
22	8.5	5.0	8.5	8.5	8.5	8.5	8.5	8.5
23	10.0	10.0	10.0	10.0	5.0	10.0	5.0	10.0
24	9.5	9.5	9.5	9.5	9.5	9.5	9.5	9.5
25	9.5	9.0	9.0	7.0	6.5	8.0	8.0	8.5
26	10.0	8.5	10.0	10.0	8.5	8.5	10.0	8.5
27	10.0	10.0	10.0	5.0	5.0	5.0	5.0	10.0
28	8.5	10.0	8.5	8.5	9.0	10.0	8.5	8.5
29	2.5	5.0	2.5	2.5	3.0	5.0	5.0	5.0
30	10.0	10.0	10.0	8.5	6.5	8.5	6.5	6.5
31	7.0	7.0	8.5	1.5	0.0	8.0	3.0	1.5
32	5.0	5.0	6.5	5.0	5.0	8.5	5.0	3.5
33	5.0	7.0	5.0	5.0	3.0	5.0	3.5	1.5
34	10.0	10.0	10.0	10.0	5.0	10.0	5.0	10.0
35	7.0	3.5	8.0	1.5	6.5	5.0	5.0	3.5
36	10.0	10.0	10.0	8.5	8.5	8.5	5.0	8.5
37	10.0	9.5	9.0	9.0	8.5	9.0	8.5	9.0
38	10.0	10.0	5.0	10.0	8.5	10.0	8.5	10.0

Respondent	Support Q21	Support Q22	Support Q23	Support Q24	Culture Q25	Culture Q26	Culture Q27	Culture Q28
39	8.5	8.5	8.0	8.5	6.5	8.5	4.5	7.0
40	1.5	3.0	5.0	5.0	0.0	5.0	1.5	5.0
41	10.0	10.0	10.0	8.5	9.0	10.0	10.0	10.0
42	10.0	10.0	10.0	10.0	10.0	10.0	8.5	10.0
43	8.5	8.5	5.0	8.5	6.5	8.5	5.0	5.0
44	10.0	10.0	10.0	10.0	8.5	10.0	8.5	10.0
45	10.0	8.5	8.5	5.0	5.0	8.5	5.0	8.5
46	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
47	6.5	4.0	7.0	5.0	3.5	6.5	10.0	8.5
48	10.0	1.5	9.0	8.5	3.5	8.5	5.0	3.5
49	8.5	9.0	8.5	8.5	5.0	8.5	5.0	8.5
50	9.5	8.5	8.5	6.5	5.0	7.0	8.5	7.0
51	10.0	10.0	10.0	8.5	7.0	8.5	8.5	10.0
52	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
53	10.0	10.0	8.5	10.0	8.5	10.0	3.0	8.5
54	10.0	10.0	10.0	9.5	8.5	9.0	8.0	7.0
55	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
56	10.0	10.0	8.5	8.5	8.5	10.0	10.0	8.5
57	10.0	9.0	5.0	8.5	8.5	8.5	8.5	7.5
58	10.0	8.5	8.5	8.5	8.5	10.0	10.0	8.5
59	8.5	10.0	8.5	8.5	8.5	8.5	6.5	6.5
60	10.0	10.0	10.0	10.0	6.5	10.0	8.5	8.5
61	5.0	3.5	7.0	3.5	7.0	7.0	2.0	5.0
62	6.5	10.0	8.5	6.5	7.0	7.0	3.0	3.5
63	10.0	10.0	8.5	8.5	5.0	10.0	8.5	10.0
64	10.0	10.0	8.5	8.5	6.5	8.5	5.0	6.5
65	10.0	10.0	10.0	8.0	8.5	10.0	8.5	9.0
66	9.0	8.0	8.5	7.5	8.0	8.5	9.0	8.5
67	8.5	5.0	5.0	5.0	5.0	8.5	8.5	7.0
68	6.5	9.5	8.0	3.0	2.0	7.0	0.0	2.5
69	10.0	10.0	10.0	10.0	8.5	10.0	10.0	10.0
70	1.5	2.0	2.5	0.0	0.0	0.0	3.0	2.5
71	10.0	10.0	8.5	10.0	6.5	8.5	6.5	8.5
72	7.0	7.0	7.0	8.5	5.0	8.5	5.0	7.0
73	10.0	10.0	8.5	10.0	8.5	8.5	6.5	8.5
74	10.0	8.5	8.5	9.0	8.5	8.5	8.5	8.5
75	7.0	9.0	5.5	5.0	7.0	5.0	5.0	5.0
76	8.0	7.0	8.5	7.0	8.0	6.5	5.0	7.0

Respondent	Support Q21	Support Q22	Support Q23	Support Q24	Culture Q25	Culture Q26	Culture Q27	Culture Q28
77	8.5	6.5	7.0	9.5	6.5	6.5	6.5	6.5
78	10.0	10.0	5.0	0.0	5.0	10.0	5.0	5.0
79	10.0	10.0	10.0	10.0	8.5	10.0	8.5	10.0
80	8.5	8.5	8.5	8.5	8.5	8.5	3.5	8.5
81	6.5	8.5	8.5	7.0	3.5	7.0	8.5	8.5
82	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
83	7.0	8.5	5.0	7.0	5.0	7.0	6.5	7.0
84	8.5	8.5	7.0	7.0	3.5	3.0	7.0	6.5
85	8.5	8.5	7.0	8.5	8.5	8.5	8.5	8.5
86	10.0	10.0	10.0	10.0	5.0	10.0	10.0	10.0
87	10.0	10.0	10.0	10.0	8.5	8.5	9.5	10.0
88	1.5	3.0	6.5	8.5	8.5	8.5	5.0	6.5
89	9.0	9.5	10.0	7.0	5.0	7.5	5.0	5.0
90	8.5	8.5	5.0	5.0	5.0	7.0	5.0	5.0
91	3.5	7.5	6.0	6.0	6.0	5.0	1.5	4.0
92	8.5	8.0	5.0	5.0	6.5	6.5	3.5	8.5
93	8.5	8.5	8.5	8.5	5.0	8.5	5.0	5.0
94	7.5	8.5	8.0	7.5	6.5	7.5	5.0	5.0
95	8.5	8.5	8.5	8.0	9.0	9.0	8.5	9.5
96	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
97	10.0	8.5	9.5	8.5	1.5	7.0	3.5	2.0
98	10.0	10.0	6.5	5.0	5.0	8.5	5.0	6.5
99	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
100	8.5	7.0	5.0	10.0	5.0	8.5	5.0	5.0
101	10.0	10.0	10.0	8.5	6.5	7.0	3.0	6.5
102	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
103	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
104	8.5	8.5	8.5	8.5	5.0	8.5	8.5	8.5
105	9.0	9.0	9.0	9.0	9.0	9.0	9.0	9.0
106	8.5	8.5	8.0	8.0	8.5	8.0	8.0	8.0
107	10.0	10.0	10.0	8.5	7.0	10.0	10.0	8.5
108	8.5	8.5	8.5	8.5	8.5	8.5	8.5	8.5
109	9.5	9.5	9.5	9.0	6.5	9.0	5.0	8.5
110	10.0	10.0	10.0	8.5	8.5	10.0	8.5	10.0
111	10.0	10.0	10.0	10.0	8.5	10.0	8.5	8.5
112	8.5	9.0	9.0	8.5	9.0	8.5	8.5	9.0
113	8.5	10.0	7.5	7.0	8.0	8.5	8.5	6.5
114	10.0	9.5	9.0	9.5	9.0	9.0	10.0	9.5

Respondent	Support Q21	Support Q22	Support Q23	Support Q24	Culture Q25	Culture Q26	Culture Q27	Culture Q28
115	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
116	9.5	10.0	10.0	10.0	9.0	10.0	7.5	10.0
117	8.5	7.0	8.5	8.5	8.5	8.5	7.5	8.5
118	10.0	10.0	10.0	10.0	10.0	10.0	8.5	10.0
119	10.0	8.5	8.5	10.0	10.0	10.0	7.0	8.5
120	5.0	5.0	5.0	5.0	6.5	7.0	5.0	5.0
121	10.0	8.5	10.0	8.0	5.0	8.0	3.5	10.0
122	10.0	9.0	8.0	7.0	7.0	8.5	3.0	5.0
123	10.0	10.0	8.5	8.5	8.5	10.0	5.0	8.5
124	8.0	6.5	8.0	8.0	3.5	5.0	5.0	6.5
125	5.0	8.5	5.0	5.0	5.0	3.5	3.0	1.5
126	8.5	8.5	5.0	5.0	5.0	5.0	5.0	3.5
127	8.5	9.0	8.5	8.5	8.5	9.0	8.5	8.5
128	10.0	10.0	9.5	8.5	8.5	8.5	8.5	8.5
129	8.5	8.5	8.5	8.5	7.0	2.0	5.0	3.5
130	8.5	8.5	8.5	7.0	5.0	3.5	5.0	8.5
131	10.0	10.0	10.0	8.5	8.5	8.5	8.5	8.5
132	9.0	9.0	9.5	7.0	7.5	8.5	8.5	8.5
133	10.0	8.5	10.0	8.0	5.0	8.0	3.5	10.0
134	10.0	9.0	8.0	7.0	7.0	8.5	3.0	5.0
135	10.0	10.0	8.5	8.5	8.5	10.0	5.0	8.5
136	8.0	6.5	8.0	8.0	3.5	5.0	5.0	6.5
137	5.0	8.5	5.0	5.0	5.0	3.5	3.0	1.5
138	8.5	8.5	5.0	5.0	5.0	5.0	5.0	3.5
139	8.5	9.0	8.5	8.5	8.5	9.0	8.5	8.5
140	10.0	10.0	9.5	8.5	8.5	8.5	8.5	8.5
141	8.5	8.5	8.5	8.5	7.0	2.0	5.0	3.5
142	8.5	8.5	8.5	7.0	5.0	3.5	5.0	8.5
143	10.0	10.0	10.0	8.5	8.5	8.5	8.5	8.5
144	9.0	9.0	9.5	7.0	7.5	8.5	8.5	8.5
145	10.0	10.0	10.0	10.0	10.0	10.0	10.0	7.0
146	9.0	8.5	7.0	6.5	7.0	7.0	5.0	5.0
147	8.5	10.0	10.0	8.5	8.5	10.0	8.5	8.5
148	10.0	10.0	10.0	8.5	6.5	6.5	6.5	6.5
149	10.0	10.0	10.0	10.0	10.0	10.0	7.0	9.5
150	10.0	5.0	5.0	7.0	5.0	5.0	5.0	6.5
151	5.0	5.0	5.0	5.0	5.0	5.0	5.0	0.0
152	9.5	9.5	9.0	8.5	8.0	9.5	8.0	9.0

Respondent	Support Q21	Support Q22	Support Q23	Support Q24	Culture Q25	Culture Q26	Culture Q27	Culture Q28
153	10.0	10.0	8.5	8.5	8.5	8.5	8.5	8.5
154	10.0	10.0	10.0	8.5	9.0	8.5	8.5	8.5
155	10.0	10.0	10.0	10.0	7.0	8.5	8.5	9.0
156	10.0	10.0	10.0	10.0	8.0	10.0	10.0	10.0
157	10.0	10.0	8.5	8.5	7.0	9.0	7.0	8.5
158	10.0	10.0	8.5	5.0	5.0	10.0	5.0	5.0
159	7.0	8.0	7.0	8.5	8.5	8.5	8.5	8.5
160	7.0	7.0	5.0	5.0	7.0	5.0	7.0	5.0
161	8.5	8.5	8.5	8.5	6.5	7.0	7.0	7.0
162	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
163	8.5	8.5	8.0	8.5	8.5	8.5	8.5	8.5
164	5.0	5.0	5.0	5.0	5.0	8.5	8.5	6.5
165	8.5	10.0	8.5	8.5	7.0	10.0	8.5	8.5
166	8.5	8.5	8.5	8.5	7.0	8.5	5.0	5.0
167	10.0	5.0	7.0	8.5	6.5	5.0	6.5	2.5
168	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
169	10.0	8.5	7.0	8.5	7.0	5.0	5.0	8.5
170	5.0	5.0	10.0	8.5	5.0	8.5	8.5	8.5
171	10.0	10.0	10.0	9.5	8.5	10.0	10.0	5.0
172	8.5	8.5	10.0	8.5	8.5	8.5	6.5	6.5
173	10.0	10.0	5.0	5.0	9.0	10.0	8.5	10.0
174	9.0	10.0	10.0	8.5	8.5	8.5	10.0	9.0
175	10.0	10.0	10.0	10.0	8.5	10.0	8.5	10.0
176	6.5	8.5	8.5	7.0	6.5	9.0	5.0	7.0
177	10.0	5.0	10.0	7.0	5.0	9.0	5.0	10.0
178	10.0	10.0	10.0	8.5	7.0	10.0	7.0	8.5
179	8.5	8.0	8.5	8.0	8.0	8.0	8.5	8.5

Survey Response Coding Legend

Responses for Questions 1		
	Non-Female	Female
Coded value	0	1

Responses for Questions 2			
	Young Adult Age 18-44	Middle Age Adult 45-64	Senior Adult Age 65+
Coded value	1	2	3

Responses for Questions 3				
	High School	Associates Degree	Bachelors Degree	Graduate Degree
Coded value	0	1	2	3

Responses for Questions 4				
	Staff	Management	Faculty	Director, Dean, or Above
Coded value	0	1	2	3

Responses for Questions 5 through 28							
	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
Coded value	0	2	4	5	6	8	10

APPENDIX D: DESCRIPTIVE STATISTICS

Descriptive statistics for indicators of Stringency of Policy

							Skewness		Kurtosis	
Indicator	**N**	**Range**	**Min**	**Max**	**Mean**	**Standard Deviation**	**Statistic**	**Standard Error**	**Statistic**	**Standard Error**
Stringency of Policy Q5	179	10	0	10	8.609	1.8897	-2.496	0.182	7.827	0.361
Stringency of Policy Q6	179	10	0	10	8.059	1.949	-1.632	0.182	3.651	0.361
Stringency of Policy Q7	179	10	0	10	7.483	2.466	-1.14	0.182	0.605	0.361
Stringency of Policy Q8	179	10	0	10	8.011	2.067	-1.31	0.182	1.652	0.361

Descriptive statistics for indicators of Behavior Deterrence

							Skewness		Kurtosis	
Indicator	**N**	**Range**	**Min**	**Max**	**Mean**	**Standard Deviation**	**Statistic**	**Standard Error**	**Statistic**	**Standard Error**
Behavior Deterrence Q9	179	10	0	10	8.609	1.8897	-2.496	0.182	7.827	0.361
Behavior Deterrence Q10	179	10	0	10	8.059	1.949	-1.632	0.182	3.651	0.361
Behavior Deterrence Q11	179	10	0	10	7.483	2.466	-1.14	0.182	0.605	0.361
Behavior Deterrence Q12	179	10	0	10	8.011	2.067	-1.31	0.182	1.652	0.361

Descriptive statistics for indicators of Employee Commitment

							Skewness		Kurtosis	
Indicator	**N**	**Range**	**Min**	**Max**	**Mean**	**Standard Deviation**	**Statistic**	**Standard Error**	**Statistic**	**Standard Error**
Employee Commitment Q13	179	10	0	10	8.609	1.8897	-2.496	0.182	7.827	0.361
Employee Commitment Q14	179	10	0	10	8.059	1.949	-1.632	0.182	3.651	0.361
Employee Commitment Q15	179	10	0	10	7.483	2.466	-1.14	0.182	0.605	0.361
Employee Commitment Q16	179	10	0	10	8.011	2.067	-1.31	0.182	1.652	0.361

Descriptive statistics for indicators of Employee Awareness

							Skewness		Kurtosis	
Indicator	**N**	**Range**	**Min**	**Max**	**Mean**	**Standard Deviation**	**Statistic**	**Standard Error**	**Statistic**	**Standard Error**
Employee Awareness Q17	179	10	0	10	8.609	1.8897	-2.496	0.182	7.827	0.361
Employee Awareness Q18	179	10	0	10	8.059	1.949	-1.632	0.182	3.651	0.361
Employee Awareness Q19	179	10	0	10	7.483	2.466	-1.14	0.182	0.605	0.361
Employee Awareness Q20	179	10	0	10	8.011	2.067	-1.31	0.182	1.652	0.361

Descriptive statistics for indicators of Management Support

							Skewness		Kurtosis	
Indicator	**N**	**Range**	**Min**	**Max**	**Mean**	**Standard Deviation**	**Statistic**	**Standard Error**	**Statistic**	**Standard Error**
Management Support Q21	179	10	0	10	8.609	1.8897	-2.496	0.182	7.827	0.361
Management Support Q22	179	10	0	10	8.059	1.949	-1.632	0.182	3.651	0.361
Management Support Q23	179	10	0	10	7.483	2.466	-1.14	0.182	0.605	0.361
Management Support Q24	179	10	0	10	8.011	2.067	-1.31	0.182	1.652	0.361

Descriptive statistics for indicators of Information Security Culture

							Skewness		Kurtosis	
Indicator	**N**	**Range**	**Min**	**Max**	**Mean**	**Standard Deviation**	**Statistic**	**Standard Error**	**Statistic**	**Standard Error**
Information Security Culture Q25	179	10	0	10	8.609	1.8897	-2.496	0.182	7.827	0.361
Information Security Culture Q26	179	10	0	10	8.059	1.949	-1.632	0.182	3.651	0.361
Information Security Culture Q27	179	10	0	10	7.483	2.466	-1.14	0.182	0.605	0.361
Information Security Culture Q28	179	10	0	10	8.011	2.067	-1.31	0.182	1.652	0.361

APPENDIX E: SPEARMAN'S RHO CORRELATION MATRIX

Correlations of indicators of Stringency of Policy

		Stringency of Policy Q5	Stringency of Policy Q6	Stringency of Policy Q7	Stringency of Policy Q8
Stringency of Policy Q5	Correl. Coeff.	1.000	.700**	.481**	.519**
	Sig. (2-tailed)		.000	.000	.000
	N	179	179	179	179
Stringency of Policy Q6	Correl. Coeff.	.700**	1.000	.670**	.599**
	Sig. (2-tailed)	.000		.000	.000
	N	179	179	179	179
Stringency of Policy Q7	Correl. Coeff.	.481**	.670**	1.000	.648**
	Sig. (2-tailed)	.000	.000		.000
	N	179	179	179	179
Stringency of Policy Q8	Correl. Coeff.	.519**	.599**	.648**	1.000
	Sig. (2-tailed)	.000	.000	.000	
	N	179	179	179	179

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

Correlations of indicators of Behavior Deterrence

		Behavior Deterrence Q9	Behavior Deterrence Q10	Behavior Deterrence Q11	Behavior Deterrence Q12
Behavior Deterrence Q9	Correl. Coeff.	1.000	.425**	.383**	.286**
	Sig. (2-tailed)		.000	.000	.000
	N	179	179	179	179
Behavior Deterrence Q10	Correl. Coeff.	.425**	1.000	.291**	.246**
	Sig. (2-tailed)	.000		.000	.001
	N	179	179	179	179
Behavior Deterrence Q11	Correl. Coeff.	.383**	.291**	1.000	.537**
	Sig. (2-tailed)	.000	.000		.000
	N	179	179	179	179
Behavior Deterrence Q12	Correl. Coeff.	.286**	.246**	.537**	1.000
	Sig. (2-tailed)	.000	.001	.000	
	N	179	179	179	179

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

Correlations of indicators of Employee Commitment

		Employee Commitment Q13	Employee Commitment Q14	Employee Commitment Q15	Employee Commitment Q16
Employee Commitment Q13	Correl. Coeff.	1.000	.484**	.539**	.678**
	Sig. (2-tailed)		.000	.000	.000
	N	179	179	179	179
Employee Commitment Q14	Correl. Coeff.	.484**	1.000	.462**	.463**
	Sig. (2-tailed)	.000		.000	.000
	N	179	179	179	179
Employee Commitment Q15	Correl. Coeff.	.539**	.462**	1.000	.595**
	Sig. (2-tailed)	.000	.000		.000
	N	179	179	179	179
Employee Commitment Q16	Correl. Coeff.	.678**	.463**	.595**	1.000
	Sig. (2-tailed)	.000	.000	.000	
	N	179	179	179	179

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

Correlations of indicators of Employee Awareness

		Employee Awareness Q17	Employee Awareness Q18	Employee Awareness Q19	Employee Awareness Q20
Employee Awareness Q17	Correl. Coeff.	1.000	.793**	.663**	.460**
	Sig. (2-tailed)		.000	.000	.000
	N	179	179	179	179
Employee Awareness Q18	Correl. Coeff.	.793**	1.000	.548**	.392**
	Sig. (2-tailed)	.000		.000	.000
	N	179	179	179	179
Employee Awareness Q19	Correl. Coeff.	.663**	.548**	1.000	.420**
	Sig. (2-tailed)	.000	.000		.000
	N	179	179	179	179
Employee Awareness Q20	Correl. Coeff.	.460**	.392**	.420**	1.000
	Sig. (2-tailed)	.000	.000	.000	
	N	179	179	179	179

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

Correlations of indicators of Management Support

		Management Support Q21	Management Support Q22	Management Support Q23	Management Support Q24
Management Support Q21	Correl. Coeff.	1.000	.734**	.607**	.598**
	Sig. (2-tailed)		.000	.000	.000
	N	179	179	179	179
Management Support Q22	Correl. Coeff.	.734**	1.000	.600**	.554**
	Sig. (2-tailed)	.000		.000	.000
	N	179	179	179	179
Management Support Q23	Correl. Coeff.	.607**	.600**	1.000	.628**
	Sig. (2-tailed)	.000	.000		.000
	N	179	179	179	179
Management Support Q24	Correl. Coeff.	.598**	.554**	.628**	1.000
	Sig. (2-tailed)	.000	.000	.000	
	N	179	179	179	179

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

Correlations of indicators of Information Security Culture

		Information Security Culture Q25	Information Security Culture Q26	Information Security Culture Q27	Information Security Culture Q28
Information Security Culture Q25	Correl. Coeff.	1.000	.644**	.632**	.580**
	Sig. (2-tailed)		.000	.000	.000
	N	179	179	179	179
Information Security Culture Q26	Correl. Coeff.	.644**	1.000	.582**	.652**
	Sig. (2-tailed)	.000		.000	.000
	N	179	179	179	179
Information Security Culture Q27	Correl. Coeff.	.632**	.582**	1.000	.643**
	Sig. (2-tailed)	.000	.000		.000
	N	179	179	179	179
Information Security Culture Q28	Correl. Coeff.	.580**	.652**	.643**	1.000
	Sig. (2-tailed)	.000	.000	.000	
	N	179	179	179	179

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

APPENDIX F: CONFIRMATORY FACTOR ANALYSIS

Comparison of parameter estimates for the Stringency of Policies measurement models

Indicator	Initial Model Std. Estimate	S.E	C.R.	P	Revised Model Std. Estimate	S.E	C.R.	P
Stringency of Policy Q5	0.783	0.143	8.342	***	0.742	0.162	7.668	***
Stringency of Policy Q6	0.967	0.172	8.803	***	1.030	0.240	7.437	***
Stringency of Policy Q7	0.678	0.179	7.543	***	0.639	0.156	8.989	***
Stringency of Policy Q8	0.601				0.544			

Note: *** means $p < 0.001$

Comparison of parameter estimates for the Behavior Deterrence measurement models

Indicator	Initial Model Std. Estimate	S.E	C.R.	P	Revised Model Std. Estimate	S.E	C.R.	P
Behavior Deterrence Q9	0.351	0.139	3.671	***	0.298	0.138	3.340	***
Behavior Deterrence Q10	0.333	0.216	3.506	***	0.263	0.214	2.986	.003
Behavior Deterrence Q11	0.783	0.305	4.256	***	0.867	0.496	3.095	.002
Behavior Deterrence Q12	0.638				0.597			

Note: *** means $p < 0.001$

Comparison of parameter estimates for the Employee Commitment measurement models

Indicator	Initial Model Std. Estimate	S.E	C.R.	P	Revised Model Std. Estimate	S.E	C.R.	P
Employee Commitment Q13	0.761	0.133	8.526	***	N/A	N/A	N/A	N/A
Employee Commitment Q14	0.502	0.170	6.548	***	N/A	N/A	N/A	N/A
Employee Commitment Q15	0.535	0.229	6.152	***	N/A	N/A	N/A	N/A
Employee Commitment Q16	0.868				N/A			

Note: *** means $p < 0.001$

Comparison of parameter estimates for the Employee Awareness measurement models

Indicator	Initial Model				Revised Model			
	Std. Estimate	S.E	C.R.	P	Std. Estimate	S.E	C.R.	P
Employee Awareness Q17	0.981	0.437	5.941	***	N/A	N/A	N/A	N/A
Employee Awareness Q18	0.857	0.382	5.951	***	N/A	N/A	N/A	N/A
Employee Awareness Q19	0.627	0.332	5.340	***	N/A	N/A	N/A	N/A
Employee Awareness Q20	0.427				N/A			

Note: *** means p < 0.001

Comparison of parameter estimates for the Management Support measurement models

Indicator	Initial Model				Revised Model			
	Std. Estimate	S.E	C.R.	P	Std. Estimate	S.E	C.R.	P
Management Support Q21	0.858	0.102	10.329	***	0.914	0.144	8.678	***
Management Support Q22	0.739	0.105	9.208	***	0.747	0.128	8.484	***
Management Support Q23	0.756	0.096	9.414	***	0.685	0.092	9.930	***
Management Support Q24	0.733				0.660			

Note: *** means p < 0.001

Comparison of parameter estimates for the Information Security Culture measurement models

Indicator	Initial Model				Revised Model			
	Std. Estimate	S.E	C.R.	P	Std. Estimate	S.E	C.R.	P
Information Security Culture Q25	0.807	0.109	10.467	***	N/A	N/A	N/A	N/A
Information Security Culture Q26	0.789	0.111	10.268	***	N/A	N/A	N/A	N/A
Information Security Culture Q27	0.752	0.093	9.789	***	N/A	N/A	N/A	N/A
Information Security Culture Q28	0.772				N/A			

Note: *** means p < 0.001

Comparison of parameter estimates for the initial and revised structural models

Indicator	Initial Model				Revised Model			
	Std. Estimate	S.E.	C.R.	P	Std. Estimate	S.E.	C.R.	P
Information Security Culture ← Stringency of Policies	0.037	0.070	0.648	0.517	Removed			
Information Security Culture ← Behavior Deterrence	0.351	0.083	4.029	***	0.304	0.103	3.245	***
Information Security Culture ← Employee Commitment	-0.111	0.100	-1.714	0.087	-0.196	0.235	-1.650	0.099
Information Security Culture ← Employee Awareness	0.374	0.126	4.219	***	0.183	0.161	1.777	0.001
Information Security Culture ← Management Support	0.666	0.089	7.128	***	0.737	0.151	4.936	***
Q5 ← Stringency of Policies	0.748	0.161	7.743	***	Removed			
Q6 ← Stringency of Policies	1.023	0.233	7.532	***	Removed			
Q7 ← Stringency of Policies	0.642	0.155	8.997	***	Removed			
Q8 ← Stringency of Policies	0.549				Removed			
Q9 ← Behavior Deterrence	0.274	0.118	2.915	0.004	0.268	0.113	2.988	0.004
Q10 ← Behavior Deterrence	0.332	0.188	3.454	***	0.270	0.174	3.025	***
Q11 ← Behavior Deterrence	0.682	0.197	4.947	***	0.653	0.148	6.208	***
Q12 ← Behavior Deterrence	0.740				0.738			
Q13 ← Employee Commitment	0.757	0.130	8.567	***	0.772	0.128	9.861	
Q14 ← Employee Commitment	0.497	0.227	6.113	***	0.552	0.241	7.040	
Q15 ← Employee Commitment	0.532	0.168	6.535	***	0.556	0.178	7.156	
Q16 ← Employee Commitment	0.876				0.798			
Q17 ← Employee Awareness	0.977	0.427	6.015	***	0.947	0.362	6.495	
Q18 ← Employee Awareness	0.859	0.379	5.971	***	0.875	0.342	6.376	***
Q19 ← Employee Awareness	0.632	0.331	5.365	***	0.659	0.308	5.751	***
Q20 ← Employee Awareness	0.429				0.453			
Q21 ← Management Support	0.867	0.108	10.068	***	0.824	0.084	11.438	***
Q22 ← Management Support	0.753	0.109	9.176	***	0.704	0.088	9.618	***
Q23 ← Management Support	0.711	0.083	10.397	***	0.767	0.075	11.329	***
Q24 ← Management Support	0.720				0.781			
Q25 ← Information Security Culture	0.724				0.759			
Q26 ← Information Security Culture	0.668	0.106	8.890	***	0.787	0.092	10.560	***
Q27 ← Information Security Culture	0.730	0.127	8.175	***	0.698	0.097	10.522	***
Q28 ← Information Security Culture	0.724	0.124	9.305	***	0.820	0.107	11.030	***

Note: *** means $p < 0.001$

Comparison of parameter estimates for the first and second revised structural models

Indicator	First Revised Model				Second Revised Model			
	Std. Estimate	S.E.	C.R.	P	Std. Estimate	S.E.	C.R.	P
Information Security Culture ← Stringency of Policies	Removed				Removed			
Information Security Culture ← Behavior Deterrence	0.304	0.103	3.245	***	0.253	0.091	3.007	0.003
Information Security Culture ← Employee Commitment	-0.196	0.235	-1.650	0.099	Removed			
Information Security Culture ← Employee Awareness	0.183	0.161	1.777	0.001	Removed			
Information Security Culture ← Management Support	0.737	0.151	4.936	***	0.774	0.097	7.714	***
Q5 ← Stringency of Policies	Removed				Removed			
Q6 ← Stringency of Policies	Removed				Removed			
Q7 ← Stringency of Policies	Removed				Removed			
Q8 ← Stringency of Policies	Removed				Removed			
Q9 ← Behavior Deterrence	0.268	0.113	2.988	0.003	0.269	0.111	3.007	0.003
Q10 ← Behavior Deterrence	0.270	0.174	3.025	0.002	0.292	0.174	3.246	0.001
Q11 ← Behavior Deterrence	0.653	0.148	6.208	***	0.674	0.157	6.065	***
Q12 ← Behavior Deterrence	0.738				0.754			
Q13 ← Employee Commitment	0.772	0.128	9.861	***	Removed			
Q14 ← Employee Commitment	0.552	0.241	7.040	***	Removed			
Q15 ← Employee Commitment	0.556	0.178	7.156	***	Removed			
Q16 ← Employee Commitment	0.798				Removed			
Q17 ← Employee Awareness	0.947	0.362	6.495	***	Removed			
Q18 ← Employee Awareness	0.875	0.342	6.376	***	Removed			
Q19 ← Employee Awareness	0.659	0.308	5.751	***	Removed			
Q20 ← Employee Awareness	0.453				Removed			
Q21 ← Management Support	0.824	0.084	11.438	***	0.764	0.082	10.248	***
Q22 ← Management Support	0.704	0.088	9.618	***	0.649	0.090	8.495	***
Q23 ← Management Support	0.767	0.767	0.767	***	0.765	0.073	11.152	***
Q24 ← Management Support	0.781				0.818			
Q25 ← Information Security Culture	0.759				0.757			
Q26 ← Information Security Culture	0.787	0.092	10.560	***	0.788	0.094	10.431	***
Q27 ← Information Security Culture	0.698	0.097	10.522	***	0.717	0.100	10.611	***
Q28 ← Information Security Culture	0.820	0.107	11.030	***	0.815	0.109	10.799	***

Note: *** means $p < 0.001$

LIST OF REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods, *Behaviour and Information Technology*. *33(3).* 237-248.

Abraham, S. (2011). Information Security Behavior: Factors and Research Directions. In *AMCIS 2011 Proceedings – All Submissions*. Paper 462.

Acuña, D. C. (2016). Effects of a Comprehensive Computer Security Policy on Computer Security Culture. *MWAIS 2016 Proceedings.* Paper 10.

Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*, *5*(1).

Ahlan, A.R., Lubis, M., Lubis, A.R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science. 72*. 361-373

Alavi, R., Islam, S., Jahankhani, H., & Al-Nemrat, A. (2013). Analyzing human factors for an effective information security management system. *International Journal of Secure Software Engineering (IJSSE)*, *4*(1), 50-74.

Alhogail, A. R. E. E. J., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology*, *64*(2), 540-549.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567-575.

Al-Kurdi, O., El-Haddadeh, R., & Eldabi, T. (2018). Knowledge sharing in higher education institutions: a systematic review. *Journal of Enterprise Information Management, 31*(2), 226-246.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443.

Aurigemma, S., Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. Computers & Security, 66, 218-234.

Badie, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. *Journal of Basic and Applied Scientific Research, 2*(9), 9331-9347.

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

Boomsma, A., & Hoogland, J. J. (2001). The robustness of LISREL modeling revisited. *Structural equation models: Present and future. A Festschrift in honor of Karl Jöreskog*, 139-168.

Box, D., & Pottas, D. (2014). A model for information security compliant behaviour in the healthcare context. *Procedia Technology. 16.* 1462-1470.

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.

Byrne, B. M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming., 2nd ed*. New York, NY, US: Routledge/Taylor & Francis Group.

Chan, H., & Mubarak, S. (2012). Significance of information security awareness in the higher education sector. *International Journal of Computer Applications*, *60*(10).

Chen, H., Li, W. (2014). Understanding organization employee's information security omission behavior: An integrated model of social norm and deterrence. *Proceedings - Pacific Asia Conference on Information Systems,* PACIS 2014.

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.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *Mis Quarterly*, *40*(1), 205-222.

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

Choi, M., Levy, Y., & Hovav, A. (2013, December). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. In *Proc. of the Pre-Int. Conference of Inform. Syst.(ICIS) SIGSEC–Workshop on Inform. Security and Privacy (WISP) 2013*.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849-1858.

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

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

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091-1124.

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

Da Veiga, A., & Martins, N. (2015a). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review, 31*(2), 243-256.

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

Dang-Pham, D., Pittayachawan, S., Bruno, V. (2016). Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace. *Information Management. 54(5),* 625-637.

Dang-Pham, D., Pittayachawan, S., Bruno, V. (2017). Investigation into the formation of information security influence: Network analysis of an emerging organisation. *Computers & Security, 70*, 111-123.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior, 26(6),* 1739-1747.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security, 56*, 63-69.

Ding, L., Velicer, W. F., & Harlow, L. L. (1995). Effects of estimation methods, number of indicators per factor, and improper solutions on structural equation modeling fit indices. *Structural Equation Modeling: A Multidisciplinary Journal, 2(2),* 119-143.

Farahmand, F., Atallah, M. J., & Spafford, E. H. (2013). Incentive alignment and risk perception: an information security application. *IEEE Transactions on Engineering Management*, *60*(2), 238-246.

Fazlida, M.R., Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance. 28*. 243-248.

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

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

Flowerday, S.V., Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers and Security*. 61. 169–183.

Florida College System. (2017). Report for the Florida College System. Retrieved from: http://www.fldoe.org/accountability/data-sys/CCTCMIS/reports.stml.

Grama, J. (2014). Just in Time Research: Data Breaches in Higher Education. *EDUCAUSE*.

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

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242-251.

Haeussinger, F., & Kranz, J. (2013). Information security Awareness: Its antecedents and mediating effects on security compliant behavior. *34th International Conference on Information Systems 2013.*

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

Hershberger, P. 2014. Security Skills Assessment and Training: The "Make or Break" Critical Security Control. SANS Institute InfoSec Reading Room.

Hipsky, S., & Younes, W. (2015). Beyond Concern: K-12 Faculty and Staff's Perspectives on Privacy Topics and Cybersafety. *International Journal of Information and Communication Technology Education (IJICTE), 11*(4), 51-66.

Hooper, D., Coughlan, J., & Mullen, M. (2008). Structural equation modelling: Guidelines for determining model fit. *Articles*, 2.

Hoyle, R. H. (1995). *Structural equation modeling: Concepts, issues, and applications*. Sage.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. doi:10.1080/10705519909540118

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, *54*(6), 54-60.

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

IBM. 2013. The 2013 IBM Cyber Security Intelligence Index. IBM Security Services.

IBM. 2015. The 2015 IBM Cyber Security Intelligence Index. IBM Security Services.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

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

Karlsson, F., Goldkuhl, G., Hedström, K. (2017). Practice-Based Discourse Analysis of Information Security Policies. *Computers & Security*. 67. 267-279.

Kline, R. (2010). Principles and Practice of Structural Equation Modeling, 3rd edn Guilford Press. *New York. USA.. ISBN, 1965705777*.

Knapp, K. J., & Ferrante, C. J. (2014). Information security program effectiveness in organizations: The moderating role of task interdependence. *Journal of Organizational and End User Computing (JOEUC), 26*(1), 27-46.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*, 224-231.

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

Lee, C., Lee, C.C., Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59*, 60-70.

McBride, M., Carter, L., & Warkentin, M. (2012). *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies*. Technical Report, RTI International.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., & Skourlas, C. (2014). Human factor and information security in higher education. *Journal of Systems and Information Technology*, *16*(3), 210-221.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48*, 267-280.

Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, *27*(5), 644-667.

Nunnally, J. C. (1978). *Psychometric theory*: New York: McGraw-Hill, c1978. 2d ed.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.

Oppong, F. B., & Agbedra, S. Y. (2016). Assessing univariate and multivariate normality. a guide for non-statisticians. *Math. Theory Modeling*, *6*(2), 26-33.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014a). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, *22*(4), 334-345.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014b). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129.

Privacy Rights Clearinghouse. (2017). Retrieved from https://www.privacyrights.org/data-breaches.

Renaud, K. (2012). Blaming noncompliance is too convenient: What really causes information breaches?. *IEEE Security & Privacy, 10(3),* 57-63.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53,* 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56,* 70-82.

Said, A. R., Abdullah, H., Uli, J., & Mohamed, Z. A. (2014). Relationship between organizational characteristics and information security knowledge management implementation. *Procedia-Social and Behavioral Sciences, 123,* 433-443.

Sari, P. K. (2012). A Concept of Information Security Management for Higher Education. In International Conference on Technology and Operation Management, 3rd. Bandung (pp. 469-477).

Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information & Computer Security*, *24*(1), 73-92.

Schumacker, R. E., & Lomax, R. G. (2016). *A beginner's guide to structural equation modeling (4th ed.)*. New York, NY US: Routledge/Taylor & Francis Group.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Computers & Security*, *49,* 177-191.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal Of Flexible Systems Management. 14(4)*. 225-239.

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

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225.

Stewart, G., & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, *20(1)*, 29-38.

Tang, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, 1-8.

Tassi, S. (2018, Feb 8). *What to Know About ED's New Stance on Data Breach Reporting*. Retrieved from https://campustechnology.com/articles/2018/02/08/what-to-know-about-eds-new-stance-on-data-breach-reporting.aspx.

Teo, P. C., Mohamad, O., & Ramayah, T. (2011). Testing the dimensionality of consumer ethnocentrism scale (CETSCALE) among a young Malaysian consumer market segment. *African Journal of Business Management*, *5*(7), 2805.

Thomson, K., & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, *20*(1), 39-46.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190-198.

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

Young, R., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems*, 26(1), 245–266.